ESCOLA DE GUERRA NAVAL

CC(T) Katia Cristina Altomare Silva

GUERRA CIBERNÉTICA NA MARINHA DO BRASIL: POSSIBILIDADES E LIMITAÇÕES PERANTE O DIREITO INTERNACIONAL DOS CONFLITOS ARMADOS

Rio de Janeiro

2021

CC(T) Katia Cristina Altomare Silva

GUERRA CIBERNÉTICA NA MARINHA DO BRASIL: POSSIBILIDADES E LIMITAÇÕES PERANTE O DIREITO INTERNACIONAL DOS CONFLITOS ARMADOS

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador: CC Miguel Henrique Alexandre Dias Alves

Rio de Janeiro
Escola de Guerra Naval
2021

AGRADECIMENTOS

Agradeço à Deus, por me guiar em todos os momentos e conceder o término de mais uma etapa.

À minha mãe e meu amor eterno, Maria de Lourdes Campos Silva, verdadeiramente a maior mestra da minha vida, pelo incentivo e exemplo de superação que me inspirou, em vida e após, a ter fé e não desistir de alcançar os objetivos.

À Capitão de Fragata (T) Maria Aparecida Almeida Machado, que me inspirou desde o processo de seleção para ingressar na Marinha do Brasil, pelas correções minuciosas de todos os textos que enviei, contribuindo significativamente com o sucesso deste trabalho.

Ao meu Orientador, Capitão de Corveta Miguel Henrique Alexandre Dias Alves, pela confiança, atenção, ensinamentos compartilhados e por orientar as minhas pesquisas de forma admirável.

Aos Professores pelos conhecimentos transmitidos, à equipe de Metodologia do Trabalho Acadêmico da Escola de Guerra Naval pelo apoio institucional e pelas facilidades oferecidas.

Ao Suboficial Rodrigues, pelo seu profissionalismo e orientações, sempre atencioso e pronto a sanar as dificuldades no decorrer deste trabalho.

À minha Encarregada, companheira de trabalho e preciosa amiga, Capitão de Corveta (T) Patrícia Amaro Rocha Arruda, pelo incentivo, apoio incondicional, amizade e força constante que fez dissipar todas as minhas inseguranças nos momentos difíceis.

A todos os meus superiores, subordinados e amigos, pelas palavras de incentivo, compreensão pelas ausências necessárias e que, de alguma forma, colaboraram para a conclusão deste trabalho.

RESUMO

Desde os primórdios da humanidade, ocorrem disputas por interesses diversos entre grupos. Os primeiros conflitos, resolvidos a mãos vazias, deram lugar ao uso de engenhosas invenções, em guerras que, muitas vezes, contavam com atividades de inteligência e de contrainteligência em sua retaguarda. Primeiro surgiram as armas de curto alcance; depois, as de alcance mais longo, as disparadas remotamente, os veículos não tripulados, os armamentos nucleares e os agentes biológicos; estas últimas, de destruição em massa. Assim, com um somatório de informação e tecnologia — em que muitas vezes, a informação é a maior arma, e, ao mesmo tempo, o alvo —, as guerras são travadas na atualidade e são conhecidas como Guerra Cibernética. A partir do início do século XXI, a Guerra Cibernética, do ponto de vista ofensivo, tem ido além de ações de sondagem, reconhecimento e espionagem cibernética. Por este motivo, questões legais devem ser levantadas para a regulação do comportamento humano, a fim de controlar as consequências possíveis diante de uma guerra na qual a arma mais poderosa é a informação. As Forças Armadas, em especial a Marinha do Brasil, têm como desafio estar sempre prontas e capacitadas para atender à Defesa Nacional, demonstrando, de maneira clara, a intenção de usar o seu potencial ofensivo em resposta a ações hostis de outro Estado, garantindo, assim, o direito de autodefesa. Diante deste desafio, propôs-se analisar o conteúdo do Manual de Tallinn, que define — a partir do conhecimento de pesquisadores de Guerra Cibernética e analistas jurídicos representantes do exército, governo, academia e indústria de vários Estados — as regras quanto à legalidade do uso da força no contexto da Guerra Cibernética, tendo como base tratados e convenções existentes em situações de conflito armado. Além disso, o presente trabalho foi fundamentado em uma metodologia de revisão bibliográfica e em uma pesquisa documental das principais leis e doutrinas condicionantes sobre esta nova modalidade de guerra, sob a ótica da Marinha do Brasil. Por fim, a pesquisa mostra que, ao regrar essa nova modalidade de guerra, a defesa cibernética realizada pelas Forças Armadas, em especial pela Marinha do Brasil, estará também respaldada por uma legislação eficiente, visando assegurar a legitimidade das ações militares e favorecer, assim, melhores condições para a obtenção do domínio do Espaço Cibernético.

Palavras-chave: Vulnerabilidades. Espaço cibernético. Ataque cibernético. Guerra cibernética. Enquadramento jurídico. Direito Internacional dos Conflitos Armados.

LISTA DE ABREVIATURAS E SIGLAS

AEN	Ações Estratégicas Navais
C2	Comando e Controle
CCDCOE	Centro de Excelência de Defesa Cibernética Cooperativa
CG	Centro de Gravidade
ComDCiber	Comando de Defesa Cibernética
CoNavOpEsp	Comando Naval de Operações Especiais
DI	Direito Internacional
DIC	Direito Internacional Consuetudinário
DICA	Direito Internacional dos Conflitos Armados
DIH	Direito Internacional Humanitário
EB	Exército Brasileiro
ECiber	Espaço Cibernético
ED	Efeito Desejado
EGC	Esquadrão de Guerra Cibernética
END	Estratégia Nacional de Defesa
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
FA	Forças Armadas
GCiber	Guerra Cibernética
IDF	Forças de Defesa de Israel (Israel Defense Forces)
IISS	International Institute for Strategic Studies
MB	Marinha do Brasil
MD	Ministério da Defesa
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
PND	Política Nacional de Defesa

RE	Regras de Engajamento
SMDC	Sistema Militar de Defesa Cibernética
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
TO	Teatro de Operações

SUMÁRIO

1 INTRODUÇÃO

Vivemos em um mundo em constante transformação; a evolução tecnológica encurtou distâncias, aumentou de forma exponencial a quantidade de informações compartilhadas, reduziu o tempo necessário para estes compartilhamentos, além de ter integrado com grande rapidez a sociedade humana. Isto se reflete não apenas no aspecto das relações sociais, mas também no da economia e da política de um Estado.

Desse modo, é pertinente dizer que o mundo ganhou maior agilidade nas relações pessoais e institucionais, transcendendo fronteiras étnicas, culturais e físicas dos Estados. Conforme mencionado por Nunes (2010), o mundo passou a estar à distância de um clique do mouse, em alusão à facilidade de acesso à informação, além de ter se tornado mais integrado, transformando-se em uma aldeia global. Atualmente, vários serviços, tais como o bancário e o controle de infraestruturas críticas[1], dependem de recursos computacionais e, assim como as mais diversas formas de interação eletrônicas disponíveis para a sociedade moderna, estão, de alguma forma, ao alcance de todos por meio da Internet.

Entretanto, com o crescimento e o desenvolvimento tecnológico, surgiram diversas vulnerabilidades, as quais trouxeram novos riscos, relacionados à exposição virtual a que todos os usuários da Internet se submetem. Atualmente, um dos recursos mais utilizados para as práticas de exploração de vulnerabilidades e ataques cibernéticos[2] são os *malwares*[3]. Esse tipo de programa, que inclui vírus, *worms*[4], cavalos de troia[5], *ransonwares*[6], *spywares*[7], dentre outros, constitui-se de poderosa arma cibernética para inutilização de sistemas, monitoramento de atividades, furtos de senhas, de informações confidenciais etc.

No início do século XXI, alguns incidentes cibernéticos utilizando *malwares* tiveram grande repercussão. Por exemplo, o ataque contra a Estônia, em 2007, e os eventos

---

1 Infraestruturas críticas: instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

2 Ataque cibernético: qualquer tentativa de acesso não autorizado, roubo, alteração, exposição, destruição ou mesmo parada de um dispositivo ou sistema.

3 Malware: é a abreviação de "software malicioso" (em inglês, *malicious software*) e refere-se a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas.

4 Worm: é um tipo de malware mais perigoso que um vírus comum, pois sua propagação é rápida e ocorre sem controle da vítima.

5 Cavalo de Troia: é um tipo de malware que, frequentemente, está disfarçado de software legítimo.

6 Ransomware: é um tipo de malware que sequestra o computador da vítima e cobra um valor em dinheiro pelo resgate, geralmente usando a moeda virtual Bitcoin, que torna quase impossível rastrear o criminoso que pode vir a receber o valor.

7 Spyware: é um tipo de malware que tenta se esconder enquanto registra secretamente informações e rastreia suas atividades on-line em seus computadores ou dispositivos móveis.

ocorridos na Geórgia em 2008, pouco antes de sua invasão pela Rússia. Além desses, destaca-se o ataque realizado pelo Stuxnet[8], que foi um tipo de *malware* mais perigoso que um vírus comum de computador. Esse *malware* se caracterizou pela sua sofisticação e efeitos práticos e reais de uma arma cibernética, destruindo parte das centrífugas iranianas de enriquecimento de urânio localizadas em Natanz, sendo considerado a primeira arma cibernética a causar efeitos no mundo real. Outro exemplo ocorreu em 2016, na Ucrânia, em que um *malware* russo, inspirado no Stuxnet, cortou 20% da energia elétrica da cidade de Kiev.

Em abril de 2020, uma central elétrica da estação de água e esgoto de Israel sofreu uma tentativa de ataque cibernético iraniano, aparentemente, com a intenção de alterar a funcionalidade das bombas, para adicionar cloro em excesso ao abastecimento de água residencial. A chefe do Departamento Cibernético Nacional de Israel, Yigal Unna, destacou que o frustrado ataque contra a estação poderia ter causado danos consideráveis à população civil. No final do mesmo ano, hackers acessaram a rede do Departamento de Energia e de Administração Nacional de Segurança Nuclear dos Estados Unidos da América, responsável pelo arsenal nuclear norte-americano. Não existem muitas informações a respeito dos sistemas afetados nem sobre quais tipos de dados que envolviam as armas nucleares poderiam ser obtidos, no entanto, a porta-voz do Departamento de Energia, Shaylyn Hynes, negou que o departamento tenha sofrido algum impacto com o ataque, afirmando, ainda, que não houve risco para a segurança nacional, uma vez que foram tomadas medidas a tempo para conter o ataque. Ela relatou, também, a sua suspeita de que o ataque tenha partido da Rússia (G1, 2020).

O caso da Geórgia mostra que este tipo de ataque cibernético, que tem como característica preceder o desenvolvimento de operações militares convencionais, provavelmente será a tendência nos próximos conflitos armados (DAVIS, 2014; GILL; DUCHEINE, 2013). Porém, o seu uso poderá não se restringir aos momentos iniciais de um conflito, ou seja, ele poderá ser empregado ao longo de toda uma operação militar, chegando, até mesmo, a substituir o emprego de armas convencionais.

Além disso, a tecnologia utilizada em ataques vem se renovando e evoluindo em um ritmo superior às soluções de segurança presentes no ambiente cibernético, expondo sistemas de informação e toda a infraestrutura à exploração de suas vulnerabilidades. A

8 Stuxnet: é um tipo de malware originalmente destinado a atacar as instalações nucleares do Irã, mas que, desde então, sofreu mutação e espalhou-se para outras instalações industriais e de produção de energia. O ataque de malware Stuxnet original tinha como alvo os controladores lógicos programáveis (CLPs — ou PLCs, na sigla em inglês) usados para automatizar os processos da máquina, sendo conhecido como o primeiro malware a ser capaz de paralisar o hardware.

gravidade do tema é apresentada pelo International Institute for Strategic Studies (IISS)[9], em sua publicação *The Military Balance 2020* (IISS, 2020), a qual relata que a República Popular da China, a França, Cingapura e os Estados Unidos da América criaram comandos militares de alto nível, os quais possuem alta capacidade cibernética. Outros Estados, como Israel e Reino Unido, também aparecem com destaque, quanto à sua capacidade cibernética avançada, ressaltando que todos estes países citados têm potencial para realizar ataques destrutivos. Como comparação, se considerarmos que em 1914 apenas poucos países possuíam aeronaves militares e que, dez anos após, a maioria dos países já possuía tal capacidade, é esperado que o número de países com alguma capacidade de ataque cibernético também cresça consideravelmente em poucos anos.

Pesquisas recentes, realizadas pela plataforma Fortinet Threat Intelligence Insider Latin America[10], alertaram que o Brasil sofreu mais de 3,4 bilhões de tentativas de ataques cibernéticos de janeiro a setembro de 2020, sendo que, em toda a América Latina e Caribe, o total foi de 20 bilhões. O estudo de Mike McGuire, especialista em crimes cibernéticos e professor de Criminologia da Universidade de Surrey, no Reino Unido, evidenciou, em números, que os conflitos armados já estão sendo realizados utilizando armas cibernéticas. O estudo *Nation States, Cyberconflict and the Web of Profit*, patrocinado pela empresa Hewlett-Packard (HP), destaca que os ataques com origem, ou financiados por, Estados-Nação têm sido frequentes e tiveram um crescimento de 100% entre 2017 e 2020 (MCGUIRE, 2021).

