FACULDADE BAIANA DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

ERIC BASTOS DEIRÓ DE MELLO

APLICABILIDADE DAS NORMAS SOBRE RESPONSABILIDADE INTERNACIONAL AOS ATAQUES CIBERNÉTICOS ATRIBUÍVEIS A ESTADOS

Salvador
2016

ERIC BASTOS DEIRÓ DE MELLO

APLICABILIDADE DAS NORMAS SOBRE RESPONSABILIDADE INTERNACIONAL AOS ATAQUES CIBERNÉTICOS ATRIBUÍVEIS A ESTADOS

Monografia apresentada ao curso de graduação em Direito, Faculdade Baiana de Direito, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientador: Prof. Thiago Carvalho Borges

Salvador
2016

TERMO DE APROVAÇÃO

ERIC BASTOS DEIRÓ DE MELLO

APLICABILIDADE DAS NORMAS SOBRE RESPONSABILIDADE INTERNACIONAL AOS ATAQUES CIBERNÉTICOS ATRIBUÍVEIS A ESTADOS

Monografia aprovada como requisito parcial para obtenção do grau de bacharel em Direito, Faculdade Baiana de Direito, pela seguinte banca examinadora:

Nome:_____

Titulação e instituição:_____

Nome:_____

Titulação e instituição: _____

Nome:_____

Titulação e instituição:_____

Salvador, ____/_____/ 2016

Aos meus pais, Márcia e Milton, por serem a base fundante pessoa que hoje sou.

Ao meu amor, Gabriela, por essa estrada que junto caminhamos, e por todas as outras que estão adiante.

Aos meus irmãos, Ellen e Neto, por toda felicidade que nutre nossas relações.

AGRADECIMENTOS

Agradeço, primeiramente, aos meus pais, que são a razão de tudo, os quais tenho a eterna gratidão por todos os ensinamentos, por toda educação que tive, suporte, incentivo e confiança que sempre depositaram em mim.

À minha noiva, por eu saber que por trás de todo grande homem existe uma grande mulher, e pela certeza de que escolhi a pessoa certa para amar e compartilhar minha vida.

Aos meus irmãos, Ellen e Neto, pela alegria e gratidão de ter irmãos como vocês.

À minha família, por todo amor que nos une.

Ao meu orientador, o professor Thiago Borges, por toda a contribuição e atenção durante a minha trajetória acadêmica.

Ao Dr. Carlos e Dr. Djalma, por tudo que me ensinaram, e pela companhia do trabalho de cada dia.

Aos meus amigos, que tornam a minha trajetória acadêmica bem mais agradável e pela felicidade de ter a companhia de vocês.

Aos professores que tive na academia, os quais tenho imensa gratidão por todos os ensinamentos.

Aos funcionários da Faculdade Baiana de Direito, os quais tornam o nosso dia-a-dia agradável e harmonioso diante do suporte e ajuda de vocês.

"*By itself, the Internet will not usher in a new era of international cooperation. That work is up to us, its beneficiaries. Together, we can work together to build a future for cyberspace that is open, interoperable, secure, and reliable. This is the future we seek, and we invite all nations, and peoples, to join us in that effort*".

Barack Obama

RESUMO

O presente trabalho monográfico visa analisar a possibilidade de aplicação das normas sobre responsabilidade internacional aos ataques cibernéticos, examinando a medida em que os elementos constitutivos do instituto do direito internacional público teriam sua incidência configurada, notadamente diante da diferença paradigmática entre as normas vigentes e modo de ocorrência dos atos realizados pela rede de computadores. Para os fins propostos, o estudo perpassará pela observação do desenvolvimento da *internet* e da infraestrutura cibernética dos Estados, a partir dos protocolos que viabilizam a comunicação e transferência de dados pelo sistema mundial de computadores. Analisa-se, pois, as formas de operações cibernéticas que podem ser consideradas como ataque. O trabalho examina, ainda, o conceito de ataque cibernético no contexto do direito internacional público, por meio do desenvolvimento histórico do conceito de ataque do direito internacional humanitário até o uso da força verberado na Carta das Nações Unidas. Assim, passa-se à análise do instituto da responsabilidade internacional do estado, atentando para seus elementos objetivo e subjetivo. Nesse sentido, estuda-se a necessidade de cumulação do ato ou omissão que resulte em descumprimento de obrigação internacional prévia ou concomitante à conduta com a necessária imputabilidade daquela ação a um determinado estado como sujeito de direito internacional público, perpassando pela análise dos patamares de controle e elementos de autoridade governamental necessários como elementos de atribuição. Por fim, o trabalho examina a aplicabilidade das normas vigentes sobre responsabilidade internacional do estado aos ataques cibernéticos, avaliando a possibilidade de incidência dos seus elementos sobre as atividades realizadas na *internet*, observando-se a possibilidade da conduta virtual poder configurar um descumprimento obrigacional necessário para ensejar a responsabilidade, além de ponderar se os critérios de imputabilidade podem ser adequadamente adaptados às operações conduzidas por meio de redes de computadores.

Palavras-chave: direito internacional público; responsabilidade internacional do estado; ataque cibernético; atribuição.

ABSTRACT

This monographic study aims to analyze the possibility of applying the rules on international responsibility to cyber attacks, examining the extent to which the constituent elements of international public law would have their incidence configured, notably when facing the paradigmatic difference between the current norms and the way of occurrence of acts performed by means of computer network. For the intended purposes, the study runs through the observation of the internet and cyber infrastructure of states development, from the protocols that enable communication and transfer of data through the global computer system. It analyzes, therefore, forms of cyber operations that may be considered as an attack. The paper examines also the concept of cyber attack in the context of international law, through the historical development of the attack concept of international humanitarian law to the use of force enshrined in the United Nations Charter. It moves on to the analysis of the international responsibility of the state institute, noting its objective and subjective elements. In this sense, it studies the need for aggregation of the act or omission that results in breach of a international obligation prior or concomitant to the conduct with the necessary imputability of that action to a particular state as a subject of public international law, passing through the analysis of degrees of control and governmental authority necessary as elements of attribution. Finally, the paper examines the applicability of existing rules on international responsibility of the state to cyber attacks, assessing the possibility of incidence of its elements on the activities undertaken on the Internet, noting the possibility of virtual conduct to configure as a breach of an obligation required in order to give rise to liability, and considers whether the accountability criteria can be suitably adapted to operations conducted through computer networks.

Keywords: public international law; international responsibility of state; cyber attack; attribution.

LISTA DE ABREVIATURAS E SIGLAS

ARPA Agência de Projetos de Pesquisa Avançada (*Advanced Research Projects Agency*)

ARPANET Rede de pesquisas da ARPA

BGP *Border Gateway Protocol*

CDI Comissão de Direito Internacional da Organização das Nações Unidas

CERT Equipe de Resposta a Incidentes em Computadores (*Computer Emergency Defense Team*)

CIJ Corte Internacional de Justiça

DARPA Posterior alteração da ARPA, que passou a se chamar *Defense Advanced Research Projects Agency*

DNS *Domain Name System*

DoD Departamento de Defesa dos Estados Unidos da América

DoS Negação de serviço (*denial-of-service*)

IP *Internet Protocol*

ONU Organização das Nações Unidas

OTAN Organização do Tratado do Atlântico Norte

TCP *Transport Control Protocol*

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

As relações entre os Estados vêm sofrendo constantes mudanças em decorrência da evolução dos meios de comunicação, o que proporciona uma maior interação informacional. Os avanços tecnológicos, de igual modo, estabelecem novos paradigmas a serem estudados, notadamente diante da insuficiência das normas atualmente vigentes para, *per se*, albergar os novos conceitos e solucionar os problemas trazidos pelos acontecimentos modernos.

Esses desenvolvimentos proporcionados à sociedade também estão disponíveis àqueles sujeitos que intentam realizar atos delituosos. A interconexão entre as nações, sobretudo por intermédio da *internet*, altera os paradigmas anteriormente estabelecidos, de modo que a preocupação dos Estados com sua segurança internacional passa a transcender os limiares fronteiriços, uma vez que operações realizadas por meio de redes de computadores podem ocasionar efeitos tão gravosos quanto os atos cinéticos. Dois fatores agravam exponencialmente essa situação: cada vez mais a infraestrutura dos países, juntamente com seus sistemas, está conectada a redes cibernéticas, aumentando o número de potenciais vítimas, ao passo que as informações de código aberto na *internet* e a propagação de atividades computacionais maliciosas pelos particulares elevam o número de potenciais perpetradores de delitos nas redes de computadores.

Não é necessário muito esforço para perceber a importância de que sejam elaboradas progressões técnicas bem como jurídicas na área. São usuais as notícias veiculadas na mídia, versando, *inter alia*, acerca de roubo de fotos e arquivos em dispositivos móveis pessoais por acesso remoto e sítios eletrônicos fraudados com o intuito exclusivo de obter indevidamente os dados do usuário. Tais delitos devem ser objurgados, mas sua relevância dificilmente extrapolaria o âmbito das políticas de segurança interna de um país.

Por outro lado, a conexão dos sistemas financeiros à *internet*, a necessidade de interconexão entre os sistemas de computadores para a defesa e comunicação militar de uma nação, e a dependência tecnológica da infraestrutura de energia, sobretudo daquelas de técnica mais avançada e sensível (como as usinas de geração de energia nuclear), torna as nações vulneráveis a agentes externos,

fazendo-se necessário revisitar os conceitos clássicos do direito internacional público. Foi isso que se constatou quando, em 2007, o sistema financeiro da Estônia ficou inoperante por dias em decorrência de um ataque de negação de serviço distribuída, em 2008, quando a Geórgia foi alvo do mesmo tipo de ataque, derrubando sítios eletrônicos governamentais, como os do Ministério da Defesa e do Gabinete da Presidência, bem como de veículos de informação, permitindo que a Rússia invadisse fisicamente o território da Ossétia do Sul sem muita oposição, e em 2010, ocasião na qual plantas do programa de enriquecimento Nuclear do Irã foram infectadas por um *malware* que afetou mais da metade dos servidores, causado vultosos prejuízos que, por pouco, não resultaram em uma catástrofe nuclear.

Todos esses ataques demonstraram a capacidade cibernética de impactar nas pessoas e entidades privadas, bem como na atividade estatal. Também demonstraram a vulnerabilidade dos Estados e de suas infraestruturas, requerendo uma elucidação de quais normas se aplicam nesses contextos.

Posto isso, a proposta do presente trabalho é discorrer sobre um tema de grande relevância para o Direito Internacional Público e para a atual conjuntura da sociedade internacional: os ataques cibernéticos. Nos anos recentes está se tornando amplo o uso de armas cibernéticas para criar desvantagem aos oponentes. Países com Austrália e Estados Unidos sempre confiaram nas suas fronteiras marítimas e nas posições físicas relativamente remotas. Contudo, a possibilidade de utilização de meios cibernéticos para a condução de ataques vem mitigando essas barreiras, e aproximando a distância entre o agente delituoso e a potencial vítima.

De plano, cumpre informar que o assunto não requer a elaboração de normas inéditas ou o completo afastamento daquelas que vigoram no âmbito internacional. Com efeito, as antigas normas do *jus in bello* e as normas atuais que regulam o uso da força podem ser aplicadas ao caso – assim como foram aproveitadas para regular outros avanços científicos ao longo da história.

Faz-se imperioso examinar, ainda, a aplicabilidade das normas de responsabilidade internacional – instituto de demasiada importância no Direito Internacional – à aludida forma de ataque, que viola a esfera de direito de outro Estado. A resposta dos sujeitos de direito internacional àqueles que praticam atos ilícitos é elemento primordial para a eficácia do ordenamento jurídico internacional, já que este carece de poder coercitivo emanado de autoridade centralizada.

Ainda sobre o instituto da responsabilidade internacional, mostra-se ponderoso realizar uma análise acerca da questão da atribuição (também chamada pela doutrina brasileira de imputabilidade ou nexo causal) do ato ou omissão violador do direito a um determinado Estado, uma vez que este é elemento constitutivo básico da aludida responsabilidade.

O estudo do mencionado instituto examinará, *inter alia*, as regras consuetudinárias, positivas não-cogentes, análise da prática dos Estados, bem como o posicionamento de relevantes Cortes Internacionais. Por vezes, será necessário propor a adaptação conceitual ou hermenêutica das normas já existentes, a fim de se adequar à moderna problemática.

Ao final, com supedâneo nos fundamentos de direito descortinados no trabalho, bem como na prática internacional, analisar-se-á a possibilidade e em que medida as normas sobre responsabilidade internacional dos Estados se aplicam aos ataques cibernéticos.

