10.21544/2359-3075.v28n2.d

O DIREITO INTERNACIONAL E A DEFESA CIBERNÉTICA DA SOBERANIA NA AMAZÔNIA AZUL: UMA ABORDAGEM SOB A LUZ DO MANUAL DE TALLINN 2.0

Alexandre Peres Teixeira[1]
Liziane Paixão Silva Oliveira[2]

RESUMO

Em 2013, foi editado o primeiro Manual de Tallinn, sobre o Direito Internacional Aplicável às Operações Cibernéticas e aludia apenas às operações cibernéticas em tempo de guerra. O segundo Manual, publicado em 2017, também considerou as operações cibernéticas realizadas em tempo de paz. Tendo em vista a importância da normatização do ciberespaço para a guerra naval, o presente artigo se propõe a analisar as regras sugeridas pelo emergente Direito Internacional Aplicado às Operações Cibernéticas, para atividades que sejam realizadas no contexto das operações navais. Desta forma, a pesquisa emprega o método de revisão bibliográfica, com base em fontes primárias e secundárias, tais como relatório do Grupo de Especialistas Governamentais da ONU (UNGGE), o Manual de Tallinn 2.0 e artigos científicos sobre o tema. Cabe ressaltar que Manual de Tallinn 2.0 promoveu o encontro do emergente Direito Internacional Aplicável às Operações Cibernéticas com a consolidada lei da guerra naval. Esse encontro gera percepções legais que devem ser avaliadas com extrema atenção.

Palavras-chave: Direito Internacional Cibernético; Guerra Cibernética; Operações Navais.

[1] Programa de Pós-Graduação do Centro de Ensino Unificado de Brasília (UNICEUB), Brasília —DF, Brasil. E-mail: alexandreperes@yahoo.com.br — ORCID https://orcid.org/0000-0002-5349-8039.

[2] Programa de Pós-Graduação do Centro de Ensino Unificado de Brasília (UNICEUB), Brasília —DF, Brasil. E-mail: lizianepaixao@outlook.com — ORCID http://orcid.org/0000-0002-6266-6073.

INTRODUÇÃO

Com a crescente dependência dos Estados em relação ao meio técnico-científico informacional[3], a dimensão cibernética passou a ser utilizada também para interações nocivas entre eles, bem como entre atores não estatais e Estados, e, consequentemente, como ferramenta para confrontos geopolíticos, que exacerbam o simples viés geográfico e possuem forte influência nas diversas manifestações do poder estatal. O fenômeno da globalização[4] serviu para exacerbar estes movimentos interestatais.

Para Saldan (2012), a Paz e a Segurança internacionais e estabilidade político jurídico institucional, delas oriunda, são os pilares do aprimoramento e do exercício dos Direitos Humanos (DH), das liberdades fundamentais, da autodeterminação dos povos e do desenvolvimento político/ econômico/ social/ cultural das sociedades. Portanto, a dinâmica das Relações Internacionais é regida por regras diplomáticas e jurídicas, construídas no decorrer da história, com a intenção de promover a convivência pacífica entre os povos e buscar formas pacíficas para a solução das controvérsias.

Como os oceanos sempre foram um ambiente determinante para a geopolítica do planeta, com a chegada da era da informação surgiu a possibilidade deste espaço geográfico se tornar propício para o desenrolar de ações cibernéticas maliciosas contra a soberania de Estados costeiros.

No caso do Brasil, com sua imensa porção costeira denominada de "Amazonia Azul"[5], o planejamento de uma defesa cibernética capaz de causar dissuasão para qualquer ator, que possua a intenção de atentar contra a soberania brasileira, por meio da utilização da guerra cibernética, é ponto de fundamental importância.

---

[3] O conceito de meio técnico-científico informacional está relacionado com processo de formação e integração espacial, ocasionado pelas técnicas digitais, bem como com a maneira que ele modifica o espaço. PENA, Rodolfo Alves. Era da informação. Mundo Educação, 2013. Disponível em: http://mundoeducacao.bol.uol.com.br/geografia/era-informacao.htm. Acesso em: 12 fev. 2020.

[4] Sobre as alterações dos elementos do conceito clássico de soberania ler: OLIVEIRA, Liziane Paixão Silva. A soberania frente à globalização. **Revista do Programa de Mestrado em Direito do UniCEUB**, Brasília, v. 2, n. 1, p. 202-225, jan./jun, 2005.

[5] Segundo Vidigal (2006, p. 18), a Amazônia Azula trata-se da extensão atlântica, que se projeta para além do litoral e das ilhas oceânicas, e corresponde a cerca de metade da superfície do Brasil, se tem chamado de Amazônia Azul. Azul por comparar-se à Verde, pela dimensão e pela biodiversidade. VIDIGAL, Armando Amorim Ferreira; BOAVISTA, Marcílio. **Amazônia Azul**: o mar que nos pertence. Rio de Janeiro: Record, 2006.

Entretanto, em que medida ações de defesa cibernética podem ser realizadas, tendo como base o que está preconizado no Direito Internacional? Mesmo sendo um tema extremamente novo, pode se considerar que já existe base legal que normatize as operações cibernéticas executadas entre Estados nos ambientes marítimos?

Em relação aos trabalhos iniciais que podem, um dia, resultar em normatização, a edição do Manual de Tallinn 2.0, de Direito Internacional Aplicado às Operações Cibernéticas[6], em 2017, assim como a do Manual de Tallinn de 2013, representam um primeiro passo no caminho para a formação de uma doutrina internacional, que seja capaz de inspirar os diversos ordenamentos jurídicos do planeta.

Fruto do esforço da OTAN, na tentativa de pacificação do uso do ciberespaço, estes Manuais figuram como as primeiras fontes de doutrina jurídica internacional organizada, que abordam as operações realizadas no domínio cibernético. Apesar de não serem impositivos, possuem a natureza jurídica de *soft law* e têm o potencial de influenciar a prática e a *opinio iuris* dos Estados, no contexto de um arcabouço jurídico que começa a ser formar em torno deste importante tema.

No que tange às Operações Navais, em situação de conflito armado, o Manual de Tallinn 2.0 preconiza que as partes de um conflito não perdem seus direitos como Estado de bandeira[7] de um navio, Estado costeiro ou Estado portuário, como também não são liberados de seus deveres e obrigações perante o Direito Internacional, exceto para os casos nos quais as disposições da Convenção das Nações Unidas para Direito do Mar (CNUDM), na qualidade de *lex generalis*, são afastadas pelas normas do Direito Internacional dos Conflitos Armados (DICA), as quais constituem *lex specialis* para tempos de guerra, muitas das quais encontram-se descritas no Manual de San Remo de Direito Internacional Aplicável a Conflitos Armados no Mar [8].

---

[6] Segundo Stockburger (2016), o Comitê Internacional da Cruz Vermelha (CICV) entende como "operações cibernéticas" aquelas que são executadas contra ou de um computador, ou sistema de computação, que sejam realizadas por meio de um fluxo de dados, que tenham como objetivo fazer perpetrar ações específicas, tais como infiltração em sistemas de dados para coleta, exportação, destruição, alteração ou criptografia de dados ou para desencadear, alterar ou manipular processos controlados pelo sistema do computador infiltrado. STOCKBURGER, Peter Z. (2016) Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum. American University International Law Review, v. 31, n. 4, 2016. Disponível em: https://digitalcommons.wcl.american.edu/auilr/vol31/iss4/2/. Acesso em: 22 fev. 2020.

[7] Estado no qual o navio ou embarcação está registrado (CNUDM, art. 91).

[8] O Manual de San Remo é um documento de Direito Internacional preparado com

Para Ribeiro (2013), a Convenção das Nações Unidas para o Direito do Mar (CNUDM) uniformizou os critérios que se prestam a delimitar a jurisdição dos Estados no ambiente marítimo, tendo uma relação direta com a expansão dos direitos soberanos dos Estados costeiros (RIBEIRO, 2013, p. 270).

Apesar de a CNUDM se reportar, mais especificamente, a uma abordagem para tempos de paz, ela também se aplica para as situações de Conflito Armado. Tal aplicação se faz dentro do que preconiza o Manual de San Remo, de 1994, que apresenta as regras para a guerra no mar. Tais regras devem ser observadas entre os beligerantes e entre estes e os Estados neutros.

Para o Brasil, que possui um litoral imenso, a tarefa de cuidar da defesa dos ativos nacionais, situados no ambiente marítimo, sempre foi uma preocupação da Marinha de Guerra. O mar, com seu potencial de suscitar disputas pelos mais variados interesses, "inspira cuidados a serem traduzidos em preocupações quanto a segurança e defesa" (REIS, SANTOS, 2014, p. 216). Desta forma, não apenas a aderência às normas internacionais, mas também a divulgação de tais normas para os operadores das ações de defesa se faz de suma importância para os esforços de dissuasão empreendidos pelo país.

Em relação às normas jurídicas internacionais contidos na CNUDM, apesar de existirem poucas divergências[9] de interpretação por parte do Brasil, tais divergências não são suficientes para serem exploradas com a finalidade de turbar a soberania brasileira em suas águas jurisdicionais. Entretanto, não apenas para o Brasil, mas para muitos Estados costeiros, a construção de regras que se prestam a equalizar os comandos da CNUDM com as peculiaridades das operações cibernéticas

coordenação do Instituto de Direito Internacional Humanitário, de San Remo, em 1994, que trata das regras para os Conflitos Armados no mar. INSTITUTO INTERNACIONAL DE DIREITO HUMANITÁRIO. Manual de Sanremo. Sanremo, Itália, 1994. *In:* **DIREITO INTERNACIONAL RELATIVO À CONDUÇÃO DAS HOSTILIDADES**: Compilação de Convenções da Haia e de alguns outros Instrumentos Jurídicos. Genebra: Comitê Internacional da Cruz Vermelha - CICV, 2001.

[9] Existem dispositivos na CNUDM que ensejam diferentes interpretações. Por exemplo, o Brasil entende que a passagem inocente de navios de guerra deve ser notificada com antecedência ao Estado costeiro, bem como exercícios militares na Zona Econômica Exclusiva requerem prévia autorização do Estado costeiro. Esses posicionamentos não são aceitos por parte da comunidade internacional. Igualmente, há governos entendem que a CNUDM não veda a realização de pesquisa científica para fins militares na ZEE de outros Estados. Esses são apenas alguns exemplos de controvérsias, dentre outros, que podem vir a turbar a soberania ou direitos soberanos em águas jurisdicionais brasileiras.

ainda figuram como um terreno novo, no qual se faz necessária a construção de convencimento em relação ao seu conteúdo.

A era da informação tem causado disrupção também nos assuntos marítimos. Não restam dúvidas de que a Era da Informação modificou muito a dinâmica de uso dos mares, como também o combate no mar. Os atuais navios privados ou de Estado estão cada vez mais bem servidos de tecnologia, para o controle e manutenção de seus sistemas de propulsão, navegação e de combate.

Segundo Fahey (2017), aproximadamente 87% da frota de navios mercantes depende do Sistema Global de Navegação por Satélite (*Global Navigation Satellite System - GNSS*), tecnologia que torna os navios mercantes "alvos fáceis" de ataques[10] cibernéticos, em virtude dos sinais fracos usados por tais sistemas, que não possuem criptografia ou autenticação[11]. O autor segue afirmando que "as vulnerabilidades cibernéticas no domínio marítimo estão se expandindo a um ritmo alarmante, e, infelizmente, a proficiência em se proteger contra essas vulnerabilidades está ritmo extremamente lento". (FAHEY, 2017, p. 2)

Embora os sistemas de computação em rede e os sistemas de navegação por satélite ofereçam tremendas vantagens para as Forças Navais e para o setor de transporte comercial, eles também criam vulnerabilidades potenciais, que geralmente evoluem mais rapidamente do que a capacidade de as combater.

O avanço da tecnologia trouxe conforto, segurança e sofisticação para o ambiente marítimo, mas trouxe também enormes vulnerabilidades, que podem ser exploradas, tanto em tempo de paz, como em tempo de Conflito Armado. Desta forma, a perfeita compressão da emergente base jurídica internacional, que se refere às operações no espaço cibernético, se apresenta de extrema importância para que se possa fazer frente a este cenário.

O propósito do presente artigo é o de identificar e analisar pontos específicos do Direito Mar e da guerra naval, sob a ótica do emergente

---

[10] BHATTI, Jahshan; HUMPHREYS, Todd. Hostile control of ships via false GPS signals: Demonstration and detection. Na Viga Tion: **Journal of the Institute of Navigation**, v. 64, n. 1, p. 51-66, 2017.

[11] Como resultado, os sistemas GNSS são suscetíveis a "falsificação" - sinais falsos enviados ao receptor GNSS do navio, geralmente por meio de um receptor de rádio definido por software (SDR), projetado para interromper ou direcionar mal a navegação. Esta vulnerabilidade não é meramente especulativa. FAHEY, Sean. Combating "ciber fatigue" in the maritime domain. Washington, Humanitarian Law & Police, 2017, p. 3. Disponível em: https://blogs.icrc.org/law-and-policy/2017/12/07/combating_cyber-fatigue-in-the-maritime-domain/. Acesso em: 22 fev. 2020.

Direito Internacional Aplicado às Operações Cibernéticas, abordado pelo recém-criado Manual de Tallinn 2.0. Para que o leitor seja situado no estado da arte do debate sobre a gênese do Direito Internacional Cibernético, será necessária uma rápida contextualização sobre o conceito de soberania, sob a ótica deste mais novo ramo do Direito Internacional Público.

Neste caminho, a abordagem sugerida contextualizará o aspecto mais amplo da soberania do Estado, tendo como referência o paradigma westfaliano, remetendo para uma análise sobre os reflexos das zonas cinzentas criadas pelo Manual de Tallinn 2.0, que estão relacionadas ao exercício desta soberania, principalmente naquilo que afeta a guerra naval.

Ao abordar os pontos de convergências entre o Direito Marítimo, Direito Internacional dos Conflitos Armados no mar e o emergente Direito Internacional Cibernético, o trabalho pretende também contribuir para o debate relacionado ao emprego do ciberespaço no contexto das operações navais. Na primeira seção do artigo, será abordado, de forma sumária, o paradigma da soberania do Estado e o seu enfraquecimento na Era da Informação; na segunda seção serão analisados alguns conceitos existentes na Convenção das Nações Unidas para o direito no Mar (CNUDM) e a relação destes conceitos com o Manual de Tallinn 2,0; a terceira seção discorrerá sobre os conceitos da Guerra Naval e suas correspondências no emergente Direito Internacional Aplicado às Operações Cibernéticas; e finalmente se seguirá uma breve conclusão.

O PARADIGMA DA SOBERANIA DO ESTADO E SEU ENFRAQUECIMENTO NA ERA DA INFORMAÇÃO

O Enfraquecimento do paradigma westfaliano:

A Era da Informação trouxe consigo conflitos cujas características desafiam o Direito Internacional. O ciberespaço atualmente se apresenta como uma nova dimensão para as relações entre os Estados. Algumas ações que ocorrem no ambiente informacional possuem o potencial de gerar agressões e interferências na soberania estatal.

Onuf (1991) acredita que, na evolução do conceito de soberania, com a finalidade de atender às demandas, cada vez mais complexas das relações internacionais, fizeram com que tal conceito se tornasse, gradativamente, mais difícil de compreensão. Por sua vez, Watts (2018) afirma que, aplicar o conceito de soberania, de maneira

coerente e fundamentada, vem se mostrando uma tarefa imensamente difícil. Para ambos os autores, esta dificuldade tem sido agravada, em contextos que carecem de padrões profundamente enraizados ou estabelecidos pela prática estatal, principalmente naquilo que concerne à territorialidade consagrada pelo paradigma westfaliano[12].