Assim, observa-se o quão nocivos a um Estado podem ser os ataques realizados no Espaço Cibernético (ECiber)[11], sejam eles para atender a operações militares ou em retaliação a divergências ideológicas, políticas e culturais, ou até mesmo para provocar prejuízos a infraestruturas críticas de um Estado. Cabe ressaltar que a segurança dessas infraestruturas críticas é de responsabilidade do Estado, conforme preconizado, no caso do Brasil, na Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC)[12], dada a sua importância para os setores estratégicos nacionais (BRASIL, 2020b). Além disso, em situações de conflito armado, o direito de legítima defesa frente a ações ofensivas nestas Infraestruturas Críticas deverá ser considerado.

---

9 IISS: Instituto de pesquisa internacional que fornece informações sobre desenvolvimento militar, geopolítico e geoeconômico que possam ocasionar conflitos.

10 Fortinet Threat Intelligence Insider Latin America: ferramenta que coleta e analisa incidentes de segurança cibernética.

11 Espaço Cibernético: espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas.

12 ENSIC: criada por meio do Decreto Nº 10.569, de 9 de dezembro de 2020, do Gabinete de Segurança Institucional da Presidência da República.

Destarte, é fundamental que se verifique a aplicabilidade do Direito Internacional dos Conflitos Armados (DICA) às operações cibernéticas desenvolvidas no contexto de um conflito armado. Jastran e Quintin (2011) expressam a importância da aplicabilidade do DICA ao mencionarem que, agora, será difícil estimar as consequências, mas que os Estados não podem correr o risco de aguardar até que seja tarde demais para se prevenirem contra os piores cenários. Nesse sentido, a Guerra Cibernética (GCiber) poderá ser a causa de novas interpretações do DICA, exigindo, então, a formulação de novas regras adicionais, ou mesmo de uma nova legislação, que venham a regular a condução cibernética dos conflitos armados.

Dessa forma, este trabalho tem como objetivo contribuir para que a Marinha do Brasil (MB) não somente garanta a proteção de seus próprios sistemas e desenvolva as suas capacidades ofensivas, mas que possa primar pelas melhores diretrizes de sua atuação no ECiber perante o Direito Internacional (DI), respondendo às seguintes questões:

1. É possível limitar ações ofensivas no ECiber perante o DICA?
2. Quais são os principais documentos, legislações e normas que regem as ações cibernéticas na MB?
3. Considerando a legislação em vigor, a MB está amparada, ao realizar ações ofensivas, perante os princípios do DICA no ECiber?

Para atingir o objetivo proposto, a abordagem desta monografia está estruturada em cinco capítulos adicionais a esta introdução. O segundo capítulo apresenta os trabalhos relacionados à GCiber quanto à necessidade da regulamentação internacional, de forma que impeça os efeitos dos ataques cibernéticos à segurança da sociedade. O terceiro capítulo relaciona as principais regras aplicadas às operações ofensivas em um conflito armado à luz do DI, de modo a prover um entendimento comum sobre este tema, que é atual e complexo. O quarto capítulo relaciona conceitos e características referentes à GCiber, além de apresentar alguns preceitos acerca de seu emprego no ambiente operacional — o ECiber — perante as Leis, Doutrinas e Normas que regulamentam o papel das Forças Armadas (FA), em especial o da MB. Após apresentada a fundamentação, o quinto capítulo analisará a aplicabilidade da GCiber na MB e suas limitações perante os princípios do DICA. O sexto capítulo finalizará este estudo apresentando a conclusão de todos os aspectos analisados.

Dessa forma, após feita a apresentação da motivação e do objetivo desta monografia, no próximo capítulo serão expostos, de forma sintetizada, os trabalhos mais relevantes sobre a GCiber e o DI.

2 A GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL

A GCiber surgiu com a popularização da Internet, na década de 1990, e estende-se até os contínuos avanços tecnológicos dos dias atuais. Segundo Hobbes (1988), se dois homens desejam a mesma coisa, eles se tornam inimigos. Assim, não há como se olvidar das relações humanas quando o tema é de extrema relevância por se tratar, justamente, de uma nova e sofisticada forma de atrito, sobretudo porque é da natureza humana se engajar em conflitos. As românticas lutas de outrora, por amor e glória, deram lugar às guerras por dinheiro e poder, extremamente sofisticadas do ponto de vista tecnológico, com grande poder de destruição e pouco esforço. Assim, diante dessa nova ameaça, é preciso manter atualizadas as normas de regulação das relações humanas e interpaíses, no que concerne às hostilidades, em âmbito internacional. É fato, contudo, que a comunidade internacional se vê diante de um arcabouço legal repleto de leis e tratados para a guerra convencional que carecem de adaptação, dadas as características específicas desta nova forma de promover ataque.

Nesse contexto, ao longo do tempo, diversas pesquisas e trabalhos sobre este tema foram realizados, no sentido de identificar os seus efeitos sob o ponto de vista da segurança de Estado. Clarke (2015) fez um resumo das experiências envolvendo confrontos cibernéticos para demonstrar que os conflitos entre Estados-Nação com ataques cibernéticos já começaram. Como exemplo, ele discorre sobre o ataque surpresa realizado por Israel à Síria, com a hipótese de que este país estaria trabalhando de forma secreta com armas nucleares. O autor cita que a guerra, na era da informação, refere-se a ações de um Estado-Nação para invadir computadores ou redes de outra nação para causar danos ou transtornos. Os israelenses utilizaram pulsos de luz e elétricos para transmitir “0s” e “1s” e controlar o que os radares da defesa aérea síria conseguiam visualizar. Em suma, em vez de estourar as defesas antiaéreas sírias, na era da GCiber, os israelenses se asseguraram de que o inimigo não poderia sequer levantar suas defesas. Outra experiência mencionada pelo autor se refere à crise ocorrida entre Moscou e Estônia, em 2007, cujo conflito mudou para o ECiber. Os servidores que hospedavam as páginas mais utilizadas na Estônia foram inundados com pedidos de acesso, ocorrendo, assim, o seu colapso, decorrente da sobrecarga, o que é conhecido por Ataque Distribuído de Negação de Serviços, ou *Distributed Denial of Service* (DDoS).

Nesse sentido, Davis (2014) realizou um estudo sobre o potencial efeito catastrófico das ações de ataque na GCiber e sobre como a dissuasão e o estabelecimento de leis e de normas internacionais consistentes e efetivas poderão reduzir estes efeitos para a

sociedade civil. Segundo o autor, somente a junção dos esforços de dissuasão com a aplicação de leis e normas internacionais efetivas pode conter os efeitos nocivos à sociedade civil. Por sua vez, Gervais (2012) buscou mostrar como funcionam os ataques cibernéticos, como estão sendo utilizados na prática e de que forma o Direito Internacional Humanitário (DIH) se relaciona com o uso de armas cibernéticas. Em seu trabalho, ele concluiu que, sem a governança e as restrições do DI, o ciberespaço continuará sendo um campo de batalha relativamente sem lei, sendo necessário, portanto, que as Regras de Engajamento (RE) no ECiber sejam acrescidas às leis convencionais de guerra.

A pesquisa de Gill e Ducheine (2013) ressalta que o atual quadro jurídico que rege o exercício do direito de legítima defesa é relevante e aplicável a ataques cibernéticos dentro das condições estabelecidas na Carta das Nações Unidas e no Direito Internacional Consuetudinário (DIC). Ou seja, embora possam haver divergências de entendimento sob o ponto de vista jurídico na aplicação da legítima defesa ao se compelir ataque realizado totalmente em ambiente cibernético, é preciso conceber a ideia de que, por conceito, a legítima defesa é caracterizada por repelir injusta agressão com a restrição de que se utilizem somente os meios necessários para fazê-lo, sem praticar excessos. E a grande questão é a dificuldade de se apurar a legitimidade da ação de defesa nos casos de ocorrência em ambiente totalmente virtual. Kostadinov (2014) afirma que, mesmo sem ser mencionado explicitamente, o DIH se estende à esfera do ECiber, com todos os seus direitos e prerrogativas, uma vez que os ataques cibernéticos podem, definitivamente, colocar em risco todos os seus princípios, ao expor perigo à integridade física e ao bem-estar de civis.

Para Nunes (2010), o Efeito Desejado (ED) com a GCiber como elemento operacional não diz respeito somente à integridade dos sistemas de Tecnologia da Informação (TI), mas também guarda relação com a preservação de vidas humanas, com a condução de campanhas militares e, primordialmente, com a própria missão. O autor propõe uma base doutrinária para operações no ECiber e ressalta a necessidade de uma doutrina conjunta com outras Forças, sob responsabilidade do Ministério da Defesa (MD).

O trabalho de Cordeiro (2016), por sua vez, analisa a Defesa Cibernética e suas ações em caso de conflito armado no nível estratégico, com base na Doutrina Militar de Defesa Cibernética — MD31-M-07 (BRASIL, 2014b). O autor conclui que, apesar de a referida doutrina abranger todo o conhecimento necessário para o direcionamento das ações no campo da Defesa Cibernética, ela carece de aprimoramentos, a fim de se evitar em conflitos com o DICA.

Os trabalhos de Clarke (2015), Davis (2014), Gervais (2012) e Kostadinov (2014) destacam, assim como no presente estudo, que o ECiber não pode ser considerado um campo de batalha sem lei; porém, eles não apontam quais são os riscos associados aos princípios e características da Guerra, sob o enfoque cibernético, que podem agravar os efeitos indesejáveis à sociedade civil. O trabalho de Gill e Ducheine (2013) reforça o que está previsto na MB, ou seja, o direito de legítima defesa perante o DIC, que deve ser levado em consideração nas Leis e Acordos Internacionais que regem a Guerra. Nunes (2010) e Cordeiro (2016) ressaltam que deve existir uma doutrina conjunta, sob responsabilidade do MD, com o intuito de direcionar e servir de base para o emprego militar nas operações em conflitos armados; sendo que, nesta monografia, é enfatizado o emprego pela MB.

Por fim, destaca-se o trabalho de Schmitt, o Manual de Tallinn 2.0, considerado a maior referência em todo o mundo sobre operações cibernéticas, que descreve 154 regras sobre operações cibernéticas que se aplicam a situações dentro ou fora de um conflito armado à luz do DIH, a partir da análise de especialistas em GCiber e DI (SCHMITT, 2017). Esta monografia tem como um dos seus objetivos analisar as principais regras do Manual de Tallinn que se aplicam às ações ofensivas em um conflito armado e que limitam a GCiber pelas FA, em especial pela MB, perante o DICA, com base nas Leis, Doutrinas e Normas em vigor.

Após a apresentação dos principais trabalhos que relacionam o DIH com a GCiber, será analisada, no próximo capítulo, a possibilidade de se impor regras que limitem as ações ofensivas no ECiber diante de um conflito armado internacional.

3 O MANUAL DE TALLINN E AS AÇÕES OFENSIVAS NA GUERRA CIBERNÉTICA

Em 2009, o Centro de Excelência de Defesa Cibernética Cooperativa (CCDCOE, na sigla em inglês), pertencente à Organização do Tratado do Atlântico Norte (OTAN) — e com sede em Tallinn (Estônia), voltado para pesquisa e treinamento e composto por um grupo diversificado de especialistas de 29 Estados[13] —, reuniu um grupo de pesquisadores em GCiber e analistas jurídicos representantes do exército, governo, academia e indústria destes Estados para produzir um manual sobre o DI que regesse a GCiber. Os especialistas se

13 Os 29 Estados são: Áustria, Bélgica, Bulgária, Croácia, República Tcheca, Dinamarca, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Itália, Letônia, Lituânia, Montenegro, Holanda, Noruega, Polônia, Portugal, Romênia, Eslováquia, Eslovênia, Espanha, Suécia, Suíça, Turquia, Reino Unido e Estados Unidos da América.

inspiraram em outros manuais, que já haviam contribuído significativamente para interpretar o DIH, tais como: o Manual de Leis e Costumes de Guerra em Oxford (1880), que serviu de base para as duas Convenções de Haia sobre guerra terrestre e seus Regulamentos anexos, adotado tanto em 1899 como em 1907; e o Manual de San Remo, documento do DI elaborado pela Cruz Vermelha, que trata dos Conflitos Armados no Mar.

O Manual de Tallinn teve como objetivo analisar a legalidade do uso da força no contexto da GCiber perante as normas existentes em situações de conflito armado. Após quatro anos de esforços nos estudos e nas interpretações das Leis, Normas em vigor e costumes, foi publicado, em 2013, o primeiro Manual de Tallinn, sobre o DI aplicável à GCiber. Desde a sua publicação, ele tem sido utilizado como um importante recurso para consultores jurídicos e acadêmicos. O CCDCOE decidiu, assim, ampliar o escopo do Manual, incluindo uma legislação sobre as operações cibernéticas em tempo de paz, sendo publicado, então, o Manual de Tallinn 2.0, em 2017.

