DA NÉVOA DA GUERRA ÀS NUVENS: A OPERAÇÃO ORCHARD E O USO DA FORÇA NO ESPAÇO CIBERNÉTICO

FROM THE FOG OF WAR TO THE CLOUDS: OPERATION ORCHARD AND THE USE OF FORCE IN CYBERSPACE

Henrique Lenon Farias Guedes[1]

Tiago Medeiros Delgado[2]

Resumo: Embora a Internet tenha nascido como estratégia de defesa dos Estados Unidos da América, nos tempos de Guerra Fria, hoje, a rede tem-se revelado insegura para indivíduos, para corporações e para Governos em todo o mundo. Além das revelações de espionagem eletrônica global e dos constantes ataques de "hackers" e de ativistas cibernéticos, paulatinamente o ciberespaço se transforma também em região de conflito entre os países. Um caso paradigmático, em que se concentra o trabalho, é a Operação Orchard empreendida no Oriente Médio, em 2007, quando jatos de caça israelenses entraram no espaço aéreo sírio e bombardearam instalações do Complexo Kibar, em que a Síria estava desenvolvendo a bomba nuclear com apoio da Coreia do Norte. Durante toda a atividade aérea de Israel na Síria, os radares deste país não detectaram qualquer presença estrangeira ou anormalidade, pois Israel reprogramou temporariamente o sistema de radares sírios, deixando-os inertes e alheios à realidade. Não havendo marco regulatório ou tratado específico para o uso do ciberespaço como mecanismo militar, o presente artigo discute se, para o existente direito internacional bélico, o "ciberataque" israelense foi um ato de guerra. A fim de responder a tal problematização, o trabalho traz um panorama dos mais relevantes "ciberataques" registrados na literatura especializada, narrando, enfim, os passos e as consequências da operação examinada. Fundamentando-se na equivalência entre "ciberataque" e ato de guerra, o artigo, valendo-se do método dedutivo, tenta compreender as consequências do uso da força no espaço cibernético.

Palavras-chave: segurança da informação; "ciberataque"; Operação Orchard.

[1] Estudante da Faculdade de Direito da Universidade Federal da Paraíba, em João Pessoa (UFPB), onde foi bolsista em atividades de pesquisa (CNPq), de monitoria e de extensão. Fundador e integrante do Conselho Deliberativo da Academia Nacional de Estudos Transnacionais (ANET). Contato: hlfguedes@gmail.com.

[2] Estudante da Faculdade de Direito da Universidade Federal da Paraíba, em João Pessoa (UFPB). Membro da Academia Nacional de Estudos Transnacionais (ANET). Bolsista do Programa Institucional de Bolsas de Iniciação Científica – PIBIC/CNPq/UFPB. Contato: medeiros_174@hotmail.com

Abstract: Although the Internet has been created as defensive strategy of the United States of America, during the Cold War era, nowadays, the net has revealed itself as unsafe to individuals, corporations and Governments across the world. Besides the global electronic spy scandals and the constant attacks from hackers and "hacktivists", the cyberspace is gradually transforming into a battlefield among countries. A paradigmatic case, on which this paper focuses, is the Operation Orchard, launched in the Middle East, in 2007, when Israeli fighter jets invaded Syrian air space and bombed the facilities of the Kibar Complex, where Syria was developing nuclear weapons with North Korean support. During all Israel's aerial activity in Syria, this country's radars could not detect any foreign presence or abnormality, because Israel temporarily reprogrammed Syrian radar systems, so that they could not realize what was happening. Facing the absence of regulatory marks or specific treaties regarding the military use of cyberspace, this paper discusses if, concerning the international law of armed conflict, the Israeli cyberattack was an act of war. In order to solve this problem, this article brings an overview of the relevant cyberattacks that have already occurred, describing the steps and consequences of the Operation Orchard. Based on the equivalence between cyberattack and act of war, the article, using deductive methods, aims at understanding the consequences of the use of force in cyberspace.
Keywords: cybersecurity; cyberattack; Operation Orchard.

Introdução

Em tempos de ubíquos Facebook e Whatsapp, atestar a relevância do ciberespaço[3] pode soar fácil, contudo, além das redes sociais e de outros usos cotidianos, como o comércio eletrônico e o compartilhamento de informações, a Internet tem-se revelado personagem de inúmeras disputas geopolíticas e, a partir delas, de questionamentos jurídicos.

Diversos campos do direito, nos últimos anos, incluíram o ciberespaço em suas preocupações: os penalistas debatem crimes cibernéticos, os civilistas se interessam pela diluição da privacidade, os trabalhistas defendem a proteção do teletrabalho e do sobreaviso, e há, ainda, discussões sobre liberdade de expressão, sobre governo eletrônico e sobre as garantias do acesso à rede como um direito humano. A aprovação da legislação nacional denominada "Marco Civil da Internet", em abril de 2014, também demonstra a importância e o alcance dos debates

[3] O texto optou por utilizar, em português, apenas as palavras com grafia autorizada pelo Vocabulário Ortográfico da Língua Portuguesa (VOLP), publicado pela Academia Brasileira de Letras. Termos como "ciberguerra" e "ciberataque", ainda não reconhecidos pelo VOLP, serão apresentados entre aspas.

regulatórios no Brasil. Além dessas relevantes discussões sobre o disciplinamento do ciberespaço pelo direito doméstico, deve-se reconhecer que, embora grandes temas das relações internacionais, hoje, sejam afetados pelo uso da Internet, a regulação internacional do espaço virtual ainda é incipiente.

Nesta década, a aglutinação do ciberespaço pela política global tornou-se bastante visível: Governos caíram por força de mobilização virtual e deixaram Estados aliados em xeque, como aconteceu entre Egito e Arábia Saudita; a Turquia, por seu turno, proibiu o acesso de seus cidadãos ao YouTube, na expectativa de reduzir algum ímpeto protestador ou revolucionário, perdendo, entretanto, chances de demonstrar sua pertinência ao liberal concerto europeu. O fato mais evidente das imbricações entre Internet e relações internacionais foi o vazamento de informações confidenciais pelo Sr. Edward Snowden, atestando que os Estados Unidos da América, por meio da National Security Agency (NSA), espionavam as comunicações telefônicas e especialmente virtuais de milhões de indivíduos de inúmeras nacionalidades, até mesmo de figuras destacadas, como Angela Merkel e Dilma Rousseff.

Apesar do alto impacto que o uso da Internet pelos Estados pode ter, o direito internacional ainda não conseguiu oferecer respostas regulatórias. O ciberespaço não tem uma organização internacional ou uma agência da ONU específica para seu controle, e não há ainda um marco regulatório de nível mundial. O pioneirismo com que foi tratado o NETmundial – Encontro Multissetorial Global Sobre o Futuro da Governança da Internet, realizado em abril de 2014, em São Paulo, reforça a carência regulatória do setor.

Outra grande evidência de certa apatia jurídica em relação ao ciberespaço é que, até hoje, mais de três décadas depois de transformar-se de rede de defesa militar americana – a ARPANET – em rede mundial de computadores pessoais, a Internet ainda é monitorada oficialmente pelo Departamento de Comércio dos Estados Unidos, que terceiriza suas operações para a Corporação da Internet Para Atribuição de Nomes e Números – ICANN, na sigla em inglês[4] –, associação privada com sede na Califórnia.