Ao contrário do que ocorre com as fronteiras físicas, a dimensão cibernética de um Estado não possui fronteiras, tal fato afeta os antigos critérios estabelecidos para a evidência da soberania e jurisdição do Estado. Desta forma, a compreensão do conceito clássico de soberania territorial do Estado se torna importante para que se possa enxergar a complexidade relacionada à adaptação deste conceito às nuances que acompanham as operações realizadas no ciberespaço.

Celso D. de Albuquerque Mello afirmava que o Estado tem como um dos seus elementos o território. "O território é onde o Estado exerce a sua soberania, dentro dos limites estabelecidos pelo Direito Internacional", desta forma, conclui o autor que "a noção de território não é geográfica, mas jurídica, tendo em vista que ele é o domínio de validade da ordem jurídica de um determinado Estado soberano" e este será o ponto de partida para caracterizarmos a porção terrestre e física de um Estado. A territorialidade ou a "existência territorial" tem sido um ponto fundamental para o entendimento da existência do Estado. (MELO, 1992, pag. 50)

Identificar uma violação de soberania com base na utilização de limites territoriais físicos é bem mais fácil do que fazê-lo quando a violação ocorre por meio de uma operação cibernética maliciosa. Margulies (2013) acredita que "a lei internacional, que aborda a responsabilização do Estado, por ataques cinéticos no mundo real, é inadequada para lidar com a responsabilidade estatal, no que tange aos ataques cibernéticos". Não apenas devido a dificuldade de detecção e atribuição dos ataques cibernéticos externos, mas também pela facilidade que o atacante possui de controlá-los de forma velada. (MARGULIES, 2013, pág. 2)

Para Watts (2018), uma das questões mais difíceis e prementes, do esforço em andamento para adaptar o direito internacional aos domínios

[12] Ferreira (1958) diz que a noção de soberania estatal está intimamente ligada à noção do surgimento do Estado. Para a maior parte da Doutrina, são elementos constitutivos do Estado: o Povo, a Soberania (ou poder político, para alguns) e o Território. Segundo o paradigma westfaliano, o território figura como evidência material para o exercício da soberania, pelo Estado. Este tem sido um dos paradigmas mais respeitados, tanto para a construção do complexo sistema internacional, como para a consolidação dos ordenamentos jurídicos nacionais. Ver: FERREIRA, Pinto. **Teoria Geral do Estado**. 2. ed. ampliada e atualizada. São Paulo: José Konkino Editor, 1958, Tomo I.

emergentes das relações internacionais, é a de como a soberania territorial deve ser considerada "no mundo interconectado, ainda difuso; virtual, ainda material; novo, ainda onipresente do domínio do ciberespaço". Mesmo divorciada do contexto único e legalmente desafiador do ciberespaço, a soberania territorial é um assunto extremamente complexo e enigmático, no âmbito do direito internacional. "Embora seja axiomaticamente fundamental para quase todos os assuntos e regras do direito internacional, a importação legal precisa do conceito de soberania territorial, do mundo real para o mundo virtual, se torna frustrantemente complicada, contextual e ilusória", segue Watts afirmando. (WATTS, 2018, pág. 812)

De fato, o ciberespaço se apresenta como um contexto no qual a aplicação do princípio da soberania se torna bem difícil, em decorrência de os Estados oferecem uma quantidade confusa de comportamentos, bem como inúmeras justificativas para as condutas que ocorrem nas zonas cinzentas, que separam a legalidade da ilegalidade, principalmente aquelas relacionadas à soberania territorial. Desta forma, várias linhas de pensamento estão surgindo em resposta a questões relativas à adequação entre o conceito de soberania e sua aplicação no ciberespaço.

Stockburger (2016) acredita que um dos maiores desafios que os Estados enfrentam no ambiente cibernético "é a questão do escopo e da maneira de aplicabilidade do direito internacional às operações cibernéticas, sejam elas ofensivas ou defensivas, ter permanecido instável desde o advento delas". Existindo, desta forma, para o autor "o risco da prática cibernética se distanciar rapidamente dos entendimentos acordados quanto ao seu regime de Direito". (STOCKBURGER, 2016, pág. 549)

Para Michael N. Schmitt[13], editor geral do Manual de Tallinn 2.0, "tornou-se comum caracterizar o ciberespaço como uma nova dimensão de guerra, desprovida do Direito Internacional e sujeita ao abuso catastrófico" e neste terreno a atuação de Estados e atores não estatais figura como grande ameaça, tanto para a segurança e a paz internacionais, como para a ordem pública interna dos Estados. (SCHMITT, 2017a, pág.7)

Apesar de ser um tema que entrou na pauta de Segurança Internacional muito recentemente, o potencial de destruição das atuais ameaças cibernéticas já foi percebido em alguns casos concretos, tais como

[13] Professor de Direito Internacional, Universidade de Exeter, Coordenador do Centro de Estudos de Direito Internacional de Stockton, Professor do U.S. Naval War College; Distinto Acadêmico da Francis Lieber, da Academia Militar de West Point. Autor e Diretor do Projeto do Manual de Tallinn Manual de 2009 a 2017.

o ataque cibernético sofrido pela Estônia, em 2007; a Operação Orchard[14], realizada por Israel, ainda em 2007; a guerra Russo-Georgiana[15], em 2008; o vírus Stuxnet[16], que infectou uma usina nuclear iraniana, em 2010; o ataque de hacker à *Sony Pictures*[17], em 2014; a denúncia de violação de e-mails da Presidente Dilma Rousseff[18] em 2015, pela Agencia de Segurança Nacional (NSA), dos EUA; e os ciberataques sofridos pelos Estados Unidos da América (EUA), em 2015 e 2016, que teve forte influência nas eleições presidências de 2017[19].

---

[14] Em setembro de 2007, Israel realizou ataque aéreo à Síria para bombardear uma suposta usina nuclear que seria construída com a Coreia do Norte; o governo israelense teria se infiltrado no sistema de defesa aérea da Síria, porque os aviões israelenses não foram detectados por radares, o que possivelmente ocorreu em razão da utilização de programas específicos para burlar os sistemas sírios de controle de tráfego, que transmitiram sinais falsos. (Idem., 2012, pág. 71).

[15] Em agosto de 2008, imediatamente antes do exército russo invadir a Geórgia, um ataque cibernético, supostamente, prejudicou os sistemas militares de TI da Geórgia, incluindo o de defesa aérea. Ver: SHACKELFORD, Scott. Estonia Two-and-A-Half Years Later: a progress report on Combating Cyber Attacks. **Journal of Internet Law, Forthcoming**, 2009. Disponível em: https://ssrn.com/abstract=1499849. Acesso em: 17 fev. 2020.

[16] Em outubro de 2010, o vírus "Stuxnet", supostamente desenvolvido pelos governos israelense e americano, foi infiltrado, possivelmente por um pen drive, nos sistemas do reator nuclear de Bushehr, no Irã, construído pela Rússia, com a finalidade de inutilizar centrífugas aumentando sua rotação, enquanto sinais de normalidade eram enviados para o controle. O episódio afetou o projeto nuclear iraniano e por isso é amplamente noticiado como espécie de ataque de guerra cibernética. A empresa russa de segurança da computação Kaspersky Labs afirmou, em dezembro de 2011, que o Stuxnet pode ser o primeiro de um conjunto de armas cibernéticas. (SALDAN, op. cit., p. 72).

[17] Em 2014, um grupo de hackers lançou um ataque cibernético à *Sony Pictures Entertainment* e divulgou, entre outras coisas, informações pessoais dos funcionários da empresa, incluindo correspondências por email e informações sobre os salários dos executivos. HABER, Eldar. The Cyber Civil War. **44 Hofstra Law Review 41**, 2015. Disponível em: https://ssrn.com/abstract=2699644. Acesso em:17 fev. 2020.

[18] Os vazamentos de Edward Snowden, publicados por muitos veículos de mídia diferentes em todo o mundo, demonstraram que os direitos mais básicos das pessoas podem ter sido, continuamente, violados, principalmente o direito à privacidade e à liberdade de expressão. Consta na revelação que a NSA (a agência responsável pela vigilância eletrônica dos EUA) teria acessado os e-mails da então Presidente do Brasil, Dilma Rousseff. Ver: MONTEIRO, Renato Leite. The Balance between Freedom and Security in the Age of Surveillance: a Brief Analysis of the Recent Intelligent Electronic Surveillance Scandals. **SSRN**, 2014. Disponível em: https://ssrn.com/abstract=2468060. Acesso em: 13 fev. 2020.

[19] Em 2015 e 2016, hackers, afiliados ao governo russo, invadiram servidores do Comitê Nacional Democrata dos EUA (DNC). A subsequente divulgação de documentos prejudicou os democratas nas eleições parlamentares, o que levou à renúncia do presidente do DNC, criou tensão entre os partidários de Clinton, de Sanders, e, acima de tudo, afetou proeminentemente a corrida presidencial. As operações russas foram mais um exemplo da eficiência que a Rússia possui em explorar as "Zonas Cinzentas" (ZC) do Direito Internacional (DI). SCHMITT, Michael. Grey Zones in the International Law of Cyberspace. **Yale Journal of International Law**, v. 42, p. 1-21, 2017a. Disponível em: https://www.yjil.yale.edu/grey-zones-in-the-international-law-of-cyberspace/. Acesso em: 13 fev. 2020.

Mesmo diante deste cenário, os esforços para sedimentar conceitos jurídicos e técnicos, que possam fazer frente a estas novas ameaças, ainda caminham de forma bem vagarosa. Isto porque as operações realizadas no ciberespaço extrapolam as fronteiras geográficas convencionais, apesar de suas estruturas físicas, lógicas, bem como os operadores "estarem abrigados em jurisdições diversas, interagindo numa relação de interdependência de estruturas cuja dinâmica não segue uma relação entre o espaço físico e o espaço virtual ou cibernético" (SALDAN, 2012, p. 27).

O fenômeno, denominado de guerra cibernética[20], ficou mais conhecido, para o público em geral, após o ano de 2007, quando a Estônia foi vítima de uma sequência de ataques cibernéticos coordenados e sistemáticos contra suas infraestruturas críticas, públicas e privadas, afetando a vida de milhões de pessoas naquele país. Tal ação se deu após uma controvérsia que envolvia a transferência de lugar de corpos de soldados russos e um monumento russo da Segunda Guerra mundial.

O ataque foi atribuído ao governo russo e figura como um dos primeiros adventos[21] de guerra cibernética registrado no planeta, segundo o Manual de Tallinn 2.0, envolvendo Estados soberanos. Como consequência deste evento crítico, a Organização do Tratado do Atlântico Norte (OTAN) estabeleceu, na cidade de Tallinn, o Centro Cooperativo de Excelência em Defesa Cibernética (NATO CCD COE).

Uma das primeiras atividades do grupo de especialistas internacionais do NATO CCD COE foi a de realizar um estudo detalhado a respeito de como o Direito Internacional poderia regular a noção de "uso da força", quando esta fosse empregada pelos Estados nas operações cibernéticas que ocorressem durante um Conflito Armado internacional. O resultado deste primeiro trabalho foi a publicação do Manual de Tallinn, em 2013.

Após a publicação deste primeiro manual, o grupo de especialistas se empenhou em estudar, sob o ponto de vista do direito intencional, o

[20] Raboin (2011) já afirmava que a guerra cibernética iria alterar a natureza inerente da própria guerra, defendendo a ideia conceitual de que a guerra cibernética não mudaria apenas os armamentos das guerras modernas, mas que representaria uma mudança radical na natureza do campo de batalha. RABOIN, Bradley. Corresponding Evolution: International Law and the Emergence of Cyber Warfare. **National Association of Administrative Law Judiciary**, v. 31, n. 2, 2011. Disponível em: http://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5. Acesso em: 17 fev. 2020, p. 604.

[21] Existe registro na literatura de que o primeiro ataque também teria se originado da Rússia e o alvo teria sido os EUA, em 1982. Ver: RICHARD, Clarke; KNAKE, Robert. **Cyber war**: the next threat to national security and what to do about it. New York: Ecco; Reprint edition, 2010, p. 92; MCLAUGHLIN, Stephen, *et al*. The cybersecurity landscape in industrial control systems. **Proceedings of the IEEExplore**, v. 104, n. 5, p. 1039-1057, 2016.

emprego de operações cibernéticas, não apenas no âmbito dos conflitos armados, mas também aquelas realizadas em tempo de paz. Desta forma, em 2017, o NATO CCD COE, em parceria com a universidade Cambridge, publicou o Manual de Tallinn 2.0, que além dos estudos elencados pelo primeiro manual de 2013, engloba também uma abordagem sobre as operações cibernéticas realizadas, por Estados, em tempos de paz, cobrindo assim tópicos como Lei do Uso do Espaço, Direitos Humanos, Direito Marítimo, Direito Diplomático, entre outros tópicos relacionados ao tempo de paz.

O processo de produção[22] deste manual seguiu os mesmos moldes do Manual de Oxford, de 1880, sobre o Direito Internacional aplicado a Guerra Terrestre; do Manual de San Remo, de 1994, sobre o Direito Internacional aplicado à Guerra Naval; e do Manual de Harvard, de 2009, sobre o Direito Internacional aplicado a Guerra Aérea e de Mísseis.

Para a confecção do manual de 2017 foi considerada uma base jurídica[23] internacional composta por 54 tratados, 51 casos concretos e 58 fontes diversas, as quais se incluem artigos, relatórios de grupos de especialistas da ONU e manuais sobre Direito Internacional.

O Manual de Tallinn 2.0 está dividido em quatro partes. A parte I trata das questões gerais de direito internacional e ciberespaço. A parte II abrange os regimes especializados de direito internacional e ciberespaço. A Parte III diz respeito à paz e a segurança internacional e atividades no ciberespaço, extraídas principalmente de do Manual de Tallinn 1.0. E a Parte IV é o restante do Manual de Tallinn 1.0, que aborda o Direito Internacional dos Conflitos Armados aplicado às operações cibernéticas[24].

Atualmente, o Manual de Tallinn 2.0 figura como o mais recente trabalho de doutrina sistematizada sobre o Direito Internacional Cibernético. Muito longe de ser considerado um documento vinculativo, o manual levanta questionamentos importantes sobre as áreas do Direito Internacional que são exploradas por Estados contumazes na execução de operações cibernéticas maliciosas. Estas áreas são denominadas de "zonas cinzentas do Direito Internacional Cibernético".

De fato, a aplicação do princípio da soberania no ciberespaço torna-se difícil, em decorrência da diversidade de atuações dos Estados nas zonas

[22] SCHMITT, Michael. T**allinn Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge: Cambridge University Press, 2017b, p. 1.

[23] SCHIMITT, 2017b, p. i a v.

[24] Id., p. v a xi.

cinzentas do emergente Direito Internacional Cibernético. Em virtude dessa complexidade diversos doutrinadores têm se lançado na análise das questões relativas à adequação entre o conceito de soberania e a sua aplicação no ciberespaço. Para Johnson e Post (1998), "a atenção acadêmica inicial tem abordado a questão fundamental da relevância geral da soberania para o ciberespaço, especialmente se o ciberespaço pode ser considerado um domínio pós-Westfaliano", que deverá ser reinventado para atender às demandas da era da informação (Johnson and Post 1996, 1370, Nossa tradução).