2 INFRAESTRUTURA CIBERNÉTICA E AS FERRAMENTAS UTILIZADAS COMO ARMAS NA *INTERNET*

A *internet* (originalmente denominada ARPANET) fora iniciada em 1969 como uma rede de pesquisas pela Agência de Projetos de Pesquisa Avançada (*Advanced Research Projects Agency* ou ARPA) e o Departamento de Defesa dos Estados Unidos da América (*Department of Defense* ou DoD). Ao final daquele ano, a ARPANET conectava quatro universidades norte americanas, quais sejam, *University of Southern California*, *Stanford Research Institute*, *University of California*, em Santa Barbara, e a *University of Utah*. Em 1973, as primeiras conexões internacionais foram feitas, ligando a ARPANET à *University College of London*, na Inglaterra, através de conexão via Noruega[1].

Nos idos de 1982, iniciou-se a formação da *internet* na forma atualmente concebida, por meio de uma rede interconectada de computadores, através de um protocolo de rede padrão. Conhecido como "TCP/IP", o conjunto de protocolos de comunicação entre computadores em rede formava – e ainda forma – a base fundante da *internet* e das comunicações em rede[2].

Impende trazer à baila explanação de Howard Lipson acerca do conceito de *internet*, em estudo realizado pela Equipe de Resposta a Incidentes em Computadores (*Computer Emergency Defense Team* ou CERT) fundado pela DARPA (posterior alteração da ARPA, que passou a se chamar *Defense Advanced Research Projects Agency*), veja-se:

> No mais alto nível de abstração, a *internet* é uma rede de computadores interconectada compreendida por uma infinidade de sistemas de servidores unidos por conexões de comunicação (cabeados e sem fio). Os sistemas de servidores se comunicam enviando mensagens uns aos outros através das conexões de comunicação, onde o pacote de protocolo de rede de computadores padrão chamado TCP/IP especifica os formatos de dados e as regras de transmissão[3] .

---

[1] LIPSON, Howard F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Pittsburgh: Carnegie Mellon Software Engineering Institute, 2002, p. 5. Disponível em: <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408853>. Acesso em: 22 nov. 2015.

[2] *Ibidem*, *loc. cit*.

[3] O texto original segue transcrito: "*At the highest level of abstraction, the Internet is a network of interconnected networks comprised of a myriad of host computer systems joined together by communications links (wired and wireless). Host computer systems communicate by sending messages to each other over the communication links, where a standard network protocol suite called*

É através da *internet*, portanto, que são realizados a grande maioria dos ataques cibernéticos, uma vez que a interconexão remota viabiliza a exploração das vulnerabilidades através da rede, sem a necessidade de uso de mecanismos cinéticos para causar prejuízos a outrem.

Posto isto, resta analisar os elementos fundamentais da arquitetura da *internet*, visando compreender como as comunicações cibernéticas ocorrem e observando as peculiaridades dos protocolos de comunicação, perpassando por suas vulnerabilidades, que permitem que os ataques cibernéticos se circunstanciem.

Ademais, serão examinadas as principais ferramentas utilizadas como armas na *internet*, a fim de aclarar a compreensão quanto ao que é, de fato, um ataque realizado pela forma cibernética.

2.1 INFRAESTRUTURA CIBERNÉTICA E ELEMENTOS FUNDAMENTAIS DA ARQUITETURA DA *INTERNET*

Para se compreender o funcionamento da *internet*, bem como sua arquitetura, faz-se imperiosa a análise dos seus elementos fundamentais. Por meio deles, toda a interação da rede de computadores se realiza, notadamente por proporcionarem a comunicação entre os sistemas e, eventualmente, a sua identificação através de endereços localizáveis no mundo digital. Nas linhas que seguem, analisar-se-á o papel do *Transport Control Protocol* (TCP) e do *Internet Protocol* (IP) na facilitação da comunicação entre sistemas e na estruturação da base fundante da rede de computadores, perpassando pela análise do *Domain Name System* (DNS) no estabelecimento de endereços para localização de outros sistemas na *internet*, bem como examinando o *Border Gateway Protocol* (BGP) e sua função de direcionar as informações, permitindo um roteamento distribuído daquelas comunicações realizadas por outros protocolos.

TCP/IP specifies the data formats and transmission rules". LIPSON, Howard F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Pittsburgh: Carnegie Mellon Software Engineering Institute, 2002, p. 7. Disponível em: <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408853>. Acesso em: 22 nov. 2015.

2.1.1 *Transport Control Protocol* (TCP) e *Internet Protocol* (IP)

Como fora explanado anteriormente, a *internet* é um sistema de comunicações. Ocorre que as mensagens não são transmitidas fisicamente, sendo necessário que a transmissão de informações seja feita através de pacotes de dados, usualmente constituídos por códigos binários (algo como milhões de números 1 e 0). A informação enviada de um servidor é transformada nesse código e transmitida outro servidor, que, por sua vez, tem a função de reorganizar o código binário em informações compreensíveis ao usuário habitual.

O *Transport Control Protocol* (TCP) e o *Internet Protocol* (IP) são os principais veículos da infraestrutura cibernética. Isto pois, o TCP/IP "descreve como a *internet* transmite informação de um lugar a outro por endereçar, fragmentar, e reorganizar os pacotes de dados entre duas fontes confiáveis"[4] .

Não obstante, suas funções são flagrantemente diferentes. O TCP é o protocolo responsável pela transformação dos dados que são a essência da comunicação a ser realizada. Em síntese, o TCP tem algumas características que permitem o recebimento de dados, de maneira intacta, por um servidor remoto[5]. Por meio desse protocolo, os dados são fragmentados em pacotes que têm a capacidade de serem transmitidos pelo IP. Contudo, não incumbe ao TCP a interpretação dos dados que estão sendo transmitidos. Esse papel não remanesce com protocolos de comunicação, mas sim com a aplicação que está sendo usada por cada uma das partes conectadas. A analogia feita entre os ensinamentos de Kevin Fall e William Richard[6] acerca do TCP é de muito proveito para a elucidação do tema e compreensão sobre o funcionamento dessa comunicação, veja-se:

---

[4] Tradução livre do original, que verbera que o TCP/IP "[...] *describe how the Internet transmits information from one place to another by addressing, fragmenting, and reassembling packets of data between two reliable hosts*". SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 118.

[5] ROWLAND, Craig. *Covert Channels in the TCP/IP Protocol Suite*. First Monday Journal, 1997, Volume 2, Number 5. Disponível em: <http://www.firstmonday.org/issues/issue2_5/rowland/>. Acesso em: 25.abr.2016.

[6] Tradução livre do original, que segue transcrito: "*The term connection-oriented means that the two applications using TCP must establish a TCP connection by contacting each other before they can exchange data. The typical analogy is dialing a telephone number, waiting for the other party to answer the phone and saying "Hello," and then saying "Who's calling?" There are exactly two end-*

> O termo *conexão orientada* significa que duas aplicações usando o TCP precisam estabelecer uma conexão do TCP por meio do contato recíproco antes que elas possam intercambiar dados. A analogia comum é discar um número de telefone, esperando que a outra parte atenda o telefone e fale "Oi" para então falar "Quem está falando?". Há exatamente duas extremidades se comunicando reciprocamente por meio de uma conexão TCP.

É importante repisar que, como fora ilustrado no excerto acima, não é seu papel interpretar os dados. Tomando como analogia o telefone, a interpretação dos dados é incumbência dos indivíduos receptores da mensagem, e não do aparelho telefônico em si. Com isso, possibilita-se a percepção de que os aludidos protocolos têm a função de comunicação de dados, não tendo sido criados para a interpretação destes[7], o que dificulta a análise de risco daquilo que está sendo transmitido.

Vê-se, portanto, que o TCP é o protocolo fundamental para que haja a *conexão orientada*, uma vez que permite a transformação de dados em pacotes navegáveis[8], dando mais confiabilidade na comunicação entre sistema de computadores. Foi essa, inclusive, a proposta dos seus criadores, Vinton Cerf e Robert Kahn, que, no artigo que introduziu academicamente os resultados dos estudos realizados com o TCP/IP, afirmaram que eles compreendem "um protocolo que suporta o compartilhamento de recursos que existem em diferentes redes de comutação de pacotes"[10].

O IP, por sua vez, é um "protocolo roteável que endereça, roteia, fragmenta, e reorganiza pacotes"[11]. Enquanto o TCP é um protocolo que fragmenta os dados para possibilitar a transmissão do computador do remetente, e reorganiza os dados no sistema do destinatário, o IP permite a navegação desses dados pela rede de computadores, proporcionando a função básica de transferência de dados[12], sem a qual restaria inviabilizada a comunicação por meio da *internet*.

---

points communicating with each other on a TCP connection". FALL, Kevin R.; STEVENS, William Richard. *TCP/IP Illustrated, volume 1*. 2. ed. Michigan: Addison-Wesley, 2012, p. 585.

[7] *Ibidem*, p. 586.

[8] *Ibidem*, *loc. cit*.

[10] O trecho mencionado fora traduzido livremente, cujo teor segue: "*A protocol that supports the sharing of resources that exist in different packet switching networks is presented*". CERF Vinton G.; KAHN Robert E. *A Protocol for Packet Network Intercommunication*. IEEE Transactions on Communications. Vol. Com-22, No. 5, May 1974, p. 1.

[11] Tradução livre do original, que verbera: "*The Internet Protocol (IP) is a routable protocol that addresses, routes, fragments, and reassembles packets*". DAVIES, Joe. *Op. cit*., 2007. Disponível em: <https://technet.microsoft.com/en-us/library/bb726993.aspx#EJAA>. Acesso em: 25.abr.2016.

[12] GONT, Fernando. *Security assessment of the internet protocol*. United Kingdom's Centre for Protection of the National Infrastructure. 2008, p. 6. Disponível em: <

A usual denominação “endereço de IP” torna cristalina a importância desse protocolo para as comunicações em rede. Todo dispositivo conectado à *internet* tem, pelo menos, um endereço de IP. Assim, a conexão de diversos dispositivos à *internet* só é possível em razão desses endereços, por meio dos quais os dados serão transmitidos, formando a estrutura fundante da rede mundial de computadores[13]. Novamente recorrendo à analogia para facilitar a compreensão, não seria possível enviar uma carta a um destinatário, pelo sistema postal, sem o conhecimento de qual seu endereço, pois o carteiro não saberia onde entregá-la. Sem o endereço de IP, a mensagem que fora fragmentada pelo TCP (e, portanto, está em condições de ser transportada) jamais poderá alcançar seu destinatário.

Ocorre que, diferente do TCP, o IP não tem relevância apenas para as duas extremidades da comunicação. Os protocolos de *internet* (IPs) dos diversos computadores interconectados auxiliam a transmissão dos dados, uma vez que permitem que os dados trafeguem do computador principal ao computador de destino[14]. Kevin Fall e William Richard[15] explanam com clareza o processo de interconexão de dispositivos por meio dos endereços de IP:

> Todo dispositivo conectado à *internet* tem pelo menos um endereço de IP. Dispositivos usados em redes de computadores privadas baseadas nos protocolos TCP/IP também requerem endereços de IP. Em qualquer caso, os procedimentos de remessa implementados pelos roteadores de IP usam endereços de IP para identificar para onde o tráfego está indo. Endereços de IP também indicam de onde o tráfego veio. Endereços de IP são semelhantes, de algum modo, aos números de telefone, mas enquanto os números de telefones são frequentemente conhecidos e usados diretamente pelos usuários finais, os endereços de IP são comumente protegidos da visão do usuário pelo DNS [*Domain Name System*] da *internet*, que permite à maioria dos usuários usar nomes ao invés de números.

---

http://web.archive.org/web/20100211145721/http://www.cpni.gov.uk/Docs/InternetProtocol.pdf>. Acesso em: 25.abr.2016.

