O PROBLEMA DA ATRIBUIÇÃO DE RESPONSABILIDADE INTERNACIONAL NOS CASOS DE ATAQUES CIBERNÉTICOS

João Glicério de Oliveira Filho[*]
Bárbara Victoria Müller Marchezan[**]

RESUMO: O presente artigo pretende analisar o vínculo necessário que um estado deve ter com o responsável por um ataque cibernético para que haja responsabilização internacional, levando em consideração, sobretudo o disposto no Projeto de Artigos sobre Responsabilidade Internacional dos Estados por Ato Internacionalmente Ilícito de 2001 elaborado pela Comissão de Direito Internacional, e os posicionamentos da Corte Internacional de Justiça e do Tribunal Penal Internacional para a Antiga Iugoslávia no que diz respeito à responsabilidade de Estados por atos privados. Defendemos que para que haja responsabilização internacional por um ataque cibernético, o vínculo necessário entre o Estado e um particular é o do controle efetivo, não devendo este ser flexibilizado em razão da dificuldade de atribuição de ataques cibernéticos e do temor da impunidade, a ponto de atingir Estados inocentes, e trazer consequências danosas pro cenário das relações internacionais.

PALAVRAS-CHAVE: Ataques cibernéticos; Responsabilidade Internacional de Estados; Atribuição de Responsabilidade Internacional; Controle Efetivo.

ABSTRACT: This article analyzes the link that a state must have with the one responsible for a cyber attack to configure international

[*] *Advogado. Doutor em Direito. Professor de Direito Empresarial da Universidade Federal da Bahia (Graduação, Mestrado, Doutorado), da UniJorge e da Ruy Barbosa. (joao@joaoglicerio.com)*
[**] *Graduanda em Direito pela Universidade Federal da Bahia (barbaramarchezan@hotmail.com)*

responsibility of states. To do so, we took in consider the International Law Commission 2001 Draft Articles on Responsibility of States for Internationally Wrongful acts, and the understanding of the International Court of Justice and the International Criminal Tribunal for the Former Yugoslavia in the matter of responsibility of states for non-state actors. We advocate that the effective control doctrine is the appropriate one for international responsibility for cyber attacks. The difficulty of attribution on cyber context e the fear of impunity cannot be used as excuses to make flexibilizations on that doctrine, once it can bring more serious damages to the international relations, as the responsibility of an innocent state.

KEYWORDS: Cyber attacks. Responsibility of states. Attribution for internationally wrongful acts. Effective control.

1 INTRODUÇÃO

A vulnerabilidade do ciberespaço e sua regulamentação jurídica tornou-se uma crescente preocupação nos últimos anos. O espaço cibernético é um cenário promissor para o desenvolvimento do contencioso bélico entre nações. Entretanto, a natureza estrutural da

internet e a forma como é arquitetada fazem com que haja grande facilidade em apagar vestígios, disfarçá-los, ou até mesmo plantar falsos vestígios. Com isso, surge o problema da atribuição de responsabilidade internacional por ataques cibernéticos.

Contudo, a dificuldade de produção de evidências no campo cibernético, e o temor da impunidade geral não devem ocasionar relativização ou flexibilização das atuais formas de atribuição de responsabilidade internacional de Estados a ponto de possibilitar a responsabilização de um Estado inocente. Tal situação poderia gerar maiores consequências negativas do que a não responsabilização. É importante lembrar que o uso de força por um Estado[1], que pode ser feito através de um ataque cibernético, implica no direito de autodefesa, de acordo com o artigo 51 da Carta da Organização das Nações Unidas (ONU).

2 CONFIGURAÇÃO DE ATAQUE CIBERNÉTICO

As definições de ataque cibernético variam, assim como a extensão das consequências que podem ser geradas por eles. De uma maneira ampla, são quaisquer atos tomados com o propósito de minar as funções de uma rede de computadores, corrompendo ou destruindo sistemas, informações ou programas contidos nesses sistemas (WAXMAN, 2015). Para alguns, a diferenciação entre um ataque cibernético de um crime cibernético reside no propósito político e/ou de segurança nacional (CROOTOF; HATHAWAY; LEVITZ, 2015).