Zonas cinzentas do Direito Internacional Cibernético e a soberania:

Como já citado, o Manual de Tallinn 2.0 pode ser considerado a primeira fonte de doutrina de Direito Internacional Cibernético, ao lado dos relatórios emitidos pelo Grupo de Especialistas Governamentais da ONU, para assuntos relacionados à tecnologia da informação (UM GGE). Desta forma, o Manual possui o potencial para orientar as operações cibernéticas realizadas por todos os Estados que compõem a sociedade internacional, principalmente no que tange à construção de tratados, convenções e acordos bilaterais internacionais sobre o tema. Desta forma, resolver as controvérsias hermenêuticas existentes no Manual é uma tarefa importante para a consolidação do Direito Internacional Cibernético.

Uma leitura cuidadosa do Manual de Tallinn 2.0 faz ressaltar que, em diversas ocasiões, o grupo de especialistas não atingiu o consenso em relação à amplitude de aplicação de algumas regras. Tal fato, tem gerado o que Schmitt (2017) denomina de zonas cinzentas do Manual de Tallinn 2.0. Essas zonas são, na prática, as diferenças de entendimentos e interpretações, de algumas regras, surgidas entre os especialistas de diversos países da Europa, durante o processo de construção do referido Manual.

Ao mencionar o complexo problema relacionado às zonas cinzentas do Manual, Schmitt (2017) cita como exemplo as eleições norte-americanas[25] de 2017, afirmando que elas sofreram uma grave influência no resultado, em decorrência de operações cibernéticas maliciosas perpetradas pela Rússia. Segundo ele, a Rússia se aproveitou das zonas cinzentas do Manual de Tallinn 2.0 para influenciar

[25] Por meio desta estratégia, a Rússia explora princípios e regras do DI que são mal demarcados ou estão sujeitos a interpretações concorrentes. Ao fazer isso, a Rússia chamou atenção para as complexas questões de responsabilidade do Estado, em relação às ações de atores não estatais, e para a questão relacionada ao controle destes atores, que, sob a visão do Direito Internacional Humanitário (DIH), pode internacionalizar um CANI. (SCHMITT, op. cit., 2017a, p. 1).

diretamente nas funções exclusivas e inerentes aos EUA, realizando algo que, sob a luz do Manual de Tallinn 2.0, pode ser considerada uma intervenção ilícita.

As principais zonas cinzentas do Manual de Tallinn 2.0, na avaliação de Schmitt (2017), estão relacionadas ao conceito de soberania, pois segundo uma abordagem de alguns funcionários[26] do Departamento de Defesa dos EUA (DoD), "soberania seria apenas um princípio fundamental que não gera nenhuma regra primária no Direito Internacional" de forma que, na visão destes funcionários, "não há proibição à violação da soberania de outro Estado" por meio de uma operação cibernética. Para estes funcionários, "as operações cibernéticas de um Estado são apenas suscetíveis de violar outras regras primárias do Direito Internacional, como a 'não-intervenção' ou a 'proibição do uso da força'". (SCHMITT, 2017a, p. 5)

É fato notório que a soberania possui tanto um componente interno, quanto um externo. A noção de soberania interna refere-se ao direito que um Estado tem de exercer seu controle sobre pessoas, incluindo pessoas coletivas, objetos e atividades em seu território. Para Schmitt (2017), é incontestável que "esse direito se estenda ao controle sobre indivíduos envolvidos em atividades cibernéticas, infraestrutura cibernética localizada no território de um Estado e quaisquer atividades cibernéticas que ocorram dentro ou através desse território". (SCHMITT, 2017b, p. 12)

A soberania externa, em contraste, refere-se ao direito dos Estados de se engajarem em Relações Internacionais, como no caso da Diplomacia e da celebração de acordos internacionais. Por exemplo, no exercício da soberania externa um Estado é livre para tornar-se, ou não, parte de um tratado que regule atividades cibernéticas. Tal soberania é também a base para a imunidade legal dos Estados. Como na soberania interna, a contestação da existência de soberania externa não está em questão.

Ao discorrer sobre o tema, Schmitt (2017) segue afirmando que existem duas importantes zonas cinzentas no que diz respeito ao conceito de soberania, sob o ponto de vista das operações cibernéticas. A primeira se localiza em torno do argumento de que "a soberania é apenas um princípio fundamental que não gera nenhuma regra primária do Direito

[26] Mais precisamente por Gary P. Corn e Robert Taylor , autores do artigo "Sovereignty in the Age of Cyber". Ver: CORN, Gary; TAYLOR, Robert. Sovereignty in the age of cyber. *In:* THE AMERICAN SOCIETY OF INTERNATIONAL LAW. **Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0**, v. 111, 2017, p. 207-212. Disponível em: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-the-age-of-cyber/02314DFCFE00BC901C95FA6036F8CC70. Acesso em: 10 maio 2020.

Internacional". Ainda segundo o autor, esta abordagem de "soberania como princípio, mas não regra" contradiz a extensa prática dos Estados e *opinio juris*[27], no contexto não-cibernético, que trata da proibição de violação da soberania alheia, como uma regra primária, de tal forma que tal violação se constituiria em um ato internacionalmente ilícito.

Em sentido diverso, alguns doutrinadores como Corn e Taylor (2017) afirmam que a natureza do ciberespaço é incompatível com os conceitos tradicionais de geografia. É difícil precisar o limite do espaço interno e internacional, logo identificar o "papel exato que o princípio de soberania nas atividades cibernéticas dos estados reguladores" (Corn and Taylor 2017, 207, Nossa tradução).

A segunda zona cinzenta, sob o enfoque da soberania do Estado, está relacionada às operações cibernéticas remotas realizadas fora do Estado alvo. Segundo uma visão minoritária do Manual de Tallinn 2.0, poderiam ser consideradas capazes de violar a soberania apenas as operações maliciosas que gerassem danos[28] físicos no Estado alvo.

Para Schmitt (2017), não resta dúvida de que uma operação cibernética remota, causando danos físicos ou ferimentos no território de outro Estado, viola a soberania deste último, uma vez que a noção bem aceita de integridade territorial e inviolabilidade está no auge quando as consequências físicas se manifestam. No entanto, a maioria deles concluiu que a perda definitiva da funcionalidade da infraestrutura cibernética pode também ser considerada uma violação da soberania do Estado, mesmo que não ocorram danos físicos (SCHMITT, 2017a, p. 3). Portanto, tanto a perda de funcionalidade, como o dano físico, para o Manual de Tallinn 2.0, podem servir como evidência de violação de soberania de Estado por meio da execução de uma operação cibernética.

Desta forma, se faz importante entender toda a polêmica gerada em torno do conceito de soberania, a fim de caminharmos adiante e verificarmos que, mesmo diante de pontos controversos e zonas cinzentas, vem sendo construído o arcabouço jurídico que tenta regulamentar a utilização das operações cibernéticas entre os Estados, tanto para os tempos de paz, como para o tempo de guerra, como é o caso da guerra naval que abordaremos mais adiante.

---

[27] A *opinio juris* é um elemento indispensável para que uma dada prática reitera dos Estados venha a adquirir o reconhecimento de norma consuetudinária internacional.

[28] Os especialistas que escreveram o Manual entenderam corretamente que há "pouca diferença prática entre o dano físico à propriedade e torná-la praticamente inoperante" (SCHMITT, 2017a, p. 3).

Em suma, no que tange às operações cibernéticas, pelo princípio da igualdade soberana entre os Estados os Estados são livres para tomar suas decisões. Portanto, o Estado afetado por uma ação cibernética maliciosa, caso decida tomar alguma ação em retaliação, deve informar qual ação tomará. Mas, de acordo com a regra[29] 4 do Manual de Tallinn 2.0, a soberania é caracterizada como uma regra primária e não como um princípio fundamental, que seja capaz de sustentar regras primárias, como o dever de não intervenção e o direito à legítima defesa. Desta forma, o Manual de Tallinn 2.0 indica que a soberania é uma "norma de direito", da qual nenhuma derrogação é permitida, aumentando a atenção para a sua não violação e para a importância de se compreender o que caracterizaria uma violação (Ghappour 2017, 225).

De fato, a aplicação de um "princípio da soberania" no ciberespaço torna-se difícil, em decorrência da diversidade de atuações dos Estados nas zonas cinzentas do emergente direito internacional cibernético. Em virtude dessa complexidade diversos doutrinadores têm se lançado na análise das questões relativas à adequação entre o conceito de soberania e a sua aplicação no ciberespaço. Para Johnson e Post (1998), "a atenção acadêmica inicial tem abordado a questão fundamental da relevância geral da soberania para o ciberespaço, especialmente se o ciberespaço pode ser considerado um domínio pós-Westfaliano", que deverá ser reinventado para atender às demandas da era da informação (Johnson and Post 1996, 1370, Nossa tradução).

Compreender os novos movimentos do Direito Internacional se torna algo de extrema relevância, uma vez que o processo de construção da base jurídica que poderá normatizar o uso do ciberespaço pode ser permeado por interesses geopolíticos, exigindo-se diligência dos Estados para que não tenham seus interesses atingidos por uma legislação tendenciosa. Para o contexto da guerra naval, trata-se de fato de extrema relevância, uma vez que as características que acompanham o emprego do poder naval de um Estado, fazem com que o meio naval de combate figure como um eficiente vetor de guerra cibernética.

PONTOS DE CONVERGÊNCIA ENTRE A CNUDM E O MANUAL DE TALLINN 2.0

Nesta seção serão abordados os principais artigos do Manual de

[29] "**Regra 4 – Violação da soberania: Um Estado não deve realizar operações cibernéticas que violem a soberania de outro Estado**" (SCHMITT, 2017b, p. 17 - Nossa tradução).

Tallinn 2.0, que se relacionam com a CNUDM. Os conceitos da CNUDM, aqui abrangidos, apesar de terem sido estabelecidos para a situação de não-guerra, são fundamentais para a compreensão das recentes criadas regras que procuram adaptar o Direito Internacional aplicado às Operações Cibernéticas às situações de conflitos armados no mar.

Cabe ressaltar que as regras do Manual de Tallinn 2.0, referentes à CNUDM, constantemente fazem alusão à situação específica de guerra naval, reportando ao Manual de San Remo.

Para Brozoski (2019), um fenômeno que tem se intensificado, nas transformações em curso no sistema internacional, é a expansão dos Estados sobre os mares. Segundo a autora, "a disputa pelo acesso a fontes de recursos energéticos e minerais e a concorrência pelo controle das principais rotas internacionais de navegação continuam compondo o núcleo da competição global de poder e, hoje, abrangem de forma mais incisiva o espaço marítimo" (BROZOSKI, 2019, p.77). Neste sentido, é inquestionável que o ambiente marítimo se traduz em um território fértil para confrontos geopolíticos. Brozoski 2019 segue afirmando o seguinte:

> Além de possuir uma extensa jurisdição marítima fartamente favorecida com recursos naturais – como as imensas jazidas de petróleo do Pré-sal –, o Brasil também é portador de um notável acervo tecnológico para a exploração de tais riquezas. Se por um lado, dispor de Ciência e Tecnologia para o aproveitamento de tais bens é uma vantagem em direção ao desenvolvimento e a autonomia, por outro lado também é um elemento a mais que instiga a projeção de interesses externos sobre o país. A nosso ver, hoje, entender a posição do Brasil no tabuleiro geopolítico global requer, necessariamente, compreender as nuances e os efeitos do processo em curso de territorialização dos espaços marítimos, tanto no âmbito regional como no internacional. Em todo o mundo grandes tem sido os esforços para incorporar os oceanos ao aparato jurídico nacional. Cresce e se generaliza a compreensão de que as políticas públicas voltadas para a industrialização, o crescimento econômico e a Defesa e Segurança devem incluir de forma mais contundente os mares em suas agendas (BROZOSKI, 2019, p.82).

No caminho para a aderência do contexto nacional que engloba a "Amazônia Azul" ao aparato jurídico nacional e internacional, o Direito do Mar[30] fornece a orientação normativa sobre operações que são realizadas no mar ou de lá são lançadas contra os espaços territoriais. O Grupo Internacional de Peritos (GIP), que trabalhou na construção do Manual de Tallinn 2.0, concordou que o Direito do Mar se aplica às operações cibernéticas realizadas a partir ou por meio de uma infraestrutura cibernética localizada no mar.

As operações cibernéticas podem ser realizadas por navios e submarinos (doravante denominados coletivamente como "embarcações") no mar, por aeronaves em sobrevoo nos mares, por instalações offshore, ou por meio de cabos de comunicação submarinos, tanto em tempos de paz como durante os conflitos armados (SCHMITT, 2017b, p. 232).

Para Rocha e Fonseca (2019), em um cenário de conflito possuir a capacidade de realizar uma intrusão cibernética em um ativo do adversário, tendo acesso a conhecimento e até mesmo o controle sobre as ações, significa a obtenção de uma vantagem estratégica (ROCHA, FONSECA, 2019, p. 518). A capacidade de realizar operações cibernéticas partindo-se do mar se traduz em uma vantagem competitiva sem precedentes. Entretanto, a capacidade de se defender contra este tipo de operação perpassa a anterior e significa o amadurecimento do Estado, em relação ao novo cenário da era da informação.

Grande parte das regras[31] do Direito Internacional consuetudinário do mar está refletida na Convenção das Nações Unidas para o Direito do Mar (CNUDM). Mesmo os Estados que não são Partes da CNUDM costumam respeitar os termos da Convenção. Esta seção do artigo se baseia fortemente nas disposições contidas na CNUDM, que para o GIP reflete o direito internacional costumeiro em relação ao tema.

Um Estado[32], contudo, pode consentir que outro Estado exerça jurisdição a bordo de navios que arvorem sua bandeira. Esse consentimento pode ser tácito, por meio de um costume, ou expresso, por meio de um acordo internacional formal (ver Regra 19). Ressalta-se que os navios também podem estar sujeitos à jurisdição do Estado costeiro, dependendo de sua localização e do tipo de atividade que estiverem desempenhando. Entretanto, conforme preconiza a Regra 5 do Manual de Tallinn 2.0,

[30] Comentário 1 do Manual de Tallinn 2.0. (SCHMITT, 2017b, p. 232).
[31] Comentário 2 do Manual de Tallinn 2.0. (SCHMITT, 2017b, p. 232).
[32] Comentário 4 do Manual de Tallinn 2.0. (SCHMITT, 2017b, p. 232).

que discorre sobre "imunidade de jurisdição", caso o navio possua tal imunidade, estará protegido da jurisdição do Estado costeiro. Além disso, indivíduos envolvidos em operações cibernéticas, a bordo de navios, estão sujeitos à jurisdição prescritiva[33], cujas bases estão estabelecidas na Regra 10. (SCHMITT, 2017b, p. 232)

O Direito do Mar[34] é um regime para tempos de paz. Apesar disso geralmente é aplicado *mutatis mutandis* durante períodos de conflito armado (ver Regras 82-83), existem várias regras permissivas e proibições, e algumas nuances específicas que são impostas pelo Direito aplicado à Guerra Naval, cuja aplicação se faz entre Estados beligerantes e entre Estados beligerantes e os Estados neutros (O Manual de San Remo prevê as regras da guerra naval). Consequentemente, as partes em um conflito armado não perdem os direitos estabelecidos na CNUDM como Estados de bandeira, como Estados portuários ou como Estados costeiros, bem como não são liberados de seus deveres e obrigações, exceto nas situações nas quais as regras da CNUDM são modificadas ou substituídas pelas regras particulares da lei da guerra naval. Um exemplo disto é o fato de que os Estados envolvidos em um conflito armado no mar podem exercer o direito de "mera passagem[35]" (ver regra 49 do Manual de Tallinn 2.0) através de mares territoriais dos Estados neutros, direito este que, em tempo de paz, é denominado de direito de "passagem inocente" (ver Artigo 48 do Manual de Tallinn 2.0). O regime da mera passagem contém nuances específicas relacionadas ao conflito armado e a neutralidade que restringem ou regulamentam condutas que de outra forma seriam permitidas de acordo com o regime de passagem inocente. (SCHMITT, 2017b, p. 233)

A partir deste momento serão detalhadas as regras do manual de Tallinn 2.0 para cada compartimento jurídico do ambiente marítimo. Inicialmente, é importante compreender o contexto no qual uma operação cibernética maliciosa poderá interferir ou violar a Soberania de um Estado costeiro ou mesmo causar danos à ordem pública deste. O passo seguinte será o de entender de que forma uma operação cibernética poderá ser utilizada como arma de guerra naval, ou em proveito de campanhas no mar.