A partir deste capítulo, serão abordadas as principais regras do Manual de Tallinn 2.0, listadas na Tabela 1, do APÊNDICE A, que abrangem as ações ofensivas da GCiber em conflitos armados quanto a dois assuntos: o *jus ad bellum*, que regulamenta o uso da força pelos Estados; e o *jus in bello*, que rege a forma como estes podem conduzir suas operações militares durante um conflito armado, proporcionando legitimidade para suas ações e oferecendo proteção à sociedade contra efeitos indesejados.

Nos tópicos a seguir, serão apresentadas as limitações da GCiber quanto a alguns aspectos que infringem o DI, de acordo com as regras do Manual de Tallinn.

3.1 Quanto à soberania

Considera-se que, devido as ações cibernéticas ocorrerem dentro de um território, envolvendo objetos e sendo conduzidas por pessoas ou entidades, sobre as quais o Estado exerce suas prerrogativas soberanas, o princípio da soberania de um Estado também se aplica ao ECiber. Além disso, a violação da soberania de outro Estado é proibida, com exceção nos casos de legítima defesa (autodefesa) individual ou coletiva ou quando autorizada pelo Conselho de Segurança da Organização das Nações Unidas (ONU), de acordo com as regras 1 e 4 da Tabela 1, do APÊNDICE A. Outro aspecto importante para identificação e responsabilização pelas possíveis violações de soberania está presente nas regras que tratam da devida diligência, ou seja, nos casos em que um Estado utilize a infraestrutura de um terceiro Estado para atingir o inimigo beligerante. Como exemplo, considere-se que um hacker ou organização localizada no Estado A realize uma ação cibernética destrutiva contra o

Estado B utilizando a infraestrutura cibernética localizada no Estado C. Se o Estado C estiver ciente e não tomar medidas cabíveis para pôr fim a ação, é uma violação do princípio de devida diligência, conforme as regras 6 e 7 da Tabela 1, do APÊNDICE A.

3.2 Quanto à legitimidade do uso da força

Uma operação cibernética que se constitua uma ameaça ou uso da força, de acordo com a regra 69 da Tabela 1, do APÊNDICE A, contra a integridade territorial ou a independência política de qualquer Estado, ou que esteja em desacordo com os propósitos da Carta das Nações Unidas, é ilegal. Segundo o Manual de Tallin, o mero fato de utilizar-se um computador no lugar de um armamento tradicional, sistema de armas, ou plataforma durante uma ação ofensiva equivale ao uso da força. Existem duas exceções amplamente reconhecidas à proibição de uso da força: o uso da força autorizado pelo Conselho de Segurança sob o Capítulo VII; e a legítima defesa nos termos do Artigo 51 da Carta, conforme as regras 19, 68, 71, 72 e 73 da Tabela 1, do APÊNDICE A. Além disso, o Estado, ao utilizar o direito de legítima defesa, deverá imediatamente comunicar o fato ao Conselho de Segurança das Nações Unidas, o qual irá avaliar se uma ação cibernética constitui uma ameaça ou violação à paz ou ato de agressão, podendo autorizar medidas não contundentes, inclusive ações cibernéticas que se caracterizam como uso da força, em resposta, de acordo com as regras 75 e 76 da Tabela 1, do APÊNDICE A.

3.3 Quanto à aplicabilidade do DICA

As ações cibernéticas executadas no contexto de um conflito armado estão sujeitas ao DICA, apesar da ausência de regras específicas quanto às ações cibernéticas dentro das leis do conflito armado. Contudo, estas ações cibernéticas também estão sujeitas a limitações geográficas impostas por leis do DI aplicáveis durante um conflito armado, como, por exemplo, no espaço sideral e em territórios neutros, conforme as regras 80, 81 e 82 da Tabela 1, do APÊNDICE A. No entanto, os especialistas do Manual de Tallin foram unânimes ao considerarem que durante um ataque cibernético, ao utilizar-se do serviço de nuvem, em que os dados de um Estado de origem são processados e podem ser replicados entre servidores de vários outros Estados, incluindo Estados neutros, deve-se observar onde o ataque é iniciado e concluído. Logo, não proíbem o tráfego de dados por áreas onde as ações cibernéticas são proibidas durante um conflito armado, como nos territórios neutros.

3.4 Quanto à responsabilidade criminal

As operações cibernéticas podem representar crimes de guerra e, portanto, dar origem à responsabilidade penal do comando ou individual, à luz do DI. Esta regra se aplica a membros das FA e civis envolvidos em ações cibernéticas associadas ao conflito armado, conforme as regras 84, 85 e 92 da Tabela 1, do APÊNDICE A. Os comandantes são responsáveis por garantir a conduta de seus subordinados em todas as operações, de acordo com as normas do DICA. O fato de não ter ordenado, autorizado ou concordado com uma ação cibernética que viole o DICA, não o exime da responsabilidade. Da mesma forma, o DICA também adota o princípio da responsabilidade individual, ou seja, o fato de um militar ou civil ter agido na qualidade de representante do Estado, baseado na obediência hierárquica, não o exime de responder por suas ações.

3.5 Quanto à distinção de pessoal combatente e não combatente

O princípio de distinção se aplica a ataques cibernéticos. Com o intuito de garantir o respeito e a proteção da população civil e objetos civis, as partes do conflito devem sempre distinguir entre a população civil e combatentes e entre objetos civis e objetivos militares e, portanto, devem dirigir suas ações somente contra pessoas ou alvos militares. Os objetos civis não devem ser alvo de ataques cibernéticos. Objetos civis são todos os objetos que não são objetivos militares. Objetivos militares são aqueles que, por sua natureza, localização, propósito, ou finalidade, contribuem efetivamente para a ação militar e cuja destruição total ou parcial, captura ou neutralização, nas circunstâncias prevalecentes no momento, oferece ou definem uma vantagem militar. Com isso, uma infraestrutura cibernética só pode ser alvo de ataque se for qualificada como objetivo militar, conforme as regras 93, 95, 96, 99. 100 e 101 da Tabela 1, do APÊNDICE A.

3.6 Quanto aos princípios da necessidade e proporcionalidade

O uso da força envolvendo operações cibernéticas realizadas por um Estado, e no exercício do seu direito de legítima defesa, deve ser necessário e proporcional. Logo, as ações cibernéticas em legítima defesa devem atender a dois critérios: necessidade e proporcionalidade. Quanto à necessidade, o uso da força — incluindo as ações cibernéticas que sejam equivalentes ao uso da força, de acordo com a regra 69 da Tabela 1, do APÊNDICE A — será necessário para impedir o sucesso de um ataque armado iminente ou que já esteja em andamento. Quanto à proporcionalidade, o critério será a escala, o escopo, a duração e a intensidade da ação necessária para inibir a situação que deu origem ao direito de legítima

defesa. Além disso, não é necessário que a ação defensiva seja de mesma natureza da que constitui o ataque armado. Logo, o uso da força por meio de uma ação cibernética pode ser feito em resposta a um ataque armado cinético e vice-versa. É proibido empregar meios ou métodos de GCiber que sejam de natureza a causar lesões ou sofrimentos desnecessários, que utilizem métodos indiscriminados ou que atinjam pessoas protegidas pelo DI, como, por exemplo, pessoal de saúde, religiosos e prisioneiros de guerra, conforme as regras 104, 105, 106, 107, 111, 113, 115, 116, 117, 119, 121, 131, 132, 133 e 135 da Tabela 1, do APÊNDICE A. A fim de se evitar consequências graves que levem a perdas entre a população civil, cuidados especiais devem ser tomados durante ataques cibernéticos contra obras e instalações, tais como barragens, diques e geradores elétricos, estações nucleares, bem como alvos localizados nas suas proximidades, de acordo com a regra 140 da Tabela 1, do APÊNDICE A.

Diante das regras do Manual de Tallinn apresentadas neste capítulo quanto às principais limitações, observa-se, do ponto de vista do planejamento das ações cibernéticas, a importância dos sistemas e redes que serão alvos das ações de exploração e ataques, que devem ser estudados, analisados e sua configuração modelada de forma a permitir a simulação das ações em ambiente controlado, para garantir os objetivos desejados sem infringir os princípios do DI.

Tendo este capítulo apresentado a interpretação realizada pelo Manual de Tallinn com relação à soberania, à legitimidade do uso da força, à aplicabilidade do DICA, à responsabilidade criminal, à distinção de pessoal combatente e não combatente e aos princípios da necessidade e proporcionalidade, que permitem limitar as ações no ECiber, será realizada, agora, uma abordagem sobre os documentos condicionantes da GCiber na MB.

4 A GUERRA CIBERNÉTICA NA MARINHA DO BRASIL

As FA têm um crucial papel na proteção de seus próprios sistemas e no desenvolvimento de capacidades potencialmente ofensivas. A partir desta percepção, a MB estabeleceu como uma de suas Ações Estratégicas Navais (AEN), por meio do Plano Estratégico da Marinha (PEM) 2040, a AEN-CIBER 1, que consiste em criar o Esquadrão de Guerra Cibernética (EGC), com o propósito de coordenar os recursos e as ações de GCiber. Atualmente, esta tarefa se encontra sob a responsabilidade do Comando Naval de Operações Especiais (CoNavOpEsp), que tem como principais atribuições afetas a este trabalho comandar e compor Forças-Tarefas de Operações Especiais e de GCiber, combinadas ou

conjuntas, quando determinado, além de conduzir as ações de GCiber de caráter operativo no âmbito da MB (BRASIL, 2020d).

Dessa forma, este capítulo tem como objetivo identificar as diretrizes de atuação cibernética da MB, consolidando conceitos e princípios referentes às ações de GCiber, buscando evidenciar as Leis e Doutrinas afetas à Força Naval que amparam o seu emprego no ambiente operacional onde o EGC atuará. Os principais documentos oficiais, legislações da área e normas se encontram listados na Tabela 2, do APÊNDICE B.

4.1 Definição de Terminologia

Dentre os documentos analisados, o único encontrado com definições pontuais a respeito de ações ofensivas da GCiber foi a Doutrina de Tecnologia da Informação da Marinha — EMA 416 (BRASIL, 2013), Volume II (Manual de Guerra Cibernética), que estabelece os princípios, as características e as ações a serem empregadas pela MB na condução da GCiber, complementando, doutrinariamente, as ações adotadas e estabelecidas para a Segurança da Informação. A Doutrina Militar Naval — EMA 305 (BRASIL, 2017b), que trata do emprego do Poder Naval para a conquista e a manutenção dos Objetivos Nacionais de Defesa, considera as ações de GCiber como um meio a ser empregado em operações de informação ou de inteligência. Apenas descrevendo o seu nível de emprego, o tipo e o ED.

4.2 Conteúdo dos Documentos

As ações de GCiber se caracterizam por envolver o emprego de diversas ferramentas disponíveis nos campos da Tecnologia da Informação e Comunicações (TIC) com o intuito de desestabilizar os ativos de informação do oponente e, com isto, possibilitar a proteção dos ativos de informação de interesse. A GCiber visa influenciar o objetivo e a capacidade de tomada de decisão do oponente. Essas ações englobam diversas técnicas, táticas e procedimentos empregados em uma operação dentro de um ambiente operacional cibernético, que permeia os demais: terrestre, marítimo e aeroespacial, sendo todos interdependentes. O domínio cibernético é qualitativamente diferente dos outros domínios. Ele se sobrepõe e opera continuamente dentro de todos eles. Além disso, possibilita que todos os instrumentos do poder nacional na esfera política, econômica, psicossocial, militar e científico-tecnológica sejam utilizados simultaneamente por meio da manipulação de dados e redes.

Por essas características, o ECiber pode ser considerado como um Centro de Gravidade (CG) para o mundo globalizado. No caso dos Estados-Nação, trata-se não apenas de uma possibilidade de CG nas operações militares, mas também para outros aspectos que atendam aos objetivos nacionais, incluindo econômicos, sociais, diplomáticos, entre outros. Logo, a soberania de um Estado se encontra constantemente ameaçada por este novo meio operacional, conforme descrito no item 3.1, regras 1 e 4 do Manual de Tallinn.

O papel das FA na garantia da soberania, bem como sua organização e seu emprego, encontram-se nos seguintes documentos presentes na Tabela 2, do APÊNDICE B:

a) Constituição Federal de 1988 (BRASIL, 1988);
b) Lei Complementar Nº 97 de 1999 (BRASIL, 1999);
c) Decreto Nº 5.484 de 2005 (PND) (BRASIL, 2005);
d) Decreto Nº 6.703 de 2008 (END) (BRASIL, 2008); e
e) Livro Branco de Defesa Nacional de 2012 (BRASIL, 2012a) e suas respectivas atualizações quadrienais.

Quanto às responsabilidades das ações cibernéticas, de acordo com o nível de decisão, destaca-se o Decreto Nº 7.276, de 2010 (BRASIL, 2010), que estabelece as seguintes responsabilidades:

a) Ao Presidente da República: determinar a ativação dos Comandos Operacionais ao Ministro de Estado da Defesa, em face de situação de crise ou conflito armado;
b) Aos Comandantes das FA: emitir diretrizes, visando ao planejamento operacional para emprego, quando da ativação de um Comando Singular a eles subordinado;
c) Ao Chefe do Estado-Maior Conjunto das FA: acompanhar o planejamento e as ações realizadas pelos Comandos Operacionais; e
d) Aos Comandantes dos Comandos Operacionais: planejar, controlar, coordenar e executar o emprego das forças sob seu comando, de acordo com o planejamento estratégico, em consonância com as diretrizes emanadas do Presidente da República e do Ministro de Estado da Defesa (BRASIL, 2010).