A expressão *cyber attack* pode descrever diferentes tipos de atos, como programas de espionagem, ataques do tipo *denial-of-service* - que buscam inutilizar de maneira temporária ou permanente um recurso computacional, como um site -, uma *logic bomb* - um tipo

[1] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Carta das Nações Unidas**. art. 2(4). 1945. Disponível em: <http://www.un.org/en/documents/charter/>. Acesso em: 15 set. 2015.

de ataque que permanece silente até encontrar certas condições para que atividades maliciosas sejam executadas -, ou ainda um cavalo de Tróia - tipo de *software* malicioso que cria uma porta para uma possível invasão, como o acesso não autorizado por uma terceira parte.

Recentemente, ameaças cibernéticas resultaram em propriedades intelectuais, pesquisas, planos militares, e informações privadas expostos. Como exemplo, tem-se o ataque promovido contra o governo e o sistema bancário da Estônia em 2007. Mais do que isso, o *worm* Stuxnet, que foi usado para atacar as centrífugas do programa nuclear iraniano, demonstrou o potencial de ataques críticos a infraestrutura, fazendo com que muitos países se preocupassem em desenvolver defesas cibernéticas e ao mesmo tempo investir em capacidades ofensivas.

Quando se trata de ataques cibernéticos, os Estados enfrentam ainda o problema da falta de regulamentação e de uniformidade nos conceitos, definições, e regras. Isso faz com que os Estados tenham que determinar suas próprias definições e políticas no assunto, que ainda é muito recente para aplicação de costumes internacionais.

3 CONCEITO DE RESPONSABILIDADE INTERNACIONAL

De acordo com James Crawford, é um princípio geral de direito internacional que uma violação de uma obrigação internacional acarreta a responsabilidade do Estado em questão. De maneira simples, o Estado responsável por um ilícito segundo o direito internacional deve ao Estado que sofreu o dano uma reparação adequada (CRAWFORD, 2012, p. 539). Mazzuoli define responsabilidade internacional como "o instituto que visa a 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).

Para que haja a configuração da prática de ato internacionalmente ilícito de uma pessoa jurídica de direito internacional dois elementos são necessários, de acordo com o artigo 2 do Projeto de Artigos sobre Responsabilidade Internacional dos Estados por Ato Internacionalmente Ilícito de 2001 - ARSIWA, elaborado pela Comissão de Direito Internacional das Nações Unidas. Estes elementos são a) atribuição ao Estado no âmbito do direito internacional e b) violação de uma obrigação internacional do Estado. Embora o Projeto de Artigos sobre Responsabilidade não tenha caráter vinculante por si só, alguns de seus artigos são considerados direito costumeiro e já foram reconhecidos como tal pela Corte Internacional de Justiça[2].

No que se refere à atribuição ao Estado, de acordo com o artigo 4 da ARSIWA, considera-se ato de Estado o comportamento de todo órgão estatal no exercício de suas funções executivas, legislativas, jurisdicionais ou de outra índole, qualquer que seja sua posição organizacional perante o governo central ou perante uma divisão territorial do Estado. Além disso, o ato de uma pessoa ou entidade que está notadamente autorizada a exercer funções típicas de autoridade pública, mesmo que não esteja enquadrada no artigo 4, deve ser atribuído ao Estado.

Há, entretanto, a possibilidade de responsabilização internacional do Estado por atos particulares, desde que estes hajam atuado sob sua direção, controle, instrução ou instigação, de acordo

[2] INTERNATIONAL COURT OF JUSTICE. **Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)**, Merits, Judgment of 26 February 2007, para. 385. Disponível em: <www.icj-cij.org> Acesso em: Acesso em: 15 set. 2015.

com o artigo 8 da ARSIWA[3]. Nesse caso, interessante ressaltar que a responsabilidade do Estado verifica-se apenas na hipótese de restar manifestamente patente a ocorrência de um **vínculo real** entre a pessoa ou grupo que realiza o ato e o correspondente aparato estatal.