---

[33] A jurisdição prescritiva, ou jurisdição legislativa, tem sido um conceito estabelecido no direito internacional. É uma das maneiras pelas quais um estado pode causar impacto sobre pessoas, propriedades ou circunstâncias. De acordo com o *American Law Institute*, jurisdição prescritiva é "prescrever, ou seja, tornar sua lei aplicável às atividades, relações ou status das pessoas, ou aos interesses das pessoas nas coisas, seja por legislação, por ato executivo ou ordem , por norma administrativa ou reconhecimento, ou por determinação judicial" (CHOY, 2019, p.1).

[34] Comentário 5 do Manual de Tallinn 2.0. (SCHMITT, 2017b, p. 233).

[35] Nome que se dá para a passagem de um navio beligerante no mar territorial de um Estado neutro, prevista na Convenção de Haia XIII, art. 10º.

As Operações Cibernéticas em Alto-Mar:

Ao abordar às operações cibernéticas em alto-mar, o Manual de Tallinn 2.0, na regra 45, que possui relação com o art. 88 da CNUDM, preconiza que "**as operações cibernéticas no alto-mar poderão ser conduzidas apenas para propósitos pacíficos, salvo disposição em contrário no Direito Internacional**" (SCHMITT, 2017b, p. 233).

Para a CNUDM, com raras exceções, os navios em alto-mar estão sujeitos à jurisdição do Estado de bandeira[36]. Esta jurisdição se estende também às operações cibernéticas conduzidas a bordo. Dependendo da localização do navio, este poderá estar sujeito à jurisdição do Estado costeiro, caso não possua imunidade de jurisdição[37]. Segundo o Manual de Tallinn 2.0, os indivíduos engajados em operações cibernéticas estão sujeitos à jurisdição prescritiva extraterritorial[38] do Estado de bandeira (SCHMITT, 2017b, p. 232).

Segundo a CNUDM, "o alto-mar é reservado para fins pacíficos", isto é norma cogente do Direito Internacional, existindo a proibição do uso da força neste espaço territorial, salvo se for permitido pelo próprio Direito (CNUDM, art.88). Reportando ao Manual de Tallinn 2.0, operações cibernéticas são permitidas, mas não podem violar nenhuma regra ou lei do Direito Internacional. O princípio da liberdade do alto-mar[39] alcança as operações cibernéticas também (SCHMITT, 2017b, p. 233).

Neste caminho segue também a liberdade relacionada ao lançamento de cabos submarinos, em alto-mar, por todos os Estados, mas tal ação não pode afetar a liberdade de os Estados utilizarem aquele espaço (SCHMITT, 2017b, p. 234). Ressalta-se que a Zona Econômica Exclusiva[40] (ZEE) possui um regime especial, que será abordado mais adiante.

---

[36] As exceções são quando houver suspeita dos seguintes crimes: pirataria, comércio de escravos, transmissões não autorizadas, nacionalidade não aparente e mesma bandeira do Navio de Guerra.

[37] É o privilégio reconhecido a certas pessoas estrangeiras, em virtude dos cargos ou funções que exercem, de escaparem à jurisdição, tanto civil quanto criminal, do Estado em que se encontram. ACCIOLY, Hildebrando; SILVA, Geraldo Eulálio do Nascimento. **Manual de Direito Internacional público**. 12. ed. São Paulo: Saraiva, 1996.

[38] Regra 10 do Manual de Tallinn 2.0 (SCHMITT, 2017b).

[39] Tais normas vinculam apenas os Estados, de modo que ações de atores não estatais, em qualquer porção do mar, podem ser consideradas ilegais sob o aspecto do Direito Internacional ou interno do Estado costeiro. (SCHMITT, 2017b, p. 233).

[40] A Zona Econômica Exclusiva (ZEE), segundo a Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), é uma faixa situada para além das águas territoriais, sobre a qual cada país costeiro tem prioridade para a utilização dos recursos naturais do mar, tanto vivos

No entendimento do GIP[41], "as operações militares, que não envolvam o emprego de força, estão no âmbito do uso pacífico do mar". Porém, considerando o local onde estas operações forem realizadas, mesmo que sejam simples operações militares cibernéticas, elas podem estar violando um tratado ou um regime especial multilateral, como por exemplo o Tratado da Antártica[42]. A realização das operações cibernéticas no mar está sujeita ao princípio da Devida Diligência[43] e podem ser questionadas ou proibidas pelo Estado costeiro (SCHMITT, 2017b, p. 234).

Ainda em relação ao uso do alto-mar, o GIP concordou que o estabelecimento de *Data Centers* submarinos é lícito. Porém, na ZEE ou no mar territorial, esses equipamentos só podem ser estabelecidos com o consentimento do Estado costeiro e sua operação está sujeita à regulamentação e jurisdição (ver regra 9 do Manual de Tallinn 2.0) desse Estado[44]. Tal proposição jurídica tende a privilegiar o princípio da soberania do Estado, no que tange ao uso do seu mar territorial e sua precedência de exploração da ZEE.

Schmitt (2017) afirma que "o direito da guerra naval permite a realização de certas operações cibernéticas, no alto-mar, no contexto de um conflito armado internacional (CAI) (ver regra 82 do Manual de Tallinn 2.0) o que de outra forma seria proibido em tempos de paz". Como exemplo, cita-se o caso das operações cibernéticas militares que são conduzidas em apoio a um bloqueio naval (Regra 128 do Manual de Tallinn 2.0). Da mesma forma, um ataque cibernético (ver regra 92 do Manual de Tallinn 2.0) a uma

como não-vivos, e responsabilidade na sua gestão ambiental. Estabelecida pela CNUDM também conhecida como Convenção de *Montego Bay*, a Zona Econômica Exclusiva se estende por até 200 milhas marinhas (ou náuticas) - o equivalente à 370 km. Além da exploração e gestão dos recursos naturais, o país costeiro exercerá nesta zona a jurisdição no que concerne ao estabelecimento e utilização de ilhas artificiais, instalações e estruturas; à investigação científica marinha; e à proteção e preservação do meio marinho. Apesar da exclusividade dada ao país costeiro na área, todos os outros Estados gozam da liberdade de navegação e sobrevoo, da colocação de cabos e dutos submarinos, e outros usos lícitos do mar.

[41] Comentário 5 do Manual de Tallinn 2.0, (SCHMITT, 2017b, p. 234).

[42] Ver decreto no 75.963, de 11 de julho de 1975. BRASIL. **Decreto nº 75.963, de 11 de julho de 1975**. Promulga o Tratado da Antártida. Brasília – DF: Presidência da República, 1975.

[43] Princípio consagrado no Direito Internacional, segundo o qual o Estado deve tomar todas as providências para que seu território não seja utilizado para a execução de atos contrários ao direito de outros Estados, neste caso, operações cibernéticas que possam prejudicar outro Estado. (SCHMITT, 2017b, p. 30).

[44] Necessário o consentimento do Estado costeiro, para o estabelecimento no mar territorial deste, pois ele exerce soberania sobre essa área e sobre o seu fundo do mar (ver Regra 2). Quanto ao estabelecimento na ZEE, ver CNUDM, art. 60º, especificamente no que se refere às instalações e estruturas para fins econômicos (SCHMITT, 2017b, p. 231).

embarcação mercante, que esteja violando um bloqueio naval, é lícito, caso a embarcação, mesmo após o alerta prévio, continue resistindo à captura[45].

Cabe ressaltar que somente os Estados estão vinculados pela regra 45 do Manual de Tallinn 2.0, em suas operações cibernéticas. As atividades de atores não estatais, no mar, podem ser ilegais e até serem caracterizadas como crime, sob a lei internacional ou doméstica, mas não implicam a restrição refletida nesta regra, a menos que tais atividades possam ser atribuíveis a um Estado.

O Direito de visita e as operações cibernéticas

Sobre o direito de visita, a regra 46, do Manual de Tallinn 2.0, que tem relação com o art. 110º da CNUDM, preconiza que "**um Navio de Guerra, ou um navio autorizado pelo Estado, pode exercer o direito de visita e abordar um navio de outro Estado, sem o consentimento deste, se houver razoáveis indícios para se suspeitar que tal navio está utilizando meios cibernéticos para engajar com pirataria, comércio de escravos, transmissões ilícitas, não aparentar nacionalidade, ou se o navio for da mesma bandeira que a do Navio de Guerra ou de Estado**"[46].

No que tange ao uso de operações cibernéticas, para o exercício do direito de visita em alto-mar, as regras gerais são as mesmas que a CNDUM estabelece, ou seja, navios de guerra ou navios autorizados[47] não podem abordar navios privados que não ostentem a bandeira de seu país. As exceções são para os mesmos casos existentes na CNUDM, que respaldam a visita física. São eles: a pirataria, o comércio de escravos, as transmissões não autorizadas, a nacionalidade não aparente e a mesma bandeira do Navio de Guerra.

Na opinião de uma minoria do grupo de especialistas do Manual de Tallinn 2.0, a simples postagem de evidências[48] de qualquer tipo de atividade ilícita, referente ao navio, em redes sociais, "pode se constituir como indício razoável que permita a visita cibernética". A ação a ser empreendida pelo Navio de Guerra ou de Estado vai depender do tipo de

[45] Ver: Manual de San Remo, parágrafo 98 (SCHMITT, 2017b, p. 235).

[46] (SCHMITT, 2017b, p. 235).

[47] O termo "navio autorizado" será utilizado para navios autorizados pelo Estado de bandeira a engajarem em ações de garantia da lei, devendo estar devidamente identificados como tal (SCHMITT, 2017b, p. 232).

[48] Membros da tripulação do navio publicando no Facebook, Instagram, ou qualquer outra rede conhecida (SCHMITT, 2017b, p. 236).

situação (dentre as 5 citadas) na qual o navio infrator pode estar incurso (SCHMITT, 2017b, p. 236).

Para o GIP, sob o ponto de vista da intersecção entre Direito Internacional Aplicado às Operações Cibernéticas e o Direito do Mar, as ações ilícitas mais relevantes serão, em ordem de prioridade: a pirataria, a realização de emissão desautorizada e a não aparente ostentação de bandeira. O comércio de escravos, na visão do GIP, também se faz relevante, mas segue uma prioridade mais baixa do que as ações supramencionadas.

Quando se tratar de pirataria, em alto-mar ou na ZEE, segundo o Manual de Tallinn 2.0, poderá ser efetuada a abordagem por meios cibernéticos e posteriormente a abordagem física, para o apresamento do navio e prisão da tripulação. Cabe ressaltar que sob o ponto de vista técnico, um navio pirata poder fazer uso de operações cibernéticas para inabilitar a manobra ou as comunicações de um navio alvo. Porém, para a legitimação do direito de visita cibernética, em qualquer das 5 situações, deve haver fundada e razoável suspeita[49] de que o navio a ser abordado está empenhado em ações ilícitas (SCHMITT, 2017b, p. 236).

Em relação às transmissões clandestinas[50], estas podem ser de sons, de rádio ou de televisão, mas devem estar caracterizadas como transmissões para consumo público, excetuando-se aquelas para pedido de socorro. Nesta situação, os navios de guerra ou de Estado, que possuem legitimidade para efetuar a visita e encerrar a transmissão, são aqueles que estejam recebendo a transmissão, ou pertencentes aos Estados que estejam sendo interferidos por elas, ou ainda dos Estados cujos navios estejam recebendo ou sendo interferidos[51] pelas transmissões clandestinas (SCHMITT, 2017b, p. 237).

O Manual de Tallinn 2.0 afirma ainda que para os navios que não tenham nacionalidade aparente[52], ou finjam ter uma nacionalidade

[49] A suspeita deve estar fundamentada em um indício forte, não pode ser "mera liberalidade" (SCHMITT, 2017b, p. 237).

[50] Em relação à transmissão via internet, com disseminação de propaganda via rede social, para ser considerada violação da soberania de outro Estado, temos que observar se existe a coerção (ter influência direta sobre as funções inerentes e exclusivas de um Estado soberano), descrita na regra 4 do Manual de Tallinn 2.0 (SCHMITT, 2017b, p. 237).

[51] Cabe ressaltar que, para CNUDM, a finalidade da proibição constante na norma está direcionada às frequências de radiodifusão, que estejam controladas pelas leis internacionais de telecomunicações, que possam produzir efeitos nocivos sobre as comunicações no território, inclusive o marítimo, de um Estado costeiro (SCHMITT, 2017b, p. 236).

[52] Tecnicamente, existe a possibilidade de se utilizar operações cibernéticas para esconder a nacionalidade de um navio no Sistema de Identificação Automática de Navios por satélite (AIS), ou fazer com que o Sistema apresente uma identificação falsa (FAHEY, op. cit., p. 3).

falsa, é permitido tanto a utilização de operações cibernéticas, para uma abordagem virtual, como a abordagem física com a finalidade de checar a verdadeira nacionalidade. Para legitimar o direito de visita, neste caso, basta que o navio tenha uma indicação eletrônica de nacionalidade suspeita. Sabe-se que atualmente não é incomum a realização de mascaramento[53] do Sistema Global de Navegação por Satélite (GNSS), por meio de operações cibernéticas (SCHMITT, 2017b, p. 238).

Cabe ressaltar que a permissibilidade da "visita virtual", para estas situações elencadas acima, não obteve consenso no grupo de especialistas. A posição majoritária entendeu que a visita virtual seria uma extensão do tradicional direito de visita; para estes especialistas, a visita virtual seria menos intrusiva do que a visita física, estando assim mais coerente com o direito em tela. Para o grupo de posição minoritária, a visita virtual, apesar de ser menos intrusiva, tem o potencial de extrapolar aquilo que a CNUDM preconiza, uma vez que o navio visitante poderia ter acesso a uma grande quantidade de dados desnecessários para a efetivação do referido direito. Fato é que, realmente, ao se abrir o precedente para Estados realizarem "visitas virtuais" em navios de outros Estados isto pode significar um convite à espionagem (SCHMITT, 2017b, p. 239).

Apesar de ser uma posição que ainda não encontrou consenso, em virtude de questões políticas, sem prejuízo do que preconiza a presente regra, o direito de visita, inclusive com abordagem forçada, pode ser autorizado por uma resolução do Conselho de Segurança das Nações Unidas (CSNU), como ocorre atualmente com os navios da Força Tarefa Marítima da Força Interina das Nações Unidas no Líbano[54] (MTF-UNIFIL).

As Operações cibernéticas na Zona Econômica Exclusiva (ZEE):

Na regra 47, do Manual de Tallinn 2.0, que se relaciona com o art. 55 e 56 da CNUDM, está definido que "**um Estado que estiver conduzindo, no exercício de seus direitos e deveres, uma operação cibernética na ZEE de outro Estado deve ter a devida consideração a respeito dos direitos e deveres do Estado costeiro, na sua ZEE, e a operação cibernética deve ser conduzida para propósitos pacíficos, salvo disposição em contrário no Direito Internacional**" (SCHMITT, 2017b, p. 239).