A necessidade de encontrar, no direito internacional, respostas para os dilemas geopolíticos da Internet oferece justificativa para o presente artigo, que se concentra especificamente em estudar o ciberespaço como campo de atuação militar dos Estados. A questão, na verdade, já é realidade: há diversos relatos de ataques entre Nações que utilizam

[4] Internet Corporation for Assigned Names and Numbers.

programas de computador como armas, a fim de minar a capacidade bélica do adversário.

Um caso paradigmático, em que se concentrará o trabalho, ocorreu no Oriente Médio, em 2007, integrando a Operação Orchard. Baseando-se em informações obtidas por "trojans"[5], jatos de caça do Estado de Israel entraram no espaço aéreo da Síria e bombardearam instalações do Complexo Kibar, em que a Síria estava desenvolvendo a bomba nuclear com apoio da Coreia do Norte – a informação, obtida por meios "piratas", seria confirmada posteriormente pela Agência Internacional de Energia Atômica. Durante toda a atividade aérea de Israel na Síria, os radares deste país não detectaram qualquer presença estrangeira ou anormalidade. De fato, antes de invadir o espaço aéreo do vizinho, Israel tinha "hackeado" o sistema de radares e de defesa sírios, em uma demonstração do surgimento de operações cibernéticas de guerra.

Não havendo marco regulatório ou tratado específico para o uso do ciberespaço como mecanismo militar, cabe intuir se as atuais disposições do direito internacional são aplicáveis no ambiente virtual. Nesse contexto, o presente artigo discute o seguinte problema: para o existente direito internacional bélico, o "ciberataque" que inutilizou os radares sírios, durante a Operação Orchard, foi um ato de guerra?

A fim de responder a tal problematização, o artigo busca trabalhar os conceitos jurídicos de guerra, de uso da força e de "ciberataque", trazendo suporte bibliográfico que equipara os ataques perpetrados por uma Nação contra outra, via Internet, aos ataques empreendidos por outros meios, seja terrestre, aéreo ou marítimo. Paralelamente, o trabalho traz um panorama dos mais relevantes "ciberataques" registrados na literatura especializada, narrando, enfim, os passos e as consequências da Operação Orchard.

Fundamentando-se na equivalência entre "ciberataque" e ato de guerra, o artigo, valendo-se do método dedutivo, tenta compreender as consequências do uso da força no espaço cibernético.

1. Da defesa ao ataque

Embora a Internet tenha nascido como estratégia de defesa dos Estados Unidos da América, nos tempos de Guerra Fria, hoje, a rede tem-se revelado insegura para indivíduos, para empresas e para Governos. A ARPANET foi criada em 1969, para integrar redes de computadores em locais distintos e garantir a perpetuidade das comunicações em caso de ataque

[5] Programas que roubam inadvertidamente informações de computadores.

a uma das bases. O termo “Internet” apareceu em 1974, enquanto a “world wide web”, permitindo o acesso a sítios virtuais em qualquer lugar do mundo, foi lançada em 1990 (HILL, 2013, p. 19).

A capilaridade da Internet pode ser atestada com dados da União Internacional de Telecomunicações (ITU): em 1997, 2% da população mundial utilizavam a rede; em 2012, tal número era 35% (HILL, 2013, p. 23). Tal crescimento deve aumentar com recentes projetos privados de levar conexões à Internet para países pobres. Baseando-se na estatística de que dois terços da população mundial ainda não tem acesso à rede mundial de computadores, o Google anunciou o Projeto Loon, em junho de 2013, “uma rede de balões que viaja pelos confins do espaço” com a finalidade de “conectar pessoas em áreas rurais e remotas, ajudar a preencher falhas de cobertura e ajudar a recuperar a conexão com a Internet em áreas que passaram por desastres” (GOOGLE, 2014).

Em fevereiro de 2014, o Facebook lançou o projeto internet.org, em cuja página se afirma que “ninguém deveria ter de escolher entre o acesso à internet e alimentos ou remédios” e que as instituições parceiras “reunirão forças para desenvolver tecnologias que reduzam o custo do envio de dados para pessoas no mundo todo, e para ajudar a expandir o acesso à internet em comunidades desfavorecidas” (INTERNET, 2014). Um aplicativo para celular que proporciona uma rede de acesso gratuito a alguns dos mecanismos mais acessados das Internet, como o buscador do Google, o aplicativo de mensagens do Facebook e a Wikipédia, foi lançado, em julho de 2014, para usuários da Zâmbia (ROSEN, 2014).

O amadurecimento da Internet e a expansão dos meios de acesso, notadamente com a recente popularização de *smartphones*, não significou, contudo, um aperfeiçoamento da segurança virtual. Ao contrário, conforme dados da Gartner, da Risk Based Security e do Ponemon Institute: em 2009, quase duzentos milhões de registros privados foram invadidos em sítios virtuais; em 2013, o número de brechas desse tipo ultrapassou oitocentos milhões, fazendo empresas como Adobe e eBay de vítimas (GILES, 2014, p. 4). Até mesmo o Ministério das Relações Exteriores do Brasil foi vítima de ataques cibernéticos, em maio de 2014, quando *e-mails* de servidores do Itamaraty foram invadidos, e telegramas diplomáticos, violados (PARAGUASSU, 2014).

As preocupações com “cibersegurança” tornam-se ainda mais altas, com o alvorecer da “Internet das coisas”. As estimativas do mercado apontam que, até o final da década, cerca de

cinquenta bilhões de aparatos pessoais ou residenciais estarão conectados à Internet: carros, televisões, refrigeradores, interruptores de luz e até aparelhos médicos. Já há, nesse contexto, relatos de invasões de "hackers" a "webcams", enquanto pesquisadores comprovam a possibilidade de se invadir os computadores de um carro e tomar-lhe o controle (GILES, 2014, p. 10-11).

Paradoxalmente, no contexto do combate difuso e, por vezes, doméstico ao terrorismo, a existência de falhas de segurança nas conexões com a Internet favorece os serviços de inteligência, que "procuram erros de programação em 'softwares', para usá-los na espionagem de terroristas e outros alvos. Se deixarem, contudo, essas falhas de segurança abertas (...), alimentam o risco de que 'hackers' hostis também as encontrem e as explorem" (GILES, 2014, p. 5, tradução nossa).[6] As brechas onipresentes na segurança da informação ficaram evidentes, para a população civil, na crise internacional causada pela denúncia do Sr. Edward Snowden, afirmando que a Agência Nacional de Segurança americana, a NSA, como parte do programa de combate ao terror, teria monitorado inúmeras contas de e-mails e de telefone de cidadãos de diversos países, incluindo mandatárias de aliados como Brasil e Alemanha (US, 2014b).

As preocupações com invasões cibernéticas também chegaram às grandes corporações. Levantamento da empresa especializada Mandiant afirma que, em 2012, "hackers" chineses investiram ataques virtuais contra empresas de tecnologia, de transportes, de navegação, de entretenimento e de engenharia, como também invadiram dados de organizações internacionais e de Governos nacionais, além de escolas e indústrias aeroespaciais (GILES, 2014, p. 6).

Em maio de 2014, o Procurador-Geral dos Estados Unidos, Eric Holder, anunciou que o Governo americano decidira processar judicialmente cinco militares chineses, sob a acusação de que os oficiais teriam roubado segredos comerciais e documentos internos de cinco companhias e de um sindicato, por meio de investidas cibernéticas. A judicialização do tema foi recebida com mal-estar em Pequim, que afirmou que a medida prejudicava as relações diplomáticas entre os dois países (US, 2014a).

