ESCOLA DE GUERRA NAVAL

MAJ (USMC) THOMAS BRENT TURNER

GUERRA CIBERNÉTICA:

A promoção do Direito Internacional Cibernético à luz do Direito do Mar

Rio de Janeiro

2016

MAJ (USMC) THOMAS BRENT TURNER

GUERRA CIBERNÉTICA:

A promoção do Direito Internacional Cibernético à luz do Direito do Mar

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF (CA) LUCIANO PONCE CARVALHO JUDICE

Rio de Janeiro

Escola de Guerra Naval

2016

A suprema arte da guerra é subjugar o inimigo sem lutar.
Sun Tzu, A Arte da Guerra (tradução nossa)

RESUMO

Um século e meio atrás, os líderes mundiais se uniram para interromper o flagelo da pirataria que estava ameaçando a economia global. Economia esta que estava experimentando uma expansão rápida através do conceito de livre comércio em alto-mar. Hoje o mundo encontra-se à beira de uma mudança como esteve em meados do século XIX. O ciberespaço é o nosso novo ambiente para comércio livre, exploração e expansão. Governos, bancos, universidades e o cidadão médio são completamente dependentes das "águas" conectivas que a internet proporciona, na busca e troca de informações e ideias, para transferir e investir moeda, para realizar negócios e para fazer compras. *Hackers* são o atual inconveniente mundial, agindo como párias no alto-mar do ciberespaço, ameaçando arruinar a livre troca de ideias e a busca de uma vida melhor por meio da expansão digital. O estudo e a análise de dois ataques cibernéticos de nível nacional sob a perspectivados tratados e legislação internacionais existentes irão demonstrar significativas deficiências na legislação atual, enquanto os governos procuram responder atos de agressão cibernética. Esta monografia visa identificar a aplicabilidade da legislação existente e, em seguida, destacar as falhas expressivas que permanecem. Através de um exame da Convenção das Nações Unidas sobre o Direito do Mar, esta monografia pretende identificar uma estrutura válida para o estabelecimento do direito internacional cibernético e proporcionar recursos para que o governo responda a ameaças cibernéticas.

Palavras-chaves: Direito Internacional da Cibernética. Ataque cibernético. Guerra cibernética. Convenção das Nações Unidas sobre o Direito do Mar. Hackers.

LISTA DE ABREVIATURAS E SIGLAS

CERT	*Computer Emergency Response Team*
CNUDM	Convenção das Nações Unidas sobre o Direito do Mar
DDOS	*Distributed Denial of Service Attack*
DHS	*Department of Homeland Security*
FBI	*Federal Bureau of Investigation*
IAB	*Internet Architecture Board*
IETF	*Internet Engineering Task Force*
IMO	*International Maritime Organization*
IP	*Internet Protocol*
ISAF	*International Security Assistance Force*
ISP	*Internet Service Provider*
NSA	*National Security Agency*
OPM	*Office of Personnel Management*
OTAN	Organização do Tratado do Atlântico Norte
SCADA	*Supervisory Control and Data Acquisition*
ONU	Organização das Nações Unidas

SUMÁRIO

1 INTRODUCÃO

Séculos atrás, uma oportunidade se apresentou em alto-mar. Enquanto o *boom* do livre comércio e da expansão colonial gozava de popularidade e ganhava força, o sucesso mais rápido e fácil era obtido saqueando-se aqueles que tinham investido e arriscado tudo por uma vida melhor. Esses piratas delinquentes operavam em organizações criminosas relativamente sofisticadas a bordo de navios ou grupos de navios. Dentro das fronteiras de uma nação desenvolvida, tais criminosos eram considerados párias, porém, no meio da mais nova zona econômica do alto-mar, portanto além das fronteiras estatais, os piratas operavam impunemente. Eles tomavam o que queriam, matavam qualquer pessoa em seu caminho, depois voltavam para a segurança de uma cidade portuária periférica que oferecesse refúgio, geralmente em troca de uma porção do lucro.

Isso não configurava o ataque a um único Estado, mas sim ao mercado global, e à busca do livre comércio por meio da conectividade do mar. O tecido desse sistema global de comércio, bem como sua exploração e expansão, estava sendo ameaçado. Nesse contexto, os Estados mais poderosos do planeta estavam sendo atingidos por pouco mais do que homens embarcados. Tudo o que era necessário para perpetrar tais ataques era alguma experiência marítima básica e a crueldade para cometer atos terríveis na busca de riquezas. Com os piratas ganhando destaque e em franca vantagem, o mundo preparou-se para agir. Lenta e cuidadosamente, as elites políticas dos maiores Estados do planeta desenvolveram um código de conduta que estabelecia um princípio geral de livre comércio em alto-mar. Em 1856, quarenta e dois países já haviam assinado a Declaração de Paris, a qual formalmente transformou os piratas de um incômodo comum em criminosos globais, a serem caçados com persistência pelas grandes potências mundiais. Além dos próprios piratas, tal declaração também serviu de alerta a qualquer outro grupo ou Estado que intentasse usar esse espaço internacional para causar danos. Em suma, os autores da mencionada Declaração se

comprometeram a manter a ordem em alto-mar para o bem de uma sociedade que contava com a conectividade social e econômica do mar (SINGER & FRIEDMAN, 2014).

Hoje o mundo encontra-se à beira de uma mudança como esteve em meados do século XIX. O ciberespaço é o nosso novo ambiente para o livre comércio, exploração e expansão. Governos, bancos, universidades e os cidadãos comuns são completamente dependentes das "águas" conectivas que a internet fornece, na busca e troca de informações e ideias, para transferir e investir dinheiro, para fazer compras, e para relaxar assistindo a filmes, shows, ou vídeos lúdicos de pessoas caindo de *skate***.** Tudo isso com o mesmo grau de importância relativa para cada um dos envolvidos nas diversas situação ora descritas.

Hackers são o atual inconveniente mundial, agindo como párias no alto-mar do ciberespaço, ameaçando arruinar a livre troca de ideias e a busca de uma vida melhor por meio da expansão digital. Como os homens com embarcações simples que enfrentaram grandes Estados de outrora, os *hackers* de hoje só precisam de um computador, um pouco de experiência técnica e uma conexão à internet. Esses atores muitas vezes anônimos, escondidos pela vastidão e profundidade do ciberespaço, lançam ataques contra Estados e corporações que restam impotentes. Eles ocasionalmente vandalizam, roubam e humilham, causando danos irreparáveis, como foi o caso da Sony em 2014, após um ataque em represália pelo seu filme que mostrou o dirigente norte-coreano Kim Jong-un sendo morto em uma explosão. Peter Elkind, em um artigo de 2014 para a revista Fortune, caracterizou a violação da Sony como uma invasão cibernética que subjugou uma empresa e aterrorizou a América corporativa.

Após uma sequência interminável de ataques de *hackers* e atos de guerra cibernética perpetrados por países e grupos de *hackers*, a comunidade global deve agir para proteger esse novo meio do qual eles se tornaram tão absolutamente dependentes. Assim como seus pares um século e meio atrás, hoje as potências mundiais estão prontas e devem agir para neutralizar

os *hackers* e para alertar os demais Estados que optem por usar o meio do ciberespaço para a guerra e violência.

As leis internacionais relacionadas à segurança e guerra cibernéticas ainda se encontram em um estágio incipiente. As Nações Unidas (ONU) e a Organização do Tratado do Atlântico Norte (OTAN) elaboraram documentos sobre o assunto, mas esses permanecem não vinculantes, subdesenvolvidos e não acompanham a evolução extraordinariamente rápida da tecnologia. A principal peça de tecnologia de conexão mais usada no planeta está funcionando no vácuo de ilegalidade. Embora a lei dos conflitos armados possa ser aplicada a esta quinta dimensão da guerra, a capacidade de uma nação atacada de reconhecer adequadamente e responder a um ataque cibernético está se tornando complicada, pois o agressor nem sempre pode ser claramente identificado, quer seja um indivíduo solitário, uma organização criminosa ou um governo estrangeiro. Quando o agressor não está positivamente identificado e não pode ser claramente associado a um país, a resposta diplomática, jurídica ou letal torna-se difícil de ser adotada. Atualmente, não há legislação no Direito Internacional que englobe precisamente os ataques cibernéticos.

Na busca clara de um ordenamento jurídico, este trabalho irá examinar tanto ataques cibernéticos históricos como também a capacidade cinética [1] que a guerra cibernética proporciona, considerando-se a proteção, resposta e retaliação no contexto do Direito Internacional dos Conflitos Armados (DICA) existente. Além disso, este trabalho irá especular sobre as considerações que devem ser feitas pela OTAN em resposta a um ataque a um de seus signatários através dos meios de ciberespaço. Finalmente, este trabalho irá voltar-se para o contexto marítimo e examinar tanto a Declaração de Paris quanto a Convenção das Nações Unidas sobre o Direito do Mar (CNUDM) de forma a considerar um quadro jurídico para

[1] "No uso comum, cinético é um adjetivo usado para descrever o movimento, mas o significado empregado pelo governo americano deriva da definição secundária, ativo, em oposição a latentes. Lançando bombas e atirando balas -- você sabe, matar pessoas -- é cinética" (Noah, 2002, p. 1, tradução nossa).

responder a *hackers* solitários ou organizações criminosas que atacam Estados soberanos ou seus territórios.

1.1 Metodologia

Utilizando o método de procedimento comparativo[2], este trabalho irá analisar ataques cibernéticos com graves repercussões nacionais, o que pode ser percebido como guerra cibernética, lançados contra nações soberanas, e considerará cada ataque em face da legislação em vigor, de modo a determinar se o aspecto cibernético do ataque poderia potencialmente receber uma resposta defensiva no mundo físico. Ao examinar os elementos de cada lei ou acordo, este trabalho irá analisar o que podem as leis internacionais ou acordos em vigor fornecer a uma nação atacada como orientação justificável, na falta de uma legislação internacional de segurança cibernética, e até que ponto o ordenamento jurídico atual é insuficiente. Após verificadas as deficiências das leis internacionais existentes para enfrentar tal desafio, este estudo especulará sobre conceitos desenvolvidos a partir da evolução do Direito do Mar, a fim de preencher lacunas nas quais a maioria dos ataques se encaixam, proporcionando aos governos mais parâmetros para a persecução de agressores cibernéticos.

[2] "Considerando que o estudo das semelhanças e diferenças entre diversos tipos de grupos, sociedades ou povos contribui para uma melhor compreensão do comportamento humano, este método realiza comparações, com a finalidade de verificar similitudes e explicar divergências. O método comparativo é usado tanto para comparações de grupos no presente, no passado, ou entre os existentes e os do passado, quanto entre sociedades de iguais ou de diferentes estágios de desenvolvimento" (MARCONI; LAKATOS, 2011, pg 107).

2 GUERRA CIBERNÉTICA E O DIREITO DOS CONFLITOS ARMADOS

Você não pode dizer que civilizações não avançam ...
emcada guerra elas te matam de uma maneira nova.[3]

Um mundo cada vez mais conectado por meio da internet é um inegável salto na evolução tecnológica e uma melhoria no cotidiano de quase todos os cidadãos. Operações bancárias são realizadas com um único clique, presentes de Natal encomendados em minutos e entregues em dias, e a opção de videoconferências gratuitas, como o *Skype*, representam milhões em economia de passagens aéreas para as corporações. Os avanços trazidos por esta "hiperconectividade" são infinitos e penetrantes, na medida em que tudo, desde o ar-condicionado na casa de uma família, até as torres de resfriamento em usinas nucleares e as bombas em uma barragem, podem ser controlados através da Internet. Essa onipresença economiza dinheiro e, mais importante, fornece flexibilidade e simplicidade na gestão de sistemas complexos através de um vasto espectro que precisa ser acessado por várias pessoas em várias localidades. A nova palavra da moda atribuída a esta "hiperconectividade" através de computadores e *smartphones* para os itens que usamos diariamente é chamada a "internet-das-coisas", em inglês a *internet-of-things (IoT)*[4].

