CIBERATAQUES: UMA REFLEXÃO SOBRE A RESPONSABILIDADE INTERNACIONAL DOS ESTADOS

CYBER ATTACKS: A REFLECTION ON THE INTERNATIONAL RESPONSIBILITY OF STATES

Gabriela Eulalio de Lima[1]
UNESC/RO

Resumo
O trabalho impulsionado pelo último ataque cibernético que atingiu mais de 100 países ao redor do mundo, dentre eles o Brasil, ponderou os impactos desses ataques para toda a sociedade pós-moderna, identificando relevantes embaraços jurídicos: um sistema legal nacional insuficiente para lutar contra tais ataques e a necessidade de discuti-los sob a lente da responsabilidade no campo internacional dos Estados-Nações, numa linha que vai além dos termos destacados pelo ARSIWA, demonstrando-os ser lacônicos e contrariamente, investidos de insegurança social. Para tanto, tomou por base a noção apresentada por Celso Renato Duvivier de Albuquerque Mello, que defende a obrigação da responsabilidade internacional abranger a necessidade do equilíbrio social, da retribuição e da justiça. O trabalho valeu dos métodos dedutivo e dialético, baseando-se na pesquisa bibliográfica e documental.
Palavras-chave
Ciberataques. Responsabilidade internacional. Segurança universal.

Abstract
The work driven by the latest cyber-attack that hit more than 100 countries around the world, including Brazil, pondered the impacts of these attacks for the whole post-modern society, identifying the relevant problems attendant legal: a national legal system is insufficient to fight against such attacks and the necessity of discussing them under the lens of the responsibility in the international field of member Nations, in a line that will in addition to the terms highlighted by the ARSIWA, demonstrating them to be vague and on the contrary, invested of social insecuri-

[1] Mestre em Direito com a linha de pesquisa Empreendimentos Econômicos, Processualidade e Relações Jurídicas pela Universidade de Marília - UNIMAR (2016). Especialista em Direito Material e Processual do Trabalho pelo Centro Universitário de Rio Preto - UNIRP (2015). Graduada em Direito pela Universidade do Estado de Minas Gerais - UEMG, campus de Frutal/MG (2010). Docente superior da Graduação em Direito das Faculdades Integradas de Cacoal - UNESC.

ty. To do so, was based on the notion presented by Celso Renato Duvivier de Albuquerque Mello, who argues for the obligation of the international responsibility to cover the need of social balance, of retribution and of justice. The work was of the methods deductive and dialectical, based on a bibliographic research and documentary.
Keysword
Cyber attacks. International Responsibility. Universal Security.

INTRODUÇÃO

A Era globalizada tem avançado a passos largos em escala mundial e com ela, a preocupação quanto à vulnerabilidade dos usuários do ciberespaço, despontando daí a necessidade da construção de uma regulamentação jurídica internacional, cujo intuito destina-se vincular uma responsabilização universal aos Estados-Nações.

No dia 12 de maio de 2017 o mundo foi surpreendido por um ataque cibernético, que atingiu cerca de 100 países, provocando neles interrupções no sistema de computadores. No Estado Brasileiro, segundo nota divulgada pelo Gabinete de Segurança Institucional – GSI da Presidência da República, o ataque sobreveio em grande quantidade, por meio de *e-mails* com arquivos infectados, que ao serem acessados pelos usuários da rede, atingiram o *hardware* e o *malware* bloqueou todo e qualquer tipo de acesso aos arquivos dentro da máquina destes; ouve o sequestro de dados com o bloqueio no acesso e para a liberação por parte dos *hackers*, foi exigido um resgate de quantia a ser paga em *Bitcoins* – cédulas virtuais (RODRIGUES, 2017); os pedidos de resgate pelos dados giraram em torno do pagamento de U$$ 300,00, a ser transferido via esta moeda virtual (GALILEU, 2017).

Ante a onda de ataques e o temor mundial por novas ações cibernéticas de amplo e grave efeito, a Microsoft informou que estava conferindo modernizações automáticas no *Windows* para proteger seus clientes do *WannaCry*, sendo disponibilizado pela Companhia uma atualização na data de 14 de março, dois dias após

o ataque, destinada a acautelar os usuários contra o *Eternal Blue*[2]. (*WINDOWS*, 2017)

Não obstante o último sobressalto mundial, não é contrassenso compreender o espaço cibernético como o ambiente propício para o desenrolar de uma gama de litígios beligerantes entre as nações, isso considerando que a arquitetura estrutural da internet condiciona operar tanto para questões benévolas quanto para o seu antônimo – operando de modo a facilitar o desaparecimento e/ou o sequestro de informações e dados pessoais, governamentais, corporativos etc.; disfarçando ou até mesmo implantando vestígios falsos para que as ações maliciosas dos *hackers* não sejam desvendadas; despontando a justificativa tão atual para o presente debate, cujo objetivo central será melhor compreender os riscos suscitados pela rede mundial de computadores à sociedade pós-moderna como um todo e a necessidade de se discutir a problemática, chamando para os Estados soberanos uma responsabilidade internacional diante de eventuais danos causados por ataques cibernéticos.