[53] Id., 2017.

[54] Os navios da MTF UNIFIL estão autorizados a abordar quaisquer navios, que não tenham imunidade de jurisdição, em alto-mar, na ZEE ou até mesmo em águas territoriais libanesas, por força da Resolução 2373 do CSNU).

A ZEE é uma área, além dos limites do mar territorial, que não pode se estender mais de 200 milhas náuticas em direção ao mar, tendo como referências as linhas de base[55] do Estado. Na ZEE, o Estado costeiro tem direitos e jurisdição para fins de exploração, pesquisa, gerenciamento, conservação dos recursos naturais da coluna d'água, fundo do mar e subsolo da zona, bem como para a produção de energia com a utilização de correntes e ventos[56]. Na ZEE, os Estados também podem exercer jurisdição sobre o estabelecimento e uso de ilhas, instalações e estruturas artificiais, para fins econômicos; pesquisa científica marinha[57]; e sobre alguns incidentes de poluição marinha, realizada por navios[58]. Por exemplo, atividades cibernéticas que interferem nas instalações de produção de energia, localizadas na ZEE, como parques eólicos ou turbinas de corrente de maré, estariam dentro da competência jurisdicional do Estado costeiro (SCHMITT, 2017b, p. 249).

Pela CNDUM, todos os Estados gozam, na ZEE, da mesma liberdade que gozam em alto-mar, no que se refere à navegação, sobrevoo, lançamentos de cabos e de oleodutos, bem como para qualquer uso internacional legal, relacionado a estas liberdades. Em relação ao trânsito de navios de guerra, existe uma prática consagrada, por algumas marinhas[59] do globo, pela qual os Estados avisam, tanto quando vão atravessar a ZEE, como quando necessitam cruzar o mar territorial de Estados costeiros.

Em relação às operações cibernéticas realizadas nesta faixa do mar, existem linhas divergentes no Manual de Tallinn 2.0, mas em geral, as operações para auxílio à navegação e as comunicações, que sejam lícitas e não maliciosas, podem ser realizadas, aplicando-se o mesmo princípio de liberdade do alto-mar. Desta forma, a posição majoritária do Manual acredita que navios e aviões possuem a mesma liberdade que experimentam em alto-mar e tal fato não incide indevidamente sobre qualquer um dos enumerados direitos de soberania dos Estados costeiros (SCHMITT, 2017b, p. 240).

Na visão do grupo de especialistas, a CNUDM falha quando não aborda, ou enumera, nenhum interesse de segurança dos Estados costeiros,

[55] CNUDM, Art. 57º.

[56] CNUDM, Art. 55º-56º.

[57] CNUDM Art. 56º (1)(b).

[58] CNUDM Art. 211º.

[59] Cumpre observar que apenas cerca de 40 países (a maioria países em desenvolvimento), entre eles o Brasil, requerem notificação prévia acerca da realização de passagem inocente por navios de guerra, bem como somente 17 países, também o Brasil entre eles, manifestaram formalmente o entendimento de que é necessária a aquiescência do Estado costeiro para a realização de atividades em sua ZEE.

em relação à realização de operações cibernéticas na ZEE. Desta forma, para os especialistas, aviões e navios que transitam na ZEE, no que tange à realização de operações cibernéticas, gozam da mesma liberdade que gozariam em alto-mar, inclusive para atividades militares[60]. Tal liberdade está sujeita à devida consideração dos direitos exclusivos do Estado[61] costeiro. Particularmente, navios e aviões de guerra, com capacidade de realização de operações cibernéticas, possuem liberdade para operar na ZEE, sem a necessidade do consentimento do Estado costeiro (SCHMITT, 2017b, p. 240).

Segundo o Manual, em relação à possibilidade de realização de atividades militares na ZEE, o grupo de especialistas ficou dividido entre duas posições. A posição majoritária[62] acredita que, pelo fato da CNUDM não elencar interesses de segurança nesta porção do mar, os Estados poderiam engajar em atividades militares, tais como coleta de inteligência por meios cibernéticos e também em exercícios militares cibernéticos, sem a necessidade de consentimento do Estado costeiro. O grupo minoritário[63] acredita que para a realização de atividades militares típicas necessitam do consentimento do Estado costeiro. Ambos os grupos concordam que as pesquisas cientificas ainda que "para o bem da humanidade", inclusive aquelas conduzidas por militares, necessitam do consentimento do Estado costeiro. Este tema tem um potencial forte para suscitar controvérsias no futuro, principalmente quando consideramos que o Manual de Tallinn 2.0 não proíbe a espionagem cibernética[64] (SCHMITT, 2017b, p. 240).

Pelo entendimento do Manual de Tallinn 2.0, o conceito de "uso com propósitos pacíficos" não proíbe a realização de contramedidas[65], partindo-se da ZEE, por parte dos Estados, incluindo-se às contramedidas cibernéticas. Neste entendimento também se incluem as operações de guerra naval entre Estados beligerantes. Tais operações devem estar em

[60] Segundo a CNUDM, são atividades de sobrevoo, manobra de Força Naval, exercícios militares, vigilância, atividades de pesquisas militares, coleta de Inteligência e lançamento de explosivos.

[61] Segundo a CNUDM, o Estado costeiro possui direitos de soberania e jurisdição para a prospecção, exploração e conservação dos recursos naturais ali existentes, inclusive para geração de energia por meio das correntes. Desta forma, nenhuma atividade cibernética executada por outro Estado, na ZEE, pode interferir com estes direitos.

[62] Para este grupo, operações tipicamente militares não possuem qualquer influência no gozo limitado da soberania dos Estados costeiros nesta faixa de mar (SCHMITT, 2017b, p. 240).

[63] Segundo a opinião deste grupo, o artigo 58, inciso 3, da CNUDM, enfatiza que deve ser dada a devida consideração aos direitos e deveres do Estado costeiro, na ZEE. Para o grupo, as questões de segurança estão incluídas neste artigo. (SCHMITT, 2017, p. 240).

[64] Regra 32 do Manual de Tallinn 2.0 (SCHMITT, 2017).

[65] Regra 20 do Manual de Tallinn 2.0 (SCHMITT, 2017).

consonância com o que preconiza o Manual de San Remo. Caso o Estado costeiro seja um Estado neutro, os beligerantes devem dar a devida consideração aos seus direitos e deveres.

As Operações cibernéticas no Mar Territorial:

Segundo a regra 48, do Manual de Tallinn 2.0, que tem relação com o art. 2º da CNUDM, "**para que um navio possa gozar do direito de passagem inocente pelo mar territorial de um Estado costeiro, qualquer operação cibernética executada pelo navio deve estar em consonância com as condições impostas ao referido direito**" (SCHMITT, 2017b, p. 241).

Talvez a passagem pelo mar territorial de um Estado costeiro seja a ação mais sensível, no que tange ao Direito Internacional Aplicado às Operações Cibernéticas. Uma série de cuidados devem ser tomados, tanto por navios mercantes, quanto por navios de Estado, a fim de que, inadvertidamente, um reconhecido e consolidado direito de passagem não possa se tornar a motivação para um grave incidente diplomático.

Para o Manual de Tallinn 2.0, os Estados costeiros gozam de soberania e jurisdição plena na faixa de mar que vai da linha de base do litoral até uma distância que não exceda 12 milhas náuticas[66]. O mar territorial, juridicamente, é uma extensão do território do Estado costeiro. Navios de todos os Estados, incluindo-se os navios de guerra, gozam do direito de passagem inocente[67] pelo mar territorial dos Estados costeiros. Aviões não gozam de direito deste direito e submarinos, para gozarem, devem navegar na superfície, ostentando a sua bandeira (SCHMITT, 2017b, p. 241).

Para o grupo de especialistas, o regime de passagem inocente[68] não requer o consentimento do Estado costeiro, porém, para navios de guerra, alguns Estados costeiros exigem a notificação prévia, para que seja

[66] Artigo 3º da CNUDM.

[67] O instituto da "passagem inocente" está previsto no art. 3º da Lei 8.617/93: Art. 3º É reconhecido aos navios de todas as nacionalidades o direito de passagem inocente no mar territorial brasileiro. § 1º A passagem será considerada inocente desde que não seja prejudicial à paz, à boa ordem ou à segurança do Brasil, devendo ser contínua e rápida. § 2º A passagem inocente poderá compreender o parar e o fundear, mas apenas na medida em que tais procedimentos constituam incidentes comuns de navegação ou sejam impostos por motivos de força ou por dificuldade grave, ou tenham por fim prestar auxílio a pessoas a navios ou aeronaves em perigo ou em dificuldade grave. § 3º Os navios estrangeiros no mar territorial brasileiro estarão sujeitos aos regulamentos estabelecidos pelo Governo brasileiro.

[68] O regime de passagem inocente não se aplica às águas interiores; para navio com imunidade de jurisdição, normalmente, é requerida a autorização diplomática para acesso a estas águas, bem como às águas interiores de Estados arquipélagos (SCHMITT, 2017b, p. 241).

dado o consentimento para a passagem. Porém, tal prática se presta mais a uma deferência diplomática do que a uma exigência legal, entre os Estados. Tendo em vista o grau de letalidade e alta tecnologia existentes nos meios de guerra naval, a aproximação de tal meio bélico do território de um Estado costeiro, sem as devidas coordenações, pode ser considerada uma grave ameaça ao Estado Costeiro, ou, no mínimo, uma séria provocação (SCHMITT, 2017b, p. 241).

A passagem inocente pode ser suspensa, pelo Estado costeiro, em áreas específicas, por motivos de segurança, mas não pode ser discriminatória[69]. Por exemplo, a passagem pode ser suspensa para a realização de um exercício com emprego de operações cibernéticas, o que poderá representar um risco de segurança cibernética para outros navios.

A passagem inocente não pode se tornar prejudicial[70] para a paz, para a ordem ou para a segurança do Estado costeiro. O Manual de Tallinn 2.0 faz um paralelo com a CNUDM, neste tópico, enumerando uma série de ações, no âmbito cibernético, que podem transformar a passagem inocente em prejudicial. São elas:

> a) Ameaça ilegal de uso de força cibernética contra o Estado costeiro;
> b) Exercício ou prática que envolva o emprego de armas cibernéticas que não se limitem exclusivamente ao navio e seus sistemas[71];

[69] A suspensão deve se aplicar a todos os Estados. (CNUDM, artigo 25º, inciso 3).

[70] A CNUDM elenca as situações que a passagem pode se tornar prejudicial, no artigo 19º, inciso 2: 2. A passagem de um navio estrangeiro será considerada prejudicial à paz, à boa ordem ou à segurança do Estado costeiro, se esse navio realizar, no mar territorial, alguma das seguintes atividades: a) qualquer ameaça ou uso da força contra a Soberania, a integridade territorial ou a independência política do Estado costeiro ou qualquer outra ação em violação dos princípios de Direito Internacional enunciados na Carta das Nações Unidas; b) qualquer exercício ou manobra com armas de qualquer tipo; c) qualquer ato destinado a obter informações em prejuízo da defesa ou da segurança do Estado costeiro; d) qualquer ato de propaganda destinado a atentar contra a defesa ou a segurança do Estado costeiro; e) o lançamento, pouso ou recebimento a bordo de qualquer aeronave; f) o lançamento, pouso ou recebimento a bordo de qualquer dispositivo militar; g) o embarque ou desembarque de qualquer produto, moeda ou pessoa com violação das leis e regulamentos aduaneiros, fiscais, de imigração ou sanitários do Estado costeiro; h) qualquer ato intencional e grave de poluição contrário à presente Convenção; i) qualquer atividade de pesca; j) a realização de atividades de investigação ou de levantamentos hidrográficos; k) qualquer ato destinado a perturbar quaisquer sistemas de comunicação ou quaisquer outros serviços ou instalações do Estado costeiro; l) qualquer outra atividade que não esteja diretamente relacionada com a passagem.

[71] Refere-se aos meios cibernéticos orgânicos do navio e fundamentais para a navegação e comunicação.

> c) Operações cibernéticas voltadas para a coleta de informações prejudiciais à segurança do Estado costeiro;
> d) Distribuição, por meio cibernético, de propaganda que seja prejudicial à segurança do Estado costeiro;
> e) Lançamento ou recebimento de aeronaves, embarcações, ou qualquer outro equipamento militar, que estejam engajados, ou tenham a capacidade de engajar em operações cibernéticas;
> f) Atividades de pesquisa ou avaliação, incluindo aquelas realizadas ou facilitadas por meios cibernéticos;
> g) Operações cibernéticas maliciosas que pretendam interferir com o sistema de comunicações ou qualquer outra instalação do Estado costeiro; e
> h) Qualquer outra atividade cibernética que não tenha relação com a navegação ou comunicações que o navio utilize para a passagem
> (SCHMITT, 2017b, p. 242).

Esta lista não é exaustiva, podendo haver outras situações[72] que sejam aptas para transformar a passagem inocente em prejudicial. O contexto da situação e a dimensão do dano devem ser fundamentais para a mensuração do prejuízo. Por exemplo, se um navio fornece acesso de internet sem fio para um grupo insurgente, estando este sinal bloqueado pelo Estado costeiro, o navio estará executando uma operação proibida. Desta forma, o ideal é que o navio, em passagem inocente, restrinja as operações cibernéticas a bordo. Apenas aquelas operações necessárias para segurança do navio devem ser realizadas.

Segundo o Manual, o grupo de especialistas também abordou a situação na qual o navio, em passagem inocente pelo mar territorial de um Estado, realiza uma operação cibernética nociva contra um 3º Estado. A posição majoritária afirma que "atividades cibernéticas realizadas

[72] Em relação a situação específica, que envolve a execução de avaliação passiva (não intrusiva) de redes cibernéticas sem fio, durante a passagem inocente, também encontra gerou controvérsia no grupo de especialistas. A posição majoritária do grupo defendeu que tal atividade é consistente com a passagem inocente, por ser passiva e não intrusiva. A parcela minoritária defendeu que tal monitoramento seria ilegal e conflitante com os interesses do Estado costeiro (SCHMITT, 2017b, p. 243).

durante a passagem inocente, não podem prejudicar a segurança ou a ordem pública do Estado costeiro, incluindo-se as relações, direitos e deveres com outros Estados". Portanto, se a operação cibernética contra um 3º Estado não afetar a segurança do Estado costeiro, para o grupo majoritário, esta operação é permitida. Para a corrente minoritária, cada caso deve ser analisado em seu mérito, enfatizando que o objeto da passagem inocente é salvaguardar interesses básicos do Estado costeiro e não de 3º Estados, ou atores não estatais. Para eles, uma operação cibernética contra um 3º Estado, ou ator não estatal, não entram diretamente em conflito com o regime da passagem inocente. Ainda segundo o grupo minoritário, para que se avalie se a operação cibernética pode ou não afetar a relação do Estado costeiro com um 3º Estado, devem ser analisados fatores específicos, tais como: a natureza da operação; bem como até que ponto a operação é evidente; e o nível de relação entre o Estado costeiro e o 3º Estado. Ressalta-se que a falta de consenso em relação a este tema tem o potencial de figurar como um sério problema à passagem inocente, principalmente se as operações cibernéticas contra o 3º Estado forem classificadas como espionagem ou guerra cibernética (SCHMITT, 2017b, p. 243).

