ESCOLA DE GUERRA NAVAL

ALEXSANDRE TEIXEIRA DE VASCONCELOS

A GUERRA CIBERNÉTICA NO CONFLITO DA RUSSIA VERSUS GEORGIA (2008):
A regulamentação da guerra cibernética em um conflito entre Estados

Rio de Janeiro

2014

ALEXSANDRE TEIXEIRA DE VASCONCELOS

A GUERRA CIBERNÉTICA NO CONFLITO DA RUSSIA VERSUS GEORGIA (2008):
A regulamentação da guerra cibernética em um conflito entre Estados

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

Orientador: CMG (FN) GUILHERME

Rio de Janeiro
Escola de Guerra Naval
2014

RESUMO

Esta monografia teve por escopo fazer uma reflexão acadêmica a respeito da aplicabilidade do Direito Internacional na guerra cibernética. O objetivo da pesquisa foi examinar se os ataques às redes de computadores e ao sistema financeiro da Geórgia, realizados durante o conflito entre Rússia e Geórgia (2008) pode ser considerado uma guerra cibernética, bem como verificar a adequação dos atuais paradigmas do jus in bello e do jus ad bellum para regulamentar os conflitos no espaço cibernético. Verificamos que a aplicação das atuais regras do Direito Internacional, combinadas com critérios técnicos seguros para determinar a autoria e a origem de um ataque, bem como a necessidade e a proporcionalidade da resposta, indicam que é possível regulamentar a guerra cibernética empregando as leis internacionais vigentes, algumas datadas do século XIX. Foi possível identificar que o Manual de Tallinn, mesmo não sendo um documento oficial, deve auxiliar as leis e regulamentos internacionais, como a Carta da ONU, o Direito Internacional Humanitário, o Direito de Genebra, de Haia e de Nova Iorque, bem como os princípios, usos e costumes do Direito Internacional, a Cláusula Martens, os tratados e as normas internas, para disciplinar a guerra cibernética, em especial no que diz respeito à proteção de bens e pessoas civis. Os principais limites são o princípio da distinção, da precaução e da vedação de ataques indiscriminados. Além disso, a ciberguerra, por sua vez, também pode levar a crimes de guerra online, e mesmo a participação direta de civis em hostilidades no espaço cibernético, pode ser balizada pelas regras dos conflitos armados, sujeitos às jurisdições nacionais e à jurisdição do Tribunal Penal Internacional, cujo Estatuto poderá, futuramente, ser alterado para incluir expressamente as armas e hostilidades cibernéticas. Esta dissertação visa ainda, demonstrar como as leis de guerra, podem ser flexíveis o suficiente para acomodar as novas realidades do conflito digital, e concluir que uma guerra não deixa de ser uma guerra, simplesmente, porque está acontecendo no mundo virtual.

PALAVRAS CHAVE – Guerra Cibernética. Armas Cibernéticas. Carta da ONU. Direito Internacional Humanitário. Princípios. Usos e Costumes da Guerra. Cláusula Martens. Tribunal Penal Internacional. Manual de Tallinn.

SUMÁRIO

1 INTRODUÇÃO

Antes de iniciarmos este estudo científico, devemos definir alguns pressupostos que ajudarão a entender melhor o problema central da tese que desenvolveremos a partir de agora.

Primeiramente, abordaremos um assunto bastante atual e que já faz parte do cotidiano de vários países no mundo, mas que no Brasil ainda é pouco comentado, tendo em vista os poucos livros e textos científicos encontrados no idioma português, que buscamos para referenciar e enriquecer esta monografia.

Como para o Prof. Richardsônia A. Clarke[1], também consideraremos a guerra cibernética "como ações de um Estado-nação para penetrar os computadores ou redes de outro Estado-nação com o propósito de causar dano ou ruptura". Desta forma para simplificar este estudo científico, nós analisaremos de forma mais particular e minuciosa o conflito[2] ocorrido no ano de 2008, entre Rússia e Geórgia, pelo domínio dos enclaves da Ossétia do Sul e Abecásia, em uma das regiões mais conturbadas e comentadas do momento, o Cáucaso. Quando a população georgiana sofreu um "cerco cibernético", ficando totalmente isolada da comunidade internacional, devido ao mal funcionamento dos seus sistemas digitais e o congestionamento proposital de sua rede de computadores.

Após a Primeira Guerra Mundial, que introduziu mudanças tecnológicas que tornaram a guerra mais destrutiva, houve a tentativa de criar a Liga das Nações, uma coalizão de estados que pudesse deter e punir agressores. Tal ação não impediu a ocorrência da Segunda Guerra Mundial, mais destrutiva e devastadora que a primeira. Assim como a Liga das Nações, a Organização das Nações Unidas foi criada depois da Segunda Guerra para impedir que a guerra acontecesse. Quarenta e nove estados se reuniram em São Francisco em 1945 para assinar uma carta que incluía inovações para reparar as deficiências da Liga.

---

1 Richard A. Clarke - autor do livro"*Cyber War: The Next Threat to National Security and What to Do About It*" (Guerra Cibernética: A Próxima Ameaça à Segurança Nacional e o que Fazer a Respeito), e também Professor da Kennedy School of Government, da Harvard University, em co-autoria com Robert K. Knake, best-seller publicado em 2010 pela Harper Collins.

2 Conflito - Segundo Julien Freund, consiste em um enfrentamento, entre dois seres ou grupos de uma mesma espécie que se hostilizam mutuamente, em geral para manter, afirmar ou restabelecer um direito, empregando muitas vezes o recurso da violência, que pode, se necessário, tender ao aniquilamento físico do adversário, ou simplesmente, pode ser uma competição consciente entre indivíduos ou grupos que visam a sujeição ou a destruição do rival.

Ao contrário do sistema de equilíbrio de poder do século XIX, o uso ofensivo da força era tornado ilegal por qualquer estado que assinasse a carta da ONU, com três exceções: qualquer uso da força tinha de ser ou defesa própria, em defesa coletiva ou pela segurança coletiva. Contudo não impediu o surgimento de uma nova era de conflitos, denominada Guerra Fria (1945 a 1989).

A queda do muro de Berlim (1989) e dissolução da URSS (1991) encerraram de maneira pacífica a Guerra Fria. Tal encerramento é considerado um dos grandes acontecimentos transformadores do século XX e pode ser explicado pelo esgotamento da ex-URSS, pela expansão excessiva do Império Soviético e a contenção do comunismo pelo EUA.

Nos dias atuais o que podemos perceber, é uma verdadeira corrida armamentista no espaço cibernético, ainda sem uma regulamentação internacional específica, mas apenas uma tentativa de orientação com o Manual de Tallinn. Nota-se também, que diversos países, inclusive o Brasil, estão se preparando para as ameaças cibernéticas. Entretanto não observamos uma evolução jurídica que acompanhe a rapidez das evoluções tecnológicas que podem ser utilizadas na guerra cibernética.

Sendo assim, o propósito deste trabalho é concluir que, apesar de não haver um consenso internacional a respeito da guerra cibernética, o Conselho de Segurança da ONU, o Comitê Internacional da Cruz Vermelha e a Corte Internacional de Justiça (embora sua vocação seja outra) podem exercer suas atribuições de interpretação para elucidar dúvidas e minimizar as lacunas a respeito das normas para a guerra cibernética. Para tal, utilizaremos como moldura temporal o período do conflito entra Rússia e Geórgia, que durou exatos cinco dias, de 08 a 12 de agosto de 2008, e desta forma concluiremos que empregando as Leis e Tratados Internacionais existentes, e usando como embasamento teórico o Manual de Tallinn, é possível regulamentar a Guerra Cibernética.