Com a internet se tornando mais invasiva a cada segundo, parece que cada nova versão de um produto antigo agora tem conectividade com a internet. O site de tecnologia *CNET* relatou, em janeiro de 2016, que a empresa Samsung criou uma geladeira conectada à internet que pode encomendar mantimentos por meio de uma plataforma de aplicação habilitada à rede

[3] Will Rogers, New York Times, Dezembro 23, 1929, (tradução nossa).

[4] "A Internet das coisas gira em torno do aumento da comunicação de máquina-a-máquina; é construída através da computação em nuvem e redes de sensores de coleta de dados; é móvel, virtual, e uma conexão instantânea; e dizem que vai tornar tudo em nossas vidas, desde a iluminação de rua até os portos marítimos, inteligentes" (BURRUS, 2014).

(BROWN, 2016). Em 2015, a revista *WIRED* informou que *hackers* conseguiram desativar um Jeep Cherokee enquanto ele viajava a 70 milhas por hora em uma rodovia de St. Louis, Missouri (GREENBURG, 2015).

Essa "hiperconectividade", apesar de transformadora, traz preocupação a alguns especialistas cibernéticos. Com cada avanço que dissolve as barreiras entre o mundo cibernético e o mundo físico, tornamo-nos vulneráveis a ataques reais e não apenas a ataques virtuais. Ataques virtuais podem causar danos graves e perdas irreparáveis, mas com a "internet-das-coisas" e a contínua dependência da conectividade da internet pela infraestrutura nacional, cria-se oportunidade para que os ataques virtuais tenham ramificações físicas, gerem danos e até mesmo morte.

Utilizando a metodologia de análise comparativa, avaliando um caso passado sob o enfoque da legislação em vigor, o presente capítulo examinará cuidadosamente o ataque cibernético de 2015 contra a Ucrânia por um suposto agressor russo e determinará se o ataque violou a soberania de um Estado e se realmente continha os elementos legais necessários para justificar uma resposta legítima e incisiva.

2.1 Quando os ataques virtuais têm ramificações físicas

Durante um discurso em 02 de março de 2016, o comandante do Comando Cibernético dos Estados Unidos, que também atua como diretor da Agência de Segurança Nacional (NSA), Almirante Mike Rogers, advertiu que um grande ataque cibernético por Estados nacionais contra infraestruturas cruciais representa uma grande ameaça à segurança. Em abril de 2016, o jornal *Washington Free Beacon* publicou um artigo, citando relatórios internos oficiais, que revelou que o Departamento de Segurança Interna dos Estados Unidos (DHS) e o Bureau Federal de Investigação (FBI) começaram um programa nacional alertando sobre iminentes

perigos para a infraestrutura crucial dos Estados Unidos da América (EUA) causados por ataques cibernéticos. Demonstrando a gravidade com que abordaram a questão, o *FBI* publicou *webinars*[5] na internet e realizou apresentações em oito cidades dos EUA para os chefes das empresas dos serviços públicos essenciais. Enquanto "ataque cibernético" e "guerra cibernética" são expressões em risco de perder a potência pelo uso excessivo, os avisos do *FBI* e as ações de acompanhamento são um sinistro lembrete dos golpes físicos que um Estado pode sofrer através do meio virtual do ciberespaço (GERTZ, 2016).

O aumento súbito da atividade do *FBI* e do *DHS* no que diz respeito a ataques cibernéticos foi motivado pelo ataque de 23 de dezembro de 2015 por *hackers* russos, os quais se acreditava terem apoio do governo russo, contra a infraestrutura de energia ucraniana. Naquele dia, um *hacker* obteve remotamente o acesso à rede de Controle e Aquisição de Dados de Supervisão (SCADA) do centro de controle de energia Prykarpattyaoblenergo, no centro de Ivano-Frankivsk, Ucrânia. Com tal acesso, o referido *hacker* começou a metodicamente ativar disjuntores e desligar subestações de energia em toda a região, literal e virtualmente mergulhando o povo da Ucrânia em uma fria escuridão. Quando o operador tentou acessar novamente, ele descobriu que a sua senha havia sido alterada e ele foi completamente impedido de parar o ataque. O sistema de energia reserva fornecida por uma fonte ininterrupta deveria ter sido ativado, no entanto, também se tornou inoperante pelo planejamento cuidadoso dos *hackers*, o que retardou ainda mais as condições perigosas experimentadas pelo povo ucraniano durante um inverno particularmente frio. O nível de sofisticação demonstrado por tal ataque foi algo nunca antes visto. Os *hackers* não só clandestinamente ganharam acesso remoto à infraestrutura crucial, mas, uma vez adquirido o acesso, tornaram os sistemas de *backup* inoperantes, bloquearam usuários autorizados, inundaram os *call centers* da empresa com chamadas falsas, e reescreveram o *firmware* para os sistemas de serviços públicos,

[5] Webinars são seminários conduzidos pela rede mundial de computadores.

impossibilitando o acesso remoto. Enquanto a conveniência do acesso remoto foi o que facilitou a intrusão, a perda dessa capacidade atrasou ainda mais a restauração da energia, já que os trabalhadores tiveram que iniciar todos os sistemas manualmente no local para cada subestação afetada (ZETTER, 2016).

A revista *WIRED* citou especialistas não especificados em seu artigo de 03 de março de 2016, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, os quais afirmaram que, apesar do revés temporário experimentado por 230.000 moradores da Ucrânia, os EUA poderiam não ter se saído tão bem. Muitos sistemas baseados nos EUA são supostamente mais sofisticados, no entanto, eles só possuem acesso remoto. Diante de um ataque similar, muitas empresas de serviços públicos dos EUA não teriam sido capazes de derrotar o ataque no período de seis horas levado pela Ucrânia, ao não dispor da funcionalidade de *backup* manual.

Kim Zetter da revista *WIRED* entrevistou um ex-oficial de operações de guerra cibernética da força aérea dos Estados Unidos e fundador da empresa Dragos Segurança, que auxiliou a investigação sobre o *hack* da rede elétrica da Ucrânia. Robert Lee considerou o ataque como brilhante e bem planejado, acreditando que a preparação logística e o planejamento operacional aumentam o nível de sofisticação visto no ataque. Lee opinou que o ataque foi, na verdade, perpetrado indiretamente pelo governo russo e pode ter sido uma forma de guerra psicológica concebida para levar o povo ucraniano a perder a confiança em seu governo e, talvez, olhar de forma mais favorável o governo russo, que tinha anexado a região da Crimeia apenas dois anos antes (ZETTER, 2016).

2.2 Aplicabilidade do Direito Internacional dos Conflitos Armados a um ataque cibernético

No caso do suposto ataque à rede de energia ucraniana pelo governo russo, o direito de um país de responder, defender ou retaliar contra um ataque a sua soberania nacional torna-se problemático. Apesar da convicção do governo ucraniano de que a Rússia estava por trás do ataque, os líderes da Rússia afirmaram categoricamente que não tiveram nada a ver com o ocorrido. Aplicando-se o DICA a este cenário específico, um exame cuidadoso pode revelar porque não houve uma escalada para o nível de guerra e talvez seja possível definir até que ponto o ataque ucraniano poderia ter sido percebido como um ato de guerra.

Embora não seja lei e de forma alguma juridicamente vinculante, o Manual Tallinn é de longe o melhor recurso para um governo quando se considera o DICA através da lente da guerra cibernética. Escrito pelo diretor do projeto, o professor Michael Schmitt, da Escola de Guerra Naval dos EUA, o Manual Tallinn foi encomendado pela OTAN em 2009, e levou três anos para ser concluído por 20 *experts* mundialmente conhecidos. O manual recebeu esse nome em razão da localização do Centro de Excelência de Defesa Cibernética Cooperativa da OTAN, na cidade de Tallinn, Estônia.

Para analisar o ataque contra a Ucrânia através da lente do DICA, deve-se considerar uma variedade de fatores. Especificamente: a soberania da vítima, o agressor, uso autorizado da força, se a autodefesa é uma necessidade e pode ser entregue com proporcionalidade, e, finalmente, a firme justificativa para retaliação através da aplicação do DICA.

A consideração da soberania no caso do ataque contra a Ucrânia é facilmente validada. O centro de controle Prykarpattyaoblenergo enquadra-se claramente dentro dos limites de soberania das fronteiras ucranianas, a empresa atacada é uma empresa de serviços públicos ucraniana e os clientes cujas vidas dependem da energia fornecida pela empresa são cidadãos

da Ucrânia e foram, além disso, indevidamente atacados. Enquanto a consideração da soberania é facilmente consignada, a ideia de jurisdição torna-se decididamente mais nebulosa.

Apesar de a empresa de energia, e também os cidadãos afetados, estarem claramente dentro da jurisdição da Ucrânia, o ataque ocorreu entre fronteiras, no ciberespaço, e foi iniciado a partir de um local desconhecido. Enquanto a Ucrânia sustenta que o ataque foi lançado da Rússia, isso por si só não esclarece a obscuridade do problema. Se foi, de fato, a Rússia que atacou a Ucrânia, é ainda mais provável que a Rússia tenha usado algum tipo de grupo não-governamental de *hackers* ou mesmo uma organização criminosa para agir em seu nome. Se descoberta, a Rússia iria simplesmente fingir espanto e se resumir a responsabilizar o ator não-estatal pelo ataque flagrante a um outro país. No final, a Ucrânia fica sem nada tangível. Eles certamente não podem lançar um contra-ataque sem a absoluta certeza de que foram previamente atacados por outro país, resultando em prejuízo. Neste caso particular, ninguém ficou ferido diretamente, mas a infraestrutura do país foi debilitada, e a possibilidade de dano futuro é grande. Dada a falta de opções de resposta, a situação se assemelha aquando um país é pego espionando outro. É fato notório que os países espionam, mas não é necessariamente menos embaraçoso ou prejudicial à nação ofendida quando detectado. Ainda que as nações sejam muitas vezes prejudicadas por vazamentos de inteligência, não se declara guerra por isso. As perdas são atribuídas ao jogo da espionagem e tratadas diplomaticamente. Se fosse para imaginar um resultado diferente, mas muito plausível, o direito de uma nação de se defender e lançar um contra-ataque, quer através de seus recursos cibernéticos ou cineticamente, poderia certamente ser justificado.

Quando se considera responder ao uso da forçada mesma forma, não é necessariamente pertinente que a força em questão tenha sido exercida através de um computador. O Manual Tallinn, considerando o Artigo 10º da Carta das Nações Unidas afirma que, “Uma operação cibernética constitui um uso de força quando a dimensão e efeitos dela são comparáveis a

operações não cibernéticas que evoluam para o nível de uso da força" (SCHMITT, 2013, p. 45, tradução nossa). Enquanto Assembleias Gerais das Nações Unidas têm discutido e rejeitado noções de que ações agressivas que afetam o caráter político ou econômico de outro país sejam percebidas como um tipo de uso da força, o Manual Tallinn afirma especificamente que as operações psicológicas cibernéticas não destrutivas destinadas exclusivamente a minar a confiança em um governo ou uma economia não se qualificam como uso da força. O ataque contra a Ucrânia, como é atualmente compreendido, provavelmente se encaixa bem dentro dessa definição. Com esse entendimento, deve-se analisar os possíveis resultados de um ataque como esse e considerar que efeitos diretos ou impactos secundários e terciários podem evoluir para o nível de uso da força e, assim, justificar uma resposta agressiva (SCHMITT, 2014).