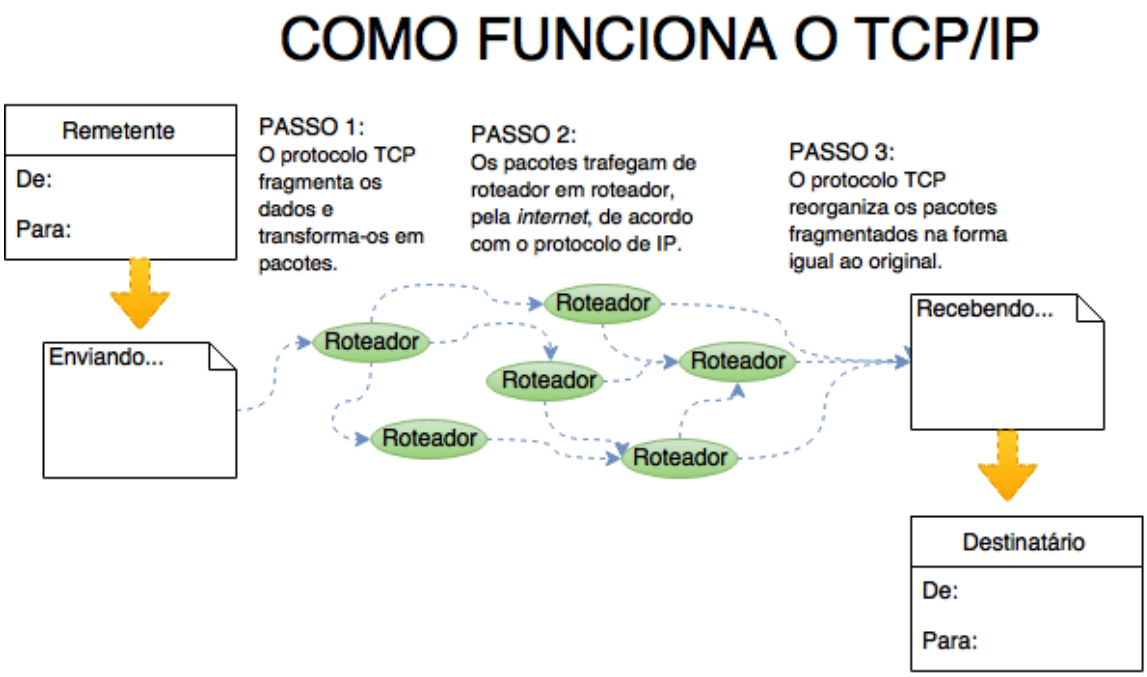
[13] FALL, Kevin R.; STEVENS, W. Richard. *TCP/IP Illustrated, volume 1*. 2. ed. Michigan: Addison-Wesley, 2012, p. 31.

[14] GONT, Fernando. *Op. cit*., 2008, p. 6. Disponível em: < http://web.archive.org/web/20100211145721/http://www.cpni.gov.uk/Docs/InternetProtocol.pdf>. Acesso em: 25.abr.2016.

[15] Tradução livre do original, que segue transcrito: “*Every device connected to the Internet has at least one IP address. Devices used in private networks based on the TCP/IP protocols also require IP addresses. In either case, the forwarding procedures implemented by IP routers use IP addresses to identify where traffic is going. IP addresses also indicate where traffic has come from. IP addresses are similar in some ways to telephone numbers, but whereas telephone numbers are often known and used directly by end users, IP addresses are often shielded from a user’s view by the Internet’s DNS, which allows most users to use names instead of numbers*”. FALL, Kevin R.; STEVENS, William Richard. *Op. cit.*, 2012, p. 31.

Portanto, os pacotes de dados fragmentados pelo TCP trafegam na *internet* por meio de outros sistemas de computadores que roteiam, pelo IP, aquela comunicação para que ela chegue ao seu destinatário final, onde o TCP novamente terá fundamental relevância ao reorganizar os dados em um fluxo coerente[16]. A imagem a seguir ilustra como funciona a comunicação por meio do TCP/IP, veja-se:

Figura 1 – Como funciona o TCP/IP



Fonte: do autor

Muito embora seja formado de dois protocolos (o TCP e o IP), diz-se, usualmente, que o TCP/IP constitui um pacote (ou *suite*) de protocolos, pois é a conjunção que viabiliza a comunicação entre sistemas de computadores.

Por serem a base fundante da *internet*, e pela eficiência comprovada, os protocolos TCP/IP são importantes para a economia global, que depende dessa ferramenta de facilitação da comunicação[17]. Contudo, sua criação ocorreu em uma época em que o ambiente virtual não era tão hostil[18], e hoje esses protocolos acabam sendo usados

[16] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 118.
[17] GONT, Fernando. *Security assessment of the internet protocol*. United Kingdom's Centre for Protection of the National Infrastructure. 2008, p. 6. Disponível em: <http://web.archive.org/web/20100211145721/http://www.cpni.gov.uk/Docs/InternetProtocol.pdf>. Acesso em: 25.abr.2016.
[18] GONT, Fernando. *Security assessment of the internet protocol*. United Kingdom's Centre for Protection of the National Infrastructure. 2008, p. 6. Disponível em: <

maliciosamente (como pela imitação de endereços de IP para forjar a identidade errônea de um remetente de dados[19]) ou suas vulnerabilidades são negativamente exploradas (como pelos ataques de negação de serviço, ou *denial of service*[20], que serão detidamente analisados adiante, em tópico próprio).

2.1.2 *Domain Name System* (DNS)

Há duas maneiras de se identificar um sítio na *internet*: por meio de seu endereço de IP ou por meio de seu nome de domínio. Isso pois, enquanto o IP é o responsável pela criação de "endereços" de computadores conectados à internet, o *Domain Name System* (DNS) torna tais endereços amigáveis à compreensão humana, facilitando o uso e a conexão pela rede de computadores aos seus usuários[21].

A facilitação do uso da *internet* por meio do DNS se dá uma vez que este "permite uma forma padrão de nomeação de vários tipos de objetos e recursos que existem nesse ambiente, e proporciona operações para armazenar e recuperar informações que existem sobre esses objetos"[22]. Isto ocorre quando uma série de números que formam o endereço do IP são localizáveis por uma determinada combinação de palavras para que seja mais compreensível e recordável.

Apenas a título exemplificativo, se diversos estudantes quisessem acessar o sítio eletrônico de uma instituição de ensino superior a qual estão vinculados seria dificultoso que eles memorizassem toda a sequência numérica que remete ao

---

http://web.archive.org/web/20100211145721/http://www.cpni.gov.uk/Docs/InternetProtocol.pdf>. Acesso em: 25.abr.2016.

[19] Computer Emergency Defense Team (CERT). *TCP SYN Flooding and IP Spoofing Attacks*. CERT Advisory CA-1996-21. 1996. Disponível em:<http://www.cert.org/historical/advisories/CA-1996-21.cfm>. Acesso em: 25.abr.2016.

[20] Computer Emergency Defense Team (CERT). *IP Denial-of-Service Attacks*. CERT Advisory CA-1997-28. 1997. Disponível em:<http://www.cert.org/historical/advisories/CA-1997-28.cfm>. Acesso em: 25.abr.2016.

[21] CONRAD, David. *Towards Improving DNS Security, Stability, and Resiliency*. Internet Society, 2012, p. 7. Disponível em: <http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf>. Acesso em: 27.abr.2016.

[22] Tradução livre do original, que verbera: "*It allows a standard way of naming the many types of objects and resources that exist in such an environment, and provides operations for storing and retrieving information about these objects*." TERRY, Douglas B.; PAINTER, Mark; RIGGLE, David W.; ZHOU, Songnian. *The Berkeley Internet Name Domain Server*. Computer Systems Research Group, 1984, p. 9. Disponível em: <http://www.eecs.berkeley.edu/Pubs/TechRpts/1984/CSD-84-182.pdf>. Acesso em: 26.abr.2016.

endereço em que aquele sistema de computador está localizado na rede mundial. O DNS traduz esse conjunto de dígitos em dados localizáveis. Assim, ao invés de terem que se recordar do número “187.45.193.152” (que é o endereço de IP), é de maior facilidade que sejam remetidos à denominação da instituição de ensino, e, ao se direcionarem ao sítio “www.faculdadebaianadedireito.com.br”[23] (que é o nome de domínio), tenham acesso à mesma página que é endereçada pelo IP.

Ocorre que o sistema que rege os nomes de domínios – o DNS – tem uma complexidade um pouco maior do que o exemplo acima, que demonstra apenas a tradução de um endereço de IP por seu nome de domínio. Tal enredamento decorre do fato de que a tradução dos rótulos alfanuméricos para nomes amigáveis à compreensão humana não se dá de forma automática. Com efeito, é necessário todo um sistema de séries de protocolos e uma base de dados para que seja possível essas operações de conversão dos endereços de IP em nomes de domínio, bem como uma catalogação destes, para que tais domínios estejam disponíveis aos computadores conectados à rede mundial[24].

Não obstante, é a função do protocolo DNS de combinar o nome de domínio ao seu endereço de IP que o torna elemento fundamental da arquitetura da *internet*[25], como demonstrado no exemplo acima. Como leciona David Conrad[26], o DNS:

> [...] proporciona a tradução de nomes amigáveis aos humanos em outros formatos de dados. Ele é uma base de dados distribuída globalmente e é um componente crítico da *internet*. O uso mais comum do DNS é a tradução de nomes como “www.exemplo.com” para os “quadros pontilhados dos

---

[23] Os dados veiculados neste exemplo representam, com veracidade, o endereço de IP e o nome de domínio da Faculdade Baiana de Direito, conforme resultado da pesquisa no sequinte *link*, disponível em: <https://www.site24x7.com/find-ip-address-of-web-site.html>. Acesso em: 1º.mai.2016.

[24] CONRAD, David. *Towards Improving DNS Security, Stability, and Resiliency*. Internet Society, 2012, p. 7. Disponível em: <http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf>. Acesso em: 27.abr.2016.

[25] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 118.

[26] Tradução livre do original, que verbera: ˜*The Domain Name System (DNS) provides translation from human-friendly names to data in other formats. It is a globally distributed database and is a critical component of the Internet. The most common use of the DNS is the translation from names such as “www.example.com” to the “dotted-quads” of IPv4 addresses, such as 192.168.1.64, or “colon separated hex” of IPv6 addresses like fd63:fad8:482a:65d3::0:f0cc. However, the DNS is used in the modern Internet for much more than that and now acts as a form of “directory assistance operator” for both human-to-machine as well as machine-to-ma- chine interactions. In addition to IP addresses, the DNS is used to look up mail servers, cryptographic keys, latitude and longitude values, and other diverse types of data. The vast majority of uses of the Internet are critically dependent on the reliable, trustworthy, and responsive operation of the DNS*” CONRAD, David. *Op. cit.*, 2012, p. 6. Disponível em: <http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf>. Acesso em: 27.abr.2016.

> endereços de IPv4, como 192.168.1.64, ou os “números hexadecimais separados por dois pontos” dos endereços de IPv6 como fd63:fad8:482a:65d3::0:f0cc. Contudo, o DNS é usado na *internet* moderna para muito mais que isso e agora atua como uma forma de “operador de assistente de diretório” para ambas as interações homem-para-máquina bem como máquina-para-máquina. Além dos endereços de IP, o DNS é usado para procurar servidores de e-mail, chaves criptográficas, valores de latitude e longitude, e outros tipos de dados diversos. A vasta maioria dos usos da *internet* são criticamente dependentes nessa confiável, precisa e responsiva operação do DNS.

Em 2008, o *hacker* Dan Kaminsky encontrou uma falha que demonstrou a vulnerabilidade do DNS[27]. Em síntese, o sistema poderia ser manipulado para que o nome de domínio remetesse a um endereço de IP errado, enganando os usuários a utilizarem o sítio eletrônico diverso ao desejado[28]. Por exemplo, poderia ocorrer do usuário escrever o nome de domínio da instituição financeira na qual possui conta, e ser endereçado a um página da *internet* falsa, criada com o intuito de coletar informações de segurança dos usuários.

A empresa russa Kaspersky Lab, uma das maiores do mundo em segurança de *software* e soluções antivírus[29], noticiou que cibercriminosos brasileiros utilizavam tais falhas para realização de ataques cibernéticos. “Nesses ataques os servidores DNS configurados no dispositivo atacado irão redirecionar a navegação da vítima para sites falsos de bancos brasileiros, programados para roubar credenciais”[30].

2.1.3 *Border Gateway Protocol* (BGP)

---

[27] WRIGHT, Cory. *Understanding Kaminsky’s DNS Bug*. Linux Journal, 2008. Disponível em: <http://www.linuxjournal.com/content/understanding-kaminskys-dns-bug>. Acesso em: 02.mai.2016.

[28] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 120.

[29] De acordo com o sítio eletrônico da empresa Kaspersky Lab, ela é uma das quatro empresas líderes mundiais em fornecimento de *software* de segurança para usuários finais. Disponível em: <http://brazil.kaspersky.com/sobre-a-kaspersky/sobre-a-empresa/>. Acesso em: 1º.mar,2016.

[30] Notícia veiculada no sítio eletrônico institucional da empresa Kaspersky Lab. Disponível em: <http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/blog-da-kaspersky/2014/pagina-web-maliciosa-ataca-roteadores>. Acesso em: 1º.mai.2016.

No subtópico que explanou o funcionamento dos protocolos TCP/IP (vide 1.1.1), fora consignado que estes tinham fundamental relevância para a transmissão das informações por meio de pacotes de dados. Pode-se dizer, assim, que o TCP/IP é o conjunto de protocolos que veicula as informações na rede de sistemas de computadores.