2 O QUINTO DOMÍNIO DA GUERRA

> Ciberespacial hás recome toe fifi domai ofá warfare, after land, sea, air and space. Some scenarios imagine toe almost instantaneous failure ofá toe systems that keep toe modern world turning. As computer networks collapse, factories and chemical plants explode, satellites spin out ofá control and toe financial and power grids fail.(Cyberwar: War in the Fifth Domain, Economist, July 1, 2010).[3]

2.1 A Guerra Clássica

Quando a Organização das Nações Unidas (ONU) foi idealizada (1945), um de seus propósitos era o de "libertar as gerações futuras do flagelo da guerra", ou seja, impedir que novas guerras acontecessem. De acordo com a Carta da ONU, documento que sela o acordo entre os países participantes, o uso ofensivo da força passou a ser tomado por ilegal entre qualquer Estado que a assinasse, salvo em três exceções: qualquer uso da força tinha de ser ou em defesa própria, defesa coletiva ou pela segurança coletiva.

Segundo Clausewitz a guerra é um ato de violência entre Estados, que visa compelir o oponente a atender a sua vontade, por meio do emprego da força, é ao uso da diplomacia, mas por outros meios. Já em 1832, a obtenção de dados que justificasse tal ação era uma preocupação para Clausewitz, que passou a discorrer acerca da dificuldade de se obter informações corretas durante a guerra, uma vez que a maioria seria contraditória, falsa ou de caráter duvidoso, e como uma névoa poderia encobrir ou distorcer uma informação. Para o autor "A grande incerteza de todos os dados na guerra é uma dificuldade peculiar, pois toda ação deve, em certa medida, ser planejada na penumbra, a qual em adição frequente – de um efeito de névoa ou luar – dá às coisas dimensões exageradas e aparência não-natural."

GROTIUS (2005:71-72), nascido em Dleft, na Holanda, e que viveu entre 1583 e 1645, escreveu sua obra-prima, O Direito da Guerra e da Paz *(De Jure Belli ac Pacis)*, inspirada na Guerra

3 O ciberespaço tornou-se o quinto domínio da guerra, depois da terra, mar, ar e espaço. Alguns cenários imaginam o fracasso quase instantâneo dos sistemas que mantêm o mundo moderno funcionando. Como colapso das redes de computadores, explosão de industrias e fábricas de produtos químicos, os satélites fora de controle e a falência das poderosas redes financeiras.(Tradução nossa).

dos Trinta Anos[4]. Em sua obra o jurista afirma que, a guerra é "um debate que se resolve pela força" e que a definição consagrada pelo uso da palavra foi o estado de guerra, no qual dois indivíduos "resolvem suas controvérsias pela força". O autor discute em sua obra a questão da justiça por meio do uso da força, indicando que se os homens fossem justos o emprego de tal força não seria necessário (p.47). Grotius lista ainda, alguns limites de uma guerra justa conduzidos para a obtenção de justiça, segundo princípios de boa-fé e respeitando o direito. Também distingue a guerra pública, realizada por uma autoridade, da guerra privada; e, na guerra pública, separa a guerra solene da não solene, sendo a guerra solene desempenhada por partes investidas "do soberano poder em sua nação" (p.168). Tudo isso diz muito sobre a burocracia do conceito da guerra à época de Grotius.

A guerra, na visão de BULL (2002:211), "é a violência organizada promovida pelas unidades políticas entre si". Bull defende o caráter oficial da guerra quando exercida entre unidades políticas, distinguindo-a dos ataques de Estados a indivíduos ou mesmo dos ataques entre indivíduos. Desta forma o emprego do termo "guerra" só se justificaria se fosse utilizado para conflitos entre Estados. Já na definição de Max Weber (1919) o Estado seria o detentor "legítimo do monopólio da violência", e a manutenção desse status quo é um dos objetivos que justifica determinadas ações de guerra.

De certa maneira o emprego de armas cibernéticas para desestabilizar inimigos com ataques precisos ou de saturação, e o posterior ou concomitantemente inicio de uma guerra clássica com armas convencionais, é uma realidade nos dias atuais e está se tornando cada vez mais comum. Tais atos, relacionados ao emprego de armas cibernéticas, diferem-se em seu modus operandi da já estudada, difundida e regulamentada guerra clássica. No entanto, a guerra cibernética, que angaria

4 Guerra dos Trinta Anos - (1618-1648) é a denominação genérica de uma série de guerras que diversas nações europeias travaram entre si a partir de 1618, especialmente na Alemanha, por motivos variados: rivalidades religiosas, dinásticas, territoriais e comerciais. As rivalidades entre católicos e protestantes e assuntos constitucionais germânicos foram gradualmente transformados numa luta europeia. As hostilidades causaram sérios problemas econômicos e demográficos na Europa Central e tiveram fim com a assinatura, em 1648, de alguns tratados que, em bloco, são chamados de Paz de Vestfália.

cada vez mais adeptos, está se tornando um complemento imprescindível para o sucesso da guerra convencional. Ato contínuo, fica cade vez mais difícil dissociar a guerra clássica da guerra cibernética.

2.2 A Guerra Além dos Limites

Os coronéis chineses Qiao Liang e Wang Xiangsui autores da Guerra Além dos Limites: Conjecturas sobre a Guerra e Tática na Era da Globalização, descrevem em sua obra que a guerra como nós a conhecíamos, gloriosa, destrutiva, de ardentes batalhas e com teatros de guerras sangrentas, passou a ter um papel secundário dentro do cenário mundial. Para os autores "Este fenômeno é realmente fantástico, e ao mesmo tempo, estimula profundas ponderações. Não nos referimos às mudanças nos instrumentos da guerra, na tecnologia dos meios empregados, nos modelos de condução da guerra, ou nos tipos de guerra, mas sim, a natureza da guerra". De fato o fenômeno, do qual os autores se referem, começa a ficar mais perceptível após a dissolução da União das Repúblicas Socialistas Soviéticas (URSS) em 1991, quando o mundo passa a ter uma potência econômica hegemônica, os Estados Unidos da América (EUA). Nesse contexto, os Estados perdem gradativamente seus papéis de destaque no cenário político mundial, dando espaço para atores transnacionais, como organismos internacionais e empresas multinacionais, que deixaram de ser meros coadjuvantes e passam a desempenhar papéis de protagonistas, operando além das fronteiras de seus países. Esse processo coincide com o início da “Era Digital”, na qual não apenas nos deparamos com o fluxo de capital, mas com o constante avanço tecnológico do ciberespaço. Assim, quando a força passou a não ser mais o único instrumento significativo de dominação, começa a surgir outros mecanismos competentes a fim de compelir um Estado a agir conforme a vontade do outro, através da manipulação econômica e da “guerra cibernética”.

A guerra cibernética é uma técnica em potencial no novo mundo da guerra, e que antes era concebida apenas a ataques de hackers oportunistas a alvos mais desprotegidos. Entretanto, o avanço tecnológico aumentou a capacidade invasiva e destrutiva, tornando qualquer sistema de

computadores vulnerável aos ataques cibernéticos, que não são mais exclusividades de “nerds” querendo demonstrar suas habilidades computacionais, mas passou a ser uma das principais armas de Estados e organismos não governamentais para alcançar seus objetivos. Esta nova tecnologia, de certa forma, também democratizou a violência, permitindo que atores não estatais usem e ameacem qualquer pessoa, organização, empresa ou país, em qualquer lugar do planeta.