Os usuários da rede compõem também os desconhecidos agentes virtuais ardilosos, que colocam a mercê toda a sociedade; o simples acesso ao campo cibernético promove riscos diversos a massa mundial e conjuntamente, destaca a dificuldade acentuada na produção de evidências da origem, dimensão e alcance dessas ações danosas neste espaço virtual, restando um temor social crescente acerca da identidade e punição dos *hackers* que por se misturarem à todos usuários, acabam recebendo tratamento geral, fruto da relativização/flexibilização e da não responsabilização internacional dos Estados nas atuais formas de coibir, monitorar e punir a ocorrência de ataques cibernéticos.

Neste passo, o trabalho se desenvolverá na busca de analisar a configuração de ataques cibernéticos, realçando os

[2] Ferramenta que permite que o *malware*, que criptografa dados em computadores, se espalhe através de protocolos de compartilhamento de arquivos configurados entre organizações, de acordo com a fonte de notícias.

termos do Alerta n.º 02/2017 emitido pelo Centro de Tratamento de Incidentes de Redes do Governo brasileiro, que apresentou nota sobre os ataques de *Ransomware* WINCRY em maio de 2017 (BRASIL, 2017), buscando evidenciar se além dos créditos de informatização, o Estado brasileiro detém normatização interna que tende a proteger o seu povo de ações perpetuadas por *hackers*; exporá sobre a abrangência do conceito de responsabilidade internacional e a falha na norma internacional acerca da necessidade de ser configurado nexo mandatório entre os atos dos particulares e o Estado para a sua constatação, todo empenho em prol de clarificar a defesa deste artigo pela consideração da responsabilidade internacional estatal frente aos ataques cibernéticos.

Contará o trabalho com o método dedutivo e dialético, abalizado na pesquisa bibliográfica e documental, organizando as vias que carecem ser percorridas para se realizar uma pesquisa fundamentada em prol da responsabilidade internacional dos Estados soberanos, aclarando o senso comum sobre o debate.

1 ALCANCE DOS ATAQUES CIBERNÉTICOS

Assim como denota dificuldade em averiguar a extensão das consequências dos danos causados por um ataque cibernético, também verifica-se embaraço quanto a definição conceitual deste tipo de ofensa.

Num primeiro plano, esbarra-se com a necessidade de se determinar a natureza e o escopo do problema a ser enfrentado, sem perder de vista que as ações praticadas no ciberespaço provocam muitas das categorias e princípios tradicionais que regem os conflitos armados sob o direito da guerra, daí despontando a urgência de uma definição precisa de ataque cibernético.

Partindo desse pressuposto, tem-se o prelúdio para uma análise de que um ciberataque deve ser conduzido pelo direito da guerra e outros corpos de leis existentes. Mas antes se ingresse no campo da responsabilização e do arcabouço legal, é necessário enfrentar este desafio da acepção, isso levando em consideração

que diante a imprecisão em identificar incidentes dos ciberataques e a ausência de uma definição compartilhada, torna ainda mais difícil exigir dos analistas de países diferentes desenvolvam recomendações de políticas coordenadas e dos governantes, para que se envolvam em ações coordenadas, a fim de acautelar os usuários dos resultados danosos.

Considerando essa missão da definição dos ciberataques o primeiro passo importante para enfrentar a crescente ameaça representada por ataques cibernéticos, referencia-se Matthew C. Waxman, que revela tratar-se de esforços destinados a alterar, interromper ou destruir sistemas ou redes de computadores – informações ou programas sobre eles – ações abrangentes que variam de alvo (militar *versus* civil, público *versus* privado), consequências (menor *versus* maior, direto *versus* indireto) e duração (temporária *versus* de longo prazo), tornando a interpretação e/ou a regulação legal internacional sobre esse tema tão abstrusa (WAXMAN, 2011). Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue e Julia Spiegel, de outro lado, ressaltam que ataque e crime cibernético possuem definições distintas, que podem ser identificadas no propósito político e/ou de segurança nacional (HATHAWAY, *et al*, 2012).

Tudo circunda a interconexão global trazida através pela rede mundial de computadores, que de um lado traz incomensuráveis benefícios a toda sociedade pós-moderna, mas também apresenta em seu bojo um conjunto novo de armas ofensivas disponíveis para os Estados e atores não-estatais, incluindo os grupos terroristas; portanto, arrisca-se a lidar tanto com a possibilidade das redes de defesa militar serem remotamente desativadas ou danificadas, como com a questão das redes do setor privado serem infiltradas, interrompidas, destruídas ou sequestradas como no ataque de maio de 2017.