À medida que continuamos a considerar o ataque de 2015 contra Ucrânia, as potenciais ramificações não podiam ter sido inteiramente conhecidas pelos *hackers*. Na ausência de um sistema de refrigeração especial, talvez um gerador tivesse explodido, matando ou ferindo diversos funcionários da usina. Talvez ainda mais plausível, cidadãos ucranianos poderiam morrer pelo impacto secundário das condições de frio intenso, dada a perda da capacidade para aquecer suas casas. Talvez vidas fossem perdidas, com a impossibilidade de os serviços de emergência responderem eficazmente às pessoas necessitadas após uma falha dos sistemas do telefone de emergência. Finalmente, talvez pessoas tivessem morrido na mesa de operação quando hospitais ficaram sem energia e os geradores de *backup* falharam. Se a Ucrânia fosse atacada e o ataque resultasse na morte de milhares de pessoas, tal Estado não teria nenhuma opção a não ser responder com força. Após a morte de milhares de pessoas, a obscuridade dos atores não-estatais pode não ser capaz de dissuadir um país indignado. Semelhante ao ataque a Nova York em 11 de setembro de 2001, os EUA não ficaram desorientados com a noção de que tinham sido atacados por um ator não-estatal. Os EUA sangraram naquele dia e estavam decididos a fazer os autores dos ataques sangrarem da mesma maneira.

Se a ideia de geradores explodindo na sequência de um ataque cibernético parece exagerada, o Departamento de Segurança Interna dos EUA em conjunto com o Departamento de Energia lançou o Projeto *Aurora* em março de 2007, no laboratório de Idaho do Departamento de Energia, para testar essa potencialidade. Enquanto suposições prévias imaginavam como o pior resultado possível para uma empresa de serviços públicos um desligamento total, esse teste provou que os resultados poderiam ser muito piores. Durante o decurso desta experiência controlada, *hackers* conseguiram penetrar nos sistemas de controle da usina. Os *hackers*, em seguida, alteraram o ciclo operacional de um gerador, fazendo com que ficasse fora de controle e explodisse (MESERVE, 2007).

Se os cidadãos de um país começarem a morrer, direta ou indiretamente, na sequência de um ataque cibernético, justificar o uso da força pode não ser tão difícil, mas determinar a proporcionalidade pode ser algo a se debater. A maioria diria que uma morte que resulta do clique de uma tecla de computador não é diferente daquela do cano de um fuzil e, por conseguinte, em resposta a um ataque cibernético, o país que está retaliando não necessariamente deve responder pelo meio cibernético para que as regras de proporcionalidade sejam respeitadas. Se o ataque sobre a Ucrânia provocasse um colapso em um único local, onde as máquinas perdessem o controle e explodissem, resultando em danos irreparáveis para a usina e a morte dos funcionários, poderia ser considerado inteiramente proporcional atacar cineticamente, embora talvez não fosse sábio sem o apoio da OTAN, mas certamente plausível e proporcional cogitar-se em lançar um ataque aéreo contra a infraestrutura crítica da Rússia, ou mesmo, mais especificamente, tendo como alvo a localização dos *hackers*. Do ponto de vista da vítima, quer tenham sido as mortes e explosões causadas por um *hacker* ou por uma bomba, os impactos físicos são assustadoramente semelhantes. Com o amadurecimento das capacidades antirradar ao longo dos anos, pode-se supor que, enquanto o subterfúgio de *hackers*

evolui, da mesma forma a capacidade de um país para encontrá-los e matá-los (SCHMITT, 2013).

Utilizando-se o Manual Tallinn e também a DICA, pode-se ver claramente como o impacto das operações cibernéticas podem ter implicações verdadeiras no mundo físico. Ramificações físicas, tais como destruição de nós fundamentais de comunicações operacionais, de infraestruturas cruciais e até mesmo a morte, direta ou indiretamente. Uma análise do ataque cibernético de 2015 contra a Ucrânia demonstrou a facilidade com que este tipo de ataque pode evoluir, ficando fora de controle, e resultar em consequências que talvez nem mesmo o agressor tenha buscado, no entanto, ainda assim, essas consequências poderiam iniciar um conflito armado.

2.3 Ciberespaço como um meio viável para guerra moderna

Seja por raiva, motivações políticas, ou pelo desejo de expandir-se geograficamente, as guerras são iniciadas por uma variedade de razões. No entanto, no âmbito da guerra intencional, armas cibernéticas podem, sem dúvida, desempenhar um papel fundamental. À medida que o mundo se torna mais conectado e dependente da tecnologia, emerge a vulnerabilidade à referida tecnologia. Durante a campanha do Pacífico na II Guerra Mundial, a preparação ou enfraquecimento do campo da batalha envolveu bombardeios intermináveis por aviões e artilharia naval. A ideia é suavizar ou debilitar o inimigo o máximo possível antes de os Fuzileiros Navais chegarem à praia. Toda ação cinética realizada antes da presença de tropas foi feita exaustivamente para garantir a vitória e reduzir a perda do recurso mais importante: os Fuzileiros Navais. Uma batalha perfeita seria aquela em que a capacidade de defesa do inimigo foi completamente diluída pela campanha aérea e as tropas de desembarque foram apenas uma equipe de limpeza, lançada para varrer as forças restantes que estivessem no caminho da vitória.

Da mesma forma poderia se empregar hoje o conceito de armas cibernéticas, guerra cibernética e ataques cibernéticos. Talvez o futuro próximo seja aquele onde a preparação ou enfraquecimento do campo da batalha seja alcançado com armas cibernéticas, em vez de simplesmente bombardeios aéreos convencionais. A perda de comunicação, a perda de sinal *GPS*, a incapacidade de sequer confiar em ordens de missão que estão sendo passadas através de uma rede informatizada, tudo isso seria devastador para uma força militar. Talvez ainda mais inverossímil, mas de todo plausível, imagine se os *chips* do computador que controlam os aviões de caça ou *drones* dos países mais avançados tivessem sido produzidos anteriormente por um Estado que tornou-se inimigo, que agora tem a capacidade para destruir tais armamentos simplesmente pelo desencadeamento de *malwares* latentes, previamente carregados nestes *microchips*. Os efeitos poderiam ser devastadores (SINGER & FRIEDMAN, 2014).

Em 2012, foi relatado pela "Era da Informação", uma publicação on-line profissional para os líderes de Tecnologia da Informação (TI), que pesquisadores da Universidade de Cambridge descobriram que microprocessadores atualmente em uso pelos militares dos EUA, mas fabricados na China, tinham sido equipados com um recurso de acesso remoto. Em um artigo de junho 2015, *The Wall Street Journal* relatou que, em um discurso proferido para a Escola de Guerra Naval dos EUA pelo futurista, estudioso de relações internacionais e cientista político Peter Singer, o aclamado autor emitiu sérios avisos sobre as atuais capacidades da China e o impacto direto que isso terá sobre a tecnologia militar dos EUA. Ele também reiterou a ideia de que os caças americanos poderiam cair em razão de um mau funcionamento desencadeado pelos *microchips* feitos na China e incorporados nos sistemas cruciais de controle da aeronave (NISSENBAUM, 2015).

Usar armas cibernéticas e um ataque cibernético para preparar o campo de batalha antes de uma invasão cinética não é apenas o futuro, é o passado recente. David Hollis escreveu um artigo para o *Small Wars Journal* intitulado "*Cyberwar Case Study: Georgia 2008"*, onde ele

afirma que, “esse parece ser o primeiro caso na história de um ataque coordenado no domínio do ciberespaço, sincronizado com grandes ações de combate nos outros domínios da guerra” (HOLLIS, 2011, pg. 2, tradução nossa). Hollis observa ainda que a Geórgia foi atacada em quatro frentes, três delas convencionais (ar, terra e mar), sendo a quarta o ciberespaço. O ataque foi realizado contra redes e sites do governo e militares, com o intuito de causar confusão e perturbar as comunicações nas horas que antecederam a invasão russa.

Enquanto inúmeros exemplos podem ser continuamente fornecidos para provar que a internet é um meio válido para conduzir ou afetar a guerra, a verdade, como evidenciado pela Geórgia, é simplesmente que já tem sido assim há algum tempo. O público pode ser o último a saber, como é frequentemente o caso, mas os militares e os governos do mundo vem observando claramente a ameça. Talvez não claramente o suficiente para estabelecer acordos internacionais, mas o suficiente para armar-se de capacidades-chave de defesa cibernética.

As primeiras “cyber-milícias” das universidades foram formadas após o incidente em 2001 na ilha de Hainan. Um piloto de caça chinês tinha voado muito perto de um avião de vigilância dos EUA, resultando em uma colisão no ar. O avião chinês caiu e o piloto foi morto, no entanto, o avião americano danificado foi forçado a fazer um pouso de emergência num campo de aviação chinês em Hainan. Enquanto as ramificações diplomáticas se seguiram, o Partido Comunista Chinês encorajou seus cidadãos a desfigurar sites da internet americanos como uma forma de protesto internacional. Jovens *hackers* avidamente se juntaram à campanha oficialmente e publicamente apoiada de vandalismo cibernético contra os EUA. Dentre os diversos alvos, um digno de nota foi o site da Casa Branca dos EUA (SINGER & FRIEDMAN, 2014).

Em 2009, o comando cibernético dos EUA foi fundado para ajudar a organizar e coordenar cada uma das unidades de guerra computacional do Departamento de Defesa.

Conforme reportado em 23 de maio de 2016 pelo *DCInno*[6], a proposta do Congresso norte-americano para os gastos na defesa de 2017, sugeriu que o comando cibernético dos EUA fosse reconhecido como um comando combatente unificado. Isso daria ao respectivo comandante livre autoridade para realizar missões de defesa global dentro dessa quinta dimensão da guerra (BING, 2016). Em 27 de maio de 2016, "The Washington Times" informou que a Academia Naval dos EUA formou a primeira turma na história especializada em operações cibernéticas. Além da especialização, a Academia tem exigido desde 2011 que todos os estudantes façam dois cursos do currículo básico em segurança cibernética (WITTE, 2016).

2.4 Síntese

Embora este trabalho vá, mais à frente, discutir estratégias para o estabelecimento de um quadro jurídico internacional para proteger a capacidade da comunidade internacional de, livremente, trocar e desfrutar do mercado internacional que é a internet, é inegável a validade do âmbito cibernético como meio viável para conduzir uma guerra. Comprovado pelo caso da Ucrânia, uma operação de cibernética bem planejada pode ser devastadora para um país inteiro. Uma análise daquele caso através da lente do DICA, alinhando as possibilidades do que poderia ter acontecido com base na ciência comprovada, revela uma realidade assustadora: uma capacidade futurística que pode fazer a ponte do meio cibernético para o mundo físico.