Na visão dos coronéis chineses, "É impossível negar o profundo impacto exercido sobre a sociedade pelas novas motivações representadas pela liberdade econômica, concepção dos direitos humanos e percepção da importância da proteção ambiental. Mas é certo que a metamorfose da guerra provocará um cenário ainda mais complexo". De fato à medida que se reduz o uso da força militar para a resolução de conflitos, aumenta a utilização de instrumentos de poder tão letais e cruéis quanto à guerra convencional, capazes de deixar Estados completamente desabastecidos, seja de alimentos ou de energia, por causa de embargos econômicos severos e desumanos, ou ainda, permitirem que a população inteira de um país fique completamente isolada da comunidade internacional, sem acesso a redes de computadores, internet, serviços bancários e à mídia internacional. Acerca do potencial da guerra cibernética, podemos elucidar sua abrangência através do conflito ocorrido entre a Rússia e a Geórgia em agosto de 2008, caso de estudo do capítulo seguinte.

Ainda segundo os autores, os novos princípios de guerra não prescrevem mais “o emprego da força armada para compelir um inimigo a submeter-se a nossa vontade”, e sim, “a utilização de todos os meios, militares e não-militares, letais e não-letais, para compelir um inimigo a submeter-se aos nossos interesses”. Esse conceito representa uma mudança significativa de paradigma, tanto no entendimento da guerra em si, quanto na utilização de diversificados modelos de combate impulsionados por variados razões, seja de origem econômica ou tecnológica. (Qiao Liang e Wang Xiangsui, 1999, p. 6 e 7).

Em vista deste novo conceito, percebemos o surgimento de um novo tipo de guerra, a

Guerra Cibernética, onde a presença no campo de batalha cede lugar à onipresença da informação. Cujo perfil permite a fusão de todas as armas com a tecnologia disponível, como e quando desejado; além de eliminar as fronteiras entre as duas ambiências, a da guerra e da paz; dos militares e dos não-militares; Trata-se portanto, de um tipo de guerra que instaura significativas mudança em seus princípios básicos e suscita a necessidade até mesmo de uma reformulação em suas regras atuais.

2.4 A Guerra Cibernética

> Atualmente, a tecnologia está se tornando cada vez mais fascinante e incontrolável. Os laboratórios da Bell e da Sony desenvolvem continuamente novos “brinquedos”; Bill gates lança uma nova versão do "Windows" a cada ano; e a "Dolly", uma ovelha gerada por clonagem, é a prova de que o homem está, agora, planejando tomar o lugar de Deus, como Criados. Dentro do rítmo alucinante em que a tecnologia se desenvolve, o surpreendente caça russo SU-27 Flanker, nem chegou a ser empregado em combate, e o SU-35 Super-Flanker já se apresenta como o seu sucessor. A tecnologia, portanto, é como um par de sapatilhas mágicas" que após serem calçadas e firmemente presas pelos interesses comerciais, não nos deixa alternativas que não a de dançar de acordo com o ritmo por elas estabelecido.(Qiao Liang e Wang Xiangsui, 1999, p. 9)

Atualmente, em um mundo de constantes transformações, com o emprego de uma multiplicidade de meios militares e não-militares, em uma guerra que pode ser declarada ou não, com a violação da internet para obtenção, obstrução ou dissimulação de informações, com o ataque a instituições financeiras a fim de desestabilizar governos, com o terrorismo empregado de uma maneira irrestrita e com a exploração e manipulação da mídia para fins belicosos, surge uma nova tecnologia, a tecnologia cibernética, que segundo os coronéis Qiao Liang e Wang Xiangsui, "foi uma novidade benéfica para a civilização". Entretanto esclarecem que uma questão permanece: quem terá o “encantamento mágico” para controlar a tecnologia cibernética? Será que a tecnologia cibernética desenvolver-se-á a ponto de não poder mais ser controlada pelo homem, transformando a humanidade em sua vítima?

De fato a guerra cibernética é um assunto bastante discutido no momento e que já faz parte do cotidiano de vários países no mundo. Mesmo no Brasil, a questão da ameaça cibernética já é uma realidade. Ela é uma questão nova e que foi inserida na agenda da Defesa Nacional através da

Estratégia Nacional de Defesa, instituída através do Decreto N° 6.703, de 18 de dezembro de 2008.

Mas o que significa a Ameaça Cibernética? o que é Poder Cibernético? neste capítulo tentaremos explicar e contextualizar alguns desses termos para melhor compreendermos o assunto.

O Poder Cibernético foi recentemente reconhecido na academia pelo Prof. Joseph S. Nye Jr, que defende, entre diversas coisas, que dois grandes deslocamentos de poder estão ocorrendo neste século: uma transição de poder entre os estados e uma difusão de poder espalhando-se de todos os estados para os atores não estatais.

Nesta difusão de poder ele dá destaque junto do Poder Militar, do Poder Econômico, e do Poder Brando, o Poder Cibernético. Segundo ele, o poder baseado em recursos de informação não é novo, mas o poder cibernético é. Ele conceitua o poder cibernético como um conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informações eletrônicas e baseadas em computador – infraestrutura, redes, software, habilidades humanas. Isso inclui não somente a internet dos computadores ligados à rede, mas também intranets, tecnologias de telefonia celular e comunicações via satélite. Definido do ponto de vista comportamental, o poder cibernético é a capacidade para obter resultados preferidos mediante o uso dos recursos de informação eletronicamente conectados do domínio cibernético (estes resultados preferidos podem ser obtidos dentro do espaço cibernético[5], ou podem ser obtidos em outros domínios fora do espaço cibernético).

Sendo assim, uma ameaça cibernética é uma atividade de "uso de poder cibernético". Mas a que ponto uma ameaça cibernética pode constituir uma Guerra Cibernética? Segundo o Prof. Richard A. Clarke , a "cyber war" (ou cyberwarfare) são " ações de um Estado-nação para penetrar os computadores ou redes de outra nação com o propósito de causar dano ou ruptura". Já o Secretário Adjunto de Defesa dos EUA, William J. Lynn, afirma (como registrado no livro do Prof. Clarke) que "como uma matéria de doutrina, o Pentágono reconhece o espaço cibernético

5 Espaço Cibernético - Ambiente intangível formado por ativo de Tecnologia da Informação (TI), onde dados e informações digitais são criados, armazenados, modificados, trafegados e processados. Possui as seguintes caracterísiticas: alcance global, ausência de fronteiras e dinamismo.

(cyberspace) como um novo domínio de guerra ... (o qual) se tornou tão crítico para operações militares quanto a terra, o mar, o ar, e o espaço".

3 A GUERRA RUSSIA VERSUS GEORGIA (2008)

Em 8 de agosto de 2008, enquanto os líderes mundiais se reuniam em Pequim para assistir à cerimônia de abertura dos Jogos Olímpicos, tanques russos invadiam a fronteira da Geórgia, sob o pretexto de proteger cidadãos russos que habitavam a Ossétia do Sul, um enclave étnico no norte da Geórgia. Os russos alegaram que na noite anterior, forças georgianas tinham respondido a ataques de separatistas na região, matando inclusive civis de nacionalidade russa.

Os ataques de Forças Armadas georgianas à capital da região, Tskhinvali, buscava retomar o território pela força. Moscou, que havia apoiado o governo separatista há mais de uma década, revidou com uma invasão em larga escala, com envio de aeronaves e colunas blindadas para a Ossétia do Sul, visando centros militares e as linhas de comunicação internas da Geórgia. A Rússia também reforçou sua presença militar na Abcázia, outra província separatista, no canto noroeste do país.

Como as tropas russas já tinham estado presentes em ambos os enclaves como forças de paz, implantados com o consentimento da Geórgia 15 anos antes. Quando o ataque georgiano à Ossétia do Sul ameaçou o status quo frágil na região, Moscou interveio com velocidade relâmpago, rechaçando os georgianos em menos cinco dias.