É justamente na análise desse vínculo entre Estados e atos de particulares que surge o problema da atribuição dos crimes cibernéticos.

4 VÍNCULO NECESSÁRIO ENTRE O ESTADO E ATOS DE PARTICULARES PARA QUE HAJA RESPONSABILIDADE INTERNACIONAL POR ATAQUES CIBERNÉTICOS

A identificação e distinção entre atos de órgãos estatais ou semelhantes, de individuais, e de individuais sob o controle e ordem estatal é de extrema dificuldade no campo cibernético. Até mesmo a identificação do Estado de origem pode ser mascarada, como no caso do ataque cibernético sofrido pela Estônia em 2007. Entretanto, a identificação não é impossível, e o desenvolvimento da tecnologia e da informática tende a tornar o processo de identificação mais fácil com o passar do tempo.

Identificada a origem do ataque, resta o verdadeiro problema, que reside na prova do envolvimento estatal a nível de responsabilidade quando este emanou de um particular dentro do Estado. O artigo 8 da ARSIWA estipula que a conduta de uma pessoa ou de um grupo de pessoas deve ser considerado um ato do Estado

[3] Essa possibilidade de responsabilização internacional do Estado por atos de particulares também foi prevista especificamente para os casos de operações cibernéticas pelo Manual Talinn, elaborado em 2009 por um grupo de especialistas a convite da OTAN, com o objetivo de tentar estabelecer regras internacionais básicas para o meio cibernético. Apesar de não ter caráter vinculante, o Manual Talinn busca aplicar as regras de direito internacional já existentes para os casos envolvendo atividades cibernéticas, e no caso de responsabilização internacional, acompanhou as normas previstas na ARSIWA.

sobre o direito internacional se a pessoa ou grupo de pessoas está agindo sobre as instruções ou o direto controle do Estado ao executar a conduta.

Esse controle direto que o Estado deve obrigatoriamente ter com o responsável foi objeto de análise pela Corte Internacional de Justiça - CIJ, pelo Tribunal Penal Internacional para a Antiga Iugoslávia - ICTY e pela doutrina.

4.1. O *effective control* da Corte Internacional de Justiça e o *overall control* do Tribunal Penal para a Antiga Iugoslávia

Ao de análise desse vínculo, a Corte Internacional de Justiça, no caso Nicarágua contra Estados Unidos, considerou que, para que houvesse responsabilização dos Estados Unidos por atos cometidos pelo grupo *contras* em suas operações militares e paramilitares, deveria restar provado que aquele tinha **controle efetivo** das operações:

> United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the contras, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself [...] for the purpose of attributing to the United States the acts committed by the contras in the course of their military or paramilitary operations in Nicaragua. [...] [What has to be proven is that] that State had **effective control** of the military or paramilitary operation in the course of which the alleged violations were committed. [4]

[4] INTERNATIONAL COURT OF JUSTICE. **Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)**, Merits, I.C.J. Reports 1986, para. 115. Disponível em: <www.icj-cij.org> Acesso em: Acesso em: 15 set. 2015.

A CIJ considerou que, ainda que os Estados Unidos de fato exercessem papel preponderante através da organização, financiamento, treinamento, e equipamento do grupo *contras*, e até mesmo na seleção de possíveis alvos para as atividades militares e paramilitares do grupo e planejando operações, ainda assim não possuía o vínculo necessário entre a operação específica em questão para ser responsabilizado internacionalmente por ela.

No Caso relativo à aplicação da Convenção de Prevenção e Repressão aos Crimes de Genocídio (Bósnia-Herzegovina *v.* Sérvia e Montenegro), a CIJ retornou ao assunto, esclarecendo que deve ser demonstrado que este controle efetivo foi exercitado, ou que instruções específicas a respeito de cada operação foram dadas pelo Estado, e não a respeito de um controle genérico do grupo que praticou as violações.[5]

Apesar da CIJ ter considerado nesse caso que as regras de atribuição de atos ilícitos internacionais a um Estado não variam de acordo com a natureza dos atos em questão na ausência de legislação especial expressa[6], o Tribunal Penal Internacional para a Antiga Iugoslávia - ICTY, no caso Dusko Tadic[7], considerou que o grau de controle pode variar de acordo com as circunstâncias fáticas de cada caso.