Em 2015, "*The Wall Street Journal"* publicou um artigo afirmando que o governo iraniano, em 2013, invadiu os sistemas de controle de uma barragem de Nova Iorque. Especialistas afirmaram que o acesso aos sistemas de controle industrial poderia ter provocado uma inundação (YARDON, 2015). Em 2014, a revista "*WIRED"* publicou um artigo sobre o vírus *Stuxnet*, que é considerado a primeira arma digital do mundo. O vírus *Stuxnet*,

[6] Disponível em <http://dcinno.streetwise.co/>. Acesso em: 01.ago.2016.

supostamente lançado por agentes de inteligência americanos e israelenses, infectou usinas de enriquecimento de urânio do Irã, fazendo com que centrífugas da usina acelerassem e desacelerassem de forma aleatória, praticamente suspendendo, por um período, a capacidade do governo iraniano de enriquecer o urânio necessário para desenvolver armas nucleares (ZETTER, 2014).

Finalmente, tendo-se em consideração que o espaço cibernético tornou-se a quinta dimensão de guerra, já não podemos abordar a capacidade cibernética como um futurismo para o qual mundo precisa se preparar. Esta é uma capacidade estabelecida, que já foi utilizada na guerra, que tem sido utilizada para prejudicar as pessoas e Estados, e uma capacidade com a qual as maiores nações do mundo estão se armando. Enquanto este capítulo falou sobre o desenvolvimento das milícias cibernéticas na China e o desenvolvimento dos comandos militares cibernéticos dos EUA, o capítulo seguinte examinará as implicações políticas, diplomáticas e jurídicas do Artigo cinco da OTAN, sua responsabilidade de defender um membro dessa Organização na sequência de um ataque, e a implicação dos ataques cibernéticos para a definição legal dada pelo tratado.

3 GUERRA CIBERNÉTICA E O DEVER DA OTAN DE DEFENDER SEUS SIGNATÁRIOS

Em seu livro "*North Atlantic Treaty Organization (NATO)"*, Phil Williams refere-se à organização como a instituição de segurança ocidental dominante desde sua criação em 04 de abril de 1949, e também a existente há mais tempo. Localizada em Bruxelas, Bélgica, a organização tem atualmente 28 Estados membros. A pedra angular do sistema de longa duração é a ideia de defesa coletiva, detalhada especificamente no Artigo 5 do Tratado. Após os ataques terroristas de 11 de setembro de 2001, os EUA apelaram à OTAN para uma resposta militar, sob os auspícios da defesa coletiva. O resultado foi a Operação "ENDURING FREEDOM" (OEF) realizada pela *International Security Assistance Force* (ISAF), organizada sob a estrutura do comando militar da OTAN. Esta foi a única vez na história que o Artigo 5 de NATO foi aplicado.

Embora o conceito pareça simples, o ato físico de obter uma resposta cinética da OTAN é uma outra questão, evidenciado pelo fato de que ocorreu apenas uma vez na história. Hoje, muitos dos signatários desfrutam da proteção proporcionada pela OTAN a ponto de fazer com que suas próprias forças armadas se atrofiem. Um artigo de janeiro 2016 da "Vice News Online" declarou que, no ano passado, quando a Rússia começou de forma agressiva a infringir a soberania da Ucrânia, líderes em Berlim e em outros lugares ao redor da Europa perceberam que tinham deixado suas forças armadas definharem e que de modo algum estavam preparados para combater a Rússia, se não fosse a proteção da OTAN e dos EUA. Isso, por si só, reduz a capacidade da OTAN e coloca uma pressão indevida sobre poucos Estados militarmente mais fortes. A história mostra que o mundo não quer a guerra e a justificativa básica necessária para fazer com que a OTAN adote uma postura ofensiva é prova suficiente, apesar do tratado. Uma

resposta armada da OTAN contra qualquer agressão teria de ser provocada por um ato especialmente terrível (DYER, 2016).

Este capítulo vai examinar o caso de *hacking* contra a Estônia em 2007, pelos supostos agressores russos, rever a contrapartida para o apoio da OTAN, e, finalmente, analisar o incidente sob o enfoque do Tratado do Atlântico Norte, também conhecido como o Tratado de Washington. Utilizando a metodologia de revisão de um caso passado e avaliando este em face do tratado em vigor, este autor pretende analisar se a OTAN poderia ter reagido após o ataque contra a Estônia e, em caso negativo, até que nível deveria um ataque cibernético semelhante evoluir para desencadear uma resposta cinética pela OTAN.

3.1 O caso da cibernética da Estónia

Em 27 de Abril de 2007, o governo da Estônia removeu uma estátua de bronze de 1,82 metros de altura localizada no centro de Tallinn, o capital da Estônia. Enquanto o ato em si não parecia ameaçador ou escandaloso, houve quem ficasse ofendido diante da remoção desse objeto. A grande estátua de bronze tinha sido inicialmente erguida em 1947 pelos soviéticos para homenagear os soldados que morreram lutando para livrar a área da ocupação nazista alemã. Os estonianos certamente não foram, e continuam não sendo, particularmente pró-nazistas, mas a ocupação pelos soviéticos após a guerra acabou sendo tão opressiva quanto à nazista, com a massa de dissidentes estonianos sendo enviados para a Sibéria, para um nada delicado treinamento de reeducação. Após 16 anos de liberdade, os estonianos ainda odiavam o que aquele monumento representava e queriam que ele desaparecesse. O observador médio poderia simplesmente considerar óbvia a atitude do governo estoniano e se perguntar porque demoraram tanto para tomá-la. No entanto, o governo russo ainda tinha alguns tentáculos sutis estendidos através da Estônia e havia deixado claro que a remoção desrespeitosa desse

memorial reverenciado seria um desastre para a Estônia. Os estonianos, não sendo completamente ingênuos, arrancaram a detestada estátua, porém, em vez de destruí-la, eles simplesmente a realocaram em um cemitério militar fora da cidade. Um ato equilibrado, que aparentava ser respeitoso com os mortos, ao mesmo tempo em que evitava que os cidadãos estonianos fossem obrigados a caminhar em meio a essa lembrança ruim em sua própria capital (DAVIS, 2007).

Considerado o Estado mais conectado na Europa, da população de 1,3 milhões da Estônia, 40% leem as notícias através da Internet todos os dias, mais de 90% das operações bancárias são feitas através da internet, e, muito antes dos EUA, estonianos votam através da internet. Redes *WiFi* gratuitas cobre as cidades e as pessoas pagam tudo, desde o estacionamento até o almoço, usando os seus *smartphones*. Isso fez com que alguns cidadãos passassem a se referir à nação como *e-Stonia*, em alusão à conectividade com a Internet extremamente difundida e penetrante. A Estônia é um vislumbre do futuro próximo, do que é possível quando um país inova intensamente para melhorar a vida de seus cidadãos através da tecnologia e conectividade com a internet. Como foi discutido no primeiro capítulo, este rápido avanço da tecnologia, com todas as suas melhorias, também traz consigo vulnerabilidades grandes. Com tantas transações bancárias sendo realizadas através da internet, de forma semelhante à dependência dos ucranianos da conveniente monitorização remota de suas usinas, a conveniência das operações bancárias on-line através da Internet normalmente também traz consigo uma enorme vulnerabilidade. No entanto, no caso da Estônia, quando se considera que 90% de todas as transações bancárias ocorrem através da internet, um ataque profundo poderia literalmente desligar o sistema financeiro do país inteiro. Isso afetaria todos os cidadãos de uma só vez (DAVIS, 2007).

Em maio de 2007, esse Estado-membro da OTAN e da União Europeia foi implacavelmente atacado por uma invasão cibernética. No artigo da revista *WIRED* de agosto

de 2007 intitulado, *Hackers Take Down the Most Wired Country in Europe*, o autor Joshua Davis observa de maneira astuta que a Estônia foi violada através de sua fronteira mais fraca: a internet. Por um período de duas semanas em maio e junho de 2007, a mídia estoniana, telecomunicações, bancos e locais de sites do governo sofreram ataque implacável de enormes proporções. O ataque foi o que se chama de "ataque distribuído de negação de serviço" (em inglês DDOS), em que hackers e proprietários desavisados de computadores hackeados chamados *bots*[7] incessantemente solicitam o acesso a uma página de internet específica. Embora não seja tecnicamente complexo, um ataque distribuído de negação de serviço está projetado para sobrecarregar um site ou rede e tornar quase impossível aos usuários legítimos obterem acesso.

Um *botnet* é o termo técnico para a coleta maciça de computadores zumbis controlados em todo o mundo, anteriormente invadidos, que estão à espera, prontos para atender ao comando do *hacker*. Muitos grupos de *hackers* gastam enormes quantidades de tempo invadindo computadores ao redor do mundo e instalando *malwares* que lhes darão acesso *backdoor* em uma data posterior. Como a invasão é limitada e não há dano ou roubo, os proprietários desses computadores zumbis não têm ideia de que suas máquinas podem um dia ser usadas como arma de ataque cibernético. Quando um exército de *botnet* de milhões de computadores é desencadeado e, em concerto, dirigido a um único alvo, o resultado é devastadoramente rápido. O alvo será desligado pelo tempo que os atacantes desejarem. É inteiramente possível que milhares de brasileiros, como proprietários de computadores potencialmente *"hackeados"*, inadvertidamente tenham participado do ataque contra a Estônia. Ao contrário dos ataques a infraestruturas críticas discutidos no primeiro capítulo, um ataque

[7] "Um bot é um único computador que está infectado com *malware*. Um *botnet* refere-se a uma rede virtual de computadores que estão infectados e que estão controlados centralmente pelos servidores de comando e controle" (Boothby, 2016, p. 391, tradução nossa).

distribuído de negação de serviço dificilmente mata alguém. Pode, no entanto, ser totalmente incapacitante para um governo que não possa se comunicar e servir seus cidadãos através da sua plataforma de serviços online, ou para a mídia que não possa divulgar a situação em que se encontram para o mundo e aos bancos e empresas que perdem dinheiro a cada minuto. Durante essas poucas semanas, a Estônia ficou paralisada (DAVIS, 2007).

3.2 Artigo 5, a pedra angular da cooperação da OTAN

O artigo 5 do Tratado de Washington 1949 afirmou que:

> As Partes concordam em que um ataque armado contra uma ou várias delas na Europa ou na América do Norte será considerado um ataque a todas, e, consequentemente, concordam em que, se um tal ataque armado se verificar, cada uma, no exercício do direito de legítima defesa, individual ou coletiva, reconhecido pelo artigo 51 da Carta das Nações Unidas, prestará assistência à Parte ou Partes armada, para restaurar e garantir a segurança na região do Atlântico assim atacadas, praticando sem demora, individualmente e de acordo com as restantes Partes, a ação que considerar necessária, inclusive o emprego da força Norte. (Tratado do Atlântico Norte, 1949, Artigo 5, tradução nossa).

Em 1949, a União Soviética foi a principal razão para o pacto ser estabelecido, devido a preocupações da Europa ocidental de que continuaria a sua expansão para o oeste, buscando controlar e doutrinar mais Estados com as filosofias *marxistas-leninistas*. Irônico, portanto, que os ataques cibernéticos previamente discutidos neste trabalho tenham sido atribuídos ao governo russo ou, pelo menos, apoiados pelo governo da Rússia.

Nenhum membro da OTAN pode invocar o Artigo 5 unilateralmente. O Artigo 5 só pode ser invocado quando todos os 28 membros da Aliança concordam em fazê-lo. Ao examinar os artigos do Tratado de Washington e avaliá-los a partir da perspectiva do ataque estoniano, este capítulo irá analisar quais os elementos necessários para gerar uma resposta pela OTAN e a que nível o ataque da Estônia teria de evoluir para justificar um ataque pela OTAN.