É interessante perceber, no contexto das discussões sino-americanas sobre "ciberataques", que a própria conceituação que a classe política de cada país confere ao termo é divergente. Enquanto o Senado americano tem equiparado as invasões a dados de empresas de

[6] Traduzido do original em inglês: "Intelligence agencies look for programming mistakes in software so they can use them to spy on terrorists and other targets. But if they leave open these security holes, know in tech jargon as 'vulnerabilities', they run the risk that hostile hackers will also find and exploit them" (GILES, 2014, p. 5).

cartão de crédito com ataques de vírus virtuais a instalações militares, a China não admite a utilização de redes sociais como o Facebook para a propagação de rumores, revelando uma falta de clareza semântica em se caracterizar todas essas três iniciativas como o mesmo problema (SINGER; FRIEDMAN, 2014, p. 68).

A relevância e amplitude alcançada pela Internet leva a segurança da informação, gradualmente, às preocupações dos Estados, que buscam proteger seus cidadãos de ataques estrangeiros tanto quanto se esforçam em proteger suas próprias capacidades militares.

2. A geopolítica do ciberespaço: o problema da atribuição

O uso de operações cibernéticas, para atingir objetivos geopolíticos e estratégicos, vem aumentando entre os Estados. Os "ciberataques", geralmente, ocorrem em conjunto com operações militares convencionais, possuindo consequências materiais limitadas. A ocorrência de operações cibernéticas maliciosas, no entanto, tende a crescer, tanto em número quanto em severidade, principalmente por seu baixo custo, relativo anonimato, ampla disponibilidade e crescente dependência da sociedade mundial em redes de computadores e sistemas de controle industrial. Nesse processo, os militares precisam de "soldados cibernéticos", e a criação de forças militares especializadas, como a Décima Frota estadunidense, pode ajudar a concentrar perícia e financiamento para projetos de longo prazo (SOLCE, 2008, p. 315). Dessa forma, os "ciberataques" relacionados a seguir podem servir como precedente para a construção de normas internacionais que regulem o uso bélico do ciberespaço, além de serem evidências de que já existe o uso militar ofensivo e defensivo de operações cibernéticas.

O primeiro exemplo que podemos citar é a série de ataques sofridos pelos Estados Unidos da América, desde 2003, e revelados em 2005, chamados pelos investigadores estadunidenses de "Titan Rain". Supostamente originados da China, os ataques tinham como alvo redes de computadores do Departamento de Defesa e outras agências governamentais do país.

A atribuição é um dos principais problemas relacionados à ocorrência de "ciberataques", o qual pôde ser evidenciado no caso em análise: enquanto alguns analistas estavam convencidos do envolvimento do Governo chinês em uma campanha de espionagem, outros afirmavam que as invasões nas redes estadunidenses eram originadas de "hackers" que apenas utilizavam as redes chinesas, para despistar a origem dos ataques (THORNBURGH, 2005).

> Três características principais da capacidade de capturar e de utilizar outros computadores são particularmente importantes. Em primeiro lugar, não há

> limites geográficos. Por exemplo, alguém no Brasil pode programar computadores na África do Sul a lançarem ataques em sistemas na China, que podem ser controlados por computadores fisicamente localizados nos Estados Unidos. Em segundo lugar, o proprietário de um computador capturado geralmente não tem ideia de que está sendo usado por um agente remoto para propósitos perniciosos. (...) Em terceiro lugar, quando alguma atividade maliciosa é perpetrada, análises sofisticadas podem, no máximo, identificar o computador que foi utilizado, para lançar o ataque. É muito mais difícil determinar se o computador está sendo operado remotamente, e, em caso afirmativo, por quem (SINGER; FRIEDMAN, 2014, p. 73, tradução nossa).[7]

Mesmo os analistas que defendiam o envolvimento oficial do Governo da China discordavam sobre se os ataques visavam à obtenção de informações industriais, ou estavam apenas testando a habilidade de se infiltrar nos sistemas militares de Nações rivais, de forma imperceptível. Essa segunda visão era sustentada pelo fato de que, apesar do grande número de dados coletados, estes pertenciam a documentos oficiais não secretos ("unclassified"), pois as redes militares secretas não se conectam diretamente à Internet. O Governo estadunidense, entretanto, tratou da matéria como uma ameaça bastante séria, tomando medidas para o aprimoramento de suas defesas cibernéticas (GRAHAM, 2005).

A China ainda seria protagonista de outro evento similar, em 2010, quando o Google decidiu encerrar a censura nas buscas chinesas, devido à invasão, atribuída ao Governo chinês, às contas do Gmail de ativistas de direitos humanos na China, nos EUA e na Europa, bem como de dados de vinte corporações (SMITH, 2010).

A Federação Russa também foi personagem central em, no mínimo, dois episódios relevantes no que se refere aos "ciberataques". O primeiro deles, envolvendo a Estônia, ocorreu em 2007, quando as autoridades do país báltico decidiram remover um monumento russo da Segunda Guerra Mundial, um "Soldado de Bronze", do centro da cidade para sua periferia. A Estônia alegava que o monumento representava a ocupação soviética do Estado, enquanto os russos argumentavam que era uma homenagem àqueles que lutaram contra o nazismo. As comunidades estonianas de língua russa e a população da vizinha Rússia sentiram-se ofendidas com o ato. Nos dias seguintes, ocorreram protestos violentos nas ruas, e, no dia 30 de abril,

[7] Traduzido do original em inglês: "Three key features of this capability to capture and utilize other computers are particularly important. First, there are no geographical limits. For example, someone in Brazil can compromise computers in South Africa to launch attacks on systems in China, which might me controlled by computers physically located in the United States. Second, the owner of a captured computer often has no idea that it is being used by a remote actor for pernicious purposes. (…) And third, when some pernicious activity is perpetrated, sophisticated analysis can typically, at best, identify the computer being used to launch the attack. It is far more difficult to determine whether that computer is being operated remotely and, if so, by whom" (SINGER; FRIEDMAN, 2014, p. 73).

notou-se um aumento vertiginoso no número de ataques distribuídos de negação de serviço (DDOS[8]).

Os ataques foram originados de aproximadamente oitenta e cinco mil computadores e continuaram por três semanas. Os serviços online do Hansapank, por exemplo, o maior banco da Estônia, ficaram indisponíveis por até duas horas no dia dez de maio. Os efeitos dos "ciberataques" na economia, no Governo e na sociedade foram notórios, causando prejuízos e assustando os governantes e a população da Estônia (RID; MCBURNEY, 2012, p. 9).

Apesar de o Governo russo ter negado envolvimento nos ataques, o Mistério da Defesa da Estônia afirmou que instruções, para contribuir com a condução da guerra cibernética, estavam disponíveis em sites russos. O Primeiro Ministro da Estônia, à época, Andrus Ansip, acusou diretamente o governo russo como responsável. Os alvos dos ataques incluíram os Ministérios da Defesa e das Relações Exteriores, bem como bancos e jornais. (ESTONIA, 2007).