Para que o pacote de dados fragmentado pelo TCP trafegue pelos endereços de IP em pacotes até chegar ao usuário final, onde o TCP reorganizará os dados, é necessário que esses comandos sejam direcionados, de forma que a a informação enviada chegue ao seu destinatário final. Nos sistemas de computadores conectados à *internet*, tal papel remanesce com o *Border Gateway Protocol* (BGP), que é o protocolo responsável pela função fundamental do roteamento, conduzindo os pacotes de dados até computador receptor da informação, informando-a como (e pra onde) se mover[31]. Nos ensinamentos de Scott J. Shackelford[32], *verbis*:

> O *Border Gateway Protocol* é o protocolo básico de roteamento de todas as redes de computadores que abrangem a *internet*. [...] Ele está encarregado de uma tarefa fundamental – mostrar à informação como se mover. Quando um email, por exemplo, é enviado de uma rede de computadores para outra, ele passa por roteadores. Quando um roteador recebe um pacote de IP, o BGP usa um algoritmo para tomar decisões sobre pra onde enviá-lo a seguir.

Como se infere do exposto, o BGP é um protocolo responsável pelo roteamento, conduzindo e direcionando o tráfego de informações. Recorrendo à comparação figurativa para melhor ilustrar a questão, se o TCP/IP fosse um carro em um rali, onde se tem um ponto de partida e um ponto de chegada estipulados, mas se pode tomar inúmeros caminhos para se chegar ao destino, o BGP seria o copiloto, que informaria as rotas a serem tomadas, auxiliando o veículo a tomar os caminhos necessários para alcançar a linha de chegada.

Ocorre que essa transmissão não é, necessariamente, instantânea ou direta. É preciso que, em cada um dos pontos roteadores, o protocolo BGP direcione os pacotes para o próximo endereço de IP, que seguirá o mesmo processo até que a

---

[31] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 123.

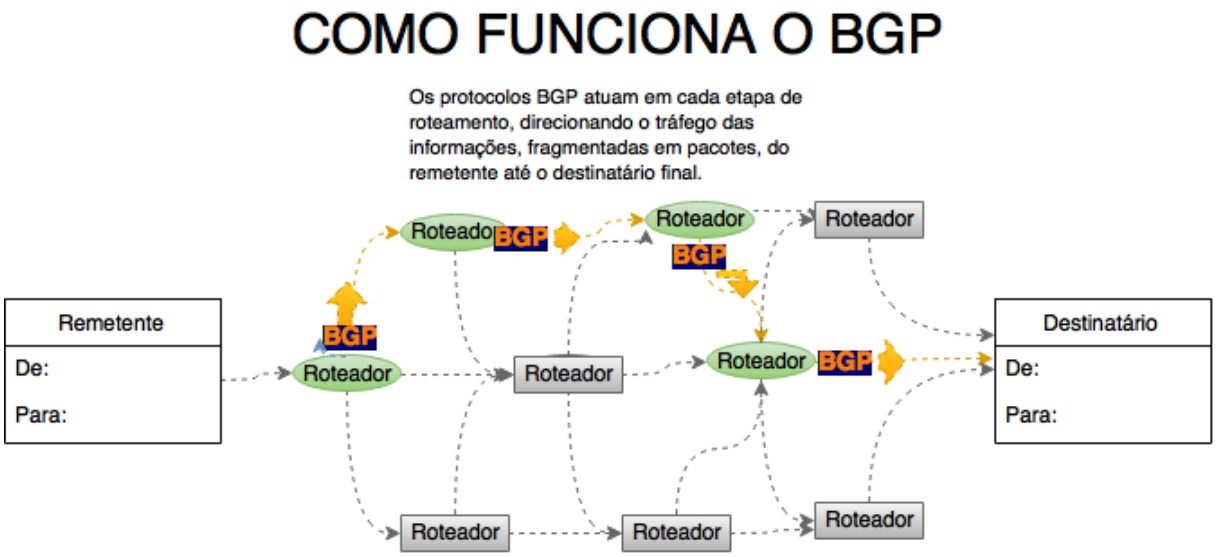
[32] Tradução livre do original, que verbera: "*The Border Gateway Protocol is the core routing protocol of all of the networks that comprise the Internet. [...] it is charged with a fundamental task – telling information how to move. When an email, for example, is sent from one network to another, it passes through routers. When a router receives an IP packet, BGP uses an algorithm to make decisions about where to route it next*". *Ibidem*, *loc. cit*.

informação chegue ao destino desejado. Impende trazer à baila as lições de Rick Kuhn, Kotikalapudi Sriram e Doug Montgomery acerca desse processo de transmissão consecutiva do protocolo BGP, veja-se:

> Muitos sistemas intermediários podem estar envolvidos na transmissão, e porque existem muitos caminhos de um ponto a outro, nem todos os pacotes seguem o mesmo caminho entre a fonte e o destino. Todos os sistemas pelos quais os pacotes passam, de um ponto a outro, precisam saber para onde encaminhar o pacote, baseado no endereço de destino e a informação correta constante na tabela de roteamento[33].

Na tentativa de demonstrar visualmente como sucederia tal processo, a imagem que segue busca elucidar o processo de direcionamento da informação por meio do protocolo BGP:

Figura 2 – Como funciona o BGP



Fonte: do autor

Assim, o aludido protocolo de roteamento é fundamental para a comunicação entre computadores, uma vez que sua função primária é garantir a alcançabilidade

[33] Tradução livre do original, que verbera: "*Many intermediate systems may be involved in the transmission, and because there are many paths from one point to another, not all packets follow the same path between source and destination. The systems that packets pass through from one point to another all need to know where to forward a packet, based on the destination address and information contained in a routing table*". KUHN, Rick; SRIRAM, Kotikalapudi; MONTGOMERY, Doug. *Border Gateway Protocol Security: Recommendations of the National Institute of Standards and Technology*. Gaithersburg: US National Institute of Standards and Technology, 2007, p. 1-1. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf>. Acesso em 5.mai.2016.

reciproca de informações entre os sistemas de protocolos BGP[34]. "É, então, aparente que a interface entre redes de computadores precisam cumprir um papel central no desenvolvimento de qualquer estratégia de interconexão entre servidores. Nós damos um nome especial a essa interface que realiza essas funções e a chamamos de *GATEWAY*"[35], que, em tradução livre, seria uma porta de acesso.

Como os demais protocolos, o BGP foi desenvolvido em uma época na qual as questões concernentes à segurança, sobretudo no âmbito cibernético, não eram assuntos de relevância precípua[36]. Pautado nesse contexto, as escolhas tomadas para fomentar o desenvolvimento da comunicação e troca de dados pelo meio digital priorizaram a velocidade e o crescimento em escala em detrimento do controle[37]. Isso acabou por acarretar a vulnerabilidade desse protocolo, o que permite que agentes maliciosos realizem ataques direcionados a esse protocolo, como, por exemplo, para desorientar o comando do BGP, direcionando a informação para um sistema de computadores que não é o real destinatário, que é um dos problemas mais recorrentes contra esse protocolo[38].

Não obstante, há outros modos de ataque conhecidos por afetarem o BGP, como a imitação de um protocolo enviado, fazendo o roteador acreditar que aquele é um comando genuíno que direciona o caminha de envio da informação, quando, na verdade, o pacote e a semelhança do protocolo de porta de acesso estão sendo forjados, fazendo com que o dado falso chegue ao destinatário[39]. Pode ocorrer, ainda, a interceptação não autorizada (chamada, no termo original em inglês, de *eavesdropping*, quando a mensagem entre os roteadores não encriptada e pode ser

---

[34] REKHTER, Yakov; LI, Tony. *A Border Gateway Protocol 4*. Internet Engineering Task Force (IETF) Request for Comments (RFC) 1771, 1995, p.1. Dispobível em: <https://tools.ietf.org/html/rfc1771>. Acesso em: 1º.mai.2016.

[35] Tradução livre do original, que verbera: "*It is thus apparent that the interface between networks must play a central role in the development of any network interconnection strategy. We give a special name to this interface that performs these functions and call it a GATEWAY*.". CERF Vinton G.; KAHN Robert E. *A Protocol for Packet Network Intercommunication*. IEEE Transactions on Communications. Vol. Com-22, No. 5, May 1974, p. 2.

[36] KUHN, Rick; SRIRAM, Kotikalapudi; MONTGOMERY, Doug. *Border Gateway Protocol Security: Recommendations of the National Institute of Standards and Technology*. Gaithersburg: US National Institute of Standards and Technology, 2007, p. 3-1. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf>. Acesso em 5.mai.2016.

[37] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 123.

[38] KUHN, Rick; SRIRAM, Kotikalapudi; MONTGOMERY, Doug. *Op. cit.*, 2007, p. 3-3. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf>. Acesso em 5.mai.2016.

[39] *Ibidem*, *loc. cit*.

explorada durante o processamento de pacotes durante a recepção e reencaminhamento dos pacotes em cada roteador[40]. Demais formas de utilização maliciosa do BGP também são comumente observadas, como no caso da negação de serviço (chamada, originalmente, de *denial-of-service* ou DoS, cuja análise será feita dentro do tópico seguinte), que, em síntese, é o direcionamento dos servidores da *internet* a um servidor específico, sobrecarregando-o e inviabilizando a sua utilização pelos usuários ordinários[41], bem como a forma de ataque conhecida como *black hole* (ou buraco negro), no qual o tráfego das informações é encaminhado a roteadores que deliberadamente abandonam alguns pacotes de dados, ou todos eles, fazendo com que aquela comunicação se perca[42].

A importância desse protocolo para as comunicações pelo âmbito cibernético faz com que os riscos decorrentes das vulnerabilidades observadas alcancem escalas vultosas, o que levou o Departamento de Segurança Nacional dos Estados Unidos a considerar que "dos muitos protocolos de roteamento em uso na *internet*, o *Border Gateway Protocol* (BGP) está sob o maior risco de ser alvo dos ataques concebidos para interromper ou degradar serviços em uma larga escala"[43].

Posto isto, impende salientar proposta desse trabalho não é discorrer exaustivamente acerca da estrutura da *internet*, sendo estas explanações apenas elucidativas para que se possibilite a compreensão, para a análise jurídica (e não da perspectiva da ciência da computação), do que são e como funcionam os ataques cibernéticos ou qualquer outra operação realizada tendo como intermédio o âmbito cibernético. Esboçada o escopo da infraestrutura e os elementos fundamentais da arquitetura da *internet*, é necessário delinear quais são as armas que podem ser usadas para realizar os ataques cibernéticos.

---

[40] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 124.
[41] KUHN, Rick; SRIRAM, Kotikalapudi; MONTGOMERY, Doug. *Border Gateway Protocol Security: Recommendations of the National Institute of Standards and Technology*. Gaithersburg: US National Institute of Standards and Technology, 2007, p. 3-9. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf>. Acesso em 5.mai.2016.
[42] *Ibidem*, p. 3-2.
[43] Tradução livre do original, que verbera: "Of the many routing protocols in use within the Internet, the Border Gateway Protocol (BGP) is at greatest risk of being the target of attacks designed to disrupt or degrade service on a large scale". UNITED STATES DEPARTMENT OF HOMELAND SECURITY. *The National Strategy to Secure Cyberspace*. Washington: US Department of Homeland Security 2003, p. 30. Disponível em: <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>. Acesso em 5.mai.2016.

2.2 FERRAMENTAS UTILIZADAS COMO ARMAS NA *INTERNET*

A infraestrutura cibernética explanada no tópico anterior tem vulnerabilidades, acarretando, através de falhas nos equipamentos (*hardwares*) e programas de computador (*softwares*), na possibilidade de exploração dos sistemas que funcionam na *internet*[44] .

A análise deste capítulo se mostra relevante pois a "paz cibernética requer não apenas inovação técnica para combater o número crescente de armas cibernéticas e sua proliferação, mas também educação e melhores práticas de gestão para ajudar a combater os perigos internos" [45].

Vê-se que a importância de dominar o conhecimento quanto às ferramentas utilizadas como armas cibernéticas transcende o interesse estatal, sendo de notável relevância para que os humanos não sofram os malefícios do uso impróprio das informações obtidas na rede de computadores.

Não obstante, as vulnerabilidades previamente mencionadas não significariam muito se não houvessem armas capazes de explorá-las[46]. É este o objetivo deste tópico: proporcionar uma compreensão lógica das ferramentas utilizadas como armas na *internet*.

Saliente-se que a caracterização de ferramentas digitais como "armas" é intrincada, haja vista que elas são, em essência, linhas de códigos de computação.

As ferramentas popularmente conhecidas por serem armas no âmbito cibernético são os *malwares*, combinação de *malicious* (malicioso) com *software* (programa de computador), conceituados como "programa que compromete a operação de um sistema ao realizar uma função ou processo não autorizado"[47].