3.1 Origens do Conflito

Os ossetianos são uma etnia originária das planícies russas ao sul do Rio Don. Eles têm identidade e cultura diferentes da dos georgianos e uma língua própria. No século 13, as invasões mongóis empurraram a etnia para as montanhas do Cáucaso, e os ossetianos se estabeleceram ao longo da atual fronteira da Geórgia com a Rússia. Os ossetianos do sul querem se juntar à Ossétia do Norte, que é uma república autônoma dentro da Federação Russa. Os georgianos são uma

minoria na Ossétia do Sul, representando menos de um terço da população. A Geórgia rejeita o nome Ossétia do Sul, preferindo chamar a região pelo nome antigo, Samachablo, ou Tskhinvali, a principal cidade da região.

A Ossétia do Sul tem tido um governo próprio desde que lutou com a Geórgia pela sua independência em 1991 e 1992, logo após o colapso da União Soviética. Durante o conflito, a região declarou sua independência, mas ela não foi reconhecida por nenhum país.

As tensões vinham aumentando desde a eleição do presidente Mikhail Saakashvili em 2004. Ele ofereceu à Ossétia do Sul diálogo e autonomia, mas no contexto de um só Estado, o da Geórgia. Em 2006, os ossetianos do sul votaram em um referendo extra-oficial em uma tentativa de fazer pressão pela independência completa, e segundo as autoridades da Ossétia, a maioria esmagadora da população o fim da união com Tblisi.

Em abril de 2008, a Organização do Tratado do Atlântico Norte (OTAN) disse que a Geórgia poderia no futuro vir a ser um membro da aliança militar, o que irritou a Rússia, que se opõe à expansão da OTAN para o leste. Semanas depois, a Rússia reforçou os seus laços com as regiões de Ossétia do Sul e Abecásia.

Em julho a Rússia admitiu que seus caças entraram no espaço aéreo da Geórgia, na região da Ossétia do Sul. Confrontos antes esporádicos se escalaram, até que, segundo informações não confirmadas, seis pessoas acabaram mortas por projéteis de forças georgianas.

À primeira vista, a guerra russo-georgiana de agosto 2008 parecia um mais um simples conflito na região do Cáucaso: uma região que possui as maiores reservas de petróleo e gás natural inexplorado do mundo e nesse contexto a Geórgia está na posição estratégica privilegiada para estabelecer ligações entre diferentes regiões. A Rússia procura manter sua influência por conceber o Cáucaso como um cinturão de segurança ao redor de suas fronteiras.

Por outro lado os Estados Unidos começaram a desenvolver na região uma política

energética alternativa ao Oriente Médio e, junto com a União Europeia consideram que a melhor rota para o escoamento dos recursos energéticos vindo do leste, era atravessar a Geórgia de maneira a contornar a Rússia. Nesse sentido tem feito investimento na construção de oleodutos na região. Mas a Geórgia também é importante por razões geoestratégicas e de segurança internacional. Como Estado fraco apresenta um forte potencial de atrair atividades terroristas, razão pela qual o país e a região do Cáucaso, ganharam grande visibilidade internacional.

A guerra dos cinco dias mataram centenas, deixou milhares de refugiados em abrigos temporários, e trouxe relações entre a Rússia e os Estados Unidos a seu ponto mais baixo desde os dias negros da Guerra Fria. Para alguns vizinhos da Rússia, como a Polônia e os países bálticos, a guerra simbolizou o retorno da velha OTAN - uma aliança tradicional fornecendo garantias de segurança, a fim de deter a agressão externa, em vez de um clube pós-moderno para a promoção da democracia e boa governança. Para Geórgia, os tanques russos que marcaram a paisagem exuberante eram uma afronta a tudo o que tinha sido alcançado desde a Revolução Rosa de 2003[6], incluindo a criação de instituições democráticas e possibilitando a implementação de uma política externa pró-EUA. Para a Rússia, a guerra era uma réplica firme para uma liderança georgiana imprudente e uma chance de levantar-se contra a influência dos EUA no quintal de Moscou.

3.2 A guerra cibernética durante o conflito

O conflito na Geórgia se assemelhava a todos os conflitos que aconteceram após a dissolvição da ex-União Soviética na década de 1990: Confrontos mais de fronteiras e identidades dentro de Estados recém-criados. As lutas territoriais sobre os enclaves de Nagorno- Karabakh (no Azerbaijão), Transnístria (na Moldávia) e Chechênia, junto com a guerra civil entre as facções regionais no Tajiquistão, tudo centrado em questões básicas de onde traçar os limites de novos estados e quais grupos - étnica, territorial ou política - deve ser dominante dentro deles. Entretanto esta guerra surpreendeu pelo impacto psicossocial na população georgiana, que ficou isolada da

6 Revolução Rosa (2003) - foi um movimento pacífico e popular ocorrido na Geórgia em 2003 que retirou do poder o presidente do país, Eduard Shevardnadze.

comunidade internacional em virtude do ataque cibernético realizado pela Rússia aos seus serviços de informação.

Segundo Richard A. Clarke, em seu livro “Cyber War: The Next Threat to National Security and What to Do About It - Guerra Cibernética: A Próxima Ameaça à Segurança Nacional e o que Fazer a Respeito", rapidamente o Exército russo expulsou o Exército georgiano da Ossétia do Sul, e ao mesmo tempo em que os tanques russos moviam-se em terreno georgiano, seus "guerreiros cibernéticos", com o objetivo de impedir que os cidadãos georgianos tomassem conhecimento do conflito, realizavam ataques DDOS[7] nos meios de comunicação georgianos e sites do governo. O acesso da Geórgia a sites da CNN e BBC também foram bloqueados. A fim de impedir o ataque cibernético russo, a Geórgia tentou bloquear todo o tráfego proveniente da Rússia. Contudo os russos redirecionaram seus ataques, aparecendo como se fossem provenientes da China. Servidores no Canadá, Turquia, e, ironicamente, Estônia, que no ano anterior também havia sofrido ataques cibernéticos atribuídos aos russos[8], também foram utilizados para infectar computadores que se tornaram verdadeiros "zumbis" (botnet)[9], totalmente dominados e vulneráveis a ataques DDOS.
A Geórgia foi obrigada a transferir a webpage[10] do Presidente para um servidor da Google, na Califórnia. O setor bancário da Geórgia fechou seus servidores para superar os ataques, imaginando que uma perda temporária de serviços bancários, fosse melhor do que ter seus dados sigilosos roubados ou danificados. Como não foi possível obter os dados bancários da Geórgia, os russos fizeram suas botnets enviarem uma enxurrada de dados falsos para a comunidade bancária internacional, simulando ataques cibernéticos provenientes da Geórgia. Tais ataques desencadearam uma resposta automática na maior parte dos bancos estrangeiros, que fecharam suas conexões com

7 DDOS (Distributed Denial of Service) - ações de ataque cibernético que visam interromper, negar, degradar, corromper ou destruir informações ou serviços no espaço cibernético de interesse.
8 Os ciberataques à Estônia em 2007 referem-se a uma série de ataques cibernéticos, com início em 27 de abril de 2007 e deixou sites do governo fora do ar. O governo estôniano acusou a Rússia, que teria se motivado a realizar os ataques por conta da remoção de uma estátua que marcava a vitória russa contra o nazismo, a estátua do Soldado de bronze de Tallinn, porém os russos não assumiram a autoria dos ataques, sendo sua origem desconhecida até hoje.
9 Botnet - computadores infectados e dominados por vírus digitais, que são empregados em ataques de DDOS.
10 Webpage - página que permite o acesso às informações disponibilizadas na "world wide web" ou rede mundial de computadores (www) e "navegar" pela internet.