As ações de GCiber são contextualizadas pela Doutrina Militar de Defesa Cibernética (MD31-M-07), de 2014 (BRASIL, 2014b), que as classifica no ECiber de acordo com o nível de decisão: Segurança da Informação e Segurança Cibernética, no nível presidencial; Defesa Cibernética, no nível ministerial; e Guerra Cibernética, nos níveis de comando e execução das atividades. Além disso, essa doutrina estabelece as Diretrizes para a

criação do Sistema Militar de Defesa Cibernética (SMDC), que tem como principal desafio conduzir ações de proteção, exploração e ataques cibernéticos em proveito da Defesa Nacional.

Os demais Decretos, Nº 10.222 (BRASIL, 2020a) e Nº 10.569 (BRASIL, 2020b), de 2020, e Portaria Nº 3.781 (BRASIL, 2020f), de 2020, respectivamente, instituem a Estratégia Nacional de Segurança Cibernética e a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), ambas com foco somente nas ações defensivas, e criam o SMDC. O SMDC estabeleceu como órgão central o Comando de Defesa Cibernética (ComDCiber), sendo este um comando operacional permanentemente ativado e com capacidade interagências, composto por militares das três FA, apesar de estar sob a cadeia de comando do Exército Brasileiro (EB). Ressalta-se, aqui, a atribuição do ComDCiber, como órgão central, de executar ações cibernéticas em situações de paz, de crise ou de conflito armado, no domínio operacional cibernético, respeitadas as competências das Forças Singulares e dos Comandos Operacionais ativados.

No entanto, os documentos listados acima não mencionam as limitações do emprego de ações cibernéticas quanto à legitimidade do uso da força, conforme mencionado nas Regras de Tallinn, apresentadas no item 3.2. Da mesma forma, eles não deixam claro a responsabilidade criminal por ações ofensivas na GCiber, conforme descrito no item 3.4, regras 19, 68, 71, 72, 73, 75 e 76 do Manual de Tallinn.

A Doutrina Militar Naval — EMA 305, por sua vez, estabelece conceitos e métodos de emprego Poder Naval em combate, com o propósito de orientar o seu planejamento, preparo e aplicação (BRASIL, 2017b). Porém, ela não discorre sobre operações de GCiber, somente a sobre operações de informação (OpInfo), mencionando que estas poderão ser desencadeadas por uma ação de GCiber.

Por último, destaca-se o Manual de Direito Internacional Aplicado às Operações Navais — EMA 135, que, em conjunto com a legislação nacional, tratados e atos internacionais assinados pelo Brasil, tem como objetivo orientar os militares da MB em situações de conflitos armados (BRASIL, 2017a). Assim como na doutrina mencionada anteriormente, este Manual não discorre sobre as operações de GCiber. Porém, conforme mencionado no item 3.3, o Manual de Tallinn, nas regras 80, 81 e 82, diz que, apesar da ausência de regras específicas quanto às ações cibernéticas dentro das leis do conflito armado, as referidas ações estão sujeitas ao DICA.

Após apresentados os principais documentos, leis e doutrinas que regem a GCiber na MB, e ressaltados os que estão associados às regras do Manual de Tallinn, no próximo

capítulo, o grande desafio será analisar as limitações da MB em inserir as possibilidades técnicas desta nova modalidade de conflito perante o DICA, em um TO novo, que é o mundo virtual, em um contexto jurídico que seja suficientemente capaz de promover segurança jurídica e de assegurar que os efeitos nocivos à sociedade civil sejam mínimos.

5 POSSIBILIDADES E LIMITAÇÕES DA GCIBER EM RELAÇÃO AOS PRINCÍPIOS DO DICA

Assim como o DIH e a Carta das Nações Unidas (ONU), o DICA tem como objetivo limitar as barbáries da guerra, sendo todos estes tratados assinados pelo Brasil. Cabe ressaltar que, embora estes tratados não especifiquem as ações da GCiber, isto não significa que estas ações não estejam sujeitas às suas regras. A ratificação pelo Brasil dos referidos tratados e documentos normativos ensejou, na convenção estabelecida pelo MD, a adoção de cinco princípios básicos, que norteiam a aplicação deste ramo do direito nas FA. Neste capítulo, tais princípios serão contextualizados para a perspectiva da GCiber, bem como serão descritas algumas das principais regras do Manual de Tallinn que podem ser aplicadas para que os mesmos sejam respeitados.

5.1 Princípios Básicos do DICA sob a Ótica do MD e do Manual de Tallinn

O Manual de Tallinn define o ataque cibernético como sendo uma ação, ofensiva ou defensiva, que cause ferimentos ou morte a pessoas, danos ou destruição de objetos, conforme a regra 92 da Tabela 1, do APÊNDICE A, a partir da caracterização de um conflito armado internacional que tenha tido como fator gerador estes ataques, de acordo com a regra 82 da Tabela 1, do APÊNDICE A. Ele considera, ainda, que algumas operações cibernéticas constituem o uso da força, conforme a regra 69 da Tabela 1, do APÊNDICE A, e que, portanto, estas operações estão sujeitas aos tratados e atos que regem o conflito armado.

5.1.1 Princípio da Distinção

O princípio da Distinção requer que se diferenciem combatentes e civis não combatentes, assim como alvos militares e bens de caráter civil. Tanto os civis não combatentes quanto os bens de caráter civil são protegidos contra os ataques, não podendo ser utilizados como objetos de represália (BRASIL, 2011).

No contexto da GCiber, a aplicação prática deste princípio se torna complexa, uma vez que os alvos estão remotos e fora da visão de seus atacantes, em infraestruturas

interconectadas que atendem da mesma forma a militares e usuários civis, os quais poderão ser atingidos por efeitos colaterais das ações de ataques no ECiber. Além disso, existe a presença simultânea de combatentes e não combatentes civis no ECiber. Cabe lembrar que neste ambiente inexistem barreiras físicas e tampouco seus usuários se distinguem por meio de uniformes ou insígnias.

Segundo o Manual de Tallinn, ataques cibernéticos que não sejam direcionados a um alvo militar e que, consequentemente, atinjam alvos civis sem distinção, são proibidos, como evidenciado na regra 111 da Tabela 1, do APÊNDICE A. Como exemplo, considere um ataque cibernético que insira um *script*[14] malicioso em um arquivo que, por sua vez, seja colocado em um site público de um serviço muito procurado de um Estado. Quando o navegador fizer o acesso ao site a partir de um computador ou dispositivo vulnerável, ele possivelmente processará este arquivo, sendo executado, então, o *script* malicioso e, consequentemente, causando danos ao computador ou dispositivo.

No entanto, mesmo que um ataque cibernético seja direcionado contra um alvo militar, existe a possibilidade de ele afetar outros usuários e sistemas, caracterizando o ataque como indiscriminado. Uma vez que uma arma cibernética (um vírus ou *worm*, por exemplo) seja empregada em um ataque, o seu autor não poderá impedir sua retransmissão e consequente infecção de outras máquinas e redes. Mesmo em redes segregadas (apartadas da Internet), o risco de contaminação existe, porque o vírus pode ser transferido por meio de mídias removíveis, como um *Hard Drive* (HD) externo ou uma *Flash Memory* (conhecida no Brasil como pen drive). Uma vez que quase toda a infraestrutura cibernética militar depende de redes e links de operadoras civis, um ataque contra a infraestrutura de TI militar pode se disseminar nos sistemas civis e, a partir deste ponto, causar efeitos em escala global (JASTRAM; QUINTIN, 2011; GERVAIS, 2012; SCHMITT, 2012; WINGFIELD, 2009).

Cabe ressaltar que, apesar da necessidade de distinção entre alvos militares e objetos civis, a infraestrutura cibernética utilizada ao mesmo tempo para fins militares e civis pode ser um alvo militar, conforme o Manual de Tallinn, de acordo com a regra 101 da Tabela 1, do APÊNDICE A. Considere uma rede que esteja sendo utilizada para fins militares e civis, dificilmente será possível distinguir qual parte desta rede de transmissão está sendo utilizada para fins militares ou não. Nesse caso, toda a rede poderá ser assumida como um alvo militar. Conforme Schmitt (2017), fazendo uma analogia com uma rede rodoviária utilizada por veículos militares e civis, embora um invasor possa não saber com precisão quais estradas

14 *Script*: é uma série de instruções para que uma máquina execute determinadas tarefas conforme o programado.

serão percorridas por forças militares inimigas (ou qual estrada será escolhida para ser bloqueada), desde que seja razoavelmente provável que uma estrada possa ser utilizada, esta estrada será um objetivo militar sujeito a ataque. Logo, não há razão para se tratar as redes de computadores de maneira diferente.

Assim, com o intuito de distinguir alvos militares e alvos civis, existe a necessidade de apoio do trabalho da inteligência — a fim de minimizar e evitar os problemas e os efeitos indesejáveis nestas ações —, que consiste em um levantamento com estudo preliminar do alvo, da necessidade de análise legal e dos cuidados na execução das operações, o que inclui a seleção de uma arma cibernética com precisão suficiente para atacar somente os alvos cibernéticos selecionados.

Nesse sentido, o trabalho de Lewis (2012) mostra que o requisito de precisão da arma cibernética foi utilizado no caso do Stuxnet, um artefato cibernético de nível militar que foi uma alternativa de precisão à realização de um ataque aéreo às instalações nucleares de enriquecimento de urânio iranianas. O ataque causou menos danos do que causaria um ataque aéreo e evitou efeitos colaterais adversos, tais como a morte de civis não combatentes, apesar de um erro de programação o ter tornado indiscriminado em seu alcance.

Tal característica levou à ideia de que a GCiber pode ser uma alternativa de menor impacto, uma vez que suas armas podem ser utilizadas no lugar de sua contraparte cinética, para se alcançar o mesmo resultado, ao mesmo tempo em que apresentam menor letalidade e causam destruição limitada. O alcance que um ataque cibernético tem para interromper, neutralizar, ou mesmo destruir um determinado objetivo, oferece maior discricionariedade do que um ataque cinético, característica que torna o ataque cibernético hiperdistintivo. Nesse sentido, em várias ocasiões, o ataque cibernético será preferível à opção cinética (JASTRAM; QUINTIN, 2011; LEWIS, 2012; GERVAIS, 2012; SCHMITT, 2012).

As seguintes regras do Manual de Tallinn 2.0 poderão ser aplicadas na MB para atender ao princípio da distinção: 81, 93, 94, 95, 96, 99, 100, 101, 105, 111, 115, 119, 131, 132, 133 e 140, presentes na Tabela 1, do APÊNDICE A.

5.1.2 Princípio da Necessidade Militar

O princípio da Necessidade Militar estabelece que, em todo conflito armado, o uso da força deve corresponder à vantagem militar que se pretende obter. Além disso, as necessidades militares não justificam condutas desumanas, tampouco atividades que sejam proibidas pelo DICA (BRASIL, 2011).

Do ponto de vista da GCiber, atualmente, as FA vêm adotando sistemas computacionais que atendem a diversas plataformas de armas e seus principais sistemas de Comando e Controle (C2)[15], contemplando praticamente todo o escopo de suas operações. Uma vez direcionados contra sistemas computacionais militares do inimigo, passam à condição de necessidade militar e tornam-se alvos em potencial de ataques cibernéticos.

Entretanto, há outros fatores a se ponderar, o que pode tornar complexa a determinação da vantagem militar. Gervais (2012) argumenta que a heterogeneidade dos sistemas de TI gera desafios ao cálculo da necessidade militar, fato este que limita os ataques cibernéticos, tornando as vantagens militares indeterminadas, uma vez que nem sempre será possível prever todos os efeitos secundários de um ataque. E, como visto anteriormente, são os efeitos de segundo nível que, normalmente, se busca alcançar. Ademais, não se pode esquecer da característica de imprevisibilidade dos efeitos do ataque cibernético, que, por si só, poderá ofuscar uma vantagem militar que justifique as ações.

Contudo, o grande desafio do ataque cibernético é que sua "vantagem militar definida" normalmente é comprovada somente após a realização da ação, fazendo-se necessário primeiro obter o sucesso para, então, considerar a vantagem. Deve-se considerar, também, a busca por efeitos secundários que efetivamente atenderão ao ED do ataque e que, dificilmente, são antecipados. Assim, uma análise anterior à execução do ataque poderá levar a uma conclusão errônea. Por tal motivo, Gervais (2012) sugere a criação de um registro que possibilite armazenar todas as informações disponíveis sobre o alvo, antes do ataque, de modo a viabilizar sua defesa jurídica perante possíveis questionamentos.

O Manual de Tallinn questiona a legitimidade do direito do uso da força como autodefesa em situações de ataque cibernético iminente, em relação ao requisito de imediatismo a partir de um ataque lançado, segundo a regra 73 da Tabela 1, do APÊNDICE A. Apesar de o Artigo 51 da Carta da ONU não prever expressamente uma ação defensiva antecipada por meio de um ataque armado, ele deixa claro que um Estado não precisa esperar ociosamente enquanto o inimigo se prepara para atacar. Com isso, entende-se que o Estado pode se defender, uma vez que seja identificado um ataque armado iminente. No DI, esta ação é conhecida como autodefesa antecipada.