Os elementos a serem examinados são o princípio da autodefesa coletiva, a definição de um ataque armado, e as ramificações políticas do acordo unânime (WILLIAMS, 1994).

Ao analisarmos a possibilidade de resposta da OTAN em relação a um ataque cibernético, é também importante reconhecer a ironia de que a única vez na história em que a OTAN aplicou o Artigo 5 e mobilizou uma resposta foi por motivos bem distintos do que os autores originalmente pretenderam. Como mencionado anteriormente, o Tratado de Washington foi concebido com a clara intenção de manter a União Soviética sob controle. O objetivo conceituado era de defesa mútua contra um ataque armado a um país soberano por outro país soberano agressor. No entanto, a única vez na história em que a OTAN foi mobilizada foi para combater uma organização terrorista sem fronteiras baseada no Afeganistão, mas com tentáculos estendendo-se para o Iêmen, Paquistão e Somália. Este fato teria aberto um precedente válido para a mobilização da OTAN em resposta a um ataque cibernético "transfronteiriço", inclusive se realizado por um ator não-estatal, como a Al-Qaeda ou o regime talibã.

Como foi citado acima, o Artigo 5 define claramente a pedra angular do tratado, o conceito de autodefesa coletiva, a noção de que um ataque a um único membro da OTAN resultaria em uma reação coletiva por todos os membros. Este tratado não foi concebido como uma ameaça para o mundo, mas como uma promessa entre os aliados, baseada na crença que é de grande importância para a segurança global garantir que esses aliados não sejam individualmente vulneráveis, mas sim, coletivamente fortes. No caso da Estônia, Estado soberano membro da OTAN desde 2004, que foi submetido a um ataque de um grupo fora de suas próprias fronteiras, o elemento de defesa coletiva é facilmente verificável.

Ao contrário da potencialidade dos ataques ucranianos de 2015, que poderia facilmente ter evoluído a nível que justificasse a resposta pelo uso de força, sob os auspícios do direito internacional dos conflitos armados, o caso da Estônia excederia os limites de uma justificativa

contra os preceitos do uso da força. O Artigo 5 fala sobre a defesa coletiva contra um ataque armado contra um ou mais membros. O Capítulo VII, Artigo 51 da Carta da ONU apoia e espelha o Tratado de Washington ao reiterar que nada na Carta da ONU vai prejudicar o direito inerente de legítima defesa individual ou coletiva contra um ataque armado, no entanto, ele não esclarece o cerne da questão. Tal ponto crucial é a definição clara e atual de ataque armado. Certamente, em 1949, quando o Tratado de Washington foi redigido, os meios de conflito armado eram decididamente limitados. Sem uma definição clara existente no direito internacional, temos que presumir que os autores pretenderam que a definição fosse a de um bombardeio físico ou ataque que, em última análise, causasse morte e destruição dentro das fronteiras desse país soberano. Com armas se desenvolvendo a ponto de *drones* não tripulados patrulharem os céus e lançarem bombas no Paquistão e Iêmen, controlados pelos operadores militares norte-americanos sentados em instalações seguras a bordo da base Nellis da Força Aérea em Nevada, não há dúvida de que os autores originais não poderiam ter considerado este nível de avanço tecnológico. Entretanto, um bombardeio de uma vila por um *drone* não tripulado pode ainda ser facilmente alinhado dentro da definição geral de um ataque armado. Embora seja um salto tecnológico, não é um salto de lógica. Ainda se tem um país intencionalmente lançando um bombardeio hostil contra outro país soberano. Mas, se dermos mais um salto tecnológico para considerar armas cibernéticas, um salto lógico adicional também deve ser dado.

O Estado soberano da Estónia foi sem dúvida atacado em 2007. Pode-se até considerar o uso do exército *botnet* como um tipo de arma, embora não convencional, cujos recursos foram mobilizados e lançados por operadores centrais com o objetivo de causar danos e destruição à infraestrutura cibernética, governamental, financeira e de comunicações desse país soberano. Se aceitarmos o salto de lógica no sentido de que os agressores se armaram com esta arma *botnet* e lançaram tal arma contra a Estónia, poderíamos livremente argumentar que se trata de

um ataque armado que atende aos princípios de ambos os artigos 5 e 6 do Tratado de Washington. Porém, tal salto interpretativo, quando o assunto é guerra, é difícil de se dar. A comunidade internacional legitimamente teme a potencialidade de uma terceira guerra mundial. A mobilização física da OTAN contra a Rússia, por algo que se alega ter sido implementado por hackers individuais, é impensável e improvável de ser acordado por um comitê lúcido da OTAN.

O medo de uma guerra maior, uma guerra que saia de controle, é uma paranoia saudável para a comunidade internacional. Os líderes do conselho da OTAN devem considerar as ramificações políticas e diplomáticas de mobilizar-se para a defesa de um de seus próprios membros. Sendo esse o caso, um ataque armado teria que ser tanto audacioso quanto notório. Qualquer sombra de dúvida sobre a identidade do invasor iria imediatamente afastar qualquer consideração de retaliação. Ocultar a identidade de alguém nas profundezas do ciberespaço não é difícil. Quando um investigador considera que um alvo foi agredido por um exército de *botnet* de milhões de computadores zumbis através de uma rede fraca e que 99% desses computadores foram induzidos a participar involuntariamente do ataque, a realidade de identificar os usuários hostis é extremamente difícil. No entanto, no caso da Estônia, alguns pesquisadores mais inventivos encontraram algumas ligações interessantes com a Rússia. Ainda que não seja prova concreta, o ataque foi lançado na sequência de uma ameaça da Rússia em relação à remoção de uma estátua memorial, muitos dos sites da internet onde se discutiam e organizavam os ataques eram em idioma russo e, mais preocupante, nas semanas anteriores ao ataque da Estônia o site de um partido de oposição russo foi atacado por remanescentes da mesma *botnet* (DAVIS, 2007).

Enquanto no caso da Estônia o resultado foi o esperado, circunstâncias ligeiramente diferentes poderiam ter levado a conclusões radicalmente diferentes. Se esse mesmo exército de *botnets,* lançado pelos mesmos hackers, supostamente apoiados pela Rússia, atacasse a torre

do controle do Aeroporto do Lennart Meri Tallinn, o maior da Estônia, e este ataque resultasse na queda de um Boeing 777, com 283 mortes, a reação seria claramente diferente. A Estônia, junto com o resto do mundo, ficaria indignada, os perpetradores seriam perseguidos e a Estônia exigiria o apoio da OTAN. Tal ato terrorista iria justificar a aplicação do DICA, bem como do Artigo 5 do Tratado de Washington.

Tal plausível ataque cibernético enfureceria a comunidade mundial, mas a relativa ocultação que o ciberespaço fornece pode ser uma sombra suficiente que permite à Rússia evitar uma resposta armada. Tal analogia não é muito diferente do incidente com o MH17 malaio 777, que atravessou a Ucrânia, em julho de 2014, e foi abatido. Embora nem a Ucrânia nem a Malásia fossem membros da OTAN, o repúdio internacional contra a Rússia foi rápido e duro. Apesar das evidências em contrário, a Rússia continua a negar as acusações e nada foi feito em resposta a essa atrocidade. Ninguém considerou um contra-ataque e a Corte Internacional de Justiça das Nações Unidas ainda não considerou seriamente as acusações. Na ausência de acordos internacionais claramente redigidos, a negligência grosseira vista no acompanhamento desta atrocidade é o futuro provável para o tipo de resposta internacional a ser esperada após ataques cibernéticos até mesmo audaciosos e flagrantes (LEE & DURANDO, 2014).

3.3 Síntese

O ataque da Estônia de 2007, embora não tenha redundado em qualquer resposta, certamente ganhou a atenção do mundo. Como foi discutido anteriormente, tal ataque provocou o estabelecimento do Centro de Excelência de Defesa Cibernética Cooperativa da OTAN localizado em Tallinn, Estônia. Além disso, como apresentado em setembro de 2014 na Cúpula de Ministros da Defesa da OTAN no País de Gales, os representantes anunciaram uma nova política de defesa cibernética que elevaria a noção de um ataque digital para atender à definição do artigo 5 e obter uma defesa coletiva. Quando questionados pela mídia, os representantes da

OTAN não deram muitos detalhes em relação a qual limiar de um ataque cibernético iria desencadear uma resposta coletiva (RANGER, 2014).

O exame ora realizado do ataque contra a Estônia, ao lado das analogias apresentadas, que aumentam os riscos significativamente, apenas revelam a complexidade da situação em questão. Enquanto a Estônia foi prejudicada pelo ataque cibernético descrito, uma certa obscuridade do agressor novamente tornou muito difícil justificar uma resposta cinética. Embora a avaliação deste trabalho tenha revelado que uma resposta hostil ao ataque da Estônia não se aproximou de uma justificativa nos termos do DICA ou do Tratado do OTAN, é surpreendente considerar como um ataque *botnet* cibernético semelhante poderia fácil e claramente motivar uma resposta justificável. A analogia do aeroporto demonstrou efetivamente como um ataque digital semelhante lançado contra um alvo diferente poderia ter resultado em mortes e destruição consideráveis. Enquanto tal analogia é muito possível e benéfica para novos debates, o triste fato é que, como com o incidente da companhia aérea malaia de 2014, o ultraje mundial virá rapidamente, mas uma resposta cinética ou até mesmo judicial permanece improvável. De forma semelhante ao fácil bode expiatório em que se tornaram os supostos rebeldes ucranianos, o ciberespaço irá criar uma rede ainda mais nebulosa de bandeiras falsas e origens incertas, em que mesmo a política de defesa cibernética da OTAN recém atualizada seria incapaz de justificar uma resposta coletiva. Aceitar a noção de que a internet certamente continuará a permear nossas vidas e nossos pertences, juntamente com a noção de que armas cibernéticas mais avançadas estão destinadas a serem criadas, a realidade da guerra cibernética causando devastação no mundo físico é uma preocupação digna de provocar a união da comunidade internacional para uma solução comum. Uma solução que, como o Tratado do Atlântico Norte, possa se revelar demasiadamente perigosa para ser testada por não signatários e servir como uma garantia duradoura entre os signatários de que a proteção coletiva permanece.

Analisando as inferidas ramificações dos ataques da Ucrânia e da Estônia por meio da aplicação do que é tecnologicamente possível, este trabalho demonstrou como as leis e os tratados vigentes poderiam ser justificadamente aplicáveis em resposta a um ataque cibernético de repercussão nacional. Enquanto o exercício comparativo destacou a forma como os países oscilam à beira de um conflito armado ou intervenção internacional simplesmente em razão da utilização indevida de uma rede de computadores, o que é mais valioso entender e destacar são as lacunas enormes que existem em resposta a ameaças e ataques cibernéticos. O DICA e o Tratado de Washington têm um padrão extraordinariamente alto a ser atendido antes que possam justificar a morte de outras pessoas. A maioria dos ataques cibernéticos cometidos no nível nacional contra outros Estados estrangeiros não atende esse alto padrão. A enorme lacuna entre o que justifica uma resposta legal e todo o resto, deixa Estados vítimas com pouco recurso na maior parte do tempo. O capítulo seguinte irá apresentar um parâmetro legal para uma lei internacional dedicada a casos de ataque cibernético no nível nacional que não preenchem os critérios para uma resposta cinética.