A ICTY adotou uma forma menos restritiva de atribuição da conduta, através do *overall control test* em oposição ao *efective control* da CIJ. Através do *overall control*, para que as ações sejam imputadas ao Estado é suficiente que este organize, coordene ou

[5] INTERNATIONAL COURT OF JUSTICE. **Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)**, Merits, Judgment of 26 February 2007, para. 400. Disponível em: <www.icj-cij.org> Acesso em: Acesso em: 15 set. 2015.

[6] *Ibidem*, para. 401.

[7] INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA. **Prosecutor v. Tadić**, Case No. IT-94-1-A, Appeals Chamber, Judgment, 15 July 1999, para. 117. Disponível em: <www.icty.org> Acesso em: 15 set. 2015.

planeje, juntamente com financiamento, treinamento, equipamento ou suporte operacional àquele grupo:

> [...] has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group [...] **regardless of any specific instructions by the controlling State concerning the commission of each of those acts**.[8] (grifo nosso)

4.2. Divergências doutrinárias

Alguns doutrinadores consideram que no caso de operações cibernéticas, a doutrina do *overall control* seria a mais adequada por facilitar a responsabilização. Na visão de James Shackelford, devido a natureza das atividade cibernéticas e da dificuldade técnica de identificação dos autores, a visão da ICTY de *overall control* deve ser usada nos casos de responsabilidade por ataques cibernéticos, em detrimento da utilizada pela CIJ (SHACKELFORD, 2009).

Nesse sentido, Peter Margulies considera que, devido a dificuldade de detectar ataques cibernéticos externamente, juntamente com a facilidade de controlar eles internamente, o vínculo a ser provado para que haja responsabilidade internacional deve ser substancialmente mais abrangente do que em outros contextos. Somente assim a soberania dos Estados poderia ser protegida de armas cibernéticas (MARGULIES, 2015). Ele ressalta que uma visão mais restritiva de responsabilidade incentivaria os agressores ao enviar a mensagem de impunidade. Ademais, a atual legislação encorajaria Estados potencialmente vítimas a se tornarem agressores usando veladamente a assistência de grupos privados.

[8] *Ibidem*, para. 137.

Entretanto, compartilhamos o entendimento de Marco Roscini, ao afirmar que é exatamente pelo caráter problemático da identificação nas atividades cibernéticas que a doutrina de *effective control* da CIJ é a mais adequada (ROSCINI, 2010) dentre os testes de atribuição desenvolvidos até o momento. Dessa forma, evita-se que Estados sejam acusados levianamente, especialmente nos casos em que o Estado vítima reivindica um direito de autodefesa, visto que inocentes poderiam ser atingidos.

Além disso, como notado por Derek Jinks, um teste mais abrangente de responsabilidade pode desencorajar Estados a financiar grupos que estejam tentando resistir a regimes tirânicos pelo medo de uso da força por estes regimes, o que teria impactos negativos na busca pela proteção dos Direitos Humanos (JINKS, 2003).

Ademais, a suposta facilidade de controle de tais ataques internamente não deve ser apontada como argumento, pois ocasionaria a aplicação errônea das normas de responsabilidade internacional. Na verdade, o campo cibernético é o lugar perfeito para atos dissimulados, ocultos e pontuais, o que dificulta a prevenção e punição interna.

O artigo 11 da ARSIWA assevera que uma conduta que não seja atribuível a um estado só será considerada um ato daquele na medida em que reconheça e adote a conduta em questão como sua própria. A ausência de atos do estado no sentido de controlar e punir o ataque não implica em atribuição do ato, na verdade, o estado será responsável por violar sua obrigação internacional de não permitir que seu território seja utilizado para atos atentatórios a direitos de outros estados[9], e não pelo ato em si.