Para o grupo de especialistas, qualquer navio que esteja em passagem inocente pode e deve executar todas as operações cibernéticas que "sejam necessárias para sua segurança e dos navios que o estiverem acompanhando, contanto que tais operações não prejudiquem a paz, a ordem pública ou segurança do Estado costeiro". Se um navio, durante a passagem inocente, for alvo de operação cibernética hostil, poderá tomar todas as ações cibernéticas necessárias[73] para encerrar a ação hostil (SCHMITT, 2017b, p. 244).

Navios que não possuem imunidade de jurisdição, durante a passagem inocente, podem ser solicitados a obedecer a leis e regulamentos do Estado costeiro, relacionadas às operações cibernéticas. Sobre este tipo de navio, o Estado costeiro tem jurisdição civil e criminal, para algumas hipóteses, quando no mar territorial. Por exemplo, os Estados costeiros podem criar leis relacionadas à segurança de navegação ou proteção de cabos submarinos que restrinjam determinadas operações cibernéticas durante a passagem inocente.

[73] Este procedimento é coerente com o que preconiza o Direito Internacional, incluindo-se, se apropriado, a utilização de contramedidas, ou até mesmo a invocação do princípio da legitima defesa (SCHMITT, 2017b, regras 20 e 71).

Enquanto o Estado costeiro possui determinada jurisdição civil e criminal sobre os navios sem imunidade de jurisdição, engajados em passagem não inocente, esta jurisdição não existe em relação aos navios com imunidade de jurisdição. Caso seja constatado que um navio imune está em passagem não inocente, o Estado costeiro poderá exigir a imediata saída do mesmo das suas águas jurisdicionais. Na opinião do grupo de especialistas, o uso de operações cibernéticas forçadas, que sejam projetadas para obrigar o navio recalcitrante, possuidor de imunidade de jurisdição, a deixar o mar territorial é uma medida permitida disponível para o Estado costeiro. (SCHMITT, 2017b, p. 244).

Esta regra se aplica *mutatis mutandis* à passagem inocente por águas de Estados arquipélagos, pelas quais não passem rotas marítimas, ou onde estas não foram designadas como "rotas normalmente usadas para a navegação internacional".

Exercício da Jurisdição sobre operações cibernéticas no Mar Territorial:

Sobre a jurisdição das operações cibernéticas realizadas no mar territorial do Estado costeiro, a regra 50, do Manual de Tallinn 2.0, que está relacionado com o art. 27º da CNUDM, preconiza que "**o Estado costeiro poderá exercer jurisdição a bordo de navios, em seu mar territorial, no que tange às atividades criminosas que envolvam operações cibernéticas se: a consequência do crime se estenda ao Estado costeiro; se o crime for capaz de causar distúrbios na ordem pública e na segurança do Estado costeiro, ou na boa ordem do mar territorial; se o Comandante do navio, ou o Estado de bandeira tiver solicitado tal ação às autoridades do Estado costeiro; se for uma ação necessária de combate ao tráfico internacional de drogas**" (SCHMITT, 2017b, p. 246).

Como regra geral, a CNUDM estabelece em seu artigo 27 que as autoridades do Estado costeiro não podem prender tripulantes, apresar navios ou conduzir investigação a bordo de navios com bandeiras de outros Estados, durante a presença destes navios em águas territoriais do Estado costeiro, salvo nos seguintes casos: a) se a infração criminal tiver consequências para o Estado costeiro; b) se a infração criminal for de tal natureza que possa perturbar a paz do país ou a ordem no mar territorial; c) se a assistência das autoridades locais tiver sido solicitada pelo capitão do navio ou pelo representante diplomático ou funcionário consular do Estado de bandeira; ou d) se essas medidas forem necessárias para a repressão do tráfico ilícito de estupefacientes ou de substâncias psicotrópicas.

Em relação à noção de "extensão de consequências" prevista no art. 50º do Manual de Tallinn 2.0, para as operações cibernéticas executadas a bordo de um navio em passagem por águas jurisdicionais de um Estado costeiro, o grupo de especialistas concordou que o Estado costeiro poderá exercer jurisdição a bordo de um navio em passagem pelo seu mar territorial se a operação cibernética oriunda deste navio violar o direito penal deste Estado e se manifestar claramente em seu território[74], incluindo-se o mar territorial (SCHMITT, 2017b, p. 246).

No que tange à escala de manifestação das consequências da operação cibernética ilícita, o grupo de especialistas ficou dividido. A corrente minoritária defende que consequências mínimas ou triviais não justificariam o exercício da jurisdição criminal por parte do Estado costeiro. Para o grupo majoritário, "qualquer grau de violação será suficiente para que o Estado costeiro possua esta prerrogativa". Houve consenso no grupo de especialistas no sentido de reconhecer que qualquer operação cibernética, conduzida por navio estrangeiro, no mar territorial do Estado costeiro, que possua efeitos generalizados[75] e, por conseguinte, perturbe o Estado costeiro, será suficiente para dar o direito, ao Estado costeiro, de exercer a jurisdição criminal a bordo do navio em tela (SCHMITT, 2017b, p. 244).

Atividades cibernéticas relacionadas ao tráfico de drogas ilícitas são base para o exercício da jurisdição criminal do Estado costeiro, em relação à navios que estejam em seu mar territorial. Considere a situação na qual um Estado está monitorando as comunicações cibernéticas de certas embarcações, localizadas em seu mar territorial, com base em dados fornecidos às autoridades policiais. Caso as autoridades identifiquem quaisquer comunicações indicando que a embarcação está sendo usada para o transporte ilegal de drogas, elas podem usar meios cibernéticos para facilitar a abordagem e parada da embarcação (SCHMITT, 2017b, p. 247).

O Manual afirma ainda que, no caso da ocorrência de uma atividade cibernética, que se constitua crime, segundo a lei doméstica, a bordo de um navio estrangeiro, antes que ele deixe o mar territorial, justifica também que o Estado costeiro exerça a jurisdição criminal a bordo daquele

[74] Por exemplo, uma operação de Negação de Serviço (*Distributed Denial-of-Service* -DDoS) iniciada de dentro de um navio contra uma infraestrutura cibernética do Estado costeiro, que viole a lei doméstica deste (SCHMITT, 2017b, p. 247).

[75] A interferência na ordem pública do mar territorial pode ser efetuada com a efetivação de uma operação cibernética que interfira nos sistemas de navegação dos navios no mar territorial e / ou com o sistema de comunicação entre os navios e as agências em terra de segurança para a navegação (SCHMITT, 2017b, p. 247).

navio. Diferentemente da jurisdição criminal, o Estado costeiro não poderá exercer jurisdição civil sobre atividades cibernéticas em navios estrangeiros que estiverem passando pelo mar territorial (SCHMITT, 2017b, p. 248).

Acordos bilaterais entre Estados podem modificar a dinâmica de aplicação da regra de jurisdição no mar territorial, bem como a situação de Conflito Armado, na qual o Estado neutro deve tomar todas as medidas possíveis para garantir o direito de mera passagem de Navios de Guerra de Estados beligerantes, por seu mar territorial. Ressalta-se também que uma Resolução do CSNU pode permitir operações cibernéticas dentro do mar territorial de um Estado costeiro, mesmo que tais operações possam descaracterizar a passagem inocente.

Operações cibernéticas na Zona Contígua (ZC)

Sobre a jurisdição das operações cibernéticas realizadas na zona contígua do Estado costeiro, a regra 51, do Manual de Tallinn 2.0, que está relacionado com o art. 33 da CNUDM, preconiza que "**no que diz respeito às embarcações localizadas na zona contígua de um Estado costeiro, esse Estado pode usar meios cibernéticos para impedir ou solucionar violações de suas leis fiscais de imigração, sanitárias ou alfandegárias, ocorridas em seu território ou no mar territorial, incluindo violações cometidas por meios cibernéticos**" (SCHMITT, 2017b, p. 248).

Os Estados podem reivindicar uma zona contígua, que se estende do limite do seu mar territorial até vinte e quatro milhas náuticas, tendo como referência a linha de base[76]. Na área da zona contígua, o Estado costeiro desfruta de duas prerrogativas de autoridade. A primeira é o direito soberano de fazer cumprir suas leis fiscais, de imigração, sanitárias e aduaneiras, contra embarcações suspeitas de violá-las enquanto estiveram nas águas internas do Estado costeiro ou no mar territorial[77] (SCHMITT, 2017b, p. 248).

A embarcação que violou leis fiscais, de imigração, sanitárias ou aduaneiras, seja por meio cibernético ou por outros meios, estiver na zona contígua, o Estado costeiro pode interditar a embarcação antes de sua partida ou abrir perseguição[78], respeitando o direito internacional, para fazê-la retornar ao porto para investigação ou abertura de processo. Para esta situação, o Estado

[76] CNUDM Art. 33º(2).
[77] CNUDM, Art. 33º (1)(b).
[78] CNUDM, Art. 111º.

costeiro pode usar meios cibernéticos como parte da operação de interdição. Por exemplo, ele pode controlar o movimento da embarcação delinquente, por meios cibernéticos, e direcioná-la de volta para as embarcações policiais (SCHMITT, 2017b, p. 248).

A outra prerrogativa de autoridade concedida ao Estado costeiro, em relação às questões de fiscalização na zona contígua, é a da prevenção[79]. Essa prerrogativa permite que o Estado costeiro use meios cibernéticos para avisar e impedir que uma embarcação, que esteja na zona contígua, execute uma violação das leis fiscais, de imigração, sanitárias e aduaneiras (SCHMITT, 2017b, p. 249).

Operações cibernéticas em estreitos internacionais e águas de Estados arquipélagos

As regras 52 e 53, do Manual de Tallinn 2.0, que estão relacionados com o Art. 41º e 46º da CNUDM preconizam que: "**regra 52- As operações cibernéticas em estreitos utilizados para a navegação internacional devem ser consistentes com o direito de passagem em trânsito" e "regra 53- As operações cibernéticas em águas de Estados arquipélagos devem ser consistentes com o direito de passagem em trânsito**" (SCHMITT, 2017b, p. 249; 250).

Os estreitos são as porções de mar utilizadas para a navegação internacional entre uma parte do alto-mar ou uma zona econômica exclusiva de um ou mais Estados, e uma outra parte do alto-mar, ou uma zona econômica exclusiva, de um ou mais Estados.

Nesta porção do mar o instituto utilizado para a navegação é o instituto da passagem em trânsito[80] e ela se difere da passagem inocente pelos seguintes pontos: "a passagem em trânsito não pode ser suspensa por nenhum dos Estados costeiros; as aeronaves também possuem o direito de passagem em trânsito; e aviões e navios podem passar em seu modo normal (um submarino pode passar submerso)" (SCHMITT, 2017b, p. 250).

Para o Manual, as atividades cibernéticas que são inconsistentes com o regime de passagem em trânsito não podem ser executadas durante a passagem. Apenas as "atividades cibernéticas relacionadas à segurança de navegação e comunicações do navio podem ser executadas". Operações cibernéticas beligerantes não são permitidas neste regime de passagem (SCHMITT, 2017b, p. 250).

[79] CNUDM, Art. 33º(1)(a).

[80] CNUDM, Art. 34.

Navios e aeronaves com imunidade de jurisdição, que executarem operações cibernéticas que violem a legislação do Estado costeiro, não serão objeto da jurisdição deste, mas "poderão ser solicitados a se retirarem do estreito"[81]. O Estado de bandeira destes navios ou aviões podem ser responsabilizados internacionalmente por qualquer dano ou perda que tais operações puderem causar nos Estados costeiros (SCHMITT, 2017b, p. 251).

Os Estados arquipélagos podem designar rotas marítimas para passagem do tráfego internacional marítimo nas quais os navios também possuirão o direito de passagem e que deverá ser realizada aos mesmos moldes da passagem inocente por mar territorial. Porém, em relação às operações cibernéticas executadas de bordo, as regras são as mesmas para a passagem em trânsito.

Os Cabos submarinos de comunicação:

Segundo a regra 54, do Manual de Tallinn 2.0, que está relacionada com o art. 112º da CNUDM, "**as regras e princípios de Direito Internacional aplicáveis aos cabos e dutos submarinos também se aplicam aos cabos submarinos de comunicação**". (SCHMITT, 2017b, p. 252).

Sabe-se que os cabos submarinos de comunicações estão sujeitos a danos, desgastes e a intercepção para coleta de dados, por meio de manipulação técnica[82], que pode ser realizada também para proporcionar um "engarrafamento" ou "alteração" dos dados que por eles transitam.

A questão do lançamento de cabos submarinos de comunicações desperta muito interesse para aqueles países que não consideram a prática da espionagem, em tempo de paz, como prática reprovável nas Relações Internacionais. Com o veloz avanço da tecnologia, supõe-se que veículos submersíveis não tripulados sejam capazes de manipular cabos submarinos de comunicações. Será visto, ainda nesta seção, que algumas conclusões atingidas pelo grupo de especialistas do Manual de Tallinn 2.0, que em sua maioria é formado por especialistas oriundos de países da OTAN, que respaldam a espionagem como prática comum em tempos de paz, não são muito bem aceitas pela Constituição brasileira de 1988.

Os direitos soberanos do Estado costeiro, no que tange ao mar territorial, também se estende aos cabos submarinos lançados nas suas plataformas continentais. Tais cabos possuem o mesmo regime jurídico

[81] CNUDM, Arts. 34º, 38º(3).

[82] Manual de Tallinn 2.0. (SCHMITT, 2017b, p. 254).

das estruturas cibernéticas localizadas no território terrestre deste Estado. Portanto, no mar territorial, os Estados costeiros possuem o direito de legislar[83] sobre as atividades de lançamento, manutenção, reparo e substituição dos cabos submarinos de comunicação, bem como de adotar leis e regulamentações também a respeito de sua proteção. No entanto, tais leis ou regulamentos não podem impor restrições à passagem inocente. (SCHMITT, 2017b, p. 253).

Em relação à ZEE ou Plataforma Continental, qualquer Estado pode lançar cabos[84] submarinos de comunicações, contanto que respeite os direitos de soberania limitada que o Estado costeiro possui naquela faixa do mar. Os Estados costeiros não podem proibir tal ação. Embora o traçado de linha de dutos pela Plataforma Continental possa estar sujeito ao consentimento prévio do Estado costeiro, tal regra não se aplica em relação aos cabos submarinos de comunicação. Tal ação somente poderá ser impedida pelo Estado costeiro caso tal medida seja considerada uma "razoável[85] ação de exploração de seus recursos naturais" (SCHMITT, 2017b, p. 254).

Os Estados sem saída para mar, a fim de exercerem o direito relacionados à liberdade de se utilizarem do alto-mar[86], bem como o direito de conectarem suas estruturas cibernéticas ao mundo, deverão ajustar, por meio de tratado bilateral, o trânsito dos cabos de comunicação pelo território dos Estados costeiros, para que tais cabos possam chegar e sair de seu território[87].(SCHMITT, 2017b, p. 255).

Existe uma prática consagrada no Direito Internacional que reconhece que o direito de lançar os cabos submarinos de comunicações vem acompanhado pelos direitos acessórios[88] de executar todas as medidas

[83] O Estado arquipélago também possui o direito de legislar sobre o lançamento de cabos submarinos de comunicações e devem autorizar o reparo de tais cabos, quando isto for solicitado por outro Estado. (SCHMITT, 2017b, p. 255).

[84] Não houve consenso no grupo de especialistas em relação ao conflito de soberanias existentes na questão do lançamento de cabos submarinos de comunicação, na ZEE. Para uma boa parte do grupo, deve-se fazer uma deferência ao Estado costeiro, mas sem deixar de considerar que tal lançamento está diretamente relacionado ao princípio da liberdade do alto-mar. (SCHMITT, 2017b, p. 256).