Contudo, os ataques cibernéticos não traduzem de uma preocupação recente. Em 2007, o método de ataque "negação de

serviço"[3] foi vivenciado pela Estônia durante um período de tensões diplomáticas com a Rússia, opositores políticos; *hackers* russos lançaram ações que interromperam funções governamentais e comerciais durante semanas no país da Estônia, inundando seus *sites*, servidores e roteadores com solicitações de dados para sobrecarregar sua capacidade de funcionar. (BIDDER, 2007)

Entre 2010 e 2011, um vírus chamado Stuxnet[4], criado pelos Estados Unidos da América – a época também teve Israel acusado de ser o seu idealizador, foi utilizado para infectar os sistemas de operação de uma usina de enriquecimento de urânio localizada em Natanz, no Irã, prejudicando significativamente o programa iraniano ao interromper parte do seu sistema de produção (DA REDAÇÃO VEJA, 2012). Essa ação cibernética foi lida em cenário internacional como uma ação que salvou o Mundo, mas que por outro lado, acabou por dar início à 3ª Guerra Mundial (SANTOS; VERSIGNASSI, 2016).

Em 2012, o Instituto Internacional de Estudos Estratégicos de Londres, destacou o crescente consenso dos conflitos entre Nações se concretizarem com o uso da ciberguerra[5], desativando infra-estrutura dos países, interferindo na integridade dos dados militares internos, transações econômicas ou para realizar qualquer outra ação que tenha por finalidade fragilizar o Estado atacado. (FERNANDES, 2012)

Em 2010, um grupo de especialistas governamentais em avanços na informática e nas telecomunicações no contexto da segurança internacional, convocado pela Organização das Nações Unidas – ONU chegaram à conclusão que as ameaças existentes e potenciais na esfera da segurança da informação estão entre os

[3] Um ataque de negação de serviço, ou DoS (*Denial of Service*), revela-se na tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores.

[4] Stuxnet é um vírus de computador criado especificamente para atacar o sistema operacional SCADA, desenvolvido pela *Siemens* e usado para controlar as centrífugas de enriquecimento de urânio iranianas.

[5] Ações de um Estado-Nação para penetrar em computadores ou redes de outra Nação, objetivando causar danos ou interrupções.

desafios mais sérios do Século XXI; seus efeitos trazem um risco significativo para a segurança pública das Nações e a estabilidade da comunidade internacional globalmente interligada como um todo. (GENERAL ASSEMBLY, 2010)

O fato é que ciberguerra, guerra cibernética, são conceitos que não distinguem dos cibercrime e ciberataque, vez que todos eles estão abertos a uma aplicação perigosamente ampla do quadro de guerra no contexto cibernético, cujos ataques podem ser perpetrados tanto pelos Estados-Nações quanto pelos atores não-estatais.

Em arremate, a interconectividade eletrônica e informacional cria enormes vulnerabilidades, geradas pela dificuldade de assimilar a natureza e o desígnio dos ataques, o que remonta um enorme desafio em avaliar como o direito nacional e o internacional devem operar para lidar com os problemas gerados por estes ataques cibernéticos.

2 O ESTADO BRASILEIRO E A SUA ESCASSA PREVISÃO LEGAL CONTRA ATAQUES CIBERNÉTICOS GLOBAIS

Datado de 12 de maio de 2017, o último ataque cibernético que atingiu cerca de 100 países pelo mundo, provocando interrupções no sistema de computadores destes, ativou um alerta internacional sobre a potência do alcance dessas ações desvirtuadas no ciberespaço. No Brasil, foi publicado o Alerta n.º 02/2017 – Ataques de *Ransomware* WINCRY, trazendo na descrição do problema que: "O atacante explora vulnerabilidades dos sistemas *Windows*, alertado no Boletim MS17-010 da Microsoft, bloqueando acesso aos arquivos e cobrando o 'resgate' em *bitcoins*." (BRASIL, 2017)

O *Ransomware*, traduzido da língua inglesa, seria a compreensão do "sequestro digital"; cuida de um código destinado a infectar máquinas que estejam conectadas a rede mundial de computadores, sequestrando ou limitando o acesso aos dados e/ou

informações dos usuários da rede, ordinariamente utilizando-se de algoritimos de encriptação (*crypto-ransoware*), para fins de extorsão; (TEIXEIRA, 2013, p. 68) utilizado no ataque de maio de 2017, foi abordado pelo Governo brasileiro como: "A mais severa das vulnerabilidades, conforme Bolentim MS17-010 da Microsoft, permite ao atacante a execução remota de código através de envio mensagens especialmente criadas em um 1.0 servidor Microsoft Server Message Block (SMBv1)." (BRASIL, 2017)