O outro episódio relevante envolvendo a Rússia deu-se no ano seguinte, 2008, quando uma série de "ciberataques" puderam ser observados durante a guerra contra a Geórgia, na região da Ossétia do Sul. Mais uma vez, devido a ataques distribuídos de negação de serviço (DDOS), o *site* da Presidência do país, então liderado por Mikheil Saakashvili, ficou inoperante por um dia inteiro. Além disso, a mídia, as comunicações, os transportes e as páginas do Ministério das Relações Exteriores e do Ministério da Defesa também foram alvo dos ataques. A inacessibilidade aos sites governamentais, inclusive, dificultou a habilidade do Governo da Geórgia de se conectar com seus simpatizantes ao redor do mundo durante o conflito com a Rússia. Moscou, novamente, negou a autoria dos ataques (MARKOFF, 2008; SWAINE, 2008).

A Operação Orchard, em que se concentra o presente artigo, tornou-se paradigmática, porque demonstrou a indispensabilidade do conhecimento cibernético e a vulnerabilidade dos sistemas de defesa, além de representar um concerto entre mecanismos militares convencionais e novos. Em 2006, um alto representante do Governo da Síria deixou seu "laptop" em um quarto de hotel, enquanto visitava Londres. Durante sua ausência, agentes da Mossad, o serviço secreto do Estado de Israel, instalaram um "trojan" no computador, a fim de monitorar as comunicações do funcionário sírio. Enquanto analisavam os arquivos guardados na máquina, os agentes israelenses

[8] DDOS é a sigla, em inglês, para "distributed denial of service". Os ataques distribuídos de negação de serviço são relativamente novos. Consistem em ataques coordenados que afetam a disponibilidade dos sistemas ou redes aos quais os ataques são direcionados, podendo provocar inúmeros prejuízos. Nesse tipo de ataque, um computador pode comandar inúmeros outros, para ampliar a escala do ataque e dificultar a atribuição, pois o grande número de computadores envolvidos prejudica a identificação do verdadeiro atacante. (SPECHT; LEE, 2004, p. 1)

encontraram, por acaso, uma foto de dois homens no deserto sírio: o chefe do programa nuclear norte-coreano e o Diretor da Comissão de Energia Atômica da Síria. Examinando planos de construção e de canos, também presentes no computador, concluíram que a Síria estava secretamente erigindo uma unidade de processamento de plutônio, com apoio da República Democrática Popular da Coreia, em Al Kibar, o que permitiria a fabricação da bomba nuclear – a informação seria confirmada posteriormente pela Agência Internacional de Energia Atômica.

Na madrugada de seis de setembro de 2007, sete jatos de caça israelenses entraram no espaço aéreo sírio, bombardeando instalações do Complexo Kibar. Durante toda a atividade aérea de Israel na Síria, os radares deste país não detectaram qualquer presença estrangeira ou anormalidade. De fato, antes de invadir o espaço aéreo do vizinho, Israel alterou, por meio de programas de computador, o sistema de radares e de defesa sírios:

> Os israelenses tinham penetrado, com sucesso, as redes computacionais militares da Síria, permitindo-lhes ver o que os sírios estavam fazendo e também inserir suas próprias transmissões de dados no sistema de defesa aéreo. Isso fez que os operadores de radares sírios vissem uma falsa imagem do que estava realmente acontecendo, enquanto os jatos de Israel atravessavam a fronteira. Ao eficazmente desligar as defesas aéreas sírias naquela noite, os israelenses não apenas chegaram a seu alvo sem perdas, como também utilizaram uma força muito menor (SINGER; FRIEDMAN, 2014, p. 128, tradução nossa[9]).

Nenhum Governo da região, inclusive o iraniano, comentou ou condenou a operação.

Outro caso paradigmático, que ficou bastante famoso, no que se refere a "ciberataques" é o do Stuxnet. Descoberto em 2012, o programa malicioso ("worm"), considerado bastante sofisticado, agressivo e autorreplicante, foi detectado, pela primeira vez, em um computador iraniano. O programa havia sido desenvolvido, para atacar e sabotar sistemas de controle industrial de instalações como redes de energia e usinas nucleares. Apesar de sua concentração no Irã, o Stuxnet foi capaz de se propagar para cento e cinquenta e cinco países. Classificado como a primeira arma cibernética com consequências devastadoras, o Stuxnet foi responsável, principalmente, por sabotar o programa nuclear iraniano.

Responsável pelo desligamento da usina iraniana de Natanz, o Stuxnet é considerado extremamente sofisticado, tendo passado despercebido por um longo período de tempo e sem

[9] Traduzido do original em inglês: "The Israelis had successfully penetrated the Syrian military's computer networks, allowing them to see what the Syrians were doing as well as direct their own data streams into the air defense network. This caused the Syrian radar operators to see a false image of what was really happening as the Israeli jets flew across the border. By effectively turning off the Syrian air defenses for the night, the Israelis not only got to their target without any losses, but they also did so with a much smaller force" (SINGER; FRIEDMAN, 2014, p. 128).

causar efeitos colaterais notáveis. Apesar de ter infectado mais de cem mil computadores, para aumentar as chances de chegar ao alvo, o Stuxnet não provocou danos nos "hospedeiros", mas apenas nos que constituíam seu objetivo. Considera-se que o Stuxnet tenha atrasado em um ou dois anos o programa nuclear iraniano (KUMAR *et alli*, 2013, p. 20).

Considerando o contexto geopolítico e o nível de sofisticação do programa, que só pode ter sido alcançado por meio de um Estado e não por "hackers" individuais, acredita-se que o Stuxnet seja uma criação conjunta de Israel e dos Estados Unidos. Ambos negam qualquer envolvimento (RID; MCBURNEY, 2012, p. 9-10).

A dificuldade em encontrar os responsáveis por "ciberataques", devido à inerente difusão do espaço cibernético, refletiu-se no Manual de Tallin, elaborado por um grupo de especialistas internacionais designados pelo Centro de Excelência de Defesa Cibernética Cooperativa da Organização do Tratado do Atlântico Norte (OTAN). A regra 07 do manual afirma que o simples fato de uma operação cibernética originar-se de uma estrutura governamental não comprova que o respectivo Estado é responsável pela operação (SCHMITT, 2013, p. 39).

Ironicamente, o manual é resultado de reuniões realizadas na Capital da Estônia, que sofreu com assaltes cibernéticos, em 2007. Embora usualmente atribuídos à Rússia, 25% dos computadores utilizados nos ataques, contudo, estavam localizados nos Estados Unidos (SINGER; FRIEDMAN, 2014, p. 73).

3. Um campo de batalha virtual?

O desenvolvimento de armas cibernéticas, como exemplificado anteriormente, tem ocasionado uma crescente preocupação mundial sobre a possível eclosão de "ciberguerras". Cada vez mais complexos, tais armamentos podem provocar danos comparáveis aos dos ataques convencionais e servir aos propósitos táticos e estratégicos de um determinado Estado. Diante desse potencial destrutivo e da aparente falta de regulação do ciberespaço, são constantes as discussões sobre a aplicabilidade das normas do direito internacional a essa nova dimensão. O debate, contudo, encontra inúmeros obstáculos na falta de precedentes e nas divergências conceituais, o que leva a um aumento no risco de percepções equivocadas e escalada dos conflitos (VIGNARD, 2011, p. 51).

Até agora, os ataques cibernéticos têm sido usados, geralmente, em conjunto com os

convencionais, de maneira a aumentar a incerteza ou o desconhecimento sobre as capacidades e ações do inimigo, durante a guerra. A preocupação com o desenvolvimento de tecnologias de informação e comunicação, como instrumentos de guerra e inteligência, é evidente e fomenta inúmeros debates nas Nações Unidas, como demonstrado pela presença constante do tópico em sua agenda. Recentemente, por exemplo, foi aprovada a Resolução A/RES/68/243, adotada na 68ª sessão da Assembleia Geral da ONU. Ainda assim, é importante ressaltar que o desenvolvimento de tratados internacionais que reflitam consenso na regulação do ciberespaço como uma dimensão bélica ainda constitui uma realidade distante (MAURER, 2011, p. 10).