---

[44] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 136.
[45] *Ibidem*, *loc. cit*.
[46] *Ibidem*, *loc. cit*.
[47] O glossário disponibilizado no sítio eletrônico do Departamento de Segurança Nacional dos Estados Unidos que *software* "[...] *compromises the operation of a system by performing an unauthorized function or process*". Disponível em: <https://niccs.us-cert.gov/glossary#letter_m>. Acesso em 22 nov. 2015.

As formas mais comuns de *malware* são os *spywares*, os vírus, os *worms*, e os Cavalos de Tróia (*Trojan Horses*)[48]. Serão analisadas, a seguir, essas e outras ferramentas, consideradas principais na utilização como armas cibernéticas.

2.2.1 *Spyware*

O *spyware* é um tipo de *malware* que é "[...] secretamente e sub-repticiamente instalado em um sistema da informação sem o conhecimento do usuário ou proprietário do sistema"[49]. Utiliza-se esse programa de computador malicioso para "monitorar secretamente a sua atividade no seu computador. Programas *spyware* reúnem informações como nomes e senhas do usuário, números de contas. Alguns *spywares* focam no monitoramento do comportamento de uma pessoa na *internet*"[50].

Assim, compreende-se como *spyware* aquele programa de computador cujo intuito é obter e reunir informação localizada em um determinado sistema de computador sem o conhecimento do seu usuário (e, consequentemente, sem o consentimento deste).

É um *malware* que usualmente instalado junto com um *software* gratuito baixado de sítios eletrônicos maliciosos, viabilizando o monitoramento do uso do computador. A despeito dos esforços para combatê-lo, estima-se que, em 2005, 80% (oitenta porcento) dos computadores estavam infectados por algum *spyware*[51]. O Gabinete de Segurança Institucional da Presidência da República do Brasil, nesse esteio, indicou a aludida forma de ataque cibernético como um desafio econômico, uma vez

---

[48] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 137.

[49] O glossário disponibilizado no sítio eletrônico do Departamento de Segurança Nacional dos Estados Unidos define *spyware* como "*Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner*". Disponível em: <https://niccs.us-cert.gov/glossary#letter_s>. Acesso em 22 nov. 2015.

[50] Conforme verbera o glossário da empresa de programas de computadores de segurança Norton, subdivisão da Symantec, ao estabelecer que o termo *spyware* "[…] is used for the programs that covertly monitor your activity on your computer. Spyware programs gather personal information like user names passwords, account numbers. Some spyware focuses on monitoring a person's Internet behavior". Disponível em: <http://us.norton.com/security_response/glossary/define.jsp?letter=s&word=spyware>. Acesso em: 7.mai.2016.

[51] SHACKELFORD, Scott J. *Op. cit.*, 2014, p. 137.

que este seria um dos mais frequentes, entre aqueles que afetavam os usuários finais[52].

A disseminação desse tipo de ataque cibernético foi tão ampla que se criou uma grade indústria anti *spyware*[53], com vários produtos lançados no mercado para inibir a instalação de *spywares*, ou a sua detecção e remoção, a exemplo do Avira, AVG, Microsoft Windows Defender e McAfee.

2.2.2 Cavalos de Tróia (*Trojan Horses*)

O *malware* conhecido como cavalo de tróia é "um programa malicioso escamoteado dentro de um arquivo legítimo"[54]. Sua terminologia fora concebida em alusão ao grande cavalo de madeira usado pelos gregos na Guerra de Tróia, que aparentava, para os troianos, um símbolo da vitória, enquanto que, em verdade, havia guerreiros inimigos ocultos no interior do mencionado cavalo, tal como fora narrado na obra Odisseia, de Homero.

No contexto dos ataques cibernéticos, os cavalos de tróia são programas de computadores utilizados como meio de distribuir e propagar códigos maliciosos (como os *spywares*) enquanto aparentam ser outro arquivo, como uma imagem[55]. Nesse sentido, Carl E. Landwehr *et al.*[56] lecionam que "[...] é um programa que se

---

[52] BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Livro verde: segurança cibernética no Brasil* (organização Claudia Canongia e Raphael Mandarino Junior). Brasília: GSIPR/SE/DSIC, 2010., p. 35.

[53] ESTADOS UNIDOS. Federal Trade Commission. *Monitoring Software on Your PC: Spyware, Adware, and Other Software*. Washington: Federal Trade Commission, 2005, p. 1. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf>. Acesso em: 8.mai.2016.

[54] Tradução livre do original, que verbera: "*Trojan horse, a malicious program concealed within a legitimate file*". SAMANI, Raj; PAGET, François. *Cybercrime exposed: cybercrime-as-a-service*. Santa Clara: McAfee, 2013, p. 8. Disponível em <http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf>. Acesso em: 7.mai.2016.

[55] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 137.

[56] Tradução livre do original, que verbera: "[...] *a program that masquerades as a useful service but exploits rights of the program's user (not possessed by the author of the Trojan horse) in a way the user does not intend*". LANDWEHR, Carl E.; BULL, Alan R.; MCDERMOTT, John P.; CHOI, William S. . *A Taxonomy of Computer Program Security Flaws, with Examples*. ACM Computing Surverys, 26,3, 1994, p. 4. Disponível em: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA465587>. Acesso em: 7.mai.2016.

mascara como um serviço útil, mas explora os direitos do usuário do programa (não possuído pelo autor do cavalo de tróia) de uma forma que o usuário não tem pretensão". De acordo com o glossário disponibilizado pela empresa de segurança tecnológica Norton, controlada pela Symantec, os cavalos de tróia são impostores, por aparentarem ser programas de interesse do usuário, quando, na verdade, seu objetivo malicioso está oculto, senão veja-se:

> Cavalos de tróia são impostores. Os arquivos aparentam ser programas desejáveis, mas eles são maliciosos. Uma distinção muito importante dos vírus reais é que eles não se replicam, como os vírus fazem. Cavalos de tróia contêm um código malicioso que, quando acionado, causa perda ou roubo de dados. Para um cavalo de tróia se espalhar, você deve convidar esse programa para o seu computador, por exemplo, ao abrir um anexo no e-mail. Cavalos de tróia também são conhecidos por criarem uma porta dos fundos no computador. A porta dos fundos confere acesso ao sistema por outro usuário, e possivelmente permite que informações confidenciais ou pessoais sejam comprometidas. Distintamente aos vírus e *worms*, cavalos de tróia não reproduzem ao infectar outros arquivos, nem se auto replicam.[57]

Como resta cristalino da análise do excerto acima, os cavalos de tróia são um tipo de *malware* que criam uma vulnerabilidade denominada "porta dos fundos", ou *backdoor*, no termo original. Por meio dessa porta dos fundos, o agente malicioso pode distribuir o programa danoso e realizar inúmeras tarefas, como baixar dados e transferí-los para outro sistema, bem como coletar informações confidenciais, como senhas e dados de cartões de crédito[58].

A possibilidade dos cavalos de tróia permanecerem escondidos enquanto instalam outros programas que ameaçam o sistema do usuário aumenta sua popularidade, de modo que uma pesquisa realizada em 2009 indicou que os ataques realizados com o auxílio dessa forma de *malware* chegam a 83% (oitenta e três por cento) do total

---

[57] Tradução livre do original, que verbera: "*Trojan horses are impostors. The files claim to be desirable programs, but they are malicious. A very important distinction from true viruses is that they do not replicate themselves, as viruses do. Trojan horses contain a malicious code which, when triggered, causes loss or theft of data. For a Trojan horse to spread, you must invite these programs onto your computer; for example, by opening an email attachment. Trojan horses are also known to create a back door on a computer. The back door gives another user access to a system, and possibly allows confidential or personal information to be compromised. Unlike viruses and worms, Trojan horses neither reproduce by infecting other files, nor do they self-replicate*". Significado do termo "Trojan horse" no glossário da empresa Norton by Symantec. Disponível em: <http://us.norton.com/security_response/glossary/define.jsp?letter=t&word=trojan-horse>. Acesso em: 7.mai.2016.

[58] CONSTANTIN, Lucian. *Computer Trojan Horse Steals Credit Card Details From Hotel Reception Software*. *PC World Australia*, 19.abr.2012. Disponível em: <http://www.pcworld.com/article/254030/computer_trojan_horse_steals_credit_card_details_from_hotel_reception_software.html>. Acesso em: 8.mai.2016.

de programas de computadores maliciosos no mundo[59]. A utilização chega a ponto tão elevado de difusão que até políticas governamentais se utilizam de *spywares* para obter dados de usuários de sistemas de computadores conectados à internet (o que os especialistas denominaram, vulgarmente, de *govware*, acrônimo de *government* e *malware*), como é o caso do programa R2D2, utilizado pelo Governo alemão para se infiltrar nos computadores de suspeitos de cometimento de crimes[60].

2.2.3 Vírus, *Worms* e Bombas lógicas (*Logic Bombs*)

Existem diversos tipos de *malware*. Cumpre destacar alguns daqueles que aparecem mais recorrentemente nos ataques cibernéticos realizados pela *internet*.

O famoso vírus é um "*malware* que, quando executado, tenta se replicar em outras máquinas executáveis ou códigos escritos; quando tem sucesso, o código é considerado infectado. Quando o código infectado é executado, o vírus também se executa"[61]. Já o *worm* é um tipo de vírus que se espalha ao criar réplicas de si em sistemas, discos ou redes de computadores. Todavia, difere do vírus por não necessitarem comando para se espalhar[62].

A Iniciativa Nacional para as Carreiras e Estudos em Segurança Cibernética, do Departamento de Segurança Nacional dos Estados Unidos, define o termo *worm*

---

[59] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 138.

[60] CUPA, Basil. Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware). In: WEBSTER, C. William R.; CLAVELL, Gemma Galdon; ZURAWSKI, Nils; BOERSMA, Kees; SÁGVÁRI, Bence; BACKMAN, Christel; LELEUX, Charles (Editores). *Living in Surveillance Societies: 'The State of Surveillance'*. Barcelona: COST, 2012 , p. 419. Disponível em: <http://www.zora.uzh.ch/81157/1/Cupa_Living_in_Surveillance_Societies_2012.pdf>. Acesso em: 8.mai.2016.

[61] Tradução livre do original, que verbera: "*Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds, the code is said to be infected. When the infected code is executed, the virus also executes*". STALLINGS, William; BROWN, Lawrie. *Computer Security: Principles and Practice*. 3. ed. New Jersey: Pearson, 2015, p. 201.

[62] O McAfee Threat Glossary define *worm* como "*A virus that spreads by creating duplicates of itself on other drives, systems, or networks. A mass-mailing worm is one that requires a user's intervention to spread, (e.g., opening an attachment or executing a downloaded file). Unlike viruses, worms do not infect other files. Most of today's email viruses are worms. A self-propagating worm does not require user intervention to spread. Examples of self-propagating worms include Blaster, Sasser, and Conficker)*". Disponível em: <http://www.mcafee.com/us/threat-center/resources/threat-glossary.aspx>. Acesso em: 22 nov. 2015.

como “um programa independente, auto-replicante e auto propagante que usa mecanismos de redes de computadores para se espalhar”[63] .

Um *worm* pode, por exemplo, enviar uma cópia dele mesmo para todos em sua lista de contatos, mesmo que você não abra sua conta de e-mail – o que exacerba sua capacidade de se espalhar com rapidez[64]. Nas lições de Lawrie Brown e William Stallings, é como se fosse:

> Um programa de computador que pode rodar independentemente e pode propagar uma versão completa de si mesmo em outros servidores de uma rede de computadores, usualmente ao explorar as vulnerabilidades do *software* do sistema alvo.[65]

Estes, por sua vez, diferem da bomba lógica, que é “um código inserido em um *malware* por um intruso. A bomba lógica permanece adormecida até que uma condição se implemente; o código, então, desencadea um ato não autorizado”[66]. Vê-se que sua definição fora elaborada em clara alusão a uma bomba que, quando atingido o seu preceito lógico ativador, inicia o procedimento de explosão.

2.2.4 Negação de serviço (*denial-of-service* ou DoS)

A utilização da ferramenta de negação de serviço (DoS) como mecanismo de ataque cibernético demonstra como a vulnerabilidade da infraestrutura cibernética e sua própria arquitetura podem ser usadas em seu desfavor.

> [...] Ataques de negação de serviço distribuída (DoS), embora prejudiciais, são métodos consideravelmente não sofisticados de ataque e são usualmente realizados através de uma *botnet* através da qual um único controlador pode aproveitar o potencial de vários computadores. O ataque inunda um alvo específico com solicitações de serviço, para que o alvo seja derrubado diante de sua inabilidade de lidar com as solicitações recebidas

---

[63] O léxico disponibilizado no sítio eletrônico do Departamento de Segurança Nacional dos Estados Unidos verbera que *worm* é “A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself”. Disponível em: <https://niccs.us-cert.gov/glossary#letter_w>. Acesso em 22 nov. 2015.