Este tipo de ataque malicioso torna a recuperação dos arquivos infectados quase impossível, considerando o sistema de criptografia que é utilizado – demasiadamente moderno e resistente, passível de ser destrancado apenas com a chave de encriptação, liberada pelos *Hackers* como pagamento do resgaste em *Bitcoins* – moeda digital. (DIEGO, 2016)

O Departamento de Segurança da Informação e Comunicações brasileiro, passado o ocorrido, orientou os usuários da rede em território nacional que a medida mais eficaz para evitar a perda de dados seria a política de *Backup* dos arquivos (BRASIL, 2017), contudo, o alerta foi publicado após o ataque, ou seja, depois do ataque ter tomado as suas proporções não só em solo pátrio, mas em todo globo. Não despreza-se a relevância do alerta publicado pelo Governo brasileiro, contudo, a medida adotada, pode até ser percebida como uma nota que evitou danos de maior extensão, mas não denotou a segurança adequada para as evidências apontadas.

E assim como acontece com a tomada de medidas retardadas, no âmbito da legislação nacional também é perceptível uma fragilidade muito intensa na questão de garantias aos usuários brasileiros da rede face à ataques cibernéticos. Ademais como aconteceu no ataque de maio de 2017, nem sempre um ciberataque deriva de um Estado-Nação, atingindo apenas os seus limites, ao contrário, Omar Kaminski, advogado especialista em Tecnologia da Informação realça que: "Embora a internet não tenha fronteiras, temos os limites de jurisdição e competência, então fica muito difícil responsabilizar um agente danoso que esteja situado no exterior" (KAMINSKI, 2009).

Não obstante este entrave do limite jurisdição e competência, para as ocorrências concretizadas em território pátrio, a legislação nacional não pode ser considerada ajustada para punir ciberataques, basicamente o vasto rol legislativo brasileiro contém apenas o artigo 266 do Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, tendo os §§ 1º e 2º sido incluídos pela Lei Federal n.º 12.737, de 30 de novembro de 2012 (BRASIL, 1940), denominada popularmente de Lei Carolina Dieckmann, apresentando uma pena abaixo da desejável; e para as ações terroristas perpetradas por "outros meios capazes de causar danos ou promover destruição em massa", punida pela Lei Federal n.º 13.260, de 16 de março de 2016 (BRASIL, 2016), que apresenta um rol de penas mais severas, mas que ainda assim é insuficiente.

Nota-se que o Brasil não detém força normativa adequada, ou seja, pode ser considerado minimamente capacitado para garantir ao seu povo um estado ideal de segurança; somado à essa questão, tem a barreira da interconectividade eletrônica e informacional desenvolvidos entre todos Estados-Nações, a rede mundial de computadores parece tratar-se de "terra de ninguém", criando enormes vulnerabilidades que transcendem o território nacional.

Ademais, no tocante ao binômio capacidade e vulnerabilidade, constata-se a existência das mais diversas desigualdades: os Estados-Nações não têm paridade no poder econômico e político para empenharem uma batalha, ao contrário, têm forças variáveis para resistir às pressões impostas; regra esta que se aplica às capacidades estatais isoladas sobre os ataques cibernéticos e de defesa contra destes, que se consolida na insuficiência e/ou na fragilidade das regras legais nacionais direcionadas aos ciberataques, dando por consequência, estratégicas díspares; o que ratifica a importância de se discutir a temática do sistema da rede mundial de computadores levantando questões jurídicas em prol de políticas públicas universais, a partir da chamada de uma responsabilidade internacional.

3 DA EXTENSÃO DA RESPONSABILIDADE INTERNACIONAL

Antes de enfrentar o ponto característico do alcance do conceito da responsabilidade civil internacional do Estado, necessário introduzir o ramo do direito o qual está inserida – o Direito Internacional; ramo autônomo da ciência jurídica, disponível para regular a coletividade composta por nacionais, constituída em territórios e governada por Estados soberanos – politicamente organizados; além de cooperar com organismos e organizações, para que conjuntamente com os Estados-Nações, possam interatuar ponderada e harmonicamente, a fim de minimizar contendas e atenuar atritos, conduzindo a sociedade como um todo da forma menos insegura possível e na direção do equilíbrio.