Porém, no contexto do ECiber, os especialistas do Manual de Tallinn foram contrários à autodefesa em situações de ataque cibernético iminente, reconhecendo que ações cibernéticas em legítima defesa são permitidas somente quando um ataque for realmente

15 Sistemas de Comando e Controle: são o conjunto de instalações, equipamentos, sistemas de informação, doutrinas, procedimentos e pessoal, essenciais para a autoridade planejar, dirigir e controlar as ações da sua organização.

lançado, ou seja, a autodefesa antecipada é proibida no ECiber. Eles alegaram que a ação de colocar minas navais em rotas de navegação que passam pelo mar territorial de um Estado-alvo são ações que caracterizam um ataque iminente, porém, são ações distintas de se colocar um *malware* a ser ativado remotamente. Se o indicador de ataque for meramente a capacidade de iniciar um ataque armado no futuro, o critério de iminência não é satisfeito.

Logo, no ECiber, o Estado vítima pode responder em legítima defesa na existência do imediatismo, que se refere ao período após a execução de um ataque cibernético. Assim, o período necessário para se identificar o atacante e o tempo necessário para se preparar uma resposta são altamente relevantes. Os autores do Manual ressaltam que o ataque cibernético armado pode ser iniciado por uma onda de ações cibernéticas contra o Estado vítima e que a autodefesa não poderá ser iniciada antes da conclusão destas ações.

Por fim, tem-se que a avaliação de um ataque cibernético quanto à observância ao princípio da necessidade militar é um exercício que deverá ser realizado caso a caso, conforme apontado por Gervais (2012), de modo análogo aos ataques cinéticos, o que demandará um esforço e trabalho contínuos de inteligência, além de um profundo conhecimento a respeito das relações de interconectividade e interdependência entre os vários sistemas existentes que poderão ser afetados pelo ataque.

As seguintes regras do Manual de Tallinn 2.0 poderão ser aplicadas na MB, para atender ao princípio da necessidade militar: 71, 72, 73, 100, 101, 104, 105 e 119, presentes na Tabela 1, do APÊNDICE A.

5.1.3 Princípio da Proporcionalidade

O princípio da Proporcionalidade tem como objetivo minimizar o sofrimento humano desnecessário, e pressupõe que a utilização dos meios e métodos de guerra deve ser proporcional à vantagem militar concreta e direta. Considera-se que nenhum alvo, mesmo sendo militar, deve ser atacado se os prejuízos e sofrimento decorrentes do ataque forem maiores que os ganhos militares esperados da ação.

Assim como o princípio da Necessidade Militar proíbe o uso excessivo de força contra combatentes, o princípio complementar da Proporcionalidade limita os efeitos de um ataque sobre os não combatentes. Essa limitação é expressa como um teste de equilíbrio, entre a vantagem militar “concreta e direta” prevista e as perdas civis esperadas. Quanto maior for o valor de um alvo em potencial, maior também será o limite de dano colateral tolerado (WINGFIELD, 2009).

Passando para a esfera cibernética, é possível afirmar que o ataque cibernético é uma opção para minimizar o dano colateral, uma vez que, como visto, ao se tratar do princípio da Distinção, os ataques cibernéticos podem diferenciar seus alvos. Dessa forma, eles causarão menos efeitos indesejados e letais que seus correspondentes cinéticos e, adicionalmente, poderão ser reversíveis. Tais características são desejáveis para a aplicação proporcional da força, para que ela não cause um número desproporcional de baixas civis (JASTRAM; QUINTIN, 2011; GERVAIS, 2012).

Ainda assim, por vezes, este princípio é negligenciado. Schmitt (2012) aponta três situações em que o princípio da Proporcionalidade é frequentemente violado: quando não se tem conhecimento completo sobre o que está sendo atacado; quando há inabilidade de moldar com precisão a quantidade de força aplicada no alvo; e quando há inabilidade em realizar um ataque "cirúrgico", ou seja, que atinja precisamente o ponto desejado. Mesmo que tenha como vantagem a possibilidade de hiperdistinção, os ataques cibernéticos ainda são questionáveis, se for levado em consideração que é extremamente difícil de se distinguir um código de programação em um computador que controle a distribuição de energia elétrica, de um sistema de armas; ou, ainda, por exemplo, um sistema de radar de alerta antecipado como alvo legítimo, de um código que controle o fornecimento de energia elétrica de um hospital. É extremamente difícil por razões técnicas, visto que os elétrons não possuem marcações nacionais, que possam garantir a sua origem. Isso se deve ao fato de os idealizadores e criadores da Internet, provavelmente, não terem considerado como necessária tal característica de identificação. Cabe lembrar que a Internet foi criada para fins militares, que se acreditava ser um canal de troca de informações confiáveis, sem a necessidade de se rastrear a origem de uma mensagem. Além disso, a Internet não foi projetada para impedir alterações maliciosas durante a transmissão de seus pacotes. Ressalta-se que, no ECiber, o princípio da Proporcionalidade, assim como o da Distinção, exige maior esforço e detalhamento na coleta e análise do alvo por parte da Inteligência.

O Manual de Tallinn não restringe que a ação em resposta a um ataque armado seja de mesma natureza, conforme a regra 72 da Tabela 1, do APÊNDICE A. Portanto, o uso da força por meio de uma ação cibernética pode ser feito em resposta a um ataque armado cinético e vice-versa. O requisito de proporcionalidade não deve ser interpretado como imposição de ter que responder na mesma moeda. Pode ser que a origem do ataque cibernético armado tenha uma estrutura excelente de defesa, sem vulnerabilidades sujeitas a operações cibernéticas. Nessa situação, nada impedirá o uso de operações cinéticas com

intuito de obrigar o atacante a desistir de suas ações, embora estas operações devam ser dimensionadas para este fim.

A revista Forbes divulgou, no dia 6 de maio de 2019, a notícia do primeiro ataque cinético em resposta a ações cibernéticas. De acordo com a matéria, as Forças de Defesa de Israel (IDF, na sigla em inglês) efetuaram um ataque cinético em resposta a ações cibernéticas do Hamas[16], durante a intensificação do conflito entre Israel e Palestina. Segundo a IDF, o ataque cinético teve como propósito parar um ataque cibernético em andamento, ao realizar o seu ataque aéreo às instalações onde supostamente estariam operando os *hackers* do Hamas, eliminando as capacidades cibernéticas do grupo (O'FLAHERTY, 2019).

As seguintes regras do Manual de Tallinn 2.0 poderão ser aplicadas na MB para atender ao princípio da proporcionalidade: 69, 71, 72, 113, 116, 117 e 119, que constam na Tabela 1, do APÊNDICE A.

5.1.4 Princípio da Humanidade

O princípio da Humanidade proíbe que se provoque sofrimento às pessoas e destruição de propriedades civis, a menos que tais atos sejam necessários para obrigar o inimigo a se render. Ressalta-se, aqui, a proibição de ataques exclusivamente contra civis, o que não impede que ocorram danos colaterais a pessoas e bens, devendo ser tomadas todas as medidas para mitigá-los (BRASIL, 2011).

O ataque cibernético se torna o método preferível ao possibilitar a obtenção do mesmo efeito com menor letalidade e destruição do que o ataque cinético. Como exemplo desse tipo de aplicação, tem-se a neutralização de um sistema de radar a partir de ações cibernéticas, evitando-se mortes desnecessárias em ambos os lados do conflito, sendo considerado um método de guerra mais humano (KOSTADINOV, 2014; JASTRAM; QUINTIN, 2011).

Segundo a avaliação dos especialistas do Manual de Tallinn, dificilmente um meio ou método utilizado na GCiber poderia violar o princípio da humanidade, de acordo com a regra 104 da Tabela 1, do APÊNDICE A. Como exemplo, considere-se um combatente inimigo que tenha um dispositivo de marcapasso, com um desfibrilador embutido, endereçável à Internet. Seria uma ação legitima assumir o controle do marca-passo para matar aquele indivíduo ou torná-lo fora de combate, por exemplo, utilizando a função de desfibrilação para parar o coração. No entanto, seria ilegítimo conduzir a operação de uma

16 Hamas (Movimento da Resistência Islâmica): é um dos grupos mais extremistas na luta contra a existência do Estado de Israel, criado após o fim da Segunda Guerra Mundial para abrigar os judeus.

maneira que almeje apenas causar dor e sofrimento, isto é, não relacionada ao objetivo militar da operação. Como exemplo, seria ilegítimo parar o coração do alvo e, em seguida, fazê-lo reviver várias vezes, antes de finalmente provocar a morte do combatente. Ações como essa levariam a sofrimentos que não servem a nenhum propósito militar (SCHMITT, 2017).

As seguintes regras do Manual de Tallinn 2.0 poderão ser aplicadas na MB para atender ao princípio da humanidade: 94, 95, 99, 104, 105, 106, 107, 111, 113, 115, 117, 119, 121, 131, 132, 133, 135, 137 e 140, presentes na Tabela 1, do APÊNDICE A.

5.1.5 Princípio da Limitação

O princípio da Limitação estabelece que a escolha dos meios para causar danos ao inimigo não é ilimitada, sendo obrigatória a exclusão de meios e métodos que levem ao sofrimento desnecessário e a danos supérfluos (BRASIL, 2011).

Do ponto de vista cibernético, pode-se argumentar que o princípio da Limitação impõe a obrigação de se escolher os meios e métodos menos letais para se alcançar os objetivos militares, sendo que o ataque cibernético poderá, em certas ocasiões, ser essa opção. A fim de se evitar consequências graves que levem a perdas entre a população civil, cuidados especiais devem ser tomados durante ataques cibernéticos contra obras e instalações consideradas de risco, tais como barragens, diques e geradores elétricos e estações nucleares. Também deve haver cuidado com instalações localizadas nas suas proximidades, conforme a regra 140 da Tabela 1, do APÊNDICE A.

Por outro lado, não existem limitações quanto às ações cibernéticas utilizadas como artifícios de guerra para enganar o inimigo. De acordo com o Manual de Tallinn, na regra 123 da Tabela 1, do APÊNDICE A, os estratagemas são permitidos em conflito armados e são atos destinados a enganar o inimigo ou induzir forças inimigas a agirem de forma imprudente, mas que não violem a lei dos conflitos armados. Não se caracterizam como perfídia porque não confundem a confiança ou a influência do inimigo com relação ao status de protegido. Seguem exemplos de artifícios permitidos na GCiber:

a) criação de um sistema de computador fictício que simule forças inexistentes;
b) transmissão de informações falsas que façam com que o oponente, erroneamente, acredite que as operações estão prestes a ocorrer ou em andamento;

c) uso de identificadores de falsos computadores, falsas redes de computadores (por exemplo, *honeynets*[17]) ou falsas transmissões de dados;
d) ordens falsas, que pareçam ter sido emitidas pelo comandante inimigo;
e) atividades de guerra psicológica[18];
f) transmissão de informações falsas de inteligência propositalmente passíveis de serem interceptadas; e
g) uso de códigos, sinais e senhas do inimigo (SCHMITT, 2017).

No entanto, as armas cibernéticas são ferramentas perecíveis, pois, uma vez utilizadas, serão, invariavelmente, ineficazes para um segundo ataque, já que as defesas cibernéticas inimigas estarão robustecidas após conhecer os meios e métodos do ataque desferido, e as vulnerabilidades exploradas serão reparadas. Logo, as armas cibernéticas serão reservadas para aplicações especiais, principalmente aquelas mais distintivas, ou seja, criadas especificamente para um determinado alvo, que explorem determinada vulnerabilidade ou que sejam utilizadas como estratagemas em conflitos armados.

As seguintes regras do Manual de Tallinn 2.0 poderão ser aplicadas na MB para atender ao princípio da limitação: 1, 4, 6, 7, 68, 73, 81,123 e 140, que constam na Tabela 1, do APÊNDICE A.

5.2 Análise das Limitações da GCiber na MB

A missão das FA, em especial a da MB, é, em geral, dissuadir forças hostis de atacarem o seu território ou bens do Estado, buscando neutralizar possíveis ações hostis e inibir as intenções hostis contra o seu território. Porém, apesar de o uso da força estar proibido por uma regra imperativa do DI, a MB deverá estar sempre pronta e capacitada, demonstrando, de maneira clara, a intenção de usar o seu potencial ofensivo sempre que se fizer necessário para garantir a autodefesa individual ou coletiva.

No entanto, questões legais são necessárias à regulação do comportamento humano, a fim de controlar as possíveis consequências diante de uma guerra na qual a arma mais poderosa é a informação. Dessa forma, a MB tem como missão não apenas garantir a proteção de seus próprios sistemas e desenvolver suas capacidades ofensivas, mas primar

17 Honeynet: é uma ferramenta de pesquisa, que consiste de uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes.

18 Guerra psicológica: é o uso tático e planejado de propaganda, ameaças e outras técnicas não-combatentes. É realizada durante diversos conflitos.

pelas melhores diretrizes de atuação cibernética, buscando respeitar as Leis e Doutrinas que amparem o seu emprego no ambiente operacional.