[64] SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 139.

[65] Tradução livre do original, que verbera: “*A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the target system*”. STALLINGS, William; BROWN, Lawrie. *Computer Security: Principles and Practice*. 3. ed. New Jersey: Pearson, 2015, p. 201.

[66] Tradução livre do original, que verbera: “*Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act*”. *Ibidem*, *loc. cit*.

> ou o alvo é efetivamente bloqueado para as solicitações legítimas, já que o ataque exaure os recursos disponíveis para alcançar e lidar com as solicitações legítimas[67] .

Recorrendo à analogia para elucidar a compreensão dessa modalidade de ataque, pode-se supor que seria como uma determinada porta de um estabelecimento que só permite o acesso de um cliente por vez. Um determinado agente, então, com o intuito de inibir o acesso dos reais usuários daquele estabelecimento, enviam mil pessoas para entrarem no mesmo ambiente pretendido pelos clientes. Por óbvio, aqueles indivíduos que pretendiam legitimamente entrar no recinto vão ser obstados pela multidão. E mesmo que consigam adentrar o estabelecimento, seu proveito do serviço desejado certamente não será o mesmo.

São muito proveitosas à compreensão global dos efeitos do ataque de negação de serviço as lições de David Conrad acerca do tema, *verbis*:

> Ataques de negação de serviço (DoS) são os mais prováveis de causarem efeitos generalizados na estabilidade da internet. Um ataque DoS pode ser contra um único nome de domínio, contra servidores raíz que mantêm unidos os sistemas de nome de domínio da internet, ou contra qualquer parte da infraestrutura integrante. O impacto do DoS pode variar a depender do alvo. Por exemplo, sem os servidores raíz, a internet iria efetivamente parar de funcionar, muito embora não fosse imediatamente.[68]

Compreendido o escopo geral da infraestrutura da *internet* e das ferramentas utilizadas como armas nela, passa-se ao exame da disciplina jurídica do ataque cibernético no direito internacional.

---

[67] O original, em inglês, verbera que "[...] *Distributed denial of service (DDoS) attacks, although disruptive, are a fairly unsophisticated method of attack and are usually carried out through the use of a botnet through which a single controller can harness the power of many computers. The attack floods a specific target with requests for service, so that either the target shuts down in the wake of its inability to cope with the incoming messages, or the target is effectively blocked to legitimate requests as the attack exhausts the resources available to the target to handle legitimate requests*". DINNISS, Heather Harrison. *Cyber warfare and the law of war*. New York: Cambridge University Press, 2012, p. 5.

[68] Tradução livre do original, que verbera: "*Denial of Service (DoS) attacks are most likely to have widespread effects on the stability of the Internet. A DoS attack could be against a single domain name, against the root servers that glue together the Internet's DNS, or against any part of the infrastructure in between. The impact of DoS would vary with the target. For example, without the root servers, the Internet would effectively cease to function, albeit not immediately*". CONRAD, David. *Towards Improving DNS Security, Stability, and Resiliency*. Internet Society, 2012, p. 2. Disponível em: <http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf>. Acesso em: 27.abr.2016.

3 ATAQUE CIBERNÉTICO NO DIREITO INTERNACIONAL

A conceituação do que se considera por ataque cibernético no direito internacional não requer análise simples. O fato das relações internacionais terem se pautado, por longo período, na noção de que os Estados poderiam recorrer livremente aos recursos bélicos fez com que houvesse diversos conceitos de ataque que não são necessariamente conexos. Antes de adentrar nas definições de ataque no *jus ad bellum*, no *jus in bello* e no contexto das operações cibernéticas, impende discorrer, com brevidade, acerca da evolução história do que se convencionou denominar de ataque cibernético.

3.1 EVOLUÇÃO HISTÓRICA

A difusão do termo ataque cibernético é recente. Chegou junto ao avanço de recursos tecnológicos, mas sua relevância no âmbito do direito internacional só ganhou destaque com os ataques de negação de serviço direcionados contra a Estônia em 2007. Outros eventos ocorreram em seguida deram ainda mais relevo ao tema[69]. Veja-se, a seguir, um breve relato dos fatos ocorridos nos três mais famosos casos nos quais o termo ataque cibernético fora utilizado para denominar o acontecimento.

3.1.1 O caso de negação de serviço (*denial-of-service*) da Estônia em 2007

Em 2007 a Estônia se tornou vítima de diversos ataques de negação de serviço (DoS). Para um país que realiza muitos serviços por meio da *internet*, como pagar o estacionamento, e votar nos seus representantes, o ataque teve consequências muito gravosas. A negação de serviço prolongada trouxe seu sistema bancário, muitos serviços do governo e grande parte da sua mídia a um impasse. Embora

[69] ARENG, Liina. International Cyber Crisis Management And Conflict Resolution Mechanisms. In: *Peacetime Regime for State Activities in CyberSpace* (Ed. Katharina Ziolkowski). Tallinn: NATO CCD COE Publication, 2013, p. 565.

nenhuma infra-estrutura crítica tenha sido comprometida, para um estado altamente dependente de tecnologia. Os prejuízos causados foram estimados em dezenas de milhões de euros. Apesar das acusações explícitas anteriores de que a Rússia estava por trás da ofensiva, não há qualquer prova substancial de que o Kremlin está envolvido na condução do ataque além dos endereços de IP do qual emanavam as solicitações de serviços terem sido rastreados em localização geográfica Russa[70].

3.1.2 O caso da Geórgia em 2008

O caso dos ataques cibernéticos ocorridos em agosto de 2008 contra a Geórgia são paradigmáticos à medida que se inserem no contexto de um conflito armado mais amplo entre a Federação da Rússia e a Geórgia sobre a Ossétia do Sul. Foi a primeira vez que se constatou um ataque híbrido, isto é, com a concomitância do uso da força cinética juntamente com operações direcionadas a redes de computadores. Antes da invasão física, sites do governo da Geórgia foram desfigurados e ficaram sofrendo ataques de negação de serviço (DoS) que continuaram durante várias semanas após o cessar-fogo e das operações militares tradicionais. Como apontou Marco Gercke:

> De todos os ataques supramencionados, os ataques de 2008 sobre os sistemas de computadores da Geórgia são os mais próximos de serem relacionados à guerra. Durante o conflito armado, diversos outros ataques direcionados as *sites* do governo da Geórgia, bem como empresas (incluindo a desfiguração de paginas da *internet* por ataques de negação de serviço distribuída) foram descobertos. A respeito do incidente da Estônia, muito fora debatido posteriormente sobre a origem do ataque. Embora algumas notícias pereciam indicar a localização geográfica do ataque, pesquisas voltadas à tecnologia apontaram o uso de redes de computadores robotizadas no ataque, o que torna a origem muito mais difícil de se determinar. A inabilidade de se determinar a origem dos ataques, bem como o fato de terem sido descobertos atos significantemente distintos àqueles dos estados de guerra tradicionais, torna muito mais difícil de considerá-los como um estado de guerra.[71]

---

[70] DINNISS, Heather Harrison. *Cyber warfare and the law of war*. New York: Cambridge University Press, 2012, p. 289.

[71] Tradução livre do original, que verbera: "*Out of the abovementioned attacks, the 2008 attacks on computer systems on Georgia are the closest to being war-related. During the armed conflict between the Russian Federation and Georgia, several attacks targeting Georgian government websites as well as businesses (including the defacement of websites Distributed Denial of Service Attacks) were discovered. With regard to the Estonian incident, the origin of the attack was much debated*

Os ataques foram dirigidos contra diversos alvos públicos e privados, incluindo o site do presidente da Geórgia, os sites do governo central, o Ministério das Relações Exteriores, Ministério da Defesa, sites de mídia e fóruns de discussão que apoiavam a independência da Geórgia. Os métodos utilizados foram semelhantes aos utilizados nos ataques contra a Estônia em 2007. Apesar da suspeita generalizada apontar para a Rússia, a qual negou qualquer envolvimento com os ataques, parece que os ataques foram realizados por "*hackers* patriotas" sem envolvimento direto por parte das autoridades da Rússia. Alguns relatórios apontaram, ainda, para a coordenação de alto nível entre os ataques cibernéticos e as operações militares no terreno; no entanto, evidências de possível envolvimento de autoridades governamentais só é circunstancial[72].

3.1.3 *Stuxnet worm* em 2010

O *Stuxnet worm* foi considerado pela Organização do Tratado do Atlântico Norte como o *malware* mais sofisticado já encontrado[73]. O aludido *malware* foi descoberto em junho de 2010, e atacava sistemas de controle industrial. O Irã foi o alvo mais fortemente atingido do *worm*, com cerca de 60% dos servidores infectados, incluindo os das suas instalações nucleares Bashir e Natanz. A complexidade e sofisticação do *worm* e sua forma multifacetada de ataque causaram suspeita de que os autores mais prováveis seriam profissionais apoiados por Estados, muito embora ninguém tenha reivindicado oficialmente a responsabilidade[74].

O *worm* é projetado para procurar o seu alvo final e causar danos, fazendo mudanças rápidas na velocidade de rotação de motores e sabotando o

---

afterwards. Albeit some news reports seemed to pinpois the geographic origin of the attack, technology-focused research points to the use of botnets in the attack, which makes the origin much more difficult to determine. The inability to determine the origin of the attacks, as well as the fact that the discovered acts signifcantly differ from traditional warfare, makes it difficult to characterize them as cyberwarfare". GERCKE, Marco. Cybercrime, Terrorist Use of the Internet and Cyberwarfare: The Importance of Clear Distinction. *In*: VOICA, Dan-Radu (Editor). *Trends and Developments in Contemporary Terrorism*. Amsterdam: IOS Press, 2012, p. 19.

[72] DINNISS, Heather Harrison. *Cyber warfare and the law of war*. New York: Cambridge University Press, 2012, p. 290.

[73] GEERS, Kenneth. *Strategic Cyber Security*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2011, p. 24.

[74] DINNISS, Heather Harrison. *Op. cit.*, 2012, p. 291.

funcionamento normal dos sistemas de controle. Ao ajustar estas velocidades do vírus pode em última análise, provocar centrífugas utilizadas nas instalações de enriquecimento nuclear oscilarem irregularmente, causando choques entre elas, o que poderia resultar numa séria catástrofe nuclear[75].

3.2 O CONCEITO DE ATAQUE CIBERNÉTICO

Compreendido o breve histórico da evolução do que se compreende por ataque cibernético, impende analisar a disciplina jurídica do termo, a partir da definição do conceito de ataque no direito internacional humanitário, sua distinção com o que se entende por ataque armado segundo o que preleciona a Carta das Nações Unidas, viabilizando, ao final, discenir qual o real conteúdo desse termo amplamente utilizado.

3.2.1 Definindo o termo “ataque”

O Direito é feito sobre palavras. O sistema jurídico, composto por normas de conduta para regular relações sociais, depende do uso apurado das palavras, a fim de que se afira o real conteúdo de uma determinada imposição. Portanto, “o significado das palavras é frequentemente uma parte integral da análise jurídica”[76].

Posto isto, faz-se imperioso que seja elucidado o escopo do que se considera por “ataque”, para que se possa discernir o conceito de ataque cibernético, diferenciando-o do que se considera, no âmbito internacional, como ataque armado. Tal distinção tem relevo haurido da natureza belicosa de alguns conflitos internacionais, como será visto nas seguintes linhas.

---

[75] DINNISS, Heather Harrison. *Cyber warfare and the law of war*. New York: Cambridge University Press, 2012, p. 291.

[76] Tradução livre do original, que verbera: “*The meaning of words is often an integral part of legal analysis*”. WALKER, Paul A. *Rethinking Computer Network “Attack”: Implications for Law and U.S. Doctrine*. American University-Washington College of Law. National Security Law Brief, vol. 1, iss. 1, 2011, p. 33. Disponível em: <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1002&context=nslb>. Acesso em: 9.mai.2016.

De plano, impende definir o termo de “ataque”, notadamente ao evidenciar os elementos endógenos do instituto, por meio da descrição das suas características essenciais.

A codificação do termo “ataque”, no direito internacional, fora realizada inicialmente por meio das Convenções de Genebra de 1949. Esses tratados consistem em quatro instrumentos principais e três protocolos adicionais, que estabelecem padrões de direito internacional para o tratamento humanitário durante as guerras. Trata-se da estrutura fundante do direito internacional humanitário, cuja valia é bem representada nas lições de Thiago Carvalho Borges[77], veja-se:

> O direito internacional humanitário situa-se num polo de tensão entre a necessidade militar e os objetivos humanitários de suas regras. Objetiva a redução do sofrimento dos envolvidos, tendo em mente que a eliminação das mazelas é impossível, a não ser pela inexistência do próprio conflito. Portanto, as normas humanitárias não visam tornar impossível, nem mais justo, o exercício do direito de guerra, mas tão somente mais humano.