Pois bem, passada esta ligeira análise intróita, extrai-se um conceito inicial, que o Direito Internacional delibera "direitos das gentes", responsável por reger a sociedade num contorno universal, distinto do direito interno por trabalhar na preservação de interesses sociais comuns. Destarte, nas relações internacionais, tal como ocorre com as outras relações, o sujeito de Direito tendo invadida a sua esfera jurídica por outrem, suscitará um encargo que compreende múltiplas formas deliberadas por um sistema jurídico reservado e em geral, a responsabilidade internacional é sopesada a propósito dos Estados serem consagrados sujeitos comuns de Direito. (BROWNLIE, 1997, p. 457)

Valério de Oliveira Mazzuoli revela que a responsabilidade pode ser compreendida: "[...] o instituto que visa responsabilizar determinado Estado pela prática de um ato atentatório ao Direito Internacional (ilícito) perpetrado contra outro Estado, prevendo certa reparação a esta último pelos prejuízos e gravames que injustamente sofreu." (MAZZUOLI, 2013, p. 184)

Destinada precipuamente para garantir a deferência à igualdade soberana dos Estados-Nações, a responsabilidade internacional é evocada quando há violação de direitos destes e da

comunidade internacional. Tal tema teve seu acabamento normativo projetado no *Draft articles on Responsibility of States for Internationally Wrongful Acts* – ARSIWA, traduzido para o idioma pátrio em Projeto da Comissão de Direito Internacional das Nações Unidas, que no artigo 2º traz a concepção de responsabilidade internacional dos Estados, relevando que um ato estatal é considerado internacionalmente ilícito quando a conduta consistir em uma ação ou omissão e é atribuível ao Estado consoante o Direito Internacional e constituir uma violação de uma obrigação internacional do Estado. (*INTERNATIONAL COURT OF JUSTICE*, 2001)

Ainda sob a interpretação concedida pela ARSIWA, o artigo 4º revela que a atribuição da conduta a um Estado deve considerar, segundo o Direito Internacional, o comportamento de qualquer órgão do Estado que exerça função legislativa, executiva, judicial ou outra qualquer que seja sua posição na organização do Estado, independendo se se trata de órgão do governo central ou de unidade territorial do Estado, além de incluir qualquer pessoa ou entidade que tenha tal *status* de acordo com o direito interno do Estado. Prevendo ainda, artigo 8º, a responsabilidade internacional para os atos praticados por agentes não estatais, desde que estes estejam agindo sob a instrução ou a direção ou o controle de determinado Estado ao executar a conduta.

O fato é que o Projeto da Comissão de Direito Internacional das Nações Unidas – ARSIWA – revela que certa reserva a constatação da responsabilidade do Estado, estando restrita a conjetura da necessidade imperiosa de ter-se revelado um vínculo real entre a pessoa e/ou o grupo que executa o ato e o adequado aparato estatal.

Contudo, a extensão da responsabilidade estatal no âmbito internacional deve ser analisada também sob a égide dos elementos essenciais da responsabilidade civil ordinária, quais sejam: a) ato ilícito; b) culpa (em *lato sensu*); c) Dano; e d) Nexo causal. A conduta ilícita compreende àquela contrária à norma de caráter

cogente, inclusive a de direito internacional; a culpa em *lato sensu* abrange a culpa e o dolo; o dano é materializado na lesão ao bem abrigado pelo ordenamento jurídico; e o nexo de causalidade é a relação de causa e efeito entre o comportamento do agente e o dano. (ROSENVALD, 2011)

Evidenciados os elementos da responsabilidade civil, no Direito Internacional a busca não é pela responsabilidade subjetiva, vigorando a objetiva, caracterizada na violação de norma internacional independentemente da apuração da conduta do agente. Entretanto, a grande contenda está no que restou sinalizado pelo ARSIWA, da conduta pessoal ou do grupo estar sendo instruída ou dirigida por determinado Estado (artigo 8º).

E é precisamente nesta dinâmica de identificar o vínculo Estados-Nações e a conduta pessoal ou de grupo de pessoas, que se percebe a grande dificuldade da norma internacional para a atribuição de responsabilidade universal no ciberespaço para os ataques cibernéticos.

4 A DIFICULDADE IMPRESSA NA ARSIWA PARA A CONFIGURAÇÃO DA RESPONSABILIDADE ESTATAL FRENTE AOS CIBERATAQUES

Identificar e assinalar ações de órgãos estatais ou semelhantes, de particulares e de particulares sob a direção ou controle estatal é, sobremaneira, tarefa penosa no cenário cibernético. Igualmente, o reconhecimento do Estado de origem dos ataques pode ser encoberto, como ocorreu com o ciberataque perpetrado contra a Estônia no ano de 2007. (OLIVEIRA FILHO, 2016, p. 151)

Ataques no ambiente virtual são imprevisíveis e ao mesmo tempo podem ser considerados comuns pela facilidade com que são desenvolvidos e disparados pela rede; podendo vir de todos os lugares do mundo, bastando que haja um usuário ou um grupo deles, com habilidades técnicas aprimoradas sobre a tecnologia informática e haja uma motivação para perpetrar determinado ato

no ciberespaço, deixando à deriva a comunidade internacional, fazendo vítimas e reféns dos ataques.