A maioria dos países aceita o ciberespaço como o quinto domínio de guerra, juntamente com a terra, os mares, o ar e o espaço. Diante disso, a maior parte deles possui um programa de defesa cibernética, e os gastos com segurança, nesse âmbito, crescem exponencialmente. É interessante notar que a interconectividade e a progressiva dependência de aparelhos eletrônicos, na sociedade, potencializa os riscos à segurança em rede, bem como os possíveis danos provocados por uma operação cibernética maliciosa. O acelerado aumento de usuários da rede mundial de computadores e o caráter pouco oneroso das operações cibernéticas relacionam-se intrinsecamente com esses fatores negativos, na medida em que um "ciberataque" lançado por um único indivíduo pode causar prejuízos bilionários, como pode ser visto no caso do vírus "Love Bug", lançado por um "hacker" filipino, o qual provocou perdas estimadas em 15 bilhões de dólares (NYE JR, 2010, p. 9). O anonimato é outro impulsionador dos "ciberataques", tanto no caso de ações individuais, quanto de ações estatais. Por meio de técnicas como "IP spoofing" ou uso de "botnets"[10], a origem de determinados ataques pode permanecer desconhecida. Além disso, mesmo o fato de um "ciberataque" aparentemente ter sido originado em um determinado local não necessariamente implica que o Estado ou os donos dos computadores envolvidos esteja ciente das ações ofensivas (ROSCINI, 2010, p. 96).

Alguns autores defendem que, caso uma guerra seja deflagrada, muito possivelmente os primeiros estágios incluiriam "ciberataques", com o objetivo de interromper o funcionamento de certas infraestruturas e, consequentemente, propiciar ganho militar (RID; MCBURNEY, 2012, p.

[10] A técnica do "IP spoofing" consiste em mascarar pacotes IP utilizando endereços de remetentes falsificados e, dessa forma, ganhar acesso a computadores não-autorizados, ou esconder a origem de suas ações. As "botnets", por sua vez, são redes de computadores infectadas por agentes de sotware ("bots") semelhantes. Os "bots" podem ser programados, para desempenhar tarefas específicas no computador infectado, o que dificulta a atribuição, pois as ações são efetuadas por um grande número de máquinas e, muitas vezes, sem que os donos dos computadores infectados tenham conhecimento.

21). Isso leva os países a terem uma preocupação cada vez maior com a defesa e segurança cibernéticas. Dos quinze Estados com os maiores orçamentos militares do mundo, todos investem em capacidades cibernéticas ofensivas (UNIDIR, 2013, p. XI; SINGER; FRIEDMAN, 2014, p. 128). Nos EUA, por exemplo, a Décima Frota ("Tenth Fleet") tem o ciberespaço como seu campo de atuação.

Além disso, os baixos custos, o anonimato e as grandes vulnerabilidades apresentadas pelos países mais desenvolvidos e com tecnologias avançadas, em virtude da dependência de equipamentos cibernéticos, fazem com que atores globais com menos importância tenham mais capacidade de exercer "soft" e "hard power", respectivamente de forma dissuasiva ou efetiva (NYE JR, 2010, p. 19). A expectativa de que, com o tempo, os ataques cibernéticos possam crescer, tanto em número quanto em severidade, portanto, faz com que haja uma grande preocupação nas Nações Unidas com o uso de tecnologias de maneira inconsistente com a manutenção da segurança e da estabilidade internacionais (ROSCINI, 2010, p. 88).

No entanto, o conceito de guerra é bastante problemático. A decisão sobre se uma operação pode ou não ser classificada como um ato de guerra baseia-se muito mais em critérios políticos que legais. A caracterização da operação cibernética como uso da força, ataque armado ou até mesmo ameaça à paz e à segurança internacionais leva a inúmeros pontos de divergência doutrinária, principalmente em virtude das consequências jurídicas[11] do pertencimento a qualquer uma dessas categorias. Assim, é bastante improvável que os Estados abdiquem dessas novas ferramentas do poder estatal, por serem relativamente baratas e oferecerem grandes vantagens estratégicas (UNIDIR, 2013, p. 57).

Dessa forma, a análise do "ciberataque" que integrou a Operação Orchard poderia ser feita, a princípio, sob inúmeras perspectivas, cada uma delas remetendo a diferentes implicações, no âmbito do direito internacional. A correta classificação do "ciberataque" é importante, na medida em que o risco de escalada de um conflito, por exemplo, é muito maior quando este configura "uso da força", reiteradamente condenado pelo direito internacional (SCHMITT, 1999, p. 17).

Primeiramente, há autores que defendem que a "ciberguerra" continua sendo apenas uma metáfora, uma vez que um ato de guerra deve ser instrumental, política e potencialmente letal, e que nenhum "ciberataque", até agora, satisfez esses critérios (RID; MCBURNEY, 2012,

[11] A Carta das Nações Unidas, por exemplo, prevê diversas consequências para o Estado que utiliza ilegitimamente a força, ameaçando a paz e a segurança internacionais, conforme seu capítulo VII.

p. 7).

A Carta das Nações Unidas, todavia, em vez de "atos de guerra", prevê o "uso da força", os "ataques armados" e as "ameaças à paz e segurança internacionais", cada um deles levando a diferentes consequências. Dessa forma, partiremos para a análise do chamado *jus ad bellum*, que regula o recurso ao uso da força nas relações internacionais.

É interessante notar, previamente, que a Carta das Nações Unidas, em seu artigo 2 (4), discorre sobre a proibição da ameaça ou uso da força. A partir da análise dos *travaux préparatoires* e de tratados posteriores, a exemplo da Declaração Sobre Relações Amigáveis, de 1970, é possível afirmar que tal proibição refere-se, especificamente, à força armada (ROSCINI, 2010, p. 105). Assim, para que o uso de "ciberataques" remeta a essa proibição, é indispensável que haja ferramentas cibernéticas consideradas "armas".

No entanto, tal necessidade encontra-se satisfeita, na medida em que, por depender da intenção do ofensor de ameaçar ou causar dano a um alvo e da percepção do alvo do dano potencial que lhe pode ser causado, a definição de "arma" é bastante ampla. Praticamente qualquer objeto pode ser considerado uma arma, se a intenção de quem a utiliza é hostil (ROSCINI, 2010, p. 22). Essa caracterização, pois, é extremamente necessária, uma vez que uma interferência não-armada em outro país tem impactos muito menores que uma armada e, somente a partir dela, podemos fazer referência ao que dispõe a Carta de São Francisco (RID; MCBURNEY, 2012, p. 11).

A proibição do uso da força está assinalada no artigo 2 (4) da Carta das Nações Unidas e é, indiscutivelmente, parte do costume internacional. É norma do chamado *jus cogens*, ou seja, é uma norma que é aceita e reconhecida pela comunidade internacional como não passível de derrogação e que possui efeito *erga omnes*, isto é, cria obrigações cujo descumprimento pode ser sancionado até por Estados cujos direitos não tenham sido violados (PETERKE, 2010, p. 102). Tal proibição está presente também em inúmeros instrumentos internacionais, a exemplo da Declaração Sobre os Princípios do Direito Internacional Relativos a Relações Amistosas e à Cooperação entre Estados em Conformidade com a Carta das Nações Unidas.