O protocolo adicional I às Convenções de Genebra estabeleceu, em seu artigo 49, parágrafo 1, que “ataques” significam “atos de violência contra o adversário, quer seja ofensivo ou defensivo”[78] Essa definição acaba por ser amplamente aceita pois se aplica aos 169 países que ratificaram o protocolo adicional I, bem como por ser considerada parcela fundamental as normas consuetudinárias que regem os conflitos armados[79]. Nos comentários ao aludido instrumento, elaborados em 1987, o Comitê Internacional da Cruz Vermelha aduziu que a única controvérsia na elaboração do texto foi o termo “contra o adversário”, mas a manutenção do retromencionado excerto fora decidida por 38 (trinta e oito) votos a favor, 18 (dezoito) votos em contrário e 10 (dez) abstenções[80].

---

[77] BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011, p.235.

[78] O texto original verbera que “ataques” são “[…] *acts of violence against the adversary, whether in offence or in defence*”. Protocolo Adicional I às Convenções de Genebra de 1949, artigo 49, parágrafo 1. Disponível em: <https://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=17E741D8E459DE2FC12563CD0051DC6C>. Acesso em: 9.mai.2016.

[79] WALKER, Paul A. *Rethinking Computer Network “Attack”: Implications for Law and U.S. Doctrine*. American University-Washington College of Law. National Security Law Brief, vol. 1, iss. 1, 2011, p. 34. Disponível em: <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1002&context=nslb>. Acesso em: 9.mai.2016.

[80] Comentários de 1987 do Comitê Internacional da Cruz Vermelha às disposições do Protocolo Adicional I às Convenções de Genebra de 1949. Disponível em: <https://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F5EA0CB6C1075C59C12563CD004345C3>. Acesso em: 9.mai.2016.

A controvérsia se repetiu em outras oportunidades. Em 1994, o Instituto Internacional de Direito Humanitário reuniu um grupo de juristas internacionais e especialistas navais para elaborar o Manual de Sanremo sobre o Direito Internacional Aplicável aos Conflitos Armados no Mar define, em sua seção V, parágrafo 13, alínea “b”, que “ataque” significa “ato de violência, quer seja ofensivo ou defensivo”[81]. Vê-se, assim, que fora decidida a exclusão do excerto controverso, que exigia que o ato de violência fosse contra o adversário.

Mais recentemente, nos idos anos de 2009, o Programa de Pesquisa em Políticas e Conflitos Humanitários da Universidade de Harvard elaborou um Manual sobre o Direito Internacional Aplicável à Guerra Aérea e por Mísseis, onde quedou consignado, na seção “A”, parágrafo 1, alínea “e”, a mesma dicção do Manual de Sanremo, considerando como “ataque” o “ato de violência, quer seja ofensivo ou defensivo”[82].

Posto isto, é curial salientar que a regra geral de interpretação das disposições codificadas impõe que os termos sejam considerados em seus significados ordinários, como verbera o artigo 31 da Convenção de Viena de 1969 sobre o Direito dos Tratados[83]. Nesse sentido, a Corte Internacional de Justiça decidiu que:

> [...] o primeiro dever de um tribunal que é chamado para interpretar e aplicar as disposições de um tratado é empreender esforços para dar efeito a elas no seu significado ordinário e natural, no contexto em que elas ocorreram. Se as palavras relevantes em seu significado ordinário e natural fazem sentido naquele contexto, isso encerra o assunto. Se, por outro lado, as palavras em seu significado ordinário e natural são ambíguas ou levam a um resultado desarrazoado, então, e apenas assim, a Corte deverá, recorrendo a outros métodos de interpretação, buscar determinar o que as partes realmente queriam dizer quando usaram aquelas palavras.[84]

---

[81] O texto original verbera que "'*attack' means an act of violence, whether in offence or in defence*". Manual de Sanremo sobre o Direito Internacional Aplicável aos Conflitos Armados no Mar de 1994, Seção V, parágrafo 13, alínea “b”. Disponível em: <http://assets.cambridge.org/97805215/58648/excerpt/9780521558648_excerpt.pdf>. Acesso em: 9.mai.2016.

[82] O texto original verbera que "'*attack' means an act of violence, whether in offence or in defence*". Manual sobre o Direito Internacional Aplicável à Guerra Aérea e por Mísseis de 2009, Seção A, parágrafo 1, alínea “e”.

[83] Convenção de Viena sobre o DIreito dos Tratados de 1969, artigo 31.

[84] Tradução livre do original, que verbera: “[...] *the first duty of a tribunal which is called upon to interpret and apply the provisions of a treaty, is to endeavour to give effect to them in their natural and ordinary meaning in the context in which they occur. If the relevant words in their natural and ordinary meaning make sense in their context, that is an end of the matter. If, on the other hand, the words in their natural and ordinary mean- ing are ambiguous or lead to an unreasonable result, then, and then only, must the Court, by resort to other methods of interpretation, seek to ascertain what the parties really did mean when they used these words*”. CORTE INTERNACIONAL DE JUSTIÇA. *Competence*

Åssim, as palavras devem ser compreendidas em seu significado ordinário e natural, mas permite implicações diferentes, notadamente quando o contexto na qual estão insertas permite uma conclusão diferente[85]. Há de se analisar, assim, o cerne da definição amplamente aceita de "ataque", a fim de destacar qual a acepção que comumente se dá ao termo.

Examinando todos os congruentes significados da palavra "ataque" (trazidos pelo Protocolo Adicional I às Convenções de Genebra de 1949, pelo Manual de Sanremo sobre o Direito Internacional Aplicável aos Conflitos Armados no Mar de 1994 e pelo Manual sobre o Direito Internacional Aplicável à Guerra Aérea e por Mísseis de 2009), infere-se que o elemento central que guia toda a estrutura definidora são os "atos de violência". As esclarecedoras lições de Paul A. Walker tornam cristalino que "[...] um ataque precisa ser um passo afirmativo, porque, em seu sentido comum, um ato é fazer algo, normalmente de forma voluntária. No caso de um ataque, o que é feito é violência, ou um esforço de força física de modo a prejudicar ou explorar"[86].

O outro elemento incontroverso da definição de ataque no direito internacional humanitário consiste na categorização ofensiva ou defensiva deste, uma vez que os supramencionados atos devem ser ofensivos ou defensivos. O grande marco dessa definição é permitir que os ataques sejam considerados como tal tanto por iniciativa do agente que instaura o ato belicoso como por aquele que apenas repele, violentamente, a agressão sofrida. A definição estabelece, assim, um:

> [...] escopo mais amplo uma vez que – justificadamente – abrange atos defensivos (particularmente "contra-ataques") bem como os atos ofensivos, eis que ambos podem afetar a população civil. É por essa razão que a escolha final foi por uma definição ampla.[87]

---

of the General Assembly for the Admission of a State to the United Nations. Parecer consultivo de 3 de março de 1950. ICJ Reports n. 33, p. 8.

[85] GARDINER, Richard. *Treaty Interpretation*. 2. ed. New York: Oxford University Press, 2015, p. 182.

[86] O texto original verbera que "[...] *an attack must be an affirmative step, because, in its ordinary sense, an "act" is "the doing of a thing," usually voluntarily. In the case of an "attack," what is done is "violence," or an "exertion of physical force so as to injure or abuse*". WALKER, Paul A. *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*. American University-Washington College of Law. National Security Law Brief, vol. 1, iss. 1, 2011, p. 39. Disponível em: <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1002&context=nslb>. Acesso em: 9.mai.2016.

[87] Tradução livre do original, que verbera: "[...] *wider scope since it -- justifiably -- covers defensive acts (particularly "counter-attacks") as well as offensive acts, as both can affect the civilian population. It is for this reason that the final choice was a broad definition*". Comentários de 1987 do Comitê Internacional da Cruz Vermelha às disposições do Protocolo Adicional I às Convenções de Genebra de 1949. Disponível em:

Por último, deve-se analisar o mais problemático elemento que define o termo "ataque", tal como amplamente aceito no direito internacional, é o requisito trazido pelas Convenções de Genebra de 1949 de que este seja "contra o adversário". Muito embora tal exigência tenha sido expressamente verberada pelo artigo 49, parágrafo 1, do aludido instrumento normativo internacional, a sua aceitação no texto fora amplamente debatida. "Aqueles que queriam deletar as palavras argumentavam que a disposição da Seção do Protocolo deveria se aplicar à população civil de todas as partes do conflito, incluindo a população civil da própria parte envolvida"[88]. Contudo, o parágrafo 2 do mencionado artigo 49 tratou de solucionar o problema, ao determinar que as disposições concernentes a ataques "se aplicam a todos os ataques em qualquer território que seja conduzido, incluindo o território nacional pertencente à parte do conflito mas sob o controle de uma parte adversária" [89].

Percebe-se, assim, que há três elementos definidores do termo "ataque", quais sejam, devem ser "atos de violência" conduzidos "ofensivamente ou defensivamente", sendo necessário – para o direito internacional humanitário – que seja realizado "contra o adversário". Enquanto a ação violenta é o elemento central, as características de serem em ataque ou contra-ataque, bem como ser realizado em face do oponente, são elementos periféricos[90].

Não obstante, pela análise do Manual de Sanremo sobre o Direito Internacional Aplicável aos Conflitos Armados no Mar de 1994 e do Manual sobre o Direito

---

<https://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F5EA0CB6C1075C59C12563CD004345C3>. Acesso em: 9.mai.2016.

[88] Tradução livre do original, que verbera: "[...]*Those who wished to delete the words argued that the provisions of this Section of the Protocol should apply to the civilian population of all the Parties to the conflict, including the civilian population of the Party concerned*". Comentários de 1987 do Comitê Internacional da Cruz Vermelha às disposições do Protocolo Adicional I às Convenções de Genebra de 1949. Disponível em: <https://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F5EA0CB6C1075C59C12563CD004345C3>. Acesso em: 9.mai.2016.

[89] Tradução livre do texto original, que verbera: "*The provisions of this Protocol with respect to attacks apply to all attacks in whatever territory conducted, including the national territory belonging to a Party to the conflict but under the control of an adverse Party.*". Protocolo Adicional I às Convenções de Genebra de 1949, artigo 49, parágrafo 2. Disponível em: <https://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=17E741D8E459DE2FC12563CD0051DC6C>. Acesso em: 9.mai.2016.

[90] WALKER, Paul A. *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*. American University-Washington College of Law. National Security Law Brief, vol. 1, iss. 1, 2011, p. 39. Disponível em: <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1002&context=nslb>. Acesso em: 9.mai.2016.

Internacional Aplicável à Guerra Aérea e por Mísseis de 2009, infere-se uma tendência crescente no direito internacional público de dispensar o requisito de que o ataque seja "contra o adversário", podendo ser definido apenas por um elemento central (ato de violência) e um periférico (ofensivo ou defensivo).

Repise-se que a importância dessa definição tem particular relevo no contexto do direito internacional humanitário, isto é, o direito que rege os conflitos armados visando mitigar o sofrimento humano desnecessário uma vez que o estado belicoso tenha sido instaurado (*jus in bello*)[91]. Muito embora ela seja uma baliza importante para a compreensão geral do termo, sua definição não se aplica com a mesma precisão sobre o conceito de ataque armado. Enquanto o termo "ataque", *per se*, é inerente ao *jus in bello*, o "ataque armado" é compreendido na noção das normas que regulam quando os Estados poderão recorrer à força para conduzir suas políticas nacionais, ou *jus ad bellum*[92].

A definição de ataque trazida nas Convenções de Genebra de 1949, mesmo que excluída a sua parte controversa, também não se subsome de forma aprumada àquilo que se considera como ataque cibernético, notadamente diante da dificuldade de se adequar o requisito de "atos de violência" ao âmbito informacional[93]. Com efeito, existem operações que podem ser dirigidas contra redes de computadores que acarretem gravosos prejuízos à parte atacada, mas que, pela ausência de força cinética, não seja vista como suficientemente violenta para configurar um ataque para o direito internacional humanitário.

Superada a definição do termo ataque no direito internacional, de grande relevo ao *jus in bello*, impende analisar, separadamente, o que se compreende por ataque armado no contexto da Carta das Nações Unidas, diferenciando-o, em seguida, ao instituto do ataque cibernético.

---

[91] JANIS, Mark Weston. *An Introduction to International Law*. 4. ed. New York: Aspen Publishers, 2003, 183.

[92] SCHMITT, Michael N. *"Attack" as a Term of Art in International Law: The Cyber Operations Context*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012, p. 284.