[9] INTERNATIONAL COURT OF JUSTICE. **Corfu Channel (United Kingdom v. Albania)**, ICJ Reports, 1949**.** Disponível em: <www.icj-cij.org> Acesso em: Acesso em: 15 set. 2015.

Outro ponto importante esquecido por aqueles que propõe o uso do *overall control* nestes casos é de que a ICTY aplica essa doutrina somente em casos de grupos organizados e hierarquicamente estruturados, como uma unidade militar ou em caso de guerra ou conflito civil, bandos armados ou rebeldes[10]. Em casos de indivíduos praticando atos ilegais específicos em outros estados, ou no caso de grupos que não se encaixam na descrição anterior, a ICTY aplica a doutrina do *effective control*.

Apesar da contratação de criminosos cibernéticos já ter sido imputada a grupos altamente organizados, como é o caso do Hamas e do Hezbollah, essa não é a realidade dominante nos casos desse tipo de ataque, o que exclui a possibilidade de aplicação do *overall control* em inúmeros casos no campo cibernético.

Sendo assim, entendemos que o vínculo necessário que um Estado deve ter com um grupo ao qual o ataque cibernético foi atribuído, para que seja configurada responsabilidade internacional, deve ser o do *effective control.* O mero suporte ou financiamento ao grupo não é necessário para provar o envolvimento do Estado, que deve exercer controle efetivo sobre a ação específica objeto de responsabilização.

5. CONCLUSÃO

Na ausência de uma legislação específica que regule o campo das operações cibernéticas ou da criação de um teste destinado especificamente aos casos cibernéticos, as regras de atribuição de atos ilícitos internacionais a um Estado não devem ser flexibilizadas sob o pretexto de dificuldade de atribuição de ataques cibernéticos e de

[10] INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA. **Prosecutor v. Tadić**, Case No. IT-94-1-A, Appeals Chamber, Judgment, 15 July 1999, para. 120. Disponível em: <www.icty.org> Acesso em: 15 set. 2015.

temor da impunidade, a ponto de atingir Estados inocentes, e trazer consequências danosas pro cenário das relações internacionais, sobretudo quando se leva em consideração o direito de autodefesa previsto no artigo 51 da Carta da ONU, e a possibilidade de um estado de guerra cibernético.

A observância das normas de direito internacional não pode pautar-se tão somente no medo de punição, seja nesse assunto ou em qualquer outro. A questão deve ser discutida com base na lógica da obediência voluntária dos países, ao buscar influenciar e incentivar determinadas condutas. Portanto, as normas relativas à responsabilização internacional por atos ilícitos não deverá ser relativizada de acordo com a matéria em questão, buscando tão somente aumentar o índice de punições.

Com a análise do artigo 8 do Projeto de Artigos sobre Responsabilidade Internacional dos Estados por Ato Internacionalmente Ilícito de 2001 elaborado pela Comissão de Direito Internacional, e os posicionamentos da Corte Internacional de Justiça, conclui-se que, para que haja responsabilização internacional por um ataque cibernético, o vínculo necessário entre o Estado e um particular é o do **controle efetivo**, não sendo suficiente para configurar a responsabilidade o mero suporte ou financiamento do grupo.

REFERÊNCIAS

CRAWFORD, **James. Browlie's Principles of Public International Law**. 8. ed. Oxford: Oxford University Press, 2012. p. 539-563.

_____ . **The International Law Commission's Articles on State Responsibility**: introduction, text and commentaries. New York: Cambridge University Press, 2003.

CROOTOF, Rebecca; HATHAWAY, Oona A.; 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: 15 set. 2015.

GRAHAM, D. Cyber threats and the law of war. **Journal of National Security Law and Policy**, 4, 87, 2010. Disponível em: <http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf> Acesso em: 22 mai. 2016.