Sobre essa matéria, a Corte Internacional de Justiça, em sua opinião consultiva, acerca da legalidade da ameaça ou uso de armas nucleares, de 8 de julho de 1996, determinou que a proibição expressa pelo referido artigo da Carta de São Francisco se estende a qualquer uso da força, independentemente das armas empregadas (CORTE, 1996).

4. O uso da força no ciberespaço

É comum os doutrinadores fazerem referência ao termo "ciberguerra", assim como inúmeros países já expressaram que consideram "ciberataques" uma forma de força armada, desenvolvendo programas de produção de capacidades cibernéticas ofensivas e defensivas. Baseado nisso, é possível afirmar que "ciberataques" podem ser classificados como "uso da força" (ROSCINI, 2010). No entanto, qual o critério para tal classificação?

Não há consenso sobre o limiar, para que uma operação cibernética seja considerada como ameaça ou uso da força, de maneira que nem as práticas estatais nem a jurisprudência internacional oferecem critérios esclarecedores (MELZER, 2011, p. 24). O Manual de Tallin, elaborado por um grupo de especialistas internacionais designados pelo Centro de Excelência de Defesa Cibernética Cooperativa da Organização do Tratado do Atlântico Norte (OTAN), sugere, em sua Regra 10, que uma operação cibernética que constitui ameaça ou uso da força contra a integridade territorial ou independência política de um Estado, ou que é, de qualquer outra maneira, inconsistente com os propósitos das Nações Unidas, é ilegal. De maneira a esclarecer o que acarretaria que uma operação cibernética constituísse uso da força, o Manual, baseado na decisão da Corte Internacional de Justiça, no caso "Nicarágua vs. Estados Unidos" (1986), recomenda que as operações sejam consideradas como tal, quando sua escala e efeitos forem comparáveis aos de operações não cibernéticas que constituem uso da força (SCHMITT, 2013, p. 47).

O critério da "escala e efeitos" pode ser bastante útil, pois, apesar de a própria Carta das Nações Unidas não determinar os critérios, para que um ato seja considerado como uso da força, é possível basear-se nos inúmeros precedentes de uso da força por métodos não cibernéticos, no entanto não se pode afirmar que tal método resolve, por completo, o problema. Como a proibição do uso da força é baseada eminentemente no costume internacional, e este requer o elemento objetivo da prática consistente ao longo do tempo e o elemento subjetivo da *opinio juris sive necessitatis*, a falta de precedentes relevantes de "ciberataques" e as várias divergências ideológico-doutrinárias ainda são obstáculos. Uma norma costumeira pode desenvolver-se ao longo do tempo, mas, no presente, ela inexiste, visto que não se observa nem a prática, nem a *opinio juris* (SCHMITT, 1999, p. 22). Além disso, o próprio Manual de Tallin, lançado em 2013, chama a atenção para o fato de que não há consenso sobre se "ciberataques" que não causam

danos físicos podem ser elevados à categoria de uso da força, ou de ataque armado.

A Carta das Nações Unidas estabelece, em seu artigo 51, que nada em seu conteúdo deve "prejudicar o direito inerente de legítima defesa individual ou coletiva no caso de ataque armado contra um membro das Nações Unidas". Cabe notar, portanto, que, diferentemente do artigo 2 (4), o artigo 51 emprega o termo "ataque armado", em vez de "uso da força". A diferença, baseada principalmente na análise da escala e efeitos da operação, conforme decidido pela Corte internacional de Justiça, no supracitado caso da Nicarágua, tem o propósito, principalmente, de evitar a escalada desnecessária dos conflitos, priorizando a preservação da paz e da segurança internacional em lugar do interesse individual dos Estados (MELZER, 2011, p. 15). Dessa forma, nem sempre o "uso da força" pode ser considerado um "ataque armado" e, por esse motivo, desencadear o direito do Estado de autodefesa individual ou coletiva, inclusive por meio da força militar.

Portanto, a caracterização de um "ciberataque" como ataque armado está de acordo com o entendimento da Corte Internacional de Justiça, no caso da Nicarágua, em que preceitua que o artigo 51 da Carta das Nações Unidas não faz referência a armas específicas, aplicando-se, portanto, independentemente das armas empregadas (CORTE, 1986).

Portanto, o principal critério, para avaliar se a ocorrência de um "ciberataque" constitui um ataque armado é o do "escala e efeitos", de tal modo que se enquadrarão, nessa categoria, aquelas operações que resultarem em danos humanos diretos ou danos físicos de consequências análogas ao de um ataque armado convencional (SCHMITT, 1999, p.24). Mesmo esse critério, no entanto, é apontado como problemático, podendo ser interpretado de maneira muito restritiva, excluindo, por exemplo, os "ciberataques" que incapacitassem a rede de energia nacional ou todo o sistema de defesa aérea, ou muito abrangente, incluindo qualquer ataque de negação de serviço – DDOS – de larga escala, ainda que apenas contra provedores puramente civis (MELZER, 2011, p. 14).

Dessa forma, na ausência de mortes, de lesões ou de destruição, seria definido como ataque armado um "ciberataque" que tivesse, como alvo, infraestruturas críticas dentro da esfera de soberania de outro Estado (MELZER, 2011, p. 16). Essas são definidas pela Resolução 58/199, de 30 de janeiro de 2004, da Assembleia Geral das Nações Unidas, como as utilizadas para, entre outras coisas, a geração, transmissão e distribuição de energia, o transporte aéreo e marítimo, os serviços bancários e financeiros, o comércio eletrônico, o fornecimento de água e a

saúde pública.

Ainda, é importante ressaltar que alguns autores defendem o direito de responder em autodefesa, mesmo que o "ciberataque" não se eleve à categoria de ataque armado. Para tanto, deve haver a confluência de três fatores: o "ciberataque" é parte de uma operação que culminará em um ataque armado; o "ciberataque" constitui um passo irrevogável para um iminente e inevitável ataque armado; o defensor está agindo antecipadamente ao ataque em si diante de sua última oportunidade disponível de conter o ataque (SCHMITT, 1999, p. 28).

Contudo, cabe destacar que há, na doutrina, interpretações mais expansivas quanto a essa possibilidade, como no caso da autodefesa preemptiva. Tal teoria, lançada pela Estratégia de Segurança Nacional dos Estados Unidos da América, no contexto da Guerra ao Terror, defende que o conceito de ameaça iminente, que constitui um dos requisitos para a defesa antecipada, deve ser adaptado aos objetivos e capacidades dos adversários contemporâneos, especialmente no que se refere ao terrorismo. Dessa forma, seria possível o uso da força militar em autodefesa, ainda que anterior à ação inimiga (AREND, 2003, p. 1 ss.).

O aumento das possibilidades de autodefesa preemptiva, todavia, pode ser bastante perigoso, pois pode tornar vago o conceito de ataque armado, ou sua ameaça, e tornar possível o abuso de definições mais amplas, o que seria extremamente prejudicial à paz e à segurança internacionais. Além disso, o artigo 51, da Carta das Nações Unidas, que dispõe sobre a autodefesa, discorre apenas sobre o ataque armado, que é uma ação real, nada dispondo sobre a ameaça de agir. A interpretação estrita, que limita as exceções para o uso da força à autorização pelo Conselho de Segurança e à autodefesa em caso de ataque armado, é a mais aceita na comunidade internacional, de maneira que se preserve o princípio da proibição do uso da força (BOTHE, 2003, p. 3).