[93] WALKER, Paul A. *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*. American University-Washington College of Law. National Security Law Brief, vol. 1, iss. 1, 2011, p. 39. Disponível em: <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1002&context=nslb>. Acesso em: 9.mai.2016.

3.2.2 Conceito de ataque armado

No século XIX, sobretudo no contexto pré-guerras na Europa, atos de força e o recurso à guerra prevaleciam como atributos inerentes aos Estados, e eram considerados como uma forma legítima de solução de disputa[94]. Todavia, diante do crescente anseio coletivo de se estabilizar as tensões e conferir maior segurança às relações entre as nações, surgiu um crescente anseio de que as guerras fossem proscritas, sendo substituída por meios heterônomos de resolução de disputas (como a arbitragem e o julgamento estatal) uma vez que a sociedade tinha se tornado bastante avançada[95].

A normatização da proibição da guerra como recurso legítimo e inerente aos poderes ordinários do Estado foi realizada de forma gradativa. Em 1899, na Primeira Conferência para a Paz ocorrida em Haia, "ficou determinada a proscrição da guerra como ato de solução de conflitos, mas muitas normas de regulamentação de atos de guerra foram adotadas"[96]. A despeito de ter representado considerável avanço, tal disposição não teve eficácia plena para toda a sociedade internacional, haja vista que no Pacto da Liga das Nações de 1919 ainda permitia o recurso à guerra como direito inerente ao Estado, desde que esgotados alguns procedimentos previstos no próprio instrumento do acordo[97].

Um importante marco do desenvolvimento da proscrição da guerra sucedeu em 1928, com o Tratado Geral de Renúncia à Guerra, conhecido como Pacto Kellogg-Briand. O artigo I do aludido instrumento condenava que as nações recorressem à guerra para a solução de controvérsias internacionais, determinando, ainda, a renúncia desses meios belicosos como instrumento de política nacional na condução das relações entre Estados[98]. Igual importância teve o artigo II, ao estabelecer que

---

[94] BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p. 744.
[95] JANIS, Mark Weston. *An Introduction to International Law*. 4. ed. New York: Aspen Publishers, 2003, p. 172.
[96] BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011, p. 234.
[97] BROWNLIE, Ian; CRAWFORD, James. *Op. cit.*, 2012, p. 744.
[98] O texto original do artigo I verbera: "*ARTICLE I - The High Contracting Parties solemly declare in the names of their respective peoples that they condemn recourse to war for the solution of international controversies, and renounce it, as an instrument of national policy in their relations with one another*". Tratado Geral de Renúncia à Guerra de 1929 (Pacto Kellogg-Briand), artigo I.

“a resolução ou solução de todas as disputas ou conflitos de qualquer natureza ou de qualquer origem que seja, os quais possam surgir entre eles [os Estados], jamais deverão ser obtidos por meios que não sejam pacíficos”[99].

Mas tais aspirações positivadas em tratados se demonstraram insuficientes para evitar que as nações recorressem a meios belicosos na tentativa de solucionar suas desavenças, e falharam ao não inibirem as mazelas ocorridas entre 1939 e 1945 na Segunda Guerra Mundial. Isso ocorreu, em grade parcela, pela disparidade entre as teorias do direito da guerra e a realidade das relações internacionais[100].

Foi no contexto do pós Segunda Guerra Mundial que um mecanismo mais eficiente de proibição dos atos de guerra, como leciona Thiago Carvalho Borges, *verbis*:

> Após a Segunda Grande Guerra, a Carta das Nações Unidas determinou a proibição formal e extensiva dos atos de guerra, tornando-a, em definitivo, um ilícito internacional, por força do art. 2º, § 4º, que determina que os membros da Organização abster-se-ão de recorrer à ameaça ou ao uso da força contra a integridade territorial ou a independência de qualquer Estado, ou de qualquer outra forma incompatível com os propósitos das Nações Unidas.

Vê-se, portanto, que o estabelecimento de uma sociedade internacional mais estruturada, e pautada em princípios previstos no seu instrumento constitutivo, representaram grande avanço à proscrição dos atos de guerra, notadamente quando a proibição do uso da força fora elencada como um dos princípios regentes da Organização, para que seja viabilizada a consecução de seu proposito precípuo, qual seja, a manutenção da paz e da segurança internacional, como disposto no artigo 1º, § 1º, do instrumento constitutivo da ONU. Veja-se a transcrição da norma principiológica elencada no artigo 2º, § 4º, da Carta das Nações Unidas[101]:

> Artigo 2

Disponível em: <https://www.uni-marburg.de/icwc/dateien/briandkelloggpact.pdf>. Acesso em: 11.mai.2016.

[99] Tradução livre do original, que verbera: “[…] *the settlement or solution of all disputes or conflicts of whatever nature or of whatever origin they may be, which may arise among them, shall never be sought except by pacific means*”. Tratado Geral de Renúncia à Guerra de 1929 (Pacto Kellogg-Briand), artigo II. Disponível em: <https://www.uni-marburg.de/icwc/dateien/briandkelloggpact.pdf>. Acesso em: 11.mai.2016.

[100] JANIS, Mark Weston. *An Introduction to International Law*. 4. ed. New York: Aspen Publishers, 2003, 175.

[101] Tradução livre do original, que verbera: “*Article 2 – The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles. [...] 4. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political inde- pendence of any state, or in any other manner inconsistent with the Purposes of the United Nations*”. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Carta das Nações Unidas*, artigo 2, § 4º.

> A Organização e seus Membros, em busca dos Propósitos mencionados no Artigo 1, deverão agir de acordo com os seguintes Princípios.
>
> [...]
>
> 4. Todos os Membros devem se abster, nas suas relações internacionais, da ameaça ou uso da força contra a integridade territorial e independência política de qualquer estado, ou em qualquer outra maneira inconsistente com os Propósitos das Nações Unidas.

Muito embora o uso de atos de guerra como política estatal tenha sido proscrito, ainda há duas alternativas que viabilizam o uso da força no âmbito da Organização das Nações Unidas, quais sejam, a autorização do uso da força pelo Conselho de Segurança da ONU, em consonância com o procedimento previsto no artigo 39 e seguintes da Carta, e o uso da força em legítima defesa a um "ataque armado", previsto no artigo 51 do mesmo instrumento normativo. É daí que surge o conceito de ataque armado no âmbito do direito internacional público.

O presente trabalho não pretende analisar a possibilidade de uso da força com a autorização do Conselho de Segurança por dois motivos: o primeiro é que ele legitimaria o ato belicoso, afastando-o da ilicitude necessária para a aplicação das normas sobre responsabilidade internacional, e segundo pois ele não concerne necessariamente à definição do termo "ataque" no direito internacional, o que não auxilia a compreensão futura do que é um "ataque cibernético". O escopo deste tópico é, tão somente, permitir que se entenda o contexto histórico e o conceito do ataque armado, permitindo distingui-lo dos demais institutos jurídicos internacionais.

Como fora mencionado, o conceito de ataque armado surgiu como requisito imprescindível à legalidade do uso da força em legítima defesa, como se infere da disposição do artigo 51 da Carta das Nações Unidas[102], *in verbis*:

> Artigo 51
>
> Nada na presente Carta deve prejudicar o direito inerente de legítima defesa individual ou coletiva se um ataque armado ocorrer contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho

[102] Tradução livre do original, que verbera: "*Article 51 –Nothing in the present Charter shall impair the inherent right of individual or collective self- defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to main- tain or restore international peace and security*". ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Carta das Nações Unidas*, artigo 2, § 4º.

> de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais.

Ocorre que da análise de toda Carta, infere-se que não há qualquer menção ao que seria um ataque armado. Essa lacuna traz imprecisão à determinação do escopo do instituto[103], o que dificulta o estabelecimento de uma noção universal e homogênea que facilite a sua aplicação no âmbito internacional, sem que haja controvérsias sobre a subversão do seu real sentido. Como leciona Heather Harrison Dinniss[104]:

> [...] assim como com o termo 'força', a Carta não estabelece uma definição para 'ataque armado'. Ademais, os antecessores históricos do sistema da Carta não oferecem nenhum auxílio interpretativo. Nem o Pacto Kellogg-Briand nem o Pacto da Liga das Nações se referem ao termo. Ambos formulam a legítima defesa como uma resposta à agressão; então, todas as tentativas de definição foram focadas nesse termo.

Não obstante haja grande parte da doutrina que se utilize do conceito de agressão para compreender o "ataque armado", a associação entre os termos não é tida como absoluta[105]. O anexo à Resolução n. 3314 (XXIX) da Assembléia Geral da ONU sobre a definição de agressão traz um texto muito parecido com aquele veiculado no artigo 2º, § 4º, da Carta. Com efeito, o artigo 1 do aludido anexo define agressão como "[…] o uso de força armada por um Estado contra a soberania, integridade territorial ou independência política de outro Estado, ou em qualquer outra maneira inconsistente com a Carta das Nações Unidas, como disposto nessa Definição"[106]. '

A Corte Internacional de Justiça não se apartou dessa definição, utilizando a noção de agressão trazida no anexo da Resolução n. 3314 (XXIX) da Assembléia Geral da ONU nos seus julgamentos para abalizar o conceito de "ataque armado". No caso

---

[103] ÖYKÜIRMAKKESEN. *The Notion of Armed Attack under the UN Charter and the Notion of International Armed Conflict – Interrelated or Distinct?*. Geneva: Geneva Academy, 2014, p. 3. Disponível em: <http://www.prix-henry-dunant.org/sites/prixhd/doc/2014_IRMAKKESEN_Paper.pdf>. Acesso em: 11.mai.2016.

[104] Tradução livre do original, que verbera: "[…] *as with the term 'force', the Charter does not provide a definition of 'armed attack'. Further, the historical predecessors to the Charter system do not offer any interpretive assistance. Neither the Kellogg-Briand Pact nor the Covenant of the League of Nations refer to the term. Both formulate self-defence as a response to aggression; hence all attempts at definition were focused on that term*". DINNISS, Heather Harrison. *Cyber warfare and the law of war*. New York: Cambridge University Press, 2012, p. 77.

[105] BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p. 749.

[106] Tradução livre do original, que verbera: "[...] *the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition*". ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembléia Geral. *Resolução n. 3314 (XXIX): Definição de Agressão*. Anexo, artigo 1.

relativo às *Military and Paramilitary Activities in and against Nicaragua*, a CIJ além de asseverar que a definição de agressão constitui norma costumeira internacional, assentou que a proibição de ataques armados se aplica sempre que constatadas a dimensão e efeitos necessários, veja-se:

> […] a Definição de Agressão anexada à resolução 3314 (XXIX) da Assembléia Geral, pode ser considerada como refletindo o direito costumeiro internacional. A Corte não vê razão para negar que, no direito consuetudinário, a proibição de ataques armados pode se aplicar ao envio por um Estado de grupos armados ao território de outro Estado, se tal operação, por causa de sua dimensão e efeitos, fosse classificada como um ataque armado ao invés de um mero incidente de fronteira se fosse conduzido por forças armadas regulares.[107]

Como se depreende do excerto transcrito acima, é necessário que o ataque armado atinja a dimensão e efeitos necessários para ser classificado como tal. Isso pois, na mesma decisão, a Corte considerou que o ataque armado é a forma mais grave de uso da força[108]. Saliente-se que o ônus de provar a ocorrência do ataque armado, demonstrando qual seria a gravosidade da conduta forçosa, reside com o Estado que pretende usar ou já fez uso da força em legítima-defesa, como afirmou a própria Corte Internacional de Justiça no caso referente às *Oil Platforms* [109].

A principal questão posta, então, no que pertine ao presente trabalho, é sobre a possibilidade de ataques cibernéticos serem considerados como ataques armados.

Analisando todas as normas expostas, não se vislumbra qualquer óbice à configuração de um ataque armado mesmo que a força seja utilizada exclusivamente pelo âmbito cibernético. Deve se atentar, contudo, à necessidade de que o uso da força, mesmo veiculado por redes de computadores, alcance a dimensão e efeitos necessários para ser considerado um ataque armado, tal como

---

[107] Tradução livre do original, que verbera: "[…] *the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law. The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces*". CORTE INTERNACIONAL DE JUSTIÇA. *Case concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. Estados Unidos). Decisão de mérito de 1986. ICJ Reports n. 520, p. 93, § 195.

[108] *Ibidem*, p. 22, § 39.

[109] CORTE INTERNACIONAL DE JUSTIÇA. *Oil Platforms* (República Islâmica do Irã v. Estados Unidos da América). Julgamento de 6 de novembro de 2003. ICJ Reports n. 876, p. 189.

ocorre nas condutas cinéticas. Compartilha desse entendimento a pesquisadora pós