Neste ínterim, desponta a grande problemática, o comportamento estatal frente a estes ciberataques. Como destacado, o Projeto da Comissão de Direito Internacional das Nações Unidas, traz condições demasiadamente fechadas e favoráveis ao Estado, consagrando-o responsável apenas para as condutas que estiverem sob a sua instrução, direção ou controle.

Amparados pela normatização internacional, percebe-se um Estado acomodado ou comedido demais na revelação de políticas públicas preventivas, de um plano de contingência sobre a tomada de iniciativa privada e pública para tratar dessas situações e assegurar a comunidade social planetária contra ataques cibernéticos.

Não obstante, o atual comportamento estatal pode derivar outras responsabilidades, remetidas a terceiros, propensas vítimas também de ataques na rede; é o que demonstra Thiago Luís Sombra citado por Fernando Martines, a partir de um exemplo: "Invadido um escritório brasileiro e dados dos clientes sendo vazados, poderá o escritório ser responsabilizado por *culpa in vigilando* e *culpa in custodiendo*, provado o dano, a culpa e o nexo causal, se não foram adotados cuidados mínimos de segurança." (SOMBRA, *apud* MARTINES, 2017)

Partindo dessa conjetura, compreende-se que é inerente a toda e qualquer teoria da responsabilidade, responsabilizar a pessoa indicada de ter praticado um ilícito, de arcar com os danos dele derivado, isso levando em consideração o direito a reparação correspondente do ofendido. E tal circunstância também deve ser estendida para os ilícitos perpetrados contra a comunidade planetária, uma vez que essa ideia de responsabilidade é indivisível e deve ser ponderada universalmente, pois está no alicerce de toda sociedade.

Veja-se, portanto, que os termos apresentados pelo ARSIWA são lacônicos a teoria da responsabilidade, pois

consideram ato do Estado apenas as condutas individuais ou coletivas, que estejam sendo instruídas, dirigidas ou controladas pelo Ente estatal; com isso, acabam por mitigar a atribuição de responsabilidade internacional pelos ataques cibernéticos cometidos em detrimento da sociedade planetária, represando o direito dos usuários da rede a terem garantida a segurança necessária para o seu amplo e não vitimado acesso. E é justamente a reverência dessa ideologia da responsabilidade penetrar a sociedade a fim de "representar uma segurança necessária", que se pondera o raciocínio de Celso Renato Duvivier de Albuquerque Mello: "[...] esta noção corresponde a uma necessidade de equilíbrio social, de retribuição, de justiça, sendo esta a razão de o seu fundamento ser ético" (MELLO, 2004, p. 526).

A leitura da responsabilidade internacional de Celso Renato Duvivier de Alburquerque Mello representa a sensatez necessária para demonstrar a íntima relação desta com o conceito da responsabilidade jurídica em sentido *lato sensu*, ou seja, ponderando o Estado responsável pelo ilícito internacional – no caso em discussão, pelos ataques cibernéticos – mesmo que não tenha sido o Ente estatal o agente imediato da antijuridicidade, pelo que, gerará a responsabilidade, a obrigação de reparar os danos originados dos atos cometidos por seus órgãos internos, agentes políticos e igualmente pelos particulares – devendo-se restar evidenciado, neste último, imprescindivelmente, dentre outros requisitos, a nacionalidade vinculada e a omissão do Estado. (MELLO, 2004, p. 523)

Por conseguinte, a responsabilidade internacional estatal abrange tanto os entes políticos quanto os seus representados, incumbindo-lhe o dever de reparar ao Estado que tenha causado danos, uma reparação adequada, excetuando-se as hipóteses de excludentes de ilicitude: consentimento, legítima defesa, contramedidas em relação a um ato internacionalmente ilícito, força maior, perigo extremo, estado de necessidade, cumprimento de normas imperativas, consequências de invocação de uma circunstância extinguindo a ilicitude. (INTERNATIONAL COURT OF JUSTICE, 2001)

A defesa ponderada no artigo não é uma crítica ou um desdém da disposição expressa no artigo 8º do ARSIWA para a constatação da responsabilidade internacional, contudo, não pode ser indicada como condição fechada, devendo-se considerar igualmente atos ilícitos perpetrados por agentes, através de seus órgãos, que tenham ferido preceitos de Direito Internacional, positivados ou consuetudinários, e que venham a atingir Estado ou organização internacional, sem que tenham motivado ações que amparasse as agressões com as excludentes de ilicitude.

No enfoque do estudo sobre os ataques cibernéticos e a defesa pelo reconhecimento da responsabilização internacional dos Estados em relação àqueles, deve-se, portanto, considerar uma interpretação mais ampla do Direito Internacional, para além do disposto no Projeto da comissão de direito internacional das Nações Unidas sobre responsabilidade internacional dos estados, isso considerando as novas tecnologias e as ameaças no espaço cibernético, e as capacidades e as vulnerabilidades dos Estados-Nações, que como destacado anteriormente, são distintas, ou seja, não existe a nível universal igualdade de defesa e condições de declaração de ciberguerras.