Com isso, os responsáveis pelo planejamento de operações navais devem estar aptos a identificar os direitos, obrigações legais e responsabilidades por quaisquer infrações graves aos costumes e às normas do DICA.

Os documentos que atualmente regem a GCiber nas FA, em especial na MB, conforme citados nos itens 4.1 e 4.2, pouco referenciam ou contextualizam as ações cibernéticas ofensivas, mesmo considerando o seu emprego secundário perante as ações cinéticas na Guerra Convencional.

A partir da contextualização dos princípios do DICA em relação à GCiber apresentada neste capítulo, com base nas regras do Manual de Tallinn, percebe-se que as ações ofensivas não devem levar em conta somente a vantagem militar almejada sobre o oponente. Outros aspectos devem ser considerados, tais como:

a) a legitimidade e a distinção de alvos combatentes e não combatentes civis, de acordo com a regra 111 da Tabela 1, do APÊNDICE A;

b) a necessidade de resposta com base no imediatismo, ou seja, após o período necessário para identificar o atacante e o tempo necessário para preparar uma resposta, conforme a regra 73 da Tabela 1, do APÊNDICE A;

c) a natureza do ataque recebido e a capacidade de defesa do atacante, conforme a regra 72 da Tabela 1, do APÊNDICE A;

d) evitar meios e métodos que provoquem o sofrimento desnecessário, conforme a regra 104 da Tabela 1, do APÊNDICE A; e

e) evitar as consequências graves que levam a perdas entre a população civil, conforme a regra 140 da Tabela 1, do APÊNDICE A.

Além disso, as ações ofensivas devem ser passíveis de controle e auditoria, para que, caso exista a necessidade, sejam verificadas as responsabilidades das ações que infrinjam os princípios do DICA, conforme as regras 84 e 85 da Tabela 1, do APÊNDICE A. Como observação final sobre os princípios, é essencial que toda e qualquer alteração nas operações cibernéticas que impliquem em utilizar novas técnicas e procedimentos de ataque seja avaliada em relação aos princípios do DICA.

Cabe ressaltar, ainda, que a GCiber se difere da Guerra Convencional em alguns aspectos do DI, como, por exemplo, destaca-se o direito à autodefesa antecipada, garantida pela Carta da ONU. De acordo com o Manual de Tallinn, regra 73 da Tabela 1, do APÊNDICE A, no contexto do ECiber, as ações cibernéticas em legítima defesa são

permitidas somente quando um ataque realmente tenha sido lançado, ou seja, a autodefesa antecipada é proibida no ECiber.

6 CONCLUSÃO

A GCiber é uma realidade e o sucesso das operações militares está se tornando cada vez mais dependente da capacidade das Forças relacionada às ações operativas no ECiber. Além disso, a capacidade ofensiva na GCiber de um Estado-Nação se torna atrativa por ser mais um fator gerador de poder em relação aos demais Estados, contribuindo para garantir a capacidade de dissuasão, enfrentamento e neutralização das ameaças cibernéticas ou cinéticas, preservando assim a sua soberania. No entanto, o ED na GCiber não deve somente objetivar comprometer a integridade dos sistemas de TIC do oponente, mas também considerar a preservação de vidas humanas, com fulcro no DIH.

A esse respeito, o presente trabalho apresentou o fundamento doutrinário utilizado pela MB, abordando os Acordos Internacionais, as Leis, as Doutrinas e as Normas que regulamentam o papel das FA, em especial o da MB. A partir dessa base doutrinária, foram contextualizados para a GCiber os princípios e as características da Guerra Convencional, bem como as principais regras aplicadas às operações ofensivas em um conflito armado à luz do DI presentes em outros trabalhos reconhecidos e, em especial, no Manual de Tallinn. Utilizou-se a premissa de que o DICA, por ser um acordo internacional ratificado pelo Brasil, tem precedência sobre qualquer doutrina de emprego das FA, cabendo, assim, uma adequação desta última em relação à primeira.

Concluiu-se que os limites impostos às ações cibernéticas na MB não estão claros o suficiente no fundamento doutrinário avaliado neste trabalho, devendo ser revistos e ampliados por meio da inclusão de conceitos norteadores, a fim de garantir a legitimidade das ações perante o DICA. Essa adequação seria de grande importância para a orientação das futuras publicações atinentes às operações cibernéticas, uma vez que, dentro da hierarquia de publicações estabelecida pelo MD e Estado-Maior da Armada, as do nível de doutrina militar precedem as normas e diretrizes de emprego operacional e tático, devendo a primeira orientar a elaboração das demais.

Sugere-se, ainda, que as Doutrinas, as Normas e demais documentos que rejam as ações ofensivas da GCiber, a serem atualizados e elaborados pelo MD e FA, em especial pela MB, adotem as regras e limitações apresentadas pelo Manual de Tallinn quanto à soberania, à legitimidade do uso da força, à aplicabilidade do DICA, à responsabilidade criminal, à

distinção de pessoal combatente e não combatente e aos princípios da necessidade e proporcionalidade, de forma que não infrinjam os tratados e atos internacionais assinados pelo Brasil.

Em suma, o principal desafio a ser enfrentado pelos combatentes cibernéticos[19] será o de assegurar a correta seleção de alvos no campo de batalha, além de mensurar os danos causados pelas operações e conciliar suas ações às limitações impostas pelos princípios do DICA; evitando-se, dessa forma, que o Estado incorra no descumprimento de Convenções e Protocolos internacionais, e zelando pelo efetivo cumprimento dos mesmos pelas demais partes vinculadas. Ao vencer esse desafio, será, então, possível avaliar os efeitos e planejar de forma adequada e eficiente as ações militares no ambiente cibernético, permitindo a inclusão dessa importante capacidade nas operações militares.

19 Combatente cibernético: é o indivíduo que tem legitimidade para participar diretamente das hostilidades em situações de conflito armado, representando seu Estado.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil,** 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 26 jan. 2021.

BRASIL. **Decreto Presidencial Nº 10.222,** de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, 2020a. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 14 jun. 2021.

BRASIL. **Decreto Presidencial Nº 10.569,** de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de infraestruturas Críticas. Brasília, 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 14 jun. 2021.

BRASIL. **Decreto Presidencial Nº 7.276,** de 25 de agosto de 2010. Estrutura Militar de Defesa. Brasília, 2010. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/decreto/d7276.htm. Acesso em: 14 jun. 2021.

BRASIL. **Decreto Presidencial Nº 9.637,** de 26 de dezembro de 2018. Institui a Política de Segurança da Informação, dispõe sobre a governança da segurança da informação. Brasília, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 14 jun. 2021.

BRASIL. Estado-Maior da Armada. **EMA-135:** manual de direito internacional aplicado às operações navais. Brasília, DF, 2017a.

BRASIL. Estado-Maior da Armada. **EMA-305:** doutrina militar naval. Brasília, DF, 2017b.

BRASIL. Estado-Maior da Armada. **EMA-416:** doutrina de tecnologia da informação da Marinha — manual de guerra cibernética. Brasília, DF, 2013. v. 2.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Decreto Nº 10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF, 2020c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 7 abr. 2021.

BRASIL. **Lei Complementar Nº 97,** de 9 de junho de 1999. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Brasília, 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm. Acesso em: 14 jun. 2021.

BRASIL. Marinha do Brasil. **Plano Estratégico da Marinha (PEM 2040)**. Marinha do Brasil. Estado-Maior da Armada, Brasília, DF, 2020d. Disponível em: https://www.marinha.mil.br/sites/all/modules/pem_2040/book.html,p.75. Acesso em: 3 mar. 2021.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. Chefia de Preparo e Emprego. **MD34-M-03:** manual de emprego do direito internacional dos conflitos

armados (DICA) nas Forças Armadas. Brasília, DF: Ministério da Defesa, 2011. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/publicacoes/md34a_ma_03a_dicaa_1aed2011.pdf/view. Acesso em: 24 jan. 2021.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD31-M-07:** doutrina militar de defesa cibernética. Brasília, DF: Ministério da Defesa, 2014. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_07a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 24 jan. 2021.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. 2012a. Disponível em: http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf. Acesso em: 11 fev. 20.

BRASIL. Ministério da Defesa. **Minutas do Livro Branco, da PND e da END estão disponíveis para leitura**. 2018b. Disponível em: http://www.defesa.gov.br/noticias/29093-minutas-do-livro-branco-da-pnd-e-da-end-estao-disponiveis-para-leitura. Acesso em: 17 jun. 2018.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END)**. Brasília, DF: Ministério da Defesa, 2012b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/estrategia-nacional-de-defesa. Acesso em: 24 jan. 2021.

BRASIL. **Portaria Nº 3.781,** de 17 de novembro de 2020. Cria o Sistema de Defesa Cibernética (SMDC). Brasília, 2020f. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860. Acesso em: 14 jun. 2021.

BRASIL. Presidência da República. **Decreto Nº 5.484,** de 30 de junho de 2005. Política de Defesa Nacional. Brasília, DF, 2005. Diário Oficial da República Federativa do Brasil, Brasília, DF, 31 jul. 2005. Disponível em: http://www.planalto.gov.br/ccivil_03 /_ato2004-2006/2005/decreto/d5484.htm. Acesso em: 14 jan. 2021.

BRASIL. Presidência da República. **Decreto Nº 6.703,** de 18 de dezembro de 2008. Estratégia Nacional de Defesa. Brasília, DF, 2008. Diário Oficial da República Federativa do Brasil, Brasília, DF, 19 dez. 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 14 jan. 2021.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra cibernética:** a próxima ameaça à segurança e o que fazer a respeito. Brasport, 2015.

CORDEIRO, Luís Eduardo. Análise da doutrina militar de defesa cibernética à luz do DIH/DICA. In: **IX Encontro Nacional da Associação Brasileira de Estudos de Defesa.** 2016. Florianópolis. Anais... Florianópolis, 2016.

DAVIS, Paul K. **Deterrence, influence, cyber attack, and cyberwar**. EUA: RAND National Security Research Division, June, 2014. 26 p. Disponível em: https://www.rand.org/pubs/external_publications/EP50950.html. Acesso em: 27 dezembro 2020.

G1. Hackers acessaram redes de órgão responsável por arsenal nuclear dos EUA. Mundo. G1 — **Globo.com.** Publicado em: 17/dez./2020. Disponível em: https://g1.globo.com/mundo/

noticia/2020/12/17/hackers-acessaram-redes-de-orgao-responsavel-por-arsenal-nuclear-dos-eua-diz-site.ghtml. Acesso em: 17 dez. 2020.

GERVAIS, Michael. Cyber attacks and the laws of war. **Berkeley Journal of International Law,** EUA, v. 30, n. 2, p. 525-579, 2012. Disponível em: https://www.semanticscholar.org/paper/Cyber-Attacks-and-the-Laws-of-War-Gervais/0c1075dc3623a88fc75a9a9b1a6ce795b28d23c9. Acesso em: 10 janeiro 2021.

GILL Terry D.; DUCHEINE, Paul A. L. **Anticipatory self-defense in the cyber context. International Law Studies**, EUA, v. 89, p. 438-471, 2013. Disponível em: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1037&context=ils. Acesso em: 1 jan. 2021.

HOBBES, Thomas. **Leviatã ou a matéria, forma e poder de um estado eclesiástico e civil**. 4. ed. São Paulo: Nova Cultural, 1988.

IISS. **The Military Balance 2020**. 14 de fev. de 2020. International Institute for Strategic Studies. Disponível em: https://www.iiss.org/press/2020/military-balance-2020. Acesso em: 4 mar. 2021.

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/wp-content/uploads/2015/04/cyberwarfare-seminar-summary-complete.pdf. Acesso em: 1 jan. 2021.

KOSTADINOV, Dimitar. **Jus in cyber bello:** how the law of armed conflict regulates cyber attacks. EUA, 10 Apr. 2014. Disponível em: https://resources.infosecinstitute.com/topic/jus-cyber-bello-law-armed-conflict-regulates-cyber-attacks-part/. Acesso em: 1 jan. 2021.

LEWIS, James A. In defense of Stuxnet. **Military and Strategic Affairs,** v. 4, n. 3, p. 65-76, 2012.

MCGUIRE, Michel. **Nation States, Cyberconflict and the Web of Profit**. [S.l.]: HP Development Company, 2021. Disponível em: https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf. Acesso em: 16 abr. 2011.

NUNES, Luiz Artur Rodrigues. **Guerra cibernética:** está a MB preparada para enfrentá-la? 2010. 108 f. Monografia (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: 1 jan. 2021.

O'Flaherty, Kate. Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First. **Forbes** — Forbes.com. Publicado em: 6/mai./2019. Disponível em: https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/?sh=8c03e06f8953. Acesso em: 2 jun. 2021.

SCHMITT, Michael N. Wired warfare: computer network attack and jus in bello. **International Review of the Red Cross,** Suíça, v. 84, n. 846, p. 365-399, June, 2012. Disponível em: https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf. Acesso em: 2 jan. 2021.

SCHMITT, Michael N. **Tallinn manual 2.0 on the international law applicable to cyber operations**. Cambridge University Press, 2017.