4 A APLICAÇÃO DA LEI MARÍTIMA COMO UMA PARADIGMA PARA RESPOSTA INTERNACIONAL A ATAQUES CIBERNÉTICOS

Quando se examina historicamente a formulação do direito marítimo internacional, torna-se claro e aparentemente profético como os autores procuraram concordância, não só em termos e definições-chave e na importância da preservação da liberdade no alto-mar, mas também procuraram acordos que considerassem como pedra angular a responsabilidade dos países de policiarem individualmente suas próprias águas. Este capítulo vai examinar tanto a histórica Declaração de Paris, elaborada em 1856, como a atual Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), e analisar o valor desses parâmetros para aplicabilidade à questão atual da liberdade econômica e pessoal no ciberespaço, à defesa contra a guerra cibernética e à retaliação contra os Estados ou atores não-estatais que lançam ataques através desse meio.

4.1 A Declaração de Paris

Enquanto o terrorismo era conhecido e a Al-Qaeda uma preocupação dos governos mundiais, em 11 de setembro de 2001, o homem comum foi audaciosamente apresentado a este inimigo sem fronteiras, cujos ataques impactaram sensivelmente os mercados financeiros globais e severamente impactaram a mobilidade pessoal e o sentido de segurança que cidadãos ocidentais anteriormente experimentavam. Sob a liderança do presidente George W. Bush, os EUA responderam com uma mão pesada, ansiosos para caçar o inimigo sem Estado, onde quer que estivesse. Como foi discutido no capítulo anterior, sob os auspícios da OTAN, grande parte

do mundo uniu-se sob a forma de uma resposta coletiva chamada ISAF[8], demonstrando conjuntamente que o mundo não iria aquiescer ao terror em silêncio. Em seu auge, quando os mercados globais foram implacavelmente assaltados mais de um século e meio atrás pela ameaça sem fronteiras da pirataria, um grupo de Estados também se uniram para desenvolver a Declaração de Paris, a qual alterou a forma como o mundo via e abordava a pirataria, eventualmente estabilizando os mercados de comércio mundial e as economias interligadas (SINGER & FRIEDMAN, 2014).

Embora a filosofia da liberdade dos mares tenha servido como um acordo internacional desde o início do século XVII, a Declaração de Paris foi o primeiro esforço concertado da comunidade internacional para escrever um acordo a ser assinado pelos países participantes, expressamente criminalizando os marginais que, com missões egoístas, estavam interrompendo o desenvolvimento de uma nova economia mundial em expansão, através da conectividade proporcionada pelo alto-mar. A premissa dos signatários foi presciente no sentido de que os fundadores sabiam a importância de destacar a responsabilidade nacional para resolver os problemas globais da época. Foi uma decisão unificada de erradicar a pirataria em benefício do comércio internacional e da segurança do alto-mar. O notório pensador P.W. Singer, anteriormente referido neste trabalho, juntamente com Allan Friedman, escreveu um livro metodicamente compilado em 2014 intitulado "*Cybersecurity and Cyberwar"* no qual escrevem:

> Logo um webwork dos acordos foi estabelecido que fixou um princípio geral de comércio aberto através dos altos-mares. Os acordos, alguns bilaterais e outros multilaterais, também afirmaram que a soberania marítima só seria respeitada quando um país assumisse a responsabilidade por quaisquer ataques que emanassem de dentro suas fronteiras. Lentamente, mas com firmeza, eles abriram o caminho em direção a um código de conduta global. Em 1856, quarenta e dois países concordaram com a Declaração de Paris que aboliu a guerra de corso e formalmente transformou os piratas de atores aceitos para párias internacionais a serem perseguidos pelas grandes potências todo o mundo (Singer & Friedman, 2014, pg. 179, tradução nossa).

[8] "ISAF foi uma das maiores coalizões da história e é a missão mais desafiadora da OTAN até a presente data. Em seu auge, a força era mais do que 130.000 fortes, com tropas de 51 países da OTAN e de parceiros" (Relatório Arquivado da OTAN, 2015, tradução nossa)

Digna de nota em particular na referência acima é a noção de que, para que a verdadeira soberania marítima ocorra em alto-mar, os países devem assumir a responsabilidade pela violência que se origina a partir do interior de suas próprias fronteiras. Esse conceito específico ecoa hoje em relação às questões de liberdade cibernética. Tome-se como exemplo os ataques contra a Ucrânia e a Estônia a partir do interior das fronteiras russas. Como sabiam os líderes mundiais com clareza presciente mais de um século e meio atrás, para que o mundo conheça verdadeiramente a segurança no ciberespaço os países de onde os ataques cibernéticos se originam devem assumir a responsabilidade por este caos. Até o momento a Rússia não fez nenhum esforço para descobrir as identidades ou legalmente perseguir os hackers envolvidos em ambos os incidentes previamente discutidos. Assim como no início do século XIX, um mundo que aceita a criminalidade e a violência irá receber exatamente isso. Apenas se as nações do mundo se unirem para reconhecer o problema e se comprometerem a, coletivamente, defender e responder aos ataques cibernéticos e também para erradicar com fervor a origem desses ataques que partam de dentro de suas próprias fronteiras, a epidemia será erradicada. Ainda que exista tal acordo, um observador casual pode considerar a apatia da Rússia em caçar esses *hackers* como, no mínimo, altamente irresponsável e, na pior das hipóteses, um indicativo de cumplicidade.

4.2 Convenção das Nações Unidas sobre o Direito do Mar (CNUDM)

O preâmbulo da CNUDM deixa claro seus princípios universais. Digna de nota foi a motivação, fundada em um desejo de se estabelecer, através da compreensão e cooperação mútuas, questões relacionadas ao mar. Conscientes de que as questões do espaço do mar estão intimamente relacionadas e devem ser consideradas como um todo, reconhecendo o devido respeito pela soberania do Estado, o desejo por uma ordem jurídica sobre o alto-mar e oceanos

para facilitar a comunicação e promover o uso pacífico e equitativo dos recursos, bem como um esforço concertado para a sua conservação, os signatários fundadores da CNUDM:

> Convencidos de que a codificação e o desenvolvimento progressivo do direito do mar alcançados na presente Convenção contribuirão para o fortalecimento da paz, da segurança, da cooperação e das relações de amizade entre todas as nações, de conformidade com os princípios de justiça e igualdade de direitos e promoverão o progresso econômico e social de todos os povos do mundo, de acordo com os Propósitos e Princípios das Nações Unidas, tais como enunciados na Carta" (Preâmbulo, CNUDM, 1982, pg 1).

Enquanto o conceito de responsabilidade nacional e autopoliciamento para o fortalecimento da comunidade internacional se alinham tanto com a caça aos piratas quanto com os hackers, os princípios estabelecidos no preâmbulo da CNUDM são essencialmente os mesmos ao que é necessário para a estabilização internacional do ciberespaço. Se seguissemos linha por linha o preâmbulo, bem além da paráfrase do parágrafo anterior, e substituíssemos mar ou oceano por ciberespaço em cada argumento, teríamos essencialmente um preâmbulo viável e bem aplicável ao mundo cibernético.

Michael W. Reed, na coleção intitulada "*Selected Contemporary Issues in the Law of the Sea",* observou que a CNUDM foi uma realização diplomática extraordinária e apropriadamente se referiu a ela como uma constituição para os oceanos. Ainda que o conceito de caça aos piratas continue aplicável, a CNUDM apresenta uma abordagem muito mais complexa para organizar os mares, de uma forma que o clamor da Declaração de Paris por uma simples ordem não alcançou, especificamente no estabelecimento de zonas econômicas exclusivas. Semelhante às águas interiores, mar territorial e zona contígua, esta zona de jurisdição marítima adicional existe com o único propósito de promover e proteger o desenvolvimento da economia internacional e do comércio livre. Na mesma linha da Declaração de Paris, a CNUDM exige responsabilidade tanto dos países envolvidos quanto dos usuários. Além do dever de um Estado em particular de vigiar suas águas, também existe uma

responsabilidade dos operadores do navio de saberem em que zona estão operando e agir em conformidade (SIMMONS, 2011).

A CNUDM não pretende regular os mares, ela simplesmente organiza esse meio massivo em algo viável. Algo com que tanto os países afetados como os usuários podem concordar. Como foi o caso com o preâmbulo, a referência ao estabelecimento das zonas também tem aplicabilidade ao ciberespaço. No ciberespaço, a questão da soberania é difícil de determinar até que o ataque cibernético transponha o mundo digital para o mundo físico. Com a soberania sendo um preceito fundamental tanto para o DICA quanto para os princípios do Tratado de Washington, seria extraordinariamente valioso buscar uma organização ampla do ciberespaço na maneira em que a CNUDM proporciona para o mar.

A aplicação de uma zona territorial ao ciberespaço, mesmo que apenas para a existência de sites do governo, ofereceria a justificativa sob as leis vigentes como um ataque contra um país soberano quando os sites do governo ou militares desse país fossem violados, desligados ou vandalizados. Além disso, o estabelecimento de uma zona econômica exclusiva cibernética semelhante teria grande aplicabilidade para a proteção deste meio, no qual, de acordo com um relatório de 2016 da Agência do Censo dos EUA, houve a troca de US$ 92,8 bilhões, considerando apenas sites de *e-commerce* de varejo americanos. O estabelecimento internacional formal de tais zonas cibernéticas, juntamente com uma comunidade internacional dedicada a mantê-las e aplicar duras consequências quando houver violação, será tremendamente positivo para a segurança e a liberdade econômica que o mundo deseja desfrutar no ciberespaço.

Como também descrito na CNUDM, o conceito de passagem inocente refere-se à passagem livre de navios pelas águas territoriais atribuídas a outros países. A lei estipula que tal passagem não deve ser prejudicial à paz, à boa ordem ou à segurança do Estado costeiro. Mais especificamente, o uso dessas águas para ameaçar ou usar a força, para testar armas de

qualquer tipo, para coletar inteligência sobre o Estado costeiro, qualquer ato de propaganda que afete a defesa do Estado, o lançamento de dispositivos militares, e também o desembarque de produto contrário às leis do país em questão, serão proibidos e a passagem desse navio será considerada prejudicial para a paz e a boa ordem. Este aspecto da lei também se alinha perfeitamente com os problemas enfrentados no ciberespaço. Assim como os autores da CNUDM tentaram dar um sentido territorial à vastidão do oceano, os líderes de hoje devem fazer o mesmo com a infinitude da internet. Definir melhor os termos, para que o ciberespaço comece a ser organizado em torno das fronteiras físicas de onde a informação emana, irá permitir que o cidadão comum desfrute de passagem inocente pelas águas territoriais de qualquer rede do ciberespaço, ao mesmo tempo que torna ilegal o uso prejudicial de tais redes no modo descrito na CNUDM.

Se um acordo cibernético, por exemplo, identificar os sites a partir dos respectivos servidores que os hospedam, originados de um Estado determinado ou cuja rede é gerida ativamente por uma empresa física localizada em um determinado país, podemos começar a organizar a responsabilidade, não para controlar, mas para gerir as questões quando e se elas surgirem. A vítima deve ter uma autoridade claramente definida dentro de suas fronteiras, que iria responder a ataques cibernéticos e que poderia, então, iniciar um inquérito e coordenar com um organismo internacional de organizações similares, ou com um semelhante serviço de investigação sobre questões digitais localizado no Estado ofensor. Assim como na passagem inocente de navios, a identificação pública com a bandeira do Estado de origem é crucial.