CONCLUSÃO

Ainda em pleno século XXI, imersos na Era globalizada, os ataques cibernéticos se apresentam como problemas abstrusos de traçar linhas e isso não apenas em cenário nacional, que como averiguou-se, possui escassa e se for analisar globalmente, fragilizada previsão legal contra os ataques cibernéticos.

O desenvolvimento e a implantação de novas tecnologias, tanto no seu potencial ofensivo quanto nas vulnerabilidades que criam para os Estados dependentes dessas tecnologias, levantam questões sobre modos permitidos ou não de conduta interestatal e das regras de responsabilidade internacional. A dificuldade de identificar a origem dos ataques, a dimensão, o alcance dessas ações

no espaço virtual e a identidade do (s) agente (s) acarretam um temor crescente, gerado por uma gama de riscos a toda sociedade pós-moderna, que são desenvolvidos distintamente, dada as discrepâncias das capacidades e das vulnerabilidades dos Estados-Nações para se posicionarem frente à rede mundial de computadores.

A presente problemática levanta a necessidade imperiosa de discutir as questões jurídicas universais, a fim de analisar até que ponto o Direito Internacional vigente é adequado para regulamentar essas capacidades hoje e no futuro.

Destacado no desenvolvimento desse artigo o Projeto da comissão de direito internacional das Nações Unidas sobre responsabilidade internacional dos estados, viu-se que esse apresenta uma responsabilidade intricada ao aspecto subjetivo, afirmando que o ato ilícito passível de ser responsabilizado internacionalmente, tenha que partir diretamente do Estado ou que seja dirigido por ele; contudo, no Direito Internacional, consagrado o "direito das gentes", incumbido de reger a sociedade num contorno universal, a busca não pode ser pela responsabilidade subjetiva, pois esta deixaria a mercê os usuários da rede, devendo vigorar a objetiva, assinalada na transgressão da segurança mundial independentemente da apuração da conduta do agente/sujeito.

E a este respeito, sintetizando esta fase conclusiva do trabalho, ratifica-se o argumento objetivo de que é justamente a reverência ideológica da responsabilidade ter que penetrar a sociedade universal com o desígnio de representar uma segurança mandatória, que se percebe a importância de tratar os Estados-Nações responsáveis internacionalmente pelos ciberataques, concretizando o imperativo do equilíbrio social, da retribuição e da justiça, aperfeiçoando a razão da extensão da responsabilidade internacional num fundamento ético, conforme assinalado por Celso Renato Duvivier de Albuquerque Mello.

REFERÊNCIAS BIBLIOGRÁFICAS

BIDDER, Benjamin. *Hackers* russos atacam oposição política. **Ipdi – Inteligência Digital**. Disponível em: <http://www.ipdi.com.br/hackers-russos-atacam-oposicao-politica/>. Acesso em 23 maio 2017.

BRASIL, Departamento de Segurança da Informação e Comunicações. **Alerta nº 02/2017 - Ataques de *Ransomware* WINCRY.** Disponível em: <https://marcusfabio.files.wordpress.com/2017/05/1_4949721797416189971.pdf>. Acesso em 22 maio 2017.

_____. **Decreto nº 19.841, de 22 de outubro de 1945**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm>. Acesso em 22 maio 2017.

_____. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940:** Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 02 jun. 2017.

_____. **Lei Federal n.º 13.260, de 16 de março de 2016:** regulamenta o disposto no inciso XLIII do art. 5o da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis nos 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm>. Acesso em 02 jun. 2017.

BROWNLIE, Ian. **Princípios de direito internacional público**. Tradução de Maria Manuela Farrajota et al. Lisboa: Fundação Calouste Gulbenkian, 1997.

DA REDAÇÃO. Governo americano criou o vírus *Stuxnet* para atacar o Irã: Segundo o jornal *The New York Times*, o *malware* foi criado pelo Pentágono para retardar o programa nuclear iraniano. **Veja**. 2012. Disponível em: <http://veja.abril.com.br/tecnologia/governo-americano-criou-o-virus-stuxnet-para-atacar-o-ira/>. Acesso em 01 jun. 2017.

DIEGO, Thomas. ***Ransomware* maior praga virtual da atualidade**. 07 nov. 2016. Disponível em: <http://thomasdiego.com/*Ransomware*-maior-praga-virtual-da-atualidade/>. Acesso em 02 jun. 2017.

FERNANDES, José Pedro Teixeira. A ciberguerra como nova dimensão dos conflitos do século XXI. **Relações Internacionais**. 2012. Disponível em: <http://www.scielo.mec.pt/pdf/ri/n33/n33a05.pdf>. Acesso em 01 jun. 2017.