o setor bancário georgiano. Sem acesso aos sistemas de liquidação europeus, as operações bancárias da Geórgia foram paralisadas. Sistemas de cartão de crédito caíram, seguidos logo depois pelo sistema de telefonia móvel.(CLARKE, 2010)

Os russos negam até hoje que foram responsáveis pelo malware[11] que atingiu a rede de computadores da Geórgia e isolou completamente o país do resto mundo. Como no conflito contra a Estônia os ataques cibernéticos foram atribuídos a hackers[12] e pessoas má intencionadas contrárias ao governo georgiano. De fato a tempestade cibernética que invadiu a Geórgia durante o conflito causou um efeito psicológico na população, que ficou sem acesso a todo tipo de informação e isolada do resto do mundo, isso de certa forma contribuiu para inibir a vontade de lutar do georgiano, que não conseguia utilizar os serviços da internet, acessar aos sítios do governo e a provedores de mídia da imprensa internacional. Os ataques cibernéticos na Geórgia mostraram a vulnerabilidade dos serviços interligados à internet e a dependência da população para realizar suas tarefas cotidianas por intermédio da rede de computadores e sítios eletrônicos, e que se tornam alvos fáceis capazes de inverter a vontade política de seguir adiante com o conflito.

3.3 Outros Casos de Ataques Cibernéticos no Mundo

Embora a internet tenha nascido no contexto da 2ª Guerra Mundial, derivada da rede Arpanet[13], somente agora, se expandiu vertiginosamente a velocidades inimagináveis. No entanto, há casos comprovados e não comprovados que, no contexto da Guerra Fria, países tenham promovido ataques cibernéticos contra outros países, empresas, infraestruturas críticas em benefício de natureza estatal ou internacional. Assim, serão exemplificados alguns casos históricos e atuais.

3.3.1 O sistema de gasoduto da Sibéria

Em 1982, o gasoduto da Sibéria, adquirido ilegalmente do Canadá, explodiu.

---

11 Malware - Software malicioso, destinado a se inflitrar em um sistema de computador alheio de forma ilícita com o intuíto de causar algum dano ou roubo de informações (classificadas ou não).

12 Hacker é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. incluindo, por exemplo, contornar as barreiras que supostamente deveriam impedir o controle de certos sistemas e acesso a certos dados.

13 Arpanet - Desenvolvida pela agência Americana ARPA (Advanced Research and Projects Agency - Agência de Pesquisas em Projetos Avançados) em 1969, tinha o objetivo de interligar as bases militares e os departamentos de pesquisa do governo americano. Esta rede teve o seu berço dentro do Pentágono e foi batizada com o nome de ARPANET ou ARPANet.

Autoridades locais afirmaram haver um mal funcionamento do sistema de controle do gasoduto, o qual era controlado por computador. Há indícios de que, a CIA tenha alterado o sistema computacional do gasoduto, de forma que o sistema de controle recebessem instruções para operar além dos limites. Embora seja um caso não comprovado, se verídico, este foi o primeiro caso de ataque cibernético a infraestruturas críticas na História.

3.3.2 A central nuclear da Síria

Em 2007, objetivando destruir uma suposta instalação nuclear na Síria, Israel promoveu um ataque aéreo, conhecido como Operação Orchard. No entanto, a Síria dispunha de um sofisticado sistema de defesa antiaérea adquirido da Rússia. Israel, então, teria alterado o sistema sírio para que este não visualizasse os aviões israelenses invadindo seu espaço aéreo. Acredita-se que, Israel tenha se utilizado de neutralização remota, mísseis antirradiação ou mesmo que os radares sírios não estivessem em operação. Embora a Síria acuse Israel de ter promovido o ataque, Israel alega inocência tanto no ataque aéreo quanto no ataque cibernético.

3.3.3 A usina nuclear do Irã

Em 2010, o Irã sofreu um poderoso ataque cibernético que afetou os computadores da central nuclear de Bushehr. O Stuxnet é um vírus sofisticado com alto valor tecnológico agregado, produzido em laboratório. Este vírus foi produzido, especialmente, para atacar as instalações nucleares iranianas, a fim de frear o programa de enriquecimento de urânio. Além de ser acionado à distância, é um vírus instável e migra com rapidez. A medida que se começa a contra-atacá-lo, o vírus muda de versão. Autoridades políticas internacionais acreditam que as reais intenções do Irã, ao enriquecer urânio em seu próprio território, sejam construir uma bomba atômica. O Governo iraniano acusa Israel e EUA por terem produzido este vírus e promovido o ataque cibernético às suas instalações nucleares. Por o Stuxnet ser uma arma cibernética, este vírus se tornou um paradigma nos estudos sobre Segurança e Defesa, a medida que provocou a reformulação de conceitos como soberania, criou novos conceitos como nação virtual e espaço cibernético e provocou uma nova corrida armamentista, sem precedentes na História, cujos danos podem ser equiparados aos provocados por armas de destruição em massa.

4 A GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL

> Apesar do estudo da evolução histórica mostrar que o Direito Internacional existe desde que foram criadas as nações, a rigor só se pode falar de direito internacional depois dos tratados de Vestifália (1648).[14](Nascimento e Silva - Accioly, 2002)

Neste capítulo analisaremos leis e regulamentos do Direito Internacional, que podem ser empregados para regulamentar a utilização da Guerra Cibernética, que aparentemente pode não ser uma guerra destrutiva, mas com uma análise minuciosa e tendo como palco a guerra da Rússia contra a Geórgia no ano de 2008, percebemos facilmente, que uma guerra cibernética irrestrita pode causar danos seríssimos não só a combatentes como aos não combatentes, e pode ser tão violenta quanto uma guerra convencional, atingindo inclusive a população civil.

4.1 A Regulamentação da Guerra Cibernética

Uma guerra cibernética sem regras pode interromper serviços essenciais como de hospitais, de telecomunicações e de instituições financeiras, além de comprometer infraestruturas críticas como usinas nucleares, usinas hidroelétricas, portos, aeroportos e ferrovias, sem falar no cerceamento de informações, que como na Geórgia isolaram o país do resto do planeta, impedindo a comunicação da sociedade georgiana com meio exterior.

Verificando, à luz do direito Internacional, as implicações e consequências da guerra cibernética contra a Geórgia, mostraremos que, apesar de não haver um consenso internacional a respeito da guerra cibernética, o Conselho de Segurança da ONU, o Comitê Internacional da Cruz Vermelha e a Corte Internacional de Justiça podem exercer suas atribuições de interpretação para elucidar dúvidas e minimizar as lacunas a respeito das normas para a guerra cibernética, utilizando para este conflito específico as Leis e Tratados Internacionais existentes que fundamentam a justiça internacional, e tendo como embasamento teórico o Manual de Tallinn. Para atingir o objetivo deste capítulo, é fundamental observar os princípios básicos do DICA, a legislação que trata do assunto do

14 Tratados de Vestefália - Tratados assinados no ano de 1648 entre a França, a Suécia, e o império germânico para pôr termo à Guerra dos Trinta Anos. Neste tratado estabeleceram-se algumas bases do direito público, e uma delas a de que a conservação do império germânico era conveniente para toda a Europa, para além de ter permitido um equilíbrio político na Europa Central até à Revolução francesa. (Infopedia Porto: Porto Editora, 2003-2014)

direito a guerra na Carta das Nações Unidas, o que diz os tratados e suas convenções a repeito dos direitos principais dos não combatentes e veremos os arcabouços teóricos que embasam o assunto de guerra cibernética pelo Manual de Tallinn.