WINGFIELD, Thomas C. International law and information operations. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. **Cyberpower and national security.** 1. ed. Dulles, EUA: National Defense University Press and Potomac Books, 2009. cap. 22, p. 525-542.

APÊNDICE A — Principais regras do Manual de Tallinn que abrangem as ações ofensivas da GCiber em conflitos armados

Regra	**Descrição da Regra**	**Legislação ou Análise dos Especialistas**
Regra 1 — Soberania (princípio geral)	Devido as ações cibernéticas ocorrerem dentro de um território, envolvendo objetos e sendo conduzidas por pessoas ou entidades, sobre as quais o Estado exerce suas prerrogativas soberanas, o princípio da soberania de um Estado também se aplica ao ECiber.	Os especialistas observaram que, embora as atividades cibernéticas possam transcender fronteiras ou ocorrer em águas nacionais, espaço aéreo internacional ou espaço sideral, todas são conduzidas por pessoas físicas ou jurídicas sujeitas à jurisdição de um ou mais Estados.
Regra 4 — Violação de soberania	Um Estado não deve realizar operações cibernéticas que violem a soberania de outro Estado.	As exceções à violação desta regra ocorrerão nos casos de legítima defesa (autodefesa) individual ou coletiva ou quando autorizadas pelo Conselho de Segurança da Organização das Nações Unidas (ONU).
Regra 6 — Devida diligência (princípio geral)	Um Estado deve exercer a devida diligência em não permitir que em seu território, ou na infraestrutura cibernética sob seu controle governamental, sejam realizadas ações cibernéticas que afetem os direitos ou produzam consequências graves e adversas a outros Estados.	Considere que um hacker ou entidade localizada no Estado A realize uma ação cibernética destrutiva contra o Estado B utilizando a infraestrutura cibernética localizada no Estado C. Se o Estado C estiver ciente e não tomar medidas cabíveis para pôr fim à ação, fica caracterizada uma violação do princípio de devida diligência.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 7 — Conformidade com o princípio de devida diligência	Conforme a Regra 6, caberá ao Estado parar as ações em seu território, mas, caso o Estado não tenha a capacidade de responder efetivamente a ações cibernéticas altamente complexas e dinâmicas envolvendo infraestrutura cibernética em seu território, o mesmo deverá contratar uma empresa privada para realizar esta tarefa.	Como um exemplo, um Estado poderia aprovar em sua legislação a exigência de que, em situações que identifiquem tráfego com assinaturas de comando e controle que caracterizem botnet e servidores configurados para estes fins em seu território, os provedores de Internet derrubem estas conexões.
Regra 19 — Circunstâncias que impedem a ilicitude das operações cibernéticas	O Tribunal Internacional de Justiça diz que a proibição do uso da força e legítima defesa, respectivamente, aplicam-se a qualquer uso da força, independentemente das armas empregadas.	Artigos 2 e 51 (Regra 71-5) da Carta das Nações Unidas. Os especialistas deste manual concordaram por unanimidade que o mero fato de que um computador (em vez de uma arma mais tradicional, sistema de arma, ou plataforma) possa ser utilizado durante uma ação ofensiva equivale a um “uso de força”.
Regra 68 — Proibição de ameaça ou uso de força	Uma operação cibernética que constitua uma ameaça ou uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou que esteja em desacordo com os propósitos da Carta das Nações Unidas, é ilegal.	Existem duas exceções amplamente reconhecidas à proibição de uso da força: uso da força autorizado pelo Conselho de Segurança, sob o Capítulo VII; e legítima defesa, nos termos do Artigo 51 da Carta.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 69 — Definição de uso da força	Uma operação cibernética constitui um uso de força quando sua escala e efeitos são comparáveis a operações não cibernéticas, chegando ao nível de uso de força.	Devido a Carta das Nações Unidas não oferecer nenhum critério para determinar quando um ato equivale ao uso da força, os especialistas consideraram a sentença de Nicarágua, que considera "escala e efeitos" para determinar se ações específicas equivalem a um "ataque armado" contra a paz e a segurança internacional.
Regra 71 — Autodefesa contra ataque armado	Um Estado que seja o alvo de uma ação cibernética que suba ao nível de um ataque armado pode exercer seu direito inerente de autodefesa. Se uma operação cibernética constitui um ataque armado, isto depende de sua escala e efeitos.	Os especialistas concordaram que uma operação cibernética que fira gravemente ou que mate uma série de pessoas ou, ainda, que cause danos significativos ou destruição de propriedade, esta operação satisfaria o requisito de escala e efeitos, conforme a Regra 69. Os especialistas consideraram que a intenção é irrelevante em qualificar uma ação como um ataque armado e que somente a escala e os efeitos são importantes. No entanto, qualquer resposta a isto teria que atender aos critérios de necessidade e proporcionalidade descritos na próxima regra (72).

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 72 — Necessidade e proporcionalidade	O uso de força envolvendo operações cibernéticas realizadas por um Estado e no exercício do seu direito de legítima defesa deve ser necessário e proporcional. Ações cibernéticas em legítima defesa devem atender a dois critérios: necessidade e proporcionalidade.	A necessidade requer que o uso da força, incluindo as ações cibernéticas que sejam equivalentes ao uso da força (Regra 69), seja necessário para impedir o sucesso de um ataque armado iminente ou que já esteja em andamento. Quanto à proporcionalidade, o critério será a escala, o escopo, a duração e a intensidade da ação necessária para inibir a situação que deu origem ao direito de legítima defesa. Além disso, não é necessário que a ação defensiva seja de mesma natureza da que constituiu o ataque armado. Logo, o uso da força por meio de uma ação cibernética pode ser utilizado em resposta a um ataque armado cinético e vice-versa.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 73 — Iminência e imediatismo	O direito do uso da força em autodefesa surge em situações em que ocorra um ataque cibernético armado iminente e ainda está sujeito a um requisito de imediatismo. Apesar de o Artigo 51 não prever expressamente uma ação defensiva antecipada de um ataque armado, um Estado não precisa esperar ociosamente enquanto o inimigo se prepara para atacar.	O Estado pode se defender, uma vez que seja identificado um ataque armado iminente. Esta ação é conhecida como autodefesa antecipada no DI. Porém, no contexto do ECiber, os especialistas foram contrários, reconhecendo que ações cibernéticas em legítima defesa são permitidas somente quando um ataque tenha sido realmente lançado, ou seja, a autodefesa antecipada é proibida no ECiber. Os especialistas ressaltam, ainda, que o ataque cibernético armado pode ser iniciado com uma onda de ações cibernéticas contra o Estado vítima e que a autodefesa não poderá ser iniciada antes da conclusão destas ações.
Regra 75 — Comunicar as medidas de autodefesa	As medidas envolvendo ações cibernéticas realizadas pelos Estados no exercício do direito de legítima defesa devem ser imediatamente comunicadas ao Conselho de Segurança das Nações Unidas.	Artigo 51 da Carta das Nações Unidas.
Regra 76 — Conselho de Segurança das Nações Unidas	O Conselho de Segurança das Nações Unidas deve determinar se uma ação cibernética constitui uma ameaça à paz, violação da paz ou ato de agressão, podendo autorizar medidas não contundentes, inclusive ações cibernéticas que se caracterizem como uso da força, em resposta.	Artigo 51 da Carta das Nações Unidas.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 80 — Aplicabilidade da lei de conflito armado	Ações cibernéticas executas no contexto de um conflito armado estão sujeitas à lei do conflito armado. Apesar da ausência de regras específicas quanto às ações cibernéticas dentro da lei do conflito armado.	Os especialistas ressaltam que a lei do conflito armado não abrange atividades particulares de indivíduos ou entidades não relacionados com o conflito armado. Como exemplo, citam a aplicação da lei do conflito armado nas ações cibernéticas que ocorreram durante o conflito internacional entre Geórgia e Rússia, em 2008, e também nas que aconteceram no conflito entre a Ucrânia e a Rússia, uma vez que estas ações foram empreendidas na promoção destes conflitos.
Regra 81 — Limitações geográficas	As ações cibernéticas estão sujeitas a limitações geográficas impostas por leis do DI aplicáveis durante um conflito armado. As ações cibernéticas podem ser conduzidas a partir de, ou causar efeitos em, todos os territórios que fazem parte do conflito, águas internacionais ou espaço aéreo e, estão sujeitas a certas limitações, como o espaço sideral. Porém, geralmente, as ações cibernéticas são proibidas em outros lugares, em particular, destacam-se os territórios neutros.	Em relação à lei da neutralidade, as ações cibernéticas, ao trafegarem por territórios neutros, podem causar efeitos tendenciosos e equivocados quanto à sua condição. No entanto, os especialistas, ao utilizarem como exemplo um ataque que faça uso de serviço de nuvem — em que dados usados para processar o ataque de um Estado podem ser replicados entre servidores em vários outros estados, incluindo Estados neutros — enfatizam que deve se observar onde o ataque é iniciado e onde é concluído. Logo, não proíbem o tráfego de dados por áreas onde as ações cibernéticas sejam proibidas durante um conflito armado, como nos territórios neutros.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 82 — Caracterização como conflito armado internacional	Existe um conflito armado internacional entre dois ou mais estados sempre que há hostilidades, podendo ser incluídas como fator gerador as ações cibernéticas.	
Regra 84 — Responsabilidade criminal individual por crimes de guerra	As operações cibernéticas podem representar crimes de guerra e, portanto, dar origem à responsabilidade penal individual, à luz do Direito Internacional. Esta regra se aplica a membros das Forças Armadas e civis envolvidos em ações cibernéticas associadas ao conflito armado.	Artigos 86 e 87 do Protocolo Adicional I da Convenção de Genebra.
Regra 85 — Responsabilidade penal de comandantes e superiores	Os Comandantes e outros superiores são criminalmente responsáveis por ordenar operações cibernéticas que constituam crimes de guerra. Os comandantes também são criminalmente responsáveis se souberem ou se, devido às circunstâncias da época, deveriam ter conhecimento de que seus subordinados estavam cometendo, estavam prestes a cometer, ou que tinham cometido crimes de guerra e falharam em tomar todas as medidas razoáveis e disponíveis capazes de prevenir o seu cometimento ou punir os responsáveis.	Artigo 49 da I Convenção de Genebra, Artigo 50 da II Convenção de Genebra, Artigo 129 da III Convenção de Genebra, Artigo 146 da IV Convenção de Genebra, Artigos 86 e 87 do Protocolo Adicional I e Artigo 25 do Estatuto de Roma.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 92 — Definição de ataque cibernético	Um ataque cibernético é uma ação cibernética, seja ofensiva ou defensiva, que cause ferimentos ou morte a pessoas, danos ou destruição de objetos.	Os especialistas ressaltam que as ações cibernéticas podem ser parte integrante de uma operação que constitua um ataque. Como exemplo, uma operação cibernética pode ser utilizada para desabilitar as defesas de um alvo que esteja sendo atacado cineticamente, como no caso de desabilitar a capacidade do alvo de empregar contramedidas eletrônicas que impeçam uma arma de identificá-lo como alvo. Neste caso, a ação cibernética é um componente de uma operação que se qualifica como um ataque, assim como o uso de bombas em ataques. A lei do conflito armado se aplica totalmente a tais operações.
Regra 93 — Distinção	O princípio da distinção se aplica a ataques cibernéticos. Com intuito de garantir o respeito e a proteção da população civil e objetos civis, as partes do conflito devem sempre distinguir entre a população civil e combatentes e entre objetos civis e objetivos militares e, portanto, devem dirigir suas ações somente contra pessoas ou alvos militares.	Artigo 48 do Protocolo Adicional I da Convenção de Genebra.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 94 — Proibição de atacar civis	A população civil não deve ser objeto de ataque cibernético.	Esta regra é baseada no princípio da distinção, conforme o Artigo 51 do Protocolo Adicional I e o Artigo 13 do Protocolo Adicional II da Convenção de Genebra.
Regra 95 — Dúvida quanto ao status das pessoas	Em caso de dúvida se uma pessoa é civil, esta pessoa deve ser considerada um civil.	Artigo 5 da III Convenção de Genebra e Artigo 45 do Protocolo Adicional I da Convenção de Genebra.
Regra 96 — Pessoas como objetivos de ataque	As seguintes pessoas podem ser objetivos de ataques cibernéticos: membros das Forças Armadas; membros de grupos armados organizados; civis, se e durante o tempo em que tomarem parte direta no conflito; e organização internacional participante de um conflito armado.	Artigos 43 e 44 do Protocolo Adicional I da Convenção de Genebra.
Regra 99 — Proibição de atacar objetivos civis	Os objetivos civis não devem ser objeto de ataques cibernéticos. Uma infraestrutura cibernética só pode ser objetivo de ataque se for qualificada como objetivo militar.	Artigos 57 e 58 do Protocolo Adicional I da Convenção de Genebra.
Regra 100 — Objetivos civis e objetivos militares	Objetivos civis são todos os objetivos que não sejam objetivos militares. Objetivos militares são aqueles que, por sua natureza, localização, propósito ou finalidade, contribuem efetivamente para a ação militar, e cuja destruição total ou parcial, captura ou neutralização, nas circunstâncias prevalecentes no momento, ofereçam ou definam uma vantagem militar.	Os especialistas consideram que a infraestrutura cibernética pode ser considerada um objetivo militar.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 101 — Objetivos usados para fins civis e militares	A infraestrutura cibernética usada para fins civis e militares é um objetivo militar. Considere uma rede que esteja sendo usada para fins militares e civis. Dificilmente será possível distinguir qual parte da rede de transmissão está sendo utilizada para fins militares. Nestes casos, toda a rede se qualifica como um objetivo militar.	A analogia é feita com uma rede rodoviária utilizada por veículos militares e civis. Embora um invasor possa não saber com certeza quais estradas serão percorridas por forças militares inimigas (ou qual estrada será tomada ou se estará bloqueada), desde que seja razoavelmente provável que uma estrada possa ser utilizada, esta será um objetivo militar sujeito a ataque. Logo, não há razão para tratar as redes de computadores de maneira diferente.
Regra 104 — Lesões supérfluas ou sofrimento desnecessário	É proibido empregar meios ou métodos de GCiber que sejam de natureza a causar lesões ou sofrimentos desnecessários.	Artigo 35 do Protocolo Adicional I da Convenção de Genebra.
Regra 105 — Meios ou métodos indiscriminados	É proibido empregar meios ou métodos de GCiber que sejam, por natureza, indiscriminados.	Meios ou métodos de GCiber são indiscriminados por natureza quando não podem ser: dirigidos a um objetivo militar específico ou limitados em seus efeitos, conforme exigido pela lei do conflito armado, e que, consequentemente, atinjam objetivos militares e civis ou objetos civis sem distinção.
Regra 106 — Armadilhas cibernéticas	É proibido o uso de armadilhas cibernéticas associadas a certos objetivos especificados na lei do conflito armado.	Como exemplo, ilustram um ataque de phishing em que um malware é inserido no e-mail a ser aberto por um funcionário de uma estação de tratamento de água. A execução deste malware poderá comprometer o funcionamento da estação, atingindo usuários civis e militares.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 107 — Inanição	A fome de civis como método de GCiber é proibida.	Considere um caso em que sejam lançadas ações cibernéticas com o propósito exclusivo de interromper o transporte de alimentos para centros populacionais civis e instalações de processamento e armazenamento de alimentos, fazendo com que os estoques de alimentos para civis estraguem. Artigos 54 e 55 do Protocolo Adicional I da Convenção de Genebra.
Regra 111 — Ataques indiscriminados	Ataques cibernéticos que não sejam direcionados a um alvo legal e que, consequentemente, atinjam objetivos civis ou objetivos civis sem distinção, são proibidos.	Consideraram como exemplo um ataque cibernético que insira um script malicioso em um arquivo colocado em um site público. Quando o navegador de um computador vulnerável processa este arquivo, o script é executado e o computador é danificado.
Regra 113 — Proporcionalidade	Um ataque cibernético que possa causar a perda acidental da vida de civis, ferimentos a civis, danos a objetivos civis ou uma combinação destes, ou que fosse excessivo em relação à vantagem militar, é proibido.	Artigos 51 e 57 do Protocolo Adicional I da Convenção de Genebra.
Regra 115 — Verificação de alvos	Aqueles que planejam ou decidem sobre a realização de um ataque cibernético devem verificar se os objetivos a serem atacados não são civis e nem objetivos que estejam sujeitos a proteção especial.	Artigos 53, 56, 59, 60 e 61-67, Anexo I, Cap. V e VI do Protocolo Adicional I da Convenção de Genebra.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 116 — Escolha de meios ou métodos	Aqueles que planejam ou decidem sobre um ataque cibernético devem tomar todas as medidas e precauções na escolha dos meios ou métodos de guerra empregados no ataque, com o objetivo de evitar, ou pelo menos minimizar, ferimentos acidentais a civis, perda de vidas civis e danos ou destruição de objetivos civis.	Artigo 51 do Protocolo Adicional I da Convenção de Genebra.
Regra 117 — Precauções quanto à proporcionalidade	Aqueles que planejam ou decidem sobre os ataques devem se abster de decidir sobre a execução de qualquer ataque cibernético que possa causar perdas acidentais de vida civil, ferimentos a civis, danos a objetivos civis, ou uma combinação dos mesmos, o que seria excessivo em relação à vantagem militar adquirida.	Artigos 51 e 57 do Protocolo Adicional I da Convenção de Genebra.
Regra 119 — Cancelamento ou suspensão do ataque	Aqueles que planejam, aprovam ou executam um ataque cibernético devem cancelar ou suspender o ataque se ficar aparente que o objetivo não é militar ou que está sujeito a proteção especial ou que se possa esperar que o ataque cause, direta ou indiretamente, a perda de civis, ferimentos a civis, danos a objetivos civis, ou uma combinação dos mesmos, o que seria excessivo em relação à vantagem militar adquirida.	Artigos 51 e 57 do Protocolo Adicional I da Convenção de Genebra.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 121 — Precauções contra os efeitos de ataques cibernéticos	As partes de um conflito armado devem, na medida do possível, tomar as precauções necessárias para proteger a população civil, indivíduos civis e objetos civis sob o seu controle, contra os perigos resultantes de ataques cibernéticos.	Artigo 51 do Protocolo Adicional I da Convenção de Genebra.
Regra 123 — Estratagemas	Operações cibernéticas que se qualifiquem como artifícios de guerra são permitidas. Os estratagemas são permitidos em conflitos armados internacionais e não internacionais. São atos destinados a enganar o inimigo ou a induzir forças inimigas a agirem de forma imprudente, mas que não violem a lei dos conflitos armados. Não se caracterizam como perfídia porque não confundem a confiança ou a influência do inimigo com relação ao status protegido.	Esta regra é extraída do Artigo 37 do Protocolo Adicional. Seguem exemplos de artifícios permitidos: criação de um sistema de computador fictício que simule forças inexistentes; transmissão de informações falsas que façam com que o oponente, erroneamente, acredite que as operações estão prestes a ocorrer ou em andamento; uso de identificadores de falsos computadores, redes de computadores (por exemplo, honeynets ou honeypots) ou transmissões de computador; ordens falsas, que pareçam ter sido emitidas pelo comandante inimigo; atividades de guerra psicológica; transmissão de informações falsas de inteligência propositalmente passíveis de serem interceptadas; e uso de códigos, sinais e senhas do inimigo.
Regra 124 — Uso impróprio dos indicadores de proteção	É proibido o uso indevido dos emblemas de proteção, sinais que são estabelecidos na lei de conflitos armados.	Artigo 38 do Protocolo Adicional I da Convenção de Genebra, Artigos 1 e 2 do Protocolo Adicional III da Convenção de Genebra.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 125 — Uso impróprio do emblema das Nações Unidas	É proibido fazer uso do emblema distintivo das Nações Unidas em operações cibernéticas, exceto se autorizado por essa organização.	Artigo 39 do Protocolo Adicional I da Convenção de Genebra.
Regra 126 — Uso impróprio de indicadores do inimigo	É proibido fazer uso das bandeiras, emblemas militares, insígnias, ou uniformes do inimigo enquanto visíveis para o inimigo durante um ataque, incluindo um ataque cibernético.	Artigo 39 do Protocolo Adicional I da Convenção de Genebra.
Regra 127 — Uso impróprio de indicadores neutros	Nas operações virtuais, é proibido fazer uso de bandeiras, emblemas, insígnias ou uniformes de Estados neutros ou de outros Estados não partes do conflito.	Artigo 39 do Protocolo Adicional I da Convenção de Genebra.
Regra 131 — Pessoal médico e religioso, unidades de transporte médico	Pessoal médico e religioso, unidades médicas de transportes devem ser respeitados e protegidos e, em particular, não podem ser objeto de ataque cibernético.	Artigos 24-27 da I Convenção de Genebra, Artigos 36 e 37 da II Convenção de Genebra, Artigo 8 do Protocolo Adicional I e Artigo 9 do Protocolo ll.
Regra 132 — Computadores médicos, redes de computadores e dados	Computadores, redes de computadores e dados que façam parte das operações ou da administração de unidades médicas e de transportes devem ser respeitados e protegidos, e, em particular, não podem ser feitos de objetivo de ataque.	Artigos 33 e 34 da I Convenção de Genebra, Artigos 28 e 38 da II Convenção de Genebra.
Regra 133 — Identificação	Todas as medidas possíveis devem ser tomadas para garantir que os computadores, redes de computadores e dados que façam parte das operações ou da administração de unidades médicas e de transportes sejam claramente identificados.	Artigos 33 e 34 da I Convenção de Genebra, Artigos 28 e 38 da II Convenção de Genebra.