[85] O sentido da palavra não foi definido pelo grupo de especialistas.

[86] CNUDM Art. 125(1) e Art. 124(1)(a).

[87] CNUDM, Art. 125º (2–3).

[88] A CNUDM só prevê o caso de substituição para os cabos antigos de Estados arquipélagos, porém a opinião majoritária do grupo de especialistas foi no sentido de que os Estados possuem o direito de efetuarem a substituição, principalmente no caso dos cabos que estiverem fora do mar territorial do Estado costeiro. Para estes especialistas, tais cabos são cruciais para a economia e para a segurança dos Estados que os lançaram. A corrente minoritária sustentou que o direito de substituição de cabos antigos somente

preparatórias para identificação de rotas apropriadas, bem como o direito de manutenção e reparo. Aos Estados que lançarem tais cabos também é franqueado o direito de monitoramento e inspeções regulares.

Não está claro na CNUDM se os Estados poderiam estabelecer "zonas de proteção", nas quais seriam restritas às atividades de ancoragem de navios, pesca de arrasto e mineração de areia, uma vez que tais atividades se constituem em ameaças à integridade dos cabos submarinos de comunicações. Ressalta-se que a Austrália e a Nova Zelândia possuem corredores / zonas de proteção de cabos submarinos de comunicação no mar territorial e na ZEE. O Direito Internacional prevê base legal para o estabelecimento de corredores / zonas de proteção de cabos no mar territorial apenas.

"A danificação proposital de cabos submarinos, resguardadas as regras do DICA, é proibida". Seria incoerente estabelecer a permissão para o lançamento de cabos aos Estados e, ao mesmo tempo, permitir que outros Estados pudessem destruir tais cabos. Porém, fica claro pelo manual, que "em caso de ações de guerra naval, caso o comandante da operação militar em andamento consiga justificar que a danificação do cabo se constitui em peça fundamental para a manobra, a ação poderá ser autorizada"[89]. Porém, tal ação não poderá causar sofrimento desnecessário à população civil, ou se constituir em grave ofensa aos Direitos Humanos. (SCHIMITT, 2017b, p. 256).

O grupo de especialistas concordou que a manipulação física dos cabos submarinos de comunicação, para coleta de dados, em águas de Estados arquipélagos e no mar territorial do Estado costeiro se constitui em grave violação da soberania dos respectivos Estados. Bem como entendeu que a utilização de veículo submarino não tripulado é inconsistente com o regime da passagem inocente. Na visão dos especialistas, para tais casos, apenas o Estado costeiro e o Estado arquipélago possuem suas Soberanias violadas, o que não ocorre com o Estado que lançou o cabo. Para o grupo, a manipulação fora das águas jurisdicionais não se constitui em violação de soberania. Na opinião do autor do presente artigo, este entendimento abre uma brecha considerável para a insegurança jurídica internacional e pode se traduzir em um franco convite para a espionagem entre Estados (SCHMITT, 2017b, p. 257).

existe para Estados arquipélagos, conforme preconiza a CNUDM. Em relação ao direito de manutenção e reparo, todos concordaram que o mesmo é franqueado aos Estados (SCHMITT, 2017b, p. 256).

[89] Manual San Remo, 1994.

PONTOS DE CONVERGÊNCIA ENTRE O MANUAL DE SAN REMO E O MANUAL DE TALLINN 2.0

Nesta seção serão abordadas as principais questões relacionadas às regras estabelecidas pelo Manual de San Remo, para a guerra naval, sob o ponto de vista do Manual de Tallinn 2.0. Cabe ressaltar que alguns conceitos já foram abordados na seção anterior, quando aludimos diretamente à CNUDM.

O Manual de San Remo constitui-se, basicamente, de uma adaptação das regras do DICA aplicado ao combate terrestre às peculiaridades da guerra naval. Desta forma, todos os princípios que regem o combate terrestre, tais como Necessidade Militar, Humanidade, Proporcionalidade e Distinção, estarão presentes nas regras para o combate naval e serão também respeitados pelo Manual de Tallinn 2.0.

Os especialistas do Manual de Tallinn 2.0 se preocuparam em estabelecer uma regra especial que tratasse da passagem de navios, tanto de Estados beligerantes, quanto de Estados neutros, pelo mar territorial de Estados costeiros, com a finalidade de estabelecer uma norma única de comportamento no que tange à execução de operações cibernéticas A preocupação da doutrina, neste caso, é tanto a de resguardar os direitos de Estados costeiros neutros como a de permitir que Estados beligerantes mantenham suas campanhas sem violar direitos alheios.

Operações cibernéticas no Mar Territorial durante um Conflito Armado:

Sobre a realização de operações cibernéticas durante um conflito armado, a regra 49, do Manual de Tallinn 2.0, que possui relação com a Seção I da Parte II do Manual de San Remo, a firma que "**durante um Conflito Armado internacional, um Estado costeiro neutro não pode fazer discriminação entre as partes beligerantes no que tange à realização de operações cibernéticas em seu mar territorial**" (SCHMITT, 2017b, p. 245).

Durante o período que durar um Conflito Armado Internacional[90] as regras para os conflitos armados no mar (Manual de San Remo) e da neutralidade se sobrepõem à CNUDM. A lei da neutralidade[91] proíbe as partes beligerantes de usarem os portos e as águas neutras, como bases de operações, contra o adversário. Mas os países neutros podem permitir, mas

[90] Regra 82 do Manual de Tallinn 2.0 (SCHMITT, 2017b, 2017).

[91] Convenção de Haia XIII, art. 9º.

não são obrigados, o exercício do direito de mera passagem em seus mares territoriais pelos países beligerantes. Podem também impor condições para este direito, que deverão se aplicar para todas as partes beligerantes (SCHMITT, 2017b, p. 245).

Durante a mera passagem, os Navios de Guerra não podem utilizar as águas dos países neutros como base de operações contra seus adversários, ou engajar em atividades beligerantes[92]. Isto inclui operações cibernéticas contra os adversários. Porém, as atividades cibernéticas necessárias à segurança do Navio de Guerra poderão ser executadas. Pelo entendimento do Manual de Tallinn 2.0, os Estados beligerantes não podem dirigir operações cibernéticas agressivas[93], de fora das águas neutras, contra um Navio de Guerra que estiver executando a mera passagem (SCHMITT, 2017b, p. 245).

Pela convenção de Haia[94], de 1907, o país beligerante é proibido de erguer qualquer tipo de infraestrutura de comunicação, de dentro das águas neutras, para se comunicar com tropas em terra. Por analogia, os especialistas entenderam que esta regra também se aplica às infraestruturas cibernéticas.

Caso um Estado beligerante resolva executar um ataque cibernético ou uma ação maliciosa de dentro do mar territorial de um Estado neutro, este Estado pode se valer de contramedidas para fazer cessar o ato ilegal do navio do Estado beligerante.

Utilização de Contramedidas:

Em relação à utilização de contramedidas, a regra 20, do Manual de Tallinn 2.0, preconiza que "**um estado pode ter o direito de tomar contramedidas, sejam elas cibernéticas ou não, em resposta a uma violação de uma obrigação legal internacional devida por outro Estado**" (SCHMITT, 2017b, p. 111).

Esta regra se faz de suma importância para o Estado costeiro neutro, que em uma situação de Conflito Armado Internacional deve realizar todas

[92] Atividades militares relacionadas ao Conflito Armado.

[93] Para o grupo de especialistas, geralmente é difícil para um Estado neutro conseguir observar uma operação cibernética agressiva, que tenha origem de um Navio de Guerra beligerante que esteja fora de suas águas jurisdicionais, porém, se o Estado neutro tomar conhecimento de tais atividades, a lei da neutralidade impõe que o Estado neutro tenha que cessar tal atividade. Podendo ser efetuado, mas não apenas, por meio de operações cibernéticas. (SCHMITT, 2017, p. 245).

[94] Convenção de Haia XIII, art. 5º.

as ações ao seu alcance para evitar que seu território seja utilizado por uma das partes beligerantes para obter vantagem sobre a outra.

No que tange à guerra naval, tais ações só podem serem tomadas pelo Estado neutro que tem afetado o seu dever de Devida Diligência. Devendo ser na justa medida para que o navio infrator do Estado beligerante cesse sua ação ilegal. A contramedida não precisa, necessariamente, ser por uma operação cibernética, pode se constituir em uma ação física, ou diplomática. A contramedida, inclusive, pode envolver a realização de ações que, sob condições normais, poderiam ser consideradas ilegais.

Cabe diferenciar a contramedida da "ação de represália[95]" entre Estados beligerantes, na situação de um Conflito Armado internacional. A represália, entre beligerantes de um conflito armado, consiste na tomada de ações normalmente ilícitas, por parte de um deles, contra o adversário, em resposta a ações ilícitas deste último e com o propósito exclusivo de persuadi-lo a respeitar o direito da guerra. Mas as represálias não podem ser consideradas contramedidas pelo fato de serem efetuadas entre beligerantes e conservarem um nexo de causalidade com o Conflito Armado. No entanto, as contramedidas podem ser tomadas, de forma cibernética ou não, como resposta a uma ação realizada por uma das partes que viole um regime legal que não seja o DICA. Cabe ressaltar que as contramedidas não podem ser executadas contra um ator não estatal, a não ser que este esteja agindo em nome de um Estado (SCHMITT, 2017b, p. 112).

Desta forma, um Estado costeiro poderá executar todas as ações ao seu alcance para fazer cessar uma operação cibernética maliciosa ou até mesmo uma ação de guerra cibernética que esteja sendo executada de dentro do seu mar territorial.

O Bloqueio Naval e Zona de Exclusão:

As regras 128 e 130, do Manual de Tallinn 2.0, que estão relacionados com os parágrafos 93 e 105, do Manual de San Remo,

[95] A represália constitui um costume consuetudinário do DICA, condicionado ao atendimento de 5 requisitos, para ser considerado válido: 1. Só é permitida em caso de grave violação ao DICA/ DIH e deve ter o propósito exclusivo de induzir o inimigo a respeitar as normas do Direito da Guerra; II. A represália só deve ser empregada como último recurso; III. A represália deve ser proporcional à violação que se deseja cessar; IV. A decisão da represália deve caber ao nível mais elevado do governo; e V. A represália deve cessar assim que o adversário passar a respeitar o Direito". Referência. ICRC. IHL Data Base. Rule 145. Reprisals.

preconizam o seguinte: "**Regra 128 - Métodos e meios de guerra cibernética podem ser utilizados para a manutenção de um bloqueio naval ou aéreo, sozinhos em combinação com outros métodos, contanto que não resultem em ações inconsistentes com o Direito Internacional dos conflitos armados." e "Regra 130 - Na medida em que os Estados estabelecerem zonas, seja em tempo de paz ou durante os conflitos armados, as operações cibernéticas lícitas podem ser usadas para que exerçam seus direitos em tais zonas**" (SCHMITT, 2017b, p. 508; 510).

Para a lei da guerra naval, o bloqueio[96] é um método de guerra que consiste de uma operação beligerante para impedir a entrada e/ou a saída de navios e aviões, inimigos ou neutros, em portos específicos, aeroportos, ou áreas costeiras pertencentes, ocupadas ou sob o controle de um Estado beligerante. Ele pode ser estabelecido como parte de uma operação militar direcionada a uma Força militar inimiga ou como uma operação de caráter econômico, com a finalidade estratégica de enfraquecer a Força militar do inimigo pela degradação de sua economia. Para Farey (2017), o bloqueio naval do futuro poderá ser executado inteiramente a partir de um *laptop*.

Tendo em vista o avanço tecnológico de computadores e sistemas computacionais que aparelham os aviões e navios, os meios cibernéticos podem ser utilizados para estabelecer ou reforçar um bloqueio naval ou aéreo. A grande questão é definir se o uso de meios cibernéticos para bloquear comunicações cibernéticas, neutras ou inimigas, para ou do território inimigo, ou áreas sob seu controle, conhecido como "bloqueio cibernético[97], está ou não sujeito à lei que rege os bloqueios tradicionais em tempos de Conflitos Armados.

Uma pequena minoria de especialistas considerou que tal operação cibernética seria um mero "bloqueio eletrônico", que se

[96] Segundo o Manual de San Remo, os elementos que caracterizam um bloqueio são os seguintes: ele deve ser declarado e notificado; o começo, a duração, a localização e a extensão devem constar na declaração; o bloqueio deve ser efetivo; as Forças de manutenção do bloqueio devem estar estacionadas a uma distância da costa determinadas pelas necessidades militares; uma combinação de métodos legais e métodos de guerra deve reforçar o bloqueio; o acesso a portos, a costa e a aeroportos neutros não podem ser bloqueados; a cessação, suspensão, reestabelecimento, ou outra alteração do bloqueio deve ser declarada e notificada; e o bloqueador deve aplicar o bloqueio imparcialmente para aviões e navios de todos os Estados (MANUAL DE SAN REMO, 1996, art. 94º a 104º).

[97] Esta questão gerou muitos debates no grupo de especialistas e tais debates giraram em torno da aplicabilidade dos critérios estabelecidos para a concretização de um bloqueio, para o contexto cibernético, a viabilidade técnica de realização de um bloqueio cibernético, e, então, a caracterização das regras para o bloqueio cibernético como *lex lata* ou *lex ferenda*. (SCHMITT, 2017b, p. 506).

confundiria com a guerra eletrônica. "A maioria foi da opinião que um bloqueio naval ou aéreo é geralmente estabelecido para criar um efeito particular[98] que pode ser atingido com o emprego de meios cibernéticos". O estabelecimento de um bloqueio naval, tradicional, requer a especificação de uma linha geográfica particular que os navios não poderão cruzar. Isto levantou a dúvida se uma linha similar pode ser articulada na declaração de um bloqueio cibernético e se tecnicamente seria possível executar o bloqueio de todos os meios de comunicação cibernéticas nesta linha. Os assessores técnicos afirmaram que é possível realizar ambas as ações (SCHMITT, 2017b, p. 506).

Uma das dificuldades de se adaptar as regras do bloqueio naval tradicional para o âmbito das operações cibernéticas está no fato de que o bloqueio Naval envolve a proibição de acesso a portos ou áreas marítimas ou costeiras. Desta forma, em virtude da relativa liberdade de navegação dos navios neutros, este tipo de bloqueio só se faz eficaz e legítimo quando executados de forma a não interferem com os direitos dos Estados neutros. A minoria do grupo de especialistas aplicou esse paradigma estritamente no contexto cibernético, e chegaram à conclusão de que seria conceitualmente impossível estabelecer um bloqueio cibernético, nos moldes do que estabelece o Manual de San Remo. A maioria concluiu que um bloqueio cibernético é uma noção significativa, no contexto da guerra naval, porque pode ser efetivamente lançado apenas a partir de um território beligerante sem romper a neutralidade dos estados adjacentes (SCHMITT, 2017b, p. 505).

O grupo internacional de especialistas discutiu muito sobre o qual seria o parâmetro de efetividade de um bloqueio naval clássico e sua aplicação aos bloqueios cibernéticos. Uma minoria de especialistas considerou que a eficácia suficiente era inatingível, porque as comunicações a serem bloqueadas poderiam ser obtidas por outros meios, como rádio e telefone. Entretanto, a maioria dos especialistas chamou a atenção para o fato de que o transporte de materiais, por via aérea, que não podem ser transportados por mar devido a um bloqueio naval, não torna o bloqueio naval ineficaz e vice-versa (SCHMITT, 2017b, p. 506).