4.1.1 O Direito Internacional dos Conflitos Armados

Segundo o Manual de Emprego do Direito Internacional dos Conflitos Armados para as Forças Armadas (MD34-M-03), são estes os princípios básicos do DICA:

a) Distinção - Este princípio prevê que as partes em conflito devem sempre, durante a condução das operações militares, distinguir entre combatentes e não combatentes. Devendo os não combatentes serem sempre protegidos contra os ataques. As respectivas ações devem ser realizadas somente contra alvos e objetivos militares, distinguindo-os dos bens de caráter civil;

b) Limitação - Este princípio restringe o direito dos beligerantes em escolher livremente os meios e métodos para empregar, sendo proibidos aqueles que levem ao sofrimento desnecessário e a danos supérfluos;

c) Proporcionalidade - Este princípio garante que a força utilizada dos meios e métodos de guerra deve ser usada na proporção correta para alcançar os objetivos militares, e obter a vantagem militar desejada, evitando-se toda forma de violência que não seja necessária ao cumprimento da missão.

d) Necessidade Militar - Este princípio garante que um Comandante poderá flexibilizar as normas estabelecidas no DICA a fim de cumprir o objetivo, sempre respeitando o princípio da proporcionalidade, onde em todo conflito armado, o uso da força deve corresponder à vantagem militar que se pretende obter. As necessidades militares não justificam condutas desumanas, tampouco atividades que sejam proibidas pelo DICA.

e) Humanidade - O princípio da humanidade busca resguardar e assegurar os direitos do ser humano, protegendo-a das arbitrariedades que possam ocorrer nos conflitos armados. Proíbe que provoque sofrimento às pessoas e destruição de propriedades desnecessários ao cumprimento da

missão, São proibidos ataques exclusivamente à civis, o que não impede que, ocasionalmente, algumas vítimas civis sofram danos, desde que todas as precauções sejam tomadas para mitigá-los.

Convém lembrar que os civis são imunes aos ataques e não podem ser considerados alvos a menos que alterem o seu status e percam a referida imunidade.

Os combatentes são legalmente considerados como alvos mesmo quando não representam uma ameaça para o seu adversário. As únicas situações, em que deixam de ser combatentes, são quando se rendem ou não tenham condições de se defender.

4.1.2 O Direito à Guerra Segundo a Carta das Nações Unidas

De acordo com o Direito Internacional Humanitário há duas vertentes que amparam questões relacionadas à guerra: A primeira, "jus ad bellum", em latim direito à guerra, representa o direito do Estado de recorrer à força em suas relações internacionais, a fim de defender seus interesses. A segunda "jus in bello", direito da guerra, tem como propósito regular o comportamento das forças armadas, ou seja, as condutas em guerra, inclusive no que concerne à proteção das vítimas.

Após a 2ª Guerra Mundial, entrou em vigor, em 1945, a Carta das Nações Unidas. A utilização da ameaça ou força para a solução de controvérsias entre Estados passou a ser proibida. A partir daquele momento, o direito à guerra deixa de existir, a guerra passa a ser condenável, e um ato ilícito (Brasil, 2009). A Carta da ONU, no entanto, prevê duas situações: a agressão, isto é, a guerra de agressão; e as contramedidas, que podem ocorrer de duas maneiras: legítima defesa individual ou coletiva, e medidas tomadas por iniciativa do Conselho de Segurança que envolvem o "emprego da força armada" (Art. 41). Assim, a agressão caracteriza-se por ato ilegal; já as contramedidas são legais, uma vez que são tomadas com a autorização do Conselho de Segurança. (NASCIMENTO E SILVA e ACCIOLY, 2002).

Todos os membros das Nações Unidas devem abster-se em suas Relações Internacionais de recorrer à ameaça ou uso da força contra a integridade territorial, e/ou contra a independência

política de qualquer Estado, ou ainda recorrer a alguma forma de agressão incompatível com os propósitos das Nações Unidas. (Carta das Nações Unidas Capítulo I, Art. 2º § 4).

"Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva, caso ocorra um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tome as medidas necessárias para manter a paz e segurança internacionais" (Carta das Nações Unidas Capítulo VII, Art. 51º).

A Corte Internacional de Justiça (CIJ) define autodefesa como um termo técnico em Direito Internacional. Autodefesa é o direito de um Estado vítima em usar a força militar ofensiva no território de um Estado responsável por um ataque armado significativo em seu território. Além disso, o uso da força militar deve respeitar dois princípios fundamentais do Direito Internacional dos Conflitos Armados: o da necessidade militar e o da proporcionalidade.

O reconhecimento do direito inerente de legítima defesa individual ou coletiva ingressou na Carta das Nações Unidas por iniciativa do bloco latino-americano. A legítima defesa representa o emprego da força por uma pessoa ilegalmente atacada por outra. Nos termos da Carta, o emprego da legítima defesa só é cabível no caso de ataque armado, ou tentativa de ataque, e a título transitório, isto é, até que o Conselho de Segurança tenha tomado as medidas cabíveis, para assegurar que o Estado agredido tenha retornado ao seu status quo anterior à agressão sofrida. Outra condição é que o revide seja proporcional. (NASCIMENTO SILVA e ACCIOLY, 2002)

4.1.3 Efeitos Jurídicos no Tocante aos Bens e às Pessoas

O interesse pela sorte dos militares postos fora de combate, por doenças contraídas em solo hostil ou por ferimentos recebidos no calor da batalha, é antigo, entre os povos do ocidente. Mas só se adotaram regras internacionais precisa a esse respeito, a partir da Conferencia de Genebra de agosto de 1864, decorrente da iniciativa dos dois filantropos genebreses Jean-Henri e Gustave Moynier.

Foram os primeiros passos para a fundação da Cruz Vermelha, 22 de agosto de 1864,

criada para prestar assistência aos feridos e enfermos nos exércitos em campanha. As quatro Convenções de Genebra de 1949 e os dois Protocolos Adicionais de 1977, constituem a essência do Direito Internacional Humanitário, que valeu-se das normas internacionais que disciplinam os métodos e meios de guerra, além de proteger pessoas e bens afetados ou que possam ser atingidos em conflitos, adotando várias medidas destinadas a assegurar o respeito a dignidade da pessoa humana e resguardar a vida e a integridade das pessoas civis, nos países beligerantes.

De tais normas convencionais destacam-se a proteção de bens e pessoas, normas de precauções e limites para os ataques, bem como para o emprego de novas armas, além das regulamentações que tutelam a condição dos combatentes, como por exemplo: a que os hospitais, ambulâncias e formações sanitárias, com o sinal da cruz vermelha, devem ser respeitados e protegidos pelos beligerantes. Entretanto a proteção concedida às organizações móveis e estabelecimentos fixos dos serviços de saúde dos exércitos beligerantes cessa, se tais organizações são utilizadas para a prática de atos hostis. Os soldados enfermos ou feridos, sem distinção de nacionalidade devem ser tratados pelo beligerante em cujo o poder se encontram.

Segundo entendimento do Comitê Internacional da Cruz Vermelha (CICV), uma organização humanitária, independente e neutra, que se esforça em proporcionar proteção e assistência às vítimas da guerra e de outras situações de violência; a necessidade militar ocorrerá quando for justificada a adoção de medidas em uma situação de urgência que não estejam proibidas pelo DICA e que sejam indispensáveis para forçar, o mais rápido possível, a rendição completa do inimigo.