GALILEU, Redação. *Hackers* atacam instituições do mundo todo e pedem "resgate" via *bitcoin*. **Revista Galileu**. Disponível em: <http://revistagalileu.globo.com/Ciencia/noticia/2017/05/hackers-atacam-instituicoes-do-mundo-todo-e-pedem-resgate-bitcoin.html>. Acesso em 22 mai. 2017.

GENERAL ASSEMBLY, United Nations. ***Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security***. Disponível em: <http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201&referer=/english/&Lang=E>. Acesso em 01 jun. 2017.

HATHAWAY, Oona A.; CROOTOF, Rebecca; LEVITZ, Philip; et al. *The law of cyber attack*. ***Faculty Scholarship Series***. Paper 3852. 2012. Disponível em: <http://digitalcommons.law.yale.edu/fss_papers/3852> Acesso em 23 maio 2017.

INTERNATIONAL COURT OF JUSTICE. **Projeto da comissão de direito internacional das Nações Unidas sobre responsabilidade internacional dos estados**. Tradução de Aziz Tuffi Saliba. Disponível em: <http://iusgentium.ufsc.br/wp-content/uploads/2015/09/Projeto-da-CDI-sobre-Responsabilidade-Internacional-dos-Estados.pdf> Acesso em 04 jun. 2017.

KAMINSKI, Omar. **A internet e o ciberespaço**. 21 jun. 2009. Disponível em: <http://www.kaminski.adv.br/diversos/artigo-a-internet-e-o-ciberespaco/>. Acesso em 02 jun. 2017.

MARTINES, Fernando. Lei brasileira dá poucas garantias contra ataques virtuais globais. **Conjur Jurídico**. Disponível em: <http://www.conjur.com.br/2017-mai-13/lei-brasileira-garantias-ataques-virtuais-globais>. Acesso em 05 jun. 2017.

MAZZUOLI, Valério de Oliveira. **Direito internacional público:** parte geral. 4. ed. São Paulo: Editora Revista dos Tribunais, 2013.

MELLO, Celso Renato Duvivier de Albuquerque. **Curso de direito internacional público**. 15. ed. Rio de Janeiro: Renovar, 2004.

OLIVEIRA FILHO, João Glicério de; MARCHEZAN, Bárbara Victoria Müller. O problema da atribuição de responsabilidade internacional nos casos de ataques cibernéticos. **Revista do**

CEPEJ, Salvador, vol. 19, Ed. Especial, pp 148 – 162, jan/jun 2016.

RODRIGUES, Luana. Ataque hacker atingiu 100 países, incluindo Brasil, "em grande quantidade". **Campo Grandes *News***. Disponível em: <https://www.campograndenews.com.br/tecnologia/ataque-hacker-atingiu-100-paises-incluindo-brasil-em-grande-quantidade>. Acesso em 22 mai. 2017.

ROSENVALD, Nelson. **Curso de direto civil:** responsabilidade civil. Disponível em: <www.stf.jus.br/.../anexo/Curso_de_Responsabilidade_Civil__Nelson_Rosenvald.doc>. Acesso em 05 jun. 2017.

SANTOS, Marcos Ricardo dos Santos; VERSIGNASSI, Alexandre. **Vírus entra em programa nuclear e salva o mundo Conheça a misteriosa história do *Stuxnet*:** o programa que salvou o planeta. Ou que acabou de dar início à 3ª Guerra Mundial. Super Interessante. Disponível em: <http://super.abril.com.br/tecnologia/virus-entra-em-programa-nuclear-e-salva-o-mundo/>. Acesso em jun. 2017.

TEIXEIRA, Paulo Alexandre Gonçalves. **O fenómeno do *phishing* enquadramento jurídico-penal**. 2013. 154 f. Dissertação (Mestrado) – Universidade Autónoma de Lisboa, Mestrado em Direito. Lisboa: UAL, 2013, p. 114. Disponível em: <http://repositorio.ual.pt/bitstream/11144/301/1/O%20fen%C3%B3meno%20do%20Phishing%20%E2%80%93%20Enquadramento%20Jur%C3%ADdico-Penal%20%282013-02%29.pdf>. Acesso em: 02 jun. 2017.

WAXMAN, Matthew C.. *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). March* 16, 2011. ***Yale Journal of International Law***, v. 36, 2011. Disponível em:

<http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1403&context=yjil>. Acesso em 23 maio 2017.

WINDOWS, Microsoft. **MS17-010:** Atualização de segurança para o servidor *Windows* SMB: terça-feira, 14 de março de 2017. Disponível e: <https://support.microsoft.com/pt-br/help/4013389/title>. Acesso em 22 maio 2017.