Continuando o tema de responsabilidade, a pedra angular da CNUDM é que o país em questão deve assumir a responsabilidade pelos navios ofensivos que operam em águas internacionais ou costeiras. Como a bandeira de origem do navio, cada usuário da internet

mantém um endereço do Protocolo de Internet (IP)[9] em particular que os identifica como sendo proveniente de um determinado país. Como faz um capitão do navio, o usuário da internet tem a responsabilidade de hastear a sua bandeira corretamente para desfrutar livremente da passagem inocente através do ciberespaço. Novamente, como tem funcionado por décadas dentro do sector marítimo, países ofendidos investigam navios ofensores e coordenam e esperam cooperação investigativa e possíveis represálias de outros. Ainda que mudar um endereço IP possa ser tão simples quanto trocar uma bandeira de pano, o objetivo é estimular a arquitetura de um acordo internacional que reconheça tanto a responsabilidade pessoal quanto a estatal quando se opera dentro de um meio internacional.

O conceito da CNUDM de perseguição imediata, ou em inglês *hot pursuit*, revela questionamentos interessantes quando se considera a questão sob a ótica do ciberespaço. A CNUDM afirma que a perseguição imediata pode ser empreendida quando um Estado acredita que um navio infrator tenha violado as suas leis e regulamentos locais. A perseguição deste navio pode ser iniciada enquanto o navio suspeito ainda está dentro das águas territoriais do país vítima e um governo pode continuar a perseguição fora de suas águas territoriais sob os auspícios da cláusula da perseguição imediata. Enquanto os ataques cibernéticos coordenados de nível nacional, sob a liderança das forças armadas, são raros, o acesso ilegal às redes de computadores soberanas por *hackers* estrangeiros é extremamente comum. Considere-se, por exemplo, a suspeitada invasão do Escritório de Gestão de Pessoal (OPM) do Governo dos EUA, em dezembro de 2014 por *hackers* supostamente trabalhando para o governo chinês. O governo

[9] "Um endereço do Internet Protocol (IP) é um identificador numérico único atribuído a cada computador conectado à Internet. Um Provedor de Serviço da Internet (a sigla em inglês é ISP) normalmente controla uma variedade de centenas ou milhares de endereços IP, que ele atribui aos clientes para a sua utilização. O ISP pode atribuir endereços do IP de maneira dinâmica ou estática. No caso da atribuição dinâmica, cada vez que o usuário acessa o ISP para se conectar à internet, o ISP atribui um dos endereços do IP disponíveis que controla para o computador do cliente para a duração da sessão do cliente (por exemplo, até que ele ou ela desconecte). Cada vez que o cliente se conecta à Internet, ele pode receber um endereço do IP diferente. Por outro lado, um usuário com um endereço do IP estático geralmente tem uma conexão de internet permanente 24 horas e um endereço do IP que permanece constante ao longo de semanas ou meses" (tradução nossa). Disponível em <http://www.adnetadvertising.com/whatis_ipaddress.html>. Acesso em: 01.ago.2016.

dos EUA teve que notificar oficialmente 22 milhões de funcionários federais e ex-membros do serviço militar deque os seus dados pessoais poderiam ter sido comprometidos. Na época da violação, o governo dos EUA tinha sido ingênuo e acabou ficando com poucos recursos para além de perseguições diplomáticas. Em dezembro de 2015, foi relatado pelo "*The Wall Street Journal"* que as autoridades chinesas haviam prendido alguns dos *hackers* que se acreditava estarem envolvidos nas múltiplas violações ao OPM. Enquanto muitos ainda acreditam que os *hackers* foram contratados pelo Ministério da Segurança do Estado chinês, na superfície, a aparência de cooperação marca a primeira vez em que governos deste nível cooperaram em relação a uma resposta jurídica na sequência de um ataque cibernético e a prisão ligada ao *cyber* crime foi a mais significativa na história. Considerando que o OPM seria um alvo tedioso para *hackers* criminosos comuns, especialistas ainda acreditam que este *seria* simplesmente um caso da espionagem cibernética perpetrado em nome de um governo estrangeiro. Enquanto os EUA aprende com essas violações e continua a desenvolver as suas defesas cibernéticas, pode-se considerar plausível que no futuro próximo será possível alertar as autoridades de defesa cibernética e imediatamente responder a sondagens ou violações em redes do governo. Considerando o caso do OPM, a arquitetura jurídica proporcionada pela política da CNUDM quanto à perseguição imediata pode fornecer um recurso expedito para os governos empregarem quando detectarem hackers tentando violar ou ativamente violando as suas redes. Ao expandir esse conceito para o domínio cibernético, pode-se ver claramente a aplicabilidade de perseguir a localização de hackers através do ciberespaço, desativando as suas redes domésticas com armas cibernéticas para garantir que todos os dados roubados sejam excluídos e para notificar as autoridades locais (Nakashima, 2015).

No artigo dois da CNUDM, um órgão internacional de especialistas é estabelecido, chamado Organização Marítima Internacional (IMO). Cada signatário está autorizado a nomear especialistas reconhecidos de setores aplicáveis para atuar neste comitê internacional,

criado para aplicara CNUDM e resolver conflitos internacionais. Ampliando a análise de questões atuais da cibernética diante do quadro da CNUDM, o observador comum pode detectar muitos paralelos. A julgar pela falta de resposta em ambos os casos da Ucrânia e Estônia já discutidos, um tal órgão internacional de especialistas com autoridade internacionalmente reconhecida para investigar e buscar arbitragem contra ofensores cibernéticos teria sido um encaixe perfeito.

Estes países foram atacados de forma indefensável e contaram com pouca capacidade para responder significativamente. De fato, as evidências descobertas em relação à Ucrânia e Estônia vieram de empresas privadas da segurança cibernética, que foram contratadas ou se ofereceram para investigar. A Estônia tinha uma força tarefa cibernética local altamente avançada conhecida como o *Computer Emergency Response Team* (CERT), a qual buscou assistência dos membros do *Internet Architecture Board* (IAB) e da *Internet Engineering Task Force* (IETF), especificamente representantes da Suécia e dos EUA, que os ajudaram principalmente a recuperar o controle de suas redes, resolver o bombardeio da atividade e restaurar a funcionalidade para os usuários nacionais, para quem uma conexão com a internet tinha se tornado tão essencial no lar quanto à eletricidade (KEATING, 2007). Apesar desses recursos incomuns, bem como das extraordinárias provas descobertas ligando o governo russo ao ataque, a investigação estagnou. No trabalho acadêmico produzido para o Centro de Excelência de Defesa Cibernética Cooperativa da OTAN escrito em 2010 intitulado *"International Cyber Incidents: Legal Considerations"*, os autores declaram que:

> O estudo de caso da Estônia fornece um exemplo de um país que tinha extensa legislação relevante para incidentes cibernéticos, mas ainda não tinham previsões legais para investigar e processar os ataques politicamente motivados que não tinham motivação de lucro. Este exemplo ilustra também a necessidade de acordos internacionais, ou padrões uniformes de melhores práticas, para as autoridades de resposta e de investigação e para a indústria privada (Tikk, Kaska & Vihul, 2010, tradução nossa).

Assim como a IMO é uma autoridade competente, sob os auspícios da ONU, criada para facilitar a conformidade com a CNUDM, o ciberespaço precisa de um órgão semelhante para facilitar a conformidade com as normas internacionais aceitas, referentes ao uso da internet por indivíduos, governos, empresas privadas e pelos militares em tempos de conflito.

4.3 Síntese

O presente trabalho destacou vários incidentes, maiores e menores, que expressam a necessidade urgente de um código de conduta internacional sobre o qual o mundo concorde, possa cumprir e possa trabalhar para aplicar globalmente. Através de uma análise detalhada tanto da Declaração de Paris e, depois, da Convenção das Nações Unidas sobre o Direito do Mar, este trabalho tem demonstrado um alinhamento entre os problemas que o mundo enfrenta hoje com a segurança cibernética e as questões que nossos antepassados enfrentaram em matéria de segurança marítima um século e meio atrás. A Declaração de Paris, no contexto das questões atuais, serve como um chamado às armas. Deve ser um alerta ao mundo, implorando pela necessidade de definir o problema e, em seguida, trabalhar em conjunto para extirpá-lo. O acordo de todos os Estados acerca de uma definição unificada de ataque cibernético e guerra cibernética, concordando com a obrigação nacional de cada país de erradicar as fontes de infrações que emanam de dentro das suas próprias fronteiras é essencial.

A CNUDM serve como uma guia estável para o futuro, um quadro válido que pode ser facilmente aplicado ao ciberespaço. A comunidade internacional deve seguir esse exemplo sob os auspícios das Nações Unidas. Ela deve redigir um preâmbulo com a contribuição internacional, indicando os motivos pelos quais a liderança global concorda com a iniciativa de produção do documento, consciente do alcance e impacto globais, o que deve ser reconhecido na busca de um acordo como esse, o que a comunidade global espera de tal acordo, o que ela

acredita ser possível, e para o que ela irá sustentar. Após a elaboração desse preâmbulo, que daria a um corpo de especialistas, selecionados globalmente, uma intenção a ser seguida, uma série de artigos pode ser elaborada. Estes artigos devem definir a forma como os recursos e os problemas associados com o uso de tais recursos não é considerada em sintonia com o bem mundial. Eles devem definir o ciberespaço em termos de governos territoriais existentes e atribuir o ônus de policiar o seu próprio ciberespaço aos respectivos governos. Eles devem descrever um código de conduta, semelhante ao de passagem inocente, apontando o que nas águas territoriais e no alto-mar do ciberespaço é aceitável e o que não é. Finalmente, deve estabelecer um órgão internacional tal qual a IMO; um grupo de especialistas que podem supervisionar os termos do acordo, resolver disputas entre Estados e atores infra estatais, facilitar as investigações quando a capacidade local ficar estagnada. Eles atuariam em coordenação, através de meios diplomáticos ou judiciais, para informar e permitir aos líderes mundiais buscar sanções contra Estados que lancem ataques cibernéticos ilegais ou que apoiem ou deem abrigo a indivíduos ou grupos que o fazem.

5 CONCLUSÃO

Na entrevista de 2007 com Joshua Davis da revista *WIRED*, o Presidente do Parlamento da Estônia, Ene Ergma disse: "Assim como a radiação nuclear, a guerra cibernética não faz você sangrar, mas pode destruir tudo". E era assim que a Estônia se sentia, como se tivesse sido bombardeada em seu interior, com pouco recurso para perseguir o que acreditava ser necessário, defesa, retribuição, talvez até mesmo vingança. Infelizmente, na ausência de verdadeiros princípios internacionais para o uso da internet, esses grupos marginais e Estados desonestos continuarão a tirar proveito dessa fronteira menos vigiada, para aterrorizar países e indivíduos que desejam explorar, trocar ideias e realizar transações via ciberespaço.

A internet está se tornando mais invasiva a cada segundo, parece que cada nova versão de um produto antigo agora tem conectividade com a internet. Esta penetração está acontecendo em uma velocidade que nossas mentes sequer conseguem acompanhar. Tais aparelhos conectados abrem enormes janelas na intimidade de nossas casas e permitirão que os *hackers* ganhem controle dos aspectos mais inócuos da vida de alguém. Se extrapolarmos o problema a partir desses itens inócuos e considerarmos as vulnerabilidades similares nos sites de nossa infraestrutura crucial nacional, as ramificações podem ser fatais. Se consideramos as vulnerabilidades semelhantes em uma usina química ou nuclear, as consequências não seriam apenas mortais, mas poderiam resultar em destruição em massa.