4.2 A Legalidade da Guerra Cibernética

Como visto anteriormente, a Carta das Nações Unidas não permite a ameaça ou o uso da força por um Estado contra outro, a menos que seja em legítima defesa, para responder a um ataque armado ou a uma ameaça iminente, e onde o Estado violado não quer ou não adota as medidas adequadas para evitar tais ameaças, ou ainda quando o uso da força é para defender um

Estado violado que não tenha poder suficiente para se contrapor ao oponente, desde que esse Estado, agredido, aceite a ajuda.

Contudo os ataques cibernéticos podem ser empregados como armas, causando danos extremamente severos ao Estado atacado, que nem sempre pode se defender ou até mesmo saber a origem dos ataques, como vimos no caso da guerra entre a Rússia e a Geórgia descrita no capítulo anterior.

Valendo-se da Carta das Nações Unidas, como descrito acima, o Estado violado tem o direito de responder a esses ataques em legítima defesa. Porém surgem alguns questionamentos quando observamos os princípios do Direito Internacional dos Conflitos Armados. Usando o princípio da proporcionalidade, o Estado atacado pode se utilizar de armas convencionais para responder uma ataque cibernético? É possível prever as consequências dos ataques cibernéticos para a população civil? Como observar os princípios que regem o direito de guerra, da necessidade e da humanidade, quando não se sabe a autoria dos ataques? Quem terá mandato e quais critérios técnicos e jurídicos devem ser utilizados para atribuição de origem e autoria de ataques, considerando a ausência de fronteiras no espaço cibernético? Os ataques cibernéticos podem configurar ou acarretar a prática de crimes de guerra, inclusive por civis? Como não envolver a população civil em uma guerra cibernética, já que o malware, quando espalhado na rede, não distingue os computadores a serem infectados. De fato, ao que parece são perguntas não muito fáceis de responder. Em uma primeira análise, parecem caminhar para atos de ilicitude ou de terrorismo, e difícil aplicar as regras que atualmente disciplinam o uso da força à guerra cibernética. Para responder tais questionamentos devem ser feitas adaptações técnicas e jurídicas.

O Manual Tallinn[15], que vem a ser uma primeira tentativa de estabelecer regras básicas internacionais aplicadas na guerra cibernética, pode ser usado no futuro como documento de auxílio

15 Manual de Tallinn - Foi publicado sob a direção da OTAN, escrito por mais de 40 acadêmicos, advogados, e especialistas dos países da OTAN. O manual com 282 páginas define as condições em que um país pode responder a um ciberataque com forças militares. (NATO Coperative Cyber Defense Centre of Exclence, Tallin Estônia. http://ccdcoe.org/tallinn-manual.)

a fundamentações jurídicas no litígio entre dois Estados por motivo de ataque com armas cibernéticas. Entretanto o Manual de Tallinn não é um documento oficial, mas sim uma expressão de opiniões de um grupo de peritos independentes sob a direção da OTAN.

A despeito da indisposição de muitos países para discutir um assunto tão delicado de forma aberta e coletiva, o conflito entre a Rússia e a Geórgia em 2008, descrito no capítulo anterior, provou que as ameaças cibernéticas são reais, bastando apenas existirem computadores ligados em rede controlando infraestruturas críticas para se causar danos relevantes.

A alta velocidade com que ocorrem os avanços tecnológicos dentro do espaço cibernético, essencialmente regido por regras técnicas, que estão em constante mutação, não podem ser acompanhados pela evolução jurídica e pela normatização de regras e leis, que amparem sistema jurídico internacional.

Se os ataques cibernéticos constituem um ato de agressão, então pelo jus ad bello se justificaria recorrer à força armada em resposta, desde que não contrariasse os preceitos de legítima defesa da Carta das Nações Unidas, contudo devem ser observadas às questões do jus in bello, ou seja, como o DICA vai disciplinar o uso da força de ataques cibernéticos durante um conflito armado, recorda Benatar (2009), principalmente sem contrariar o princípio da proporcionalidade.

O aparecimento da guerra cibernética traz a discussão termos, métodos e meios de guerra que não constam e não são empregados no contexto das Leis, Normas e Tratados que regem o Direito Internacional Humanitário: como "ataques cibernéticos", "operações cibernéticas" ou "ataques de redes de computadores", portanto não têm um significado legal acordado internacionalmente e são usados em diferentes conceitos (nem sempre limitados aos conflitos armados) e com diferentes significados.

O Manual de Tallinn pode vir a ser o documento que fundamente e auxilie a interpretação de tais termos quando empregados nas discussões jurídicas do Direito Internacional Humanitário.

Cabe ressaltar que o Direito Internacional Humanitário só pode ser utilizado nas operações cibernéticas cometidas durante um conflito armado – seja ele entre Estados, entre Estados e organizações armadas ou entre organizações armadas. Portanto, precisamos distinguir a questão específica das operações cibernéticas empregadas como armas.

Ataques cibernéticos dirigidos a causar danos físicos a bens tangíveis ou intangíveis, ferimento ou morte de seres humanos podem ser caracterizados como agressão. Mas e como no caso especifico do conflito armado entre a Rússia e Geórgia, apresentado anteriormente, as perturbações de ordem econômica, que também ameaçam a paz e causam danos principalmente a população civil, que fica sem acesso aos seus recursos e dependendo do prolongamento das ações pode vir a ficar até em dificuldade de comprar gêneros para sua sobrevivência.

É importante definir o uso da força no espaço cibernético, para que seja perfeitamente enquadrado no conceito de uso da força do artigo 2º § 4º da Carta da ONU a fim de utilizar o direito à legítima defesa ou a adoção de medidas pelo Conselho de Segurança da ONU. Além disso, também existem controvérsias a respeito do exercício do direito à legítima defesa, particularmente no tocante à possibilidade ou não de um país se antecipar a um ataque, como no caso do ataque cibernético a usina nuclear do Irã.

Outra questão delicada é a atribuição de autoria, a identificação da origem de um ataque e a caracterização da intenção hostil, como no conflito entre a Rússia e a Geórgia, no qual os russos negam a autoria dos ataques cibernéticos que isolaram os georgianos da comunidade internacional. Este conflito demonstra como técnicas possibilitam a utilização de estruturas e atores inocentes, que foram facilmente cooptados ou induzidos a espalharem voluntariamente o malware que infectou os computadores georgianos. Sendo assim a regra da legítima defesa não autoriza atos de defesa ativa além das fronteiras se a provocação não puder ser atribuída a outro país, assim como protege pessoas e bens civis.

Um sistema normativo que exige a determinação da autoria e a caracterização da

intenção hostil do ataque cibernético – requisitos passíveis de manipulação quando não se tornam inviáveis - para então autorizar o exercício da legítima defesa , é incompatível com a realidade cibernética e ineficiente para lidar com protagonistas que atuam sem as restrições impostas pela legalidade. O diálogo das fontes jurídicas e técnicas deverá ajudar a comunidade internacional a definir as cautelas necessárias.

5 CONCLUSÃO

Por tudo que foi exposto, pode-se concluir que, as relações de insegurança e de instabilidade entre os estados, que temem perder suas soberanias e não conseguirem defender os seus interesses e de seus cidadãos, remetem a uma eterna situação de hostilidade e conflitos de todas as naturezas, onde a guerra seria sempre a solução e o meio mais eficaz para se conseguir a paz.

A criação da Organização das Nações Unidas (ONU) causou uma falsa sensação de segurança coletiva, onde uma "nova ordem mundial" parecia convergir para a paz entre os estados. O uso da força para agredir e causar dano a outro Estado tornava-se ilegal, a não ser por três exceções: qualquer uso da força tinha de ser em defesa própria, defesa coletiva ou pela segurança coletiva. Parecia que os Estados estariam dispostos a se apoiarem mutuamente, partindo para um mundo globalizado e multipolar, sobre a égide de uma organização internacional capaz de intermediar as controvérsias entra os estados e arbitrar as questões divergentes. Mas os interesses econômicos, étnicos, religiosos, ideológicos e territoriais estiveram sempre acima da racionalidade humana.