Por fim, cabe lembrar que, além de "uso da força" ou "ataque armado", um "ciberataque" pode ainda ser classificado como "ameaça à paz e segurança internacionais" ou "violação da paz ou ato de agressão", o que enseja sua apreciação pelo Conselho de Segurança da Nações Unidas, conforme o capítulo VII da Carta de São Francisco (ROSCINI, 2010, p. 110).

Para isso, devemos considerar os fatores ator, tempo, alvo e consequência. (SCHMITT, 1999, p. 25). Diante disso, o Conselho de Segurança tomará as providências que considerar cabíveis e razoáveis, para dar fim à ameaça ou violação em questão. Essas podem incluir recomendações, medidas para prevenir a escalada da crise e medidas envolvendo ou não o uso da

força, conforme disposto nos artigos 39 a 42 da Carta.

Conclusão

Para analisar o ataque cibernético realizado por Israel contra a Síria, no contexto da Operação Orchard, parte-se de duas premissas. A primeira delas considera possível que ataques cibernéticos sejam classificados como uso da força ou ataques armados, ensejando a referência aos artigos 2 (4) e 51, da Carta das Nações Unidas. A segunda é que não é necessário haver destruição física para que o "ciberataque" seja classificado como uso da força ou ataque armado, na medida em que, por exemplo, por meio de um "ciberataque", pode-se interromper o funcionamento das redes de energia a nível nacional, sem que, para isso, ocorra destruição física.

O Manual de Tallin, apesar de reiterar não haver consenso quanto à segunda premissa, admite que uma operação cibernética lançada por um Estado e direcionada contra infraestruturas localizadas em outro Estado pode violar a soberania deste último, bem como pode ser classificado como uso da força ou ataque armado.

Em uma primeira análise, é possível afirmar que, apesar de ter incapacitado o sistema de defesa aérea da Síria, tornando-a extremamente vulnerável, o "ciberataque" promovido por Israel não pode ser classificado nem mesmo como uso da força. Primeiramente, o dano provocado é indireto e aponta muito mais para uma preparação para um ataque, que para um ataque em si. Além disso, não ocorreram mortes, destruição de propriedades, danos físicos ou lesões graves.

O contraste dessa primeira análise com as demais é importante, na medida em que, da mesma forma que a aplicação das normas e princípios presentes na Carta da ONU deve zelar pela manutenção da paz e da segurança internacionais, evitando a escalada dos conflitos, a Carta não pode permitir que a proibição do uso interestatal da força seja driblada pela aplicação de medidas e métodos não violentos que, por todas as intenções e propósitos, sejam equivalentes a uma ruptura da paz entre os Estados envolvidos. A busca por normas que ponderem essa dupla faceta da regulação internacional do ciberespaço é importante, de maneira a evitar definições meramente políticas ou unilaterais, que contribuam para a escalada desnecessária de conflitos. Como exemplo, pode-se citar o caso da Federação Russa, que afirma que o uso de guerra de informação contra suas forças armadas será considerada uma fase militar do conflito, havendo perdas humanas ou não. Segundo essa definição, por exemplo, o "ciberataque" da Operação Orchard poderia facilmente ser considerado uso da força ou ataque armado.

É evidente, apesar de tudo, que o "ciberataque" israelense constitui, em tese, uma ameaça à paz, previamente à sua caracterização como uso da força ou ataque armado. Para tal conclusão, consideram-se critérios como tempo, lugar, alvo, ator e consequência. Primeiramente, o contexto conturbado das relações sírio-israelenses é um fator de relevo, ao avaliar fatos que podem levar à escalada de conflitos. As relações pouco amistosas entre os dois Estados tornam-se ainda mais graves, quando se demonstra a situação de extrema vulnerabilidade que atingiu a Síria em decorrência da incapacitação de seu sistema de defesa aéreo. A ameaça à paz restaria caracterizada pelo fato de que, além do ganho militar, não haveria sentido em promover a referida incapacitação, se esta não fosse seguida de um ataque convencional, evidentemente pelo ar. O desenvolvimento de cada um dos critérios apresentados deixa ainda mais clara a referida ameaça, o que ensejaria a apreciação pelo Conselho de Segurança.

Diante das circunstâncias, os defensores da autodefesa preemptiva poderiam, inclusive, utilizar-se dessa teoria, para justificar a ação militar israelense. Considerando o contexto das relações tensas e conflitantes entre os vizinhos Síria e Israel, as armas nucleares desenvolvidas no Complexo Kibar certamente seriam utilizadas contra o Estado israelense, o que o levaria a argumentar que o risco da inação era demasiadamente elevado diante de tal ameaça. Apesar disso, a doutrina da autodefesa preemptiva é amplamente condenada, tendo em vista que as exceções legítimas para o uso da força são apenas a autorização pelo Conselho de Segurança das Nações Unidas e a autodefesa, em caso de ataque armado.

Os argumentos em prol da ilegalidade do "ciberataque" israelense e a consequente relação com os artigos 2(4) e 51, da Carta de São Francisco, também não são poucos. Pode-se apontar, por exemplo, o ganho militar direto e imediato, por parte dos israelenses.

Considerando, também o critério da escala e efeitos, é fácil encontrar argumentos que sustentam essa posição. Podem ser apontados, por exemplo, as consequências debilitantes graves para a segurança nacional e o impacto em infraestruturas militares essenciais para a manutenção da segurança, principalmente quando atentamos para o contexto turbulento e conflitante das relações entre Síria e Israel.

A carência regulatória da Internet, embora não seja suficiente, para esvaziar o debate jurídico, tira-lhe elementos de certeza na qualificação do "ciberataque" como ato de guerra. Sem critérios e categorias jurídicas explícitas, resta ao ciberespaço a arbitrariedade e a imprevisibilidade das escolhas políticas. Apesar dos inúmeros precedentes relatados, não se pode

observar ainda uma "ciberguerra" em que se articule uma reação bélica a um "ciberataque" – ou seja, em que se verifiquem, explicitamente, um ataque ou uma ameaça à paz e à segurança internacionais, de um lado, e o consequente uso da força de forma legítima, de outro. Por ora, o problema da atribuição prejudica a identificação de autores e uma responsabilização dos responsáveis por instâncias internacionais como o Conselho de Segurança. Além de inexistir uma regulação prévia, também não se encontra nenhum precedente de "ciberataque" com condenação específica de órgãos internacionais – e essa dupla ausência, no plano do dever-ser e da realidade, impede, no atual estágio, uma classificação definitiva do "ciberataque" como ato de guerra.

Referências

ACADEMIA Brasileira de Letras. **Vocabulário ortográfico da língua portuguesa**. São Paulo: Global, 2009.

ANTOLIN-JENKINS, Vida M. Defining the Parameters of Cyberwar Operations: looking for law in all the wrong places? **Naval Law Review**, v. 51, p. 132-174, 2005.

AREND, Anthony Clark. **International Law and the Preemptive Use of Military Force**. Washington: The Center for Strategic and International Studies and the Massachusetts Institute of Technology, 2003.

BOADLE, Anthony. Brazil's anti-spy Internet bill clears lower house vote. **Reuters**, 25 mar. 2014. Disponível em: <http://www.reuters.com/article/2014/03/26/us-brazil-internet-idUSBREA2P08I20140326>. Acesso em: 18 mai. 2014.