Após analisar os fatos relativos ao ataque cibernético contra a Ucrânia à luz do DICA, ficou claro que, embora tivesse sido altamente perturbador e prejudicial, não teria atendido a todos os princípios necessários para justificar uma resposta armada. No entanto, isso não nega a possibilidade de consequências letais resultantes do mesmo ataque. Na verdade, são possíveis e até prováveis, dadas as mesmas circunstâncias. Nesse caso, a análise habilmente demonstrou que o mesmo ataque com consequências diferentes poderia ter atingido os princípios

necessários para justificar o uso da força física contra o país ofensor, na forma de retaliação. Como é explicado detalhadamente no Manual de Tallinn, existe a possibilidade, no âmbito da legislação internacional em vigor, de lançar um contra-ataque contra um país ou contra um *hacker* na sequência de um ataque cibernético que justifique o uso da força com base no DICA.

Uma análise do ataque à Estônia sob a consideração de uma resposta armada da OTAN resultou em uma negativa clara. No entanto, ao contrário DICA, a OTAN vem com uma característica muito mais politicamente orientada. Mesmo com resultados de um ataque DDOS semelhante contra um alvo mais criticamente vulnerável, como o exemplo da torre de controle do ar, a análise ainda assim resultou em uma provável resposta negativa da OTAN. Considerando que a OTAN exige unanimidade para gerar uma resposta coletiva, a vítima, apesar do ataque, terá que enfrentar o posicionamento político de cada Estado-Membro. Provavelmente, os outros signatários da OTAN terão menos apetite para a guerra, estarão decididamente menos incomodados que o país em questão, e se prenderão mais facilmente às dúvidas acerca da responsabilidade geradas pela nebulosidade do ciberespaço.

Após a análise dos dois ataques cibernéticos de nível nacional, ao mesmo tempo em que conclui-se que, sob circunstâncias específicas, as leis internacionais existentes poderiam ser aplicáveis para orientar a resposta de um governo, ainda existem lacunas consideráveis. Na busca de um parâmetro aplicável a partir do qual se inicie o diálogo sobre um código de conduta cibernético internacional, este artigo reavaliou tanto a Declaração de Paris como a Convenção das Nações Unidas sobre o Direito do Mar.

Após examinar a Declaração de Paris de 1856, deve-se reconhecer o grandioso esforço diplomático que resultou em definições marítimas internacionalmente reconhecidas, possibilitando acordos para perseguir os criminosos de então. Uma análise da atual Convenção das Nações Unidas sobre o Direito do Mar, alinhada com os problemas enfrentados no ciberespaço, apurou que a CNUDM oferece estrutura aplicável sobre a questão da segurança

cibernética. Para avançar, os líderes mundiais devem se unir para fornecer uma intenção clara e um grupo de especialistas deve ser formado para considerar uma série de artigos a respeito dos quais os países do mundo possam concordar. Para além de qualquer lei que possa ser escrita, a análise dos acordos existentes resultou na avaliação de que a pedra angular de qualquer tratado bem-sucedido será a aceitação de cada Estado em assumir a responsabilidade pelo que ocorre ou emana de suas "águas cibernéticas" territoriais.

Assim como o mundo um século e meio atrás estava pronto para agir contra o flagelo da pirataria que estava devastando a economia internacional, a nossa sociedade se encontra hoje no precipício de uma mudança necessária, da mesma forma que nossos antepassados. O tema da discussão pode ser diferente, a tecnologia certamente anos-luz à frente, no entanto, a raiz do problema é exatamente a mesma. Uma sociedade ansiando pela liberdade de navegar, sem medo de ataque, pelo seu recém-descoberto meio que os conecta ao mundo à sua volta.

REFERÊNCIAS

BING, Chris. *As US Cyber Command's Future Is Decided, Eyes Turn to Maryland.* DCInno, 2016. Disponível em: <http://dcinno.streetwise.co/2016/05/23/2017-defense-bill-how-uscybercom-becomes-unified-command-md/>. Acesso em: 27 de maio de 2016.

BOOTHBY, William, H. *Weapons and the Law of Armed Conflict.* Oxford University Press, 2009. 464 p.

BROWN, Rich. *Touchscreen refrigerators and talking everything at CES 2016.*CNET, 2016. Disponível em: <http://www.cnet.com/news/touchscreen-refrigerators-and-talking-everything-at-ces-2016/>. Acesso em: 30 de maio de 2016.

BURRUS, Daniel. *The Internet of Things Is Far Bigger Than Anyone Realizes.* WIRED Magazine, 2014. Disponível em: <http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/>. Acesso em: 30 de maio de 2016.

DAVIS, Joshua. *Hackers Take Down the Most Wired Country in Europe*. WIRED Magazine, 2007. Disponível em: <http://www.wired.com/2007/08/ff-estonia/>. Acesso em: 11 de abril de 2016.

DYER, John. *German Official Sounds Alarm Over the Dilapidated State of the Country's Military.* Vice News, 2016. Disponível em: <https://news.vice.com/article/german-official-sounds-alarm-over-the-dilapidated-state-of-the-countrys-military>. Acesso em: 27 de maio de 2016.

ELKIND, Peter. *Inside the Hack of the Century.* Fortune Magazine, 2014. Disponível em: <http://fortune.com/sony-hack-part-1/>. Acesso em: 30 de maio de 2016.

GERTZ, Bill. *FBI Warns of Cyber Threat to Electric Grid: DHS intel report downplayed cyber threat to power grid.* The Washington Free Beacon, 2016. Disponível em: <http://freebeacon.com/issues/fbi-warns-cyber-threat-electric-grid/>. Acesso em: 09 de abril de 2016.

GREENBERG, Andy. *Hackers Remotely Kill a Jeep on the Highway—With Me in It.* WIRED Magazine, 2015. Disponível em: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>. Acesso em: 30 de maio de 2016.

HOLLIS, David. *Cyberwar Case Study: Georgia 2008*. Small Wars Journal, 2011. Disponível em: <http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>. Acesso em: 10 de julho de2016.

INFORMATION AGE. *Security backdoor found in China-made US military chip: Cambridge University researchers find that a microprocessor used by the US military but made in China contains secret remote access capability.* Information Age, 2012. Disponível em: <http://www.information-age.com/technology/security/2105468/security-backdoor-found-in-china-made-us-military-chip>. Acesso em: 27 de maio de 2016.

KEATING, Joshua. *The 13 geeks who rule the Internet.* Foreign Policy Magazine, 2007. Disponível em: <http://foreignpolicy.com/2007/09/05/the-13-geeks-who-rule-the-internet-updated>. Acesso em: 30 de maio de 2016.

LEE, Jolie; DURANDO, Jessica. *Malaysia Airlines Flight 17 crash: What we know.* USA Today, 2014. Disponível em: <http://www.usatoday.com/story/news/nation-now/2014/07/18/malaysian-airlines-mh17-crash/12825433/>. Acesso em: 30 de maio de 2016.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Metodologia científica*: ciência e conhecimento científico, métodos científicos, teoria, hipóteses e variáveis e metodologia jurídica. 6. ed. São Paulo: Atlas, 2011.

MESERVE, Jeanne. *Staged Cyber Attack Reveals Vulnerability in Power Grid.* CNN, 2007. Disponível em: <http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html>. Acesso em: 26 de maio de 2016.

NAKASHIMA, Ellen. *Chinese Government Has Arrested Hackers it Says Breached OPM database.* The Wall Street Journal, 2015. Disponível em: <https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html>. Acesso em: 16 de julho de 2016.

NISSENBAUM, Dion. *Author Warns U.S. Military to Focus on China.* The Wall Street Journal, 2015. Disponível em: <http://www.wsj.com/articles/author-warns-u-s-military-to-focus-on-china-1435539010>. Acesso em: 27 de maio de2016.

NOAH, Timothy. *Birth of a Washington Word: when warfare gets "kinetic."* Slate Magazine, 2002. Disponível em: <http://www.slate.com/articles/news_and_politics/chatterbox/2002/11/birth_of_a_washington_word.html>. Acesso em: 27 de maio de 2016.

NORTH ATLANTIC TREATY ORGANIZATION. *Collective Defense - Article 5.* NATO Archived Reports, 2016. Disponível em: <http://www.nato.int/cps/en/natohq/topics_110496.htm>. Acesso em: 29 de maio 2016.

NORTH ATLANTIC TREATY ORGANIZATION. *ISAF's Mission in Afghanistan (2001-2014).* NATO Archived Reports, 2015. Disponível em: <http://www.nato.int/cps/en/natohq/topics_110496.htm>. Acesso em: 27 de maio de 2016.

NORTH ATLANTIC TREATY ORGANIZATION. *The North Atlantic Treaty.* Washington, D.C., 1949. Disponível em: <http://www.nato.int/cps/en/natolive/official_texts_17120.htm>. Acesso em: 27 de maio de 2016.

RANGER, Steve. *NATO Updates Policy: Offers Members Article 5 Protection Against Cyber Attacks.* Atlantic Council, 2014. Disponível em: <http://www.atlanticcouncil.org/blogs/natosource/nato-updates-policy-offers-members-article-5-protection-against-cyber-attacks?tmpl=component&print=1>. Acesso em: 27 de maio de 2016.

SCHMITT, Michael, N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, England, 2013. 282 p.

SIMMONS, Clive R. *Selected Contemporary Issues in the Law of the Sea.* Martinus Nijhoff Publishers, The Netherlands, 2011. 359 p.

SINGER, Peter W; FRIEDMAN, Allan. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press, England, 2014, 306 p.

TIKK, Eneken; KASKA, Kadri; VIHUL, Liis. *International Cyber Incidents: Legal Considerations.* Cooperative Cyber Defense Center of Excellence, 2010. Disponível em: <https://ccdcoe.org/publications/books/legalconsiderations.pdf>. Acesso em: 27 de maio de 2016.

UNITED NATIONS. *Chapter VII: Action With Respect To Threats To The Peace, Breaches Of The Peace, And Acts Of Aggression.* United Nations Charter, 1945. Disponível em: <http://www.un.org/en/sections/un-charter/chapter-vii/index.html>. Acesso em: 29 de maio de 2016.

UNITED NATIONS. *United Nations Convention on the Law of the Sea.* United Nations, 1982. Disponível em: <http://www.un.org/depts/los/convention_agreements/texts/CNUDM/CNUDM_e.pdf>. Acesso em: 11 de abril de 2016.

UNITED STATES CENSUS BUREAU. *Quarterly Retail E-Commerce Sales, 1st Quarter 2016.* United States Department of Commerce, Washington, D.C, 2016. Disponível em: <https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf>. Acesso em: 29 de maio de 2016.

WILLIAMS, Phil. *North Atlantic Treaty Organization: NATO.* Clio Press, Oxford, England, 1994. 285 p.

WITTE, Brian. *Defense Secretary Discusses Concerns in South China Sea.* The Washington Times, 2016. Disponível em: <http://m.washingtontimes.com/news/2016/may/27/usna-to-graduate-first-students-with-cyber-operati/>. Acesso em: 27 de maio de 2016.

YARDON, Danny. *Iranian Hackers Infiltrated New York Dam in 2013: Cyberspies had access to control system of small structure near Rye in 2013, sparking concerns that reached to the White House.* The Wall Street Journal, 2015. Disponível em: <http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559>. Acesso em: 27 de maio de 2016.

ZETTER, Kim. *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. WIRED Magazine, 2014. Disponível em: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>. Acesso em: 27 de maio de 2016.

ZETTER, Kim. *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.* WIRED Magazine, 2016. Disponível em: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>. Acesso em: 09 de abril de 2016.