O conflito entre a Rússia e a Geórgia (2008), deixou claro que os ataques cibernéticos que isolaram os cidadãos georgianos da comunidade internacional e paralisaram os sistemas financeiros e de telefonia no país, podem ser equiparados a armas cibernéticas, tão destrutivas e violentas quanto as armas convencionais, e portanto podem configurar uma agressão ou uso da força à luz da Carta da ONU, e mesmo sem a identificação de sua autoria, mostrou que a legítima

defesa ou o sistema de segurança coletiva podem ser autorizados, desde que a resposta seja pautada em dois princípios básicos do DICA: da necessidade e da proporcionalidade, a fim de garantir a dose correta do revide e a obtenção da vantagem militar pretendida, sem exageros ou danos desnecessários.

Percebe-se que as disposições da Carta da ONU, principalmente os conceitos de uso da força, legítima defesa, necessidade e proporcionalidade e os critérios para identificação de autoria e caracterização da hostilidade precisam ser revistas para a guerra cibernética.

O emprego das armas cibernéticas deve ser conduzido pelos preceitos do direito internacional humanitário que protegem bens e pessoas civis, pautado no princípio da distinção, que não permite ataques indiscriminados, sem distinguir o combatente do não combatente, portanto não deve de maneira alguma afetar civis que não estejam engajados em armas, que como no caso da guerra anteriormente citada, na qual a população civil georgiana foi afetada pelo ataque cibernético sofrido, que deixou o país sem inúmeros serviços, causando sofrimento desnecessário a civis, e no caso do prolongamento dos ataques poderia resultar em consequências imprevisíveis e danos superiores ou desproporcionais aos objetivos militares. A participação de civis e atores não estatais nas hostilidades, georgianos pró-Rússia, na condição de voluntários, recrutados pelo exército russo para deliberadamente espalhar o malware aos computadores em rede de todo o país, potencializou ainda mais os ataques DDOS.

Os principais desafios técnicos e jurídicos para a regulamentação da guerra cibernética decorrem das constantes inovações tecnológicas dentro do espaço cibernético, sem que haja o acompanhamento do desenvolvimento correspondente, das ferramentas que permitam assegurar a implementação das medidas jurídicas e normativas necessárias para identificar a origem e autoria de um ataque cibernético, julgar e eventualmente punir o Estado agressor.

Para superar desafios elencados, será necessário o auxílio do Manual de Tallinn para identificar os critérios técnicos e jurídicos, além de definir mandato para conduzir as investigações

relacionadas aos ataques cibernéticos e para julgar os eventuais crimes de guerra deles decorrentes.

A complexidade dos ataques cibernéticos torna ainda mais difícil o estabelecimento dos critérios citados acima, já que as tradicionais definições de uso da força não são suficientes para esclarecer quais ataques cibernéticos são permitidos, bem como a medida da necessidade e da proporcionalidade da resposta.

O Manual de Tallinn não representa as opiniões da OTAN ou qualquer outra organização ou Estado. No entanto, representa a aplicação do direito internacional e da interpretação no contexto cyber, e, sem sombra de dúvida, terá um efeito sobre a forma como os Estados e as organizações irão regulamentar e normatizar a guerra cibernética bem como reformular o direito internacional no contexto cibernético.

REFERÊNCIAS

ALMEIDA, José Eduardo Portella. A tendência mundial para a defesa cibernética . p. 86. Disponível em: <http://www.sae.gov.br/site/wp- content/uploads/Seguranca_Cibernetica_web.pdf>. Acesso em: 24 jun. 2014.

BONANATE, Luigi. *A guerra*. São Paulo: Estação Liberdade, 2001.

CLARKE, Richard A.; KNAKE, Robert K., Cyber War: The Next Threat to Nacional Security and What to do About it. Estados Unidos: HarperCollins, 2010

DELIBASIS, Dimitrios. Cyberspace warfare and self-defence (October 10, 2011). Disponível em: <http://ssrn.com/abstract=1942279>. Acesso em: 25 jul 2014..
115
_____. Cyberspace warfare attacks and non state actors. 2011. Disponível em: <http://ssrn.com/abstract=1942283>. Acesso em: 25 jul 2014..

DOROTHY Denning. Reflections on cyberweapons controls. Disponível em: < http://faculty.nps.edu/dedennin/publications/reflections_on_cyberweapons_controls.p df>. Acesso em: 15 jul 2014..

DROEGE, Cordula. Não há brechas jurídicas no ciberespaço. Disponível em: <http://www.icrc.org /por/resources/documents/interview/2011/cyber-warfare- interview-2011-08-16.htm>. Acesso em: 15 jul 2014.

FRANÇA, Junia Lessa. Manual para Normalização de publicações técnico-científicas. Belo Horizonte: Ed UFMG, 2007.

GERVAIS, Michael. Cyber attacks and the laws of war. 2011 Disponível em: < http://ssrn.com/abstract=1939615 or http://dx.doi.org/10.2139/ssrn.1939615>. Acesso em 20 jul 2014.

GRAHAM, David E. Cyber threats and the law of war. 2010.

HOLLIS, Duncan B., Why States Need an International Law for Information Operations. Lewis & Clark Law Review, Vol. 11, p. 1023, 2007; Temple University Legal Studies Research Paper No. 2008-43. Disponível em: <http://ssrn.com/abstract=1083889>. Acesso em: 15 jul 2014.

KEEGAN, John. *Uma história da guerra*. São Paulo: Companhia das Letras, 1995.

_____. *História ilustrada da Primeira Guerra Mundial*. Rio de Janeiro: Ediouro, 2003.

KESAN, Jay P.; HAYES, Carol M. Mitigative counterstriking: self-defense and deterrence in cyberspace. (April 7, 2011). Illinois Public Law Research Paper No. 10- 35; Illinois Program in Law, Behavior and Social Science Paper No. LBSS11-18; Harvard Journal of Law and Technology, Forthcoming. Disponível em: <http://ssrn.com/abstract=1805163>. Acesso em: 15 jul 2014.

LESSIG, Laurence. Code. New York: Basic Books, 2006, p. 1. Disponível em: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em: 20 jul 2014.

KESAN, Jay P.; HAYES, Carol M. Mitigative counterstriking: self-defense and deterrence in cyberspace. (April 7, 2011). Illinois Public Law Research Paper No. 10- 35; Illinois Program in Law, Behavior and Social Science Paper No. LBSS11-18; Harvard Journal of Law and Technology, Forthcoming. Disponível em: <http://ssrn.com/abstract=1805163>. Acesso em: 15 jul 2014..

LESSIG, Laurence. Code. New York: Basic Books, 2006, p. 1. Disponível em: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em: 15 jul 2014..

MANDARINO JÚNIOR, Raphael. Segurança e defesa do espaço cibernético brasileiro. Recife: Cubzac, 2010.

MELZER, Nils. Interpretative guidance on the notion of direct participation in hostilities under international humanitarian law. 2009. Disponível em: <http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf>. Acesso em: 15 jul 2014.

NYE JR, Joseph S. *Cooperação e conflito nas relações internacionais*. São Paulo: Gente, 2009.

SILVA, Geraldo Eulálio do Nascimento e HILDEBRANDO, Accioly , Manual do Direito Internacional Público. São Paulo: Saraiva, 2002.