[98] Como exemplo o bloqueio que é criado para atingir efeitos econômicos negativos na economia inimiga, uma vez que a atividade econômica é conduzida, em grande parte, por comunicação via internet, o grupo majoritário de especialistas concluiu que seria razoável aplicar a lei do bloqueio em operações militares planejadas para bloquear as comunicações cibernéticas em um território sob o controle do inimigo (SCHMITT, 2017b, p. 505).

Um bloqueio naval cibernético pode ser completado por outros meios, além dos cibernéticos, como por exemplo: combinação de operações cibernéticas (negar o acesso a um roteador de internet pela modificação das tabelas de roteamento), com uma ação de guerra eletrônica (empregando interferidores para afetar às transmissões de rádio do inimigo) e com meios cinéticos também (derrubar o serviço de internet e destruir os centros de internet do inimigo por meio de um ataque aéreo ou bombardeio naval). Porém, deve-se estar atento para que tais ações não afetem os Estados neutros (SCHMITT, 2017b, p. 506).

Resumindo, alguns especialistas rejeitaram completamente a ideia de adaptação do bloqueio naval cibernético às regras existentes para o bloqueio naval tradicional, do Manual de San Remo. Outros especialistas aceitaram esta adaptação conceitualmente, mas entenderam a dificuldade prática de adaptação dos conceitos, ou até mesmo tiveram enfoques diferentes em relação à aplicabilidade no contexto cibernético. Alguns outros acreditaram que o conceito de bloqueio naval cibernético é legítimo, está em consonância com o DICA, tem adaptabilidade com o conceito tradicional do bloqueio naval e são exequíveis do ponto de vista prático e técnico. Tendo em vista que os especialistas não conseguiram chegar a um consenso mínimo, em relação a possibilidade de estabelecimento do bloqueio naval cibernético, os artigos 128 a 130 se limitam a abordar como as operações cibernéticas podem ser usadas em apoio ao bloqueio naval clássico.

A condução de operações cibernéticas em apoio a um bloqueio naval pode ser uma excelente ferramenta na mão de um comandante, a fim de manter a efetividade do bloqueio. Operações cibernéticas que visem o acesso remoto ao sistema de propulsão e navegação de um navio é um bom exemplo do tipo de operação que poderá ser utilizada em apoio a um bloqueio naval. Cabe ressaltar que qualquer uso de meios ou métodos cibernéticos, no contexto de uma guerra naval para o reforço de um bloqueio, estará sujeito às regras para condução da guerra naval. A distinção entre objetivos civis e milites e o princípio da proporcionalidade devem ser observados. Se as operações cibernéticas em apoio ao bloqueio naval causarem danos à população civil, aos navios neutros ou forem desproporcionais à vantagem militar alcançada, este bloqueio será ilegal. As ações cibernéticas em apoio ao bloqueio não podem afetar o acesso dos países neutros às suas estruturas cibernéticas ou às suas comunicações cibernéticas.

Em relação à aplicação do conceito de "zonas de exclusão naval", já sedimentado na doutrina naval da maioria dos Estados, desde

a edição do Manual de San Remo, tais zonas não são áreas de fogo livre ou de guerra irrestrita. Ao invés disto, tratam-se de áreas que são especificamente demarcadas, em um teatro de operações marítimas, que permanecem vinculadas ao Direito Internacional aplicado à guerra naval. Navios neutros e outros meios que gozem de proteção, pelo Direito Internacional, preservam sua proteção quando atravessando tais zonas, mesmo que ignorem as instruções da parte beligerante que estabeleceu a referida zona (SCHMITT, 2017b, p. 508).

No que tange ao estabelecimento de uma "zona de exclusão naval" cibernética, segundo os especialistas, dois contextos foram analisados: o uso de meios e métodos cibernéticos para o reforço do estabelecimento de uma "zona de exclusão naval" e o estabelecimento, propriamente dito, de uma "zona de exclusão naval cibernética". A primeira abordagem pode ser implementada, conforme foi visto com relação ao bloqueio naval. Já quanto à segunda abordagem, os especialistas enfatizaram a dificuldade de se delimitar uma "zona" no espaço cibernético. Além disso, o cumprimento do que o Manual de San Remo preconiza para o estabelecimento de uma "zona de exclusão naval" pode ser tecnicamente desafiador, uma vez que, em muitos casos, as comunicações cibernéticas podem se basear em uma infraestrutura cibernética sobre a qual o operador não terá o controle. Desta forma, o estabelecimento de uma "zona de exclusão cibernética" no mar, sob o ponto de vista do Direito Internacional, é algo bem difícil. Ações cibernéticas de detecção podem ser empregadas em proveito das atividades de controle de uma Zona de Exclusão, bem como operações que proporcionem uma visita cibernética em navios suspeitos de desrespeitar as regras da zona (SCHMITT, 2017b, p. 508).

CONCLUSÃO

A Era da Informação chegou para modificar completamente a arte da guerra. Além das armas cinéticas arrasadoras, conhecidas há tempos pela humanidade, surge uma nova dimensão do combate, cujas parafernálias tecnológicas, apesar de atuarem de modo sorrateiro e subreptício, possuem um potencial extremamente letal, capaz de causar desde simples congestionamentos de dados até destruição e morte em larga escala.

A soberania do Estado, outrora inabalável elemento de evidência do poder estatal, chega ao século XXI sob séria ameaça desta nova dimensão da guerra. O espaço cibernético, que até então figurava como palco de

anarquia, se encontra com o Direito Internacional e vagarosamente vai obtendo contornos de legalidade, que se prestam à manutenção da Paz e Segurança internacionais.

Em relação à guerra naval, ainda existe um caminho considerável a ser desbravado, mas a regulação de operações cibernéticas, desenvolvidas a bordo das belonaves, sob o foco do Direito Internacional Humanitário, já pode ser considerada um passo extremamente importante para o contexto da guerra no mar.

Cabe o cuidado e a diligência com a defesa cibernética da Amazônia Azul. O Brasil precisa estar atento para os trabalhos, ainda que lentos, de normatização do ciberespaço, para que não tenha seus interesses estratégicos atingindos.

Acredita-se que, em um futuro não muito distante, os guerreiros se apresentem em compartimentos segregados, de bases secretas, para empreenderem um combate diferente, que em contraste com o silêncio e clandestinidade peculiares, se mostrará assustadoramente ameaçador.

INTERNATIONAL LAW AND THE CYBERNET DEFENSE OF SOVEREIGNTY IN THE BLUE AMAZON: AN APPROACH IN THE LIGHT OF THE TALLINN 2.0 MANUAL

ABSTRACT

In 2013, the first Tallinn Manual on International Law Applicable to Cyber Operations was published and that manual referred only to cyber operations in times of war. The second manual, published in 2017, also considered cyber operations carried out in peacetime. Bearing in mind the importance of the regulation of cyberspace for naval warfare, this article proposes to analyze the rules suggested by the emerging International Law Applied to Cybernetic Operations, for activities that are carried out in the context of naval operations. Thus, the research employs the literature review method, based on primary and secondary sources, such as the report of the UN Governmental Experts Group (UNGGE), the Tallinn 2.0 Manual and scientific articles on the subject. It is noteworthy that Tallinn Manual 2.0 promoted the meeting of the emerging International Law Applicable to Cybernetic Operations with the consolidated Law of "Naval War". This meeting generates legal perceptions that must be carefully evaluated.

Keysword: International Cyber Law; Cyberwarfare; Naval Operations.

REFERÊNCIAS

ACCIOLY, Hildebrando; SILVA, Geraldo Eulálio do Nascimento. **Manual de Direito Internacional público**. 12. ed. São Paulo: Saraiva, 1996.

BHATTI, Jahshan; HUMPHREYS, Todd. Hostile control of ships via false GPS signals: Demonstration and detection. **Journal of the Institute of Navigation**, *[S.L]*, v. 64, n. 1, p. 51-66, 2017.

BRASIL. **Decreto no 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília – DF: Presidência da República, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em: 11 set. 2021.

BRASIL. **Decreto nº 75.963, de 11 de julho de 1975**. Promulga o Tratado da Antártida. Brasília – DF: Presidência da República, 1975.

BROZOSKI, Fernanda Pacheco de Campos. A Disputa Global por Recursos Energéticos Oceânicos e sua Repercussão na Geopolítica Mundial da Energia. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 25, n. 1, p. 63-88. jan./abr. 2019. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/796. Acesso em: 28 set. 2021.

CHOY, Yeong. Prescriptive Jurisdiction in the Law of the Sea: Cases of Contentions and Evolution. **Journal of Territorial and Maritime Studies**, [S.l.: s.n.], 2019. Disponível em: https://www.journalofterritorialandmaritimestudies.net/post/2019/12/13/prescriptive-jurisdiction-in-the-law-of-the-sea-cases-of-contentions-and-evolution. Acesso em: 23 set. 2022.

CORN, Gary; TAYLOR, Robert. Sovereignty in the age of cyber. *In:* Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0. **American Journal of International Law**, EUA, v. 111, p. 207-212, 22 Aug. 2017. Disponível em: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-the-age-of-cyber/02314DFCFE00BC901C95FA6036F8CC70. Acesso em: 10 jul. 2021.

FAHEY, Sean. Combating "ciber fatigue" in the maritime domain. **Humanitarian Law & Police**, [*S.l.*: s. n.], 7 Dec. 2017 Disponível em: https://blogs.icrc.org/law-and-policy/2017/12/07/combating_cyber-fatigue-in-the-maritime-domain/. Acesso em: 22 set. 2021.

FERREIRA, Pinto. **Teoria Geraldo Estado**. 2. ed. ampliada e atualizada. São Paulo: José Konkino Editor, 1958.

GHAPPOUR, Ahmed. Tallinn, Hacking, and Customary International Law. **Boston University School of Law**, [*S.l.*], v. 111, n. 224, 24 Aug. 2017. Disponível em: https://ssrn.com/abstract=3024380. Acesso em: 22 set. 2021.

HABER, Eldar. The Cyber Civil War. **44 Hofstra Law Review**, [*S.L.*: s.n.], v. 41, 7 Dec. 2015. Disponível em: https://ssrn.com/abstract=2699644. Acesso em:17 ago. 2021.

INTERNATIONAL COMMITTEE OF THE RED CROSS. **Convenção XIII**: Direitos e deveres das Potências neutras na guerra naval. Haia, 18 Oct. 1907. Disponível em: Disponível em: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/240. Acesso em: 12 de set. 2021.

JOHNSON, David Reynold; POST, David G. Law and Borders: The Rise of Law in Cyberspace. **Stanford Law Review**, [*S.l.*: s.n.], v. 48, p. 1-1367, 1 Feb. 1996. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535. Acesso em: 17 out. 2021.

MANUAL San Remo de Direito Internacional Aplicável a Conflitos Armados no Mar. Direito Internacional sobre a conduta de hostilidades, **Comitê Internacional da Cruz Vermelha - CICV**, Suíça, 1996.

MARGULIES, Peter. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. **Melbourne Journal of International Law**, [*S.l.*], v. 14, n. 155, p. 1-496, 2013. Disponível em: https://ssrn.com/abstract=2557517. Acesso em: 15 jun. 2021.

MCLAUGHLIN, Stephen. et al. The cybersecurity landscape in industrial control systems. **Proceedings of the IEEExplore**, [*S.l.*], v. 104, n. 5, p. 1039-1057, 2016.

MELLO, Celso D. de Albuquerque. **Curso de direito internacional público**. v. II. Rio de Janeiro: Renovar, 1992.

MONTEIRO, Renato Leite. **The Balance between Freedom and Security in the Age of Surveillance**: a Brief Analysis of the Recent Intelligent Electronic Surveillance Scandals. SSRN, 2014. Disponível em: https://ssrn.com/abstract=2468060. Acesso em: 15 ago. 2021.

OLIVEIRA, Liziane Paixão Silva. A soberania frente à globalização. **Revista do Programa de Mestrado em Direito do UniCEUB**, Brasília, v. 2, n. 1, p. 202-225, jan./jun, 2005.

ONUF, Nicholas Greenwood. Sovereignty: outline of a conceptual history. **Alternatives**: Global, Local, Political, [S.l.], v. 16, n. 4, p. 425-446, 1991.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **Convenção das Nações Unidas sobre o Direito do Mar**. Convenção de Montego- Bay, 28 jul. 1994. Disponível em: https://www2.camara.leg.br/legin/fed/decret/1990/decreto-99165-12-marco-1990-328535-publicacaooriginal-1-pe.html. Acesso em: 12 set. 2021.

PENA, Rodolfo Alves. **Era da informação**. [*S.l.*]: Mundo Educação, 2013. Disponível em: https://mundoeducacao. bol.uol.com.br/geografia/era-informacao.htm. Acesso em: 13 ago. 2021.

RABOIN, Bradley. Corresponding Evolution: International Law and the Emergence of Cyber Warfare. **National Association of Administrative Law Judiciary**, [*S.l.*], v. 31, n. 2, 2011. Disponível em: https://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5. Acesso em: 17 ago. 2021.

REIS, Marcos; SANTOS, Tamiris P. Análise das Ameaças Transnacionais Contemporâneas no Entorno Atlântico Brasileiro: A Terceirização da Segurança e a Revisão Dos Estudos de Política de Defesa. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 20, n. 1, p. 211-229, jan./jun. 2014. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/195. Acesso em: 20 jul. 2021.

RIBEIRO, António Silva. A Expansão dos Direitos Soberanos nos Oceanos. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 19, n. 2, p. 269 - 276, jul./dez. 2013. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/198. Acesso em: 17 mar. 2021.

RICHARD, Clarke; KNAKE, Robert. **Cyber war**: the next threat to national security and what to do about it. New York: Ecco, 2010, 320 p. [Reprint edition].

ROCHA, Marcio; FONSECA, Daniel Farias da. A Questão Cibernética e o Pensamento Realista. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 25, n. 2, p. 517-543 maio/ago. 2019. Disponível em: https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/849. Acesso em: 21 jul. 2021.

SALDAN, Eliane. **Os desafios jurídicos da guerra no espaço cibernético**. 2012. 118 fl. Dissertação (Mestrado em Direito Constitucional) – Instituto Brasiliense de Direito Público, Brasília, 2012.

SCHMITT, Michael. Grey Zones in the International Law of Cyberspace. **Yale Journal of International Law**, [*S.l.*], v. 42, p. 1-21, 2017a. Disponível em: https://www.yjil.yale.edu/grey-zones-in-the-international-law-of-cyberspace/. Acesso em: 13 jul. 2021.

SCHMITT, Michael. **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge: Cambridge University Press, 2017b.

SHACKELFORD, Scott. Estonia Two-and-A-Half Years Later: a progress report on Combating Cyber Attacks. **Journal of Internet Law, Forthcoming**, [*S.l.*], 2009. Disponível em: https://ssrn.com/abstract=1499849. Acesso em: 17 out. 2021.

STOCKBURGER, Peter Z. Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum. **American University International Law Review**, [*S.l.*], v. 31, n. 4, 2016. Disponível em: https://digitalcommons.wcl.american.edu/auilr/vol31/iss4/2/. Acesso em: 22 ago. 2021.

VIDIGAL, Armando Amorim Ferreira; BOAVISTA, Marcílio. **Amazônia Azul**: o mar que nos pertence. Rio de Janeiro: Record, 2006.

WATTS, Sean; RICHARD, Theodore T. Baseline territorial sovereignty and cyberspace, 2018. **Lewis & Clark Law Review**, [*S.l.*: s.n]. Disponível em: https://ssrn.com/abstract=3142272. Acesso em: 13 jul. 2021.

*** Recebido em 0 de dezembro de 2021, e aprovado para publicação em 15 de setembro de 2022.**