BOTHE, Michael. **Terrorism and the Legality of Pre-emptive force**. Frankfurt: EJIL, 2003.

BRASIL. Decreto Nº 19.841, de 22 de Outubro de 1945. Promulga a Carta das Nações Unidas, da qual faz parte integrante o anexo Estatuto da Corte Internacional de Justiça, assinada em São Francisco, a 26 de junho de 1945, por ocasião da Conferência de Organização Internacional das Nações Unidas. **Coleção de Leis do Brasil de 1945**, Poder Executivo, Brasília, DF, 22 out. 1945.

CORTE Internacional de Justiça. **Case concerning the military and paramilitary activities in and against Nicaragua** (Nicaragua v. United States of America). A Haia, 27 jun. 1986. Disponível em: <http://www.icj-cij.org/docket/index.php?sum=367&p1=3&p2=3&case=70&p3=5>. Acesso em: 21 jul. 2014.

_____. **Legality of the threat or use of nuclear weapons**. A Haia, 08 jul. 1996. Disponível em: <http://www.icj-cij.org/docket/files/95/7497.pdf> Acesso em: 21 jul. 2014.

DICKINSON, Elizabeth. How Qatar Lost the Middle East. **Foreign Policy**, 05 mar. 2014. Disponível em:

<http://www.foreignpolicy.com/articles/2014/03/05/how_qatar_lost_the_middle_east>. Acesso em: 17 mai. 2014.

ESTONIA hit by 'Moscow cyber war'. **BBC News**, 17 mai. 2007. Disponível em: <http://news.bbc.co.uk/2/hi/europe/6665145.stm>. Acesso em: 21 jul. 2014.

GILES, Martin. Defending the final frontier. Special report on cyber-security. **The Economist**, Londres, 12 jul. 2014, p. 3-12.

GOLDSMITH, Jack. What is the domestic legal basis for planned cyberattacks in Syria? *In*: **Lawfare**, 25 fev. 2014. Disponível em: <http://www.lawfareblog.com/2014/02/what-is-the-domestic-legal-basis-for-planned-cyberattacks-in-syria/>. Acesso em: 14 mai. 2014.

GOOGLE. **Internet via balão para todos**. Disponível em: <http://www.google.com/loon/>. Acesso em: 29 jul. 2014.

GRAHAM, Bradley. Hackers attack via Chinese Website. **The Washington Post**, 25 ago. 2005. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html>. Acesso em: 21 jul. 2014.

HATHAWAY, Oona *et al*. **The law of Cyber Attack.** California Law Review, 2012.

HILL, Symon. **Digital revolutions**: activism in the internet age. Oxford: New Internationalist Publications, 2013.

KUMAR, Manish; HANUMANTHAPPA, M.; KUMAR, T. V. Cyber Weapons: invisible weapons for next generation warfare. **CSI Communications**, dez. 2013. Disponível em: <http://www.csi-india.org/c/document_library/get_file?uuid=97cc3d99-d9e6-4ea2-9cce-4f43d0a207f4&groupId=10157>. Acesso em: 21 jul. 2014.

MARKOFF, John. Before the Gunfire, Cyberattacks. **The New York Times**, 12 ago. 2008. Disponível em: <http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0>. Acesso em: 21 jul. 2014

MAURER, Tim. **Cyber Norm Emergence at the United Nations**: an analysis of the UN activities regarding cyber-security. Cambridge: Belfer Center for Science and International Affairs, 2011.

MELZER, Nils. **Cyberwarfare and International Law**. Genebra: United Nations Institute for Disarmament Research, 2011.

NEUNECK, Götz. **Transparency and confidence-building measures**: applicability to the cyber sphere? Genebra: United Nations Institute for Disarmament Research, 2013.

NYE JR., Joseph. **Cyber Power**. Cambridge: Belfer Center for Science and International Affairs, 2010.

PARAGUASSU, Lisandra. Hackers atacam sistema de e-mails do Itamaraty. **EXAME.com**. São Paulo, 27 mai. 2014. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/hackers-atacam-sistema-de-e-mails-do-itamaraty/>. Acesso em: 30 jun. 2014.

PETERKE, Sven (Coord.). **Manual Prático de Direitos Humanos Internacionais**. Brasília: Escola Superior do Ministério Público da União, 2010.

RID, Thomas; MCBURNEY, Peter. Cyber Weapons. **Rusi Journal February**, v. 157, n.1, p. 6-13, mar. 2012.

ROSCINI, Marco. World Wide Warfare: jus ad bellum and the use of cyber force. **Max Planc Yearbook of United Nations Law**, v. 14, p. 85-130, 2010.

ROSEN, Guy. **Introducing the Internet.org App**. Disponível em: <http://newsroom.fb.com/news/2014/07/introducing-the-internet-org-app/>. Acesso em: 31 jul. 2014.

SCHMITT, Michael. Computer Network Attack and the use of force in International Law**:** thoughts on a normative framework. **The Columbia Jounal of Transnational Law**, v.37, p. 885-937, 1999.

_____ (Ed.). **Tallinn Manual On The International Law Applicable To Cyber Warfare**. Cambridge: Cambridge University Press, 2013.

SINGER, P. W.; FRIEDMAN, Alan. **Cybersecurity and cyberwar**: what everyone needs to know. New York: Oxford University Press, 2014.

SMITH, Graham. Google threatens China to pullout after attacks on Gmail accounts of human rights activists. **Daily Mail**, 13 jan. 2010. Disponível em: <http://www.dailymail.co.uk/sciencetech/article-1242775/Google-threatens-China-pullout-attacks-Gmail-accounts-human-rights-activists.html>. Acesso em: 21 jul. 2014

SOLCE, N. The battlefield of cyberspace: the inevitable new military branch - The cyber force. **Albany Law Journal of Science and Technology**, v. 18, p. 315-327, 2008.

SOLOMON, Howard. U.S. to drop Internet control. **IT World Canada**, 17 mar. 2014. Disponível em: <http://www.itworldcanada.com/article/u-s-to-drop-internet-control/90392>. Acesso em: 17 mai. 2014.

SPECHT, Stephen; LEE, Ruby. **Distributed Denial of Service**: taxonomies of attacks, tools and countermeasures. Princeton: Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, 2004.

SWAINE, Jon. Georgia: Russia 'conducting cyber war'. **The Telegraph,** 11 ago. 2008. Disponível em: <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html>. Acesso em: 21 jul. 2014

THORNBURGH, Nathan. Inside the Chinese Hack Attack. **Time,** 25 ago. 2005. Disponível em: <http://content.time.com/time/nation/article/0,8599,1098371,00.html>. Acesso em: 21 jul. 2014

TIKK, Enneken. Ten rules for Cyber Security. **Survival,** v. 53, n. 3, p. 119-132, jun-jul. 2011.

UNIDIR. **The Cyber Index**: International Security Trends and Realities. Geneva: United Nations Publications, 2013.

US justice department charges Chinese with hacking. **BBC News**, 19 mai. 2014. Disponível em: <http://www.bbc.com/news/world-us-canada-27475324>. Acesso em: 21 jul. 2014.

US spying row: Germany investigates new case. **BBC News**, 09 jul. 2014. Disponível em: <http://www.bbc.com/news/world-europe-28228647>. Acesso em: 21 jul. 2014.

VIGNARD, Kerstin (Ed.). **Confronting cyberconflict**. Geneva: United Nations Institute for Disarmament Research, 2011.