Regra	Descrição da Regra	Legislação ou Análise dos Especialistas
Regra 135 — Proteção de pessoas detidas	Prisioneiros de guerra, pessoas protegidas internadas e outros detidos devem ser protegidos dos efeitos prejudiciais das operações cibernéticas.	Artigo 12 da I Convenção de Genebra, Artigo 12 da II Convenção de Genebra, Artigo 10 do Protocolo Adicional I e Artigo 7 do Protocolo ll.
Regra 137 — Participação forçada em atividades militares	Prisioneiros de guerra e pessoas protegidas internadas não devem ser estimulados a participar ou apoiar ações cibernéticas dirigidas contra seu próprio país.	Artigos 49-54 da III Convenção de Genebra,
Regra 140 — Dever de cuidar durante ataques a barragens, diques, armas nucleares e estações geradoras de eletricidade	A fim de se evitar consequências graves que levam a perdas entre a população civil, cuidados especiais devem ser tomados durante ataques cibernéticos contra obras e instalações de risco, tais como barragens, diques e geradores elétricos e estações nucleares; bem como instalações localizadas nas suas proximidades também devem ficar sob atenção.	

Tabela 1 — Adaptado do Manual de Tallinn 2.0: principais regras que abrangem as ações ofensivas da GCiber em conflitos armados — Vide Referência.

APÊNDICE B — Legislação de Defesa e Segurança Cibernética

Documentos Oficias	**Órgão**	**Data**	**Contextualização**
Constituição Federal	Presidência da República	5 de outubro de 1988	Define o papel fundamental das FA na garantia da soberania nacional nos casos de ameaça estrangeira (defesa da Pátria), da segurança da República, dos seus cidadãos e da ordem constitucional vigente.
Lei Complementar Nº 97	Presidência da República	9 de junho de 1999	Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas.
Decreto Nº 5.484	Presidência da República	30 de junho de 2005	Aprova a Política Nacional de Defesa (PND).
Doutrina de Tecnologia da Informação da Marinha — EMA 416, Volume II (Manual de Guerra Cibernética)	Estado-Maior da Armada — Marinha do Brasil	18 de dezembro de 2007	Apresenta os preceitos doutrinários e as orientações relacionadas à GCiber no âmbito da Marinha do Brasil (MB), além de estabelecer as ações a serem empregadas pela MB na condução da GCiber, complementando, doutrinariamente, as ações adotadas e estabelecidas para a Segurança da Informação.
Decreto Nº 6.703	Presidência da República	18 de dezembro de 2008	Aprova a Estratégia Nacional de Defesa (END).
Livro Branco de Defesa Nacional (LBDN)	Presidência da República	2012	Ampliar o acompanhamento dos temas militares pelo conjunto da sociedade, ao apresentar as potencialidades e as necessidades de nossa Defesa ao debate público.
Livro Branco, Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END)	Presidência da República	25 de setembro de 2013	Atualização do Livro Branco, a PND e a END, que definem qual é o papel das FA na sociedade brasileira. A END enfatiza a importância de setores estratégicos, tais como o espacial, o nuclear e o cibernético, no contexto da possibilidade de conflitos, reforçando a importância da Estratégia Cibernética para o país. Foram realizadas revisões em 2016 e 2020, ainda não aprovadas.

Documentos Oficias	Órgão	Data	Contextualização
Decreto Nº 7.276	Presidência da República	25 de agosto de 2010	Aprova a Estrutura Militar de Defesa e dá outras providências.
Doutrina Militar de Defesa Cibernética — MD31-M-07	Ministério da Defesa	18 de novembro de 2014	Tem como objetivo proporcionar um alinhamento sobre o assunto no âmbito do MD, em prol da operação conjunta das FA no ambiente cibernético.
Manual do Direito Internacional aplicado às Operações Navais — EMA 135	Estado-Maior da Armada — Marinha do Brasil	2017	Orienta os militares da MB nas questões envolvendo o Direito Internacional.
Doutrina Militar Naval — EMA 305	Estado-Maior da Armada — Marinha do Brasil	2017	Estabelece conceitos e métodos de emprego em combate com o propósito de orientar o planejamento, preparo e aplicação do Poder Naval.
Decreto Nº 9.637	Presidência da República	26 de dezembro de 2018	Institui a Política Nacional de Segurança da Informação; dispõe sobre a governança da segurança da informação.
Decreto Nº 10.222	Presidência da República	5 de fevereiro de 2020	Aprova a Estratégia Nacional de Segurança Cibernética.
Portaria Nº 3.781	Ministério da Defesa	17 de novembro de 2020	Cria o Sistema Militar de Defesa Cibernética (SMDC).
Decreto Nº 10.569	Presidência da República	9 de dezembro de 2020	Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas.

Tabela 2 — Adaptado da legislação de Defesa e Segurança Cibernética — Vide Referência.