HUNKER, J.; HUTCHINSON, B.; MARGULIES, J. Role and Challenges for Sufficient Cyber-Attribution. Disponível em: <http://www.scis.nova.edu/~cannady/ARES/hunker.pdf> Acesso em: 22 mai. 2016.

INTERNATIONAL COURT OF JUSTICE. **Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)**, Merits, I.C.J. Reports 1986, para. 115. Disponível em: <www.icj-cij.org> Acesso em: Acesso em: 15 set. 2015.

_____ . **Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)**, Merits, Judgment of 26 February 2007, para. 400-401. Disponível em: <www.icj-cij.org> Acesso em: Acesso em: 15 set. 2015.

_____ . **Corfu Channel (United Kingdom v. Albania)**, ICJ Reports, 1949**.** Disponível em: <www.icj-cij.org> Acesso em: Acesso em: 15 set. 2015.

INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA. **Prosecutor v. Tadić**, Case No. IT-94-1-A, Appeals

Chamber, Judgment, 15 July 1999, para. 117-137. Disponível em: <www.icty.org> Acesso em: 15 set. 2015.

JINKS, Derek. State Responsibility for the Acts of Private Armed Groups. **Chicago Journal of International Law** 83, 2003. Disponível em: <http://chicagounbound.uchicago.edu/cjil/vol4/iss1/8 > Acesso em: 15 set. 2015.

MARGULIES, Peter. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. **Melbourne Journal of International Law**, 14, jan. 2015. Disponível em: <http://ssrn.com/abstract=2557517> Acesso em: 15 set. 2015.

MAZZUOLI, Valério de Oliveira. **Direito internacional público:** parte geral. 4. ed. São Paulo: Editora Revista dos Tribunais, 2013. p.184

NIELSEN, Elizabeth. State Responsibility for Terrorist Groups. **U.C. Davis Journal of International Law & Policy,** 17.1, 2010. Disponível em: <http://jilp.law.ucdavis.edu/issues/volume-17-1/151-191.pdf> Acesso em: 15 set. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Carta das Nações Unidas**. 1945. Disponível em: <http://www.un.org/en/documents/charter/>. Acesso em: 15 set. 2015.

_____ . **Yearbook of the International Law Commission 2001.** Vol. II, p. 33. 2005. Disponível em: <http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf> Acesso em: 15 set. 2015.

REED, Chris. **Making Laws for cyber space.** Oxford: Oxford University Press, 2012.

ROSCINI, Marco. World Wide Warfare - 'Jus Ad Bellum' and the Use of Cyber Force. **Max Planck Yearbook of United Nations Law**, 14,

jun. 2010. Disponível em: <http://ssrn.com/abstract=1683370> Acesso em: 15 set. 2015.

SCHMMIT, Michael N. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. **Harvard International Law Journal,** 54, 13, 2012. Disponível em: <http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf> Acesso em: 22 mai. 2016.

_____. **Tallinn Manual on the International Law Applicable to Cyber Warfare**. New York: Cambridge University Press, 2013.

SCHMMIT, Michael N; VIHUL, Liis. Proxy Wars in Cyber Space: The Evolving International Law of Attribution. **Fletcher Security Review**, 2, 55, 2014. Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/c28a64_2fdf4e7945e9455cb8f8548c9d328ebe.pdf> Acesso em: 22 mai. 2016.

SHACKELFORD, S.J. State Responsibility for cyber attacks: Compending Standards for a growing problem, **Goegetown Journal of International Law,** 42, 2011. Disponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Shackelford%20-%20State%20Responsibility%20for%20Cyber%20Attacks%20Competing%20Standards%20for%20a%20Growing%20Problem.pdf> Acesso em: 15 set. 2015.

_____ . "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", **Berkeley Journal of International Law** 27, 2009. p. 191-251 Disponível em: <http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7> Acesso em: 15 set. 2015.

WAXMAN, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4) **Yale Journal of International Law**, Vol.

36, mar. 2011. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1674565> Acesso em: 15 set. 2015.

Recebido em 22 de maio de 2016
Aprovado em 16 de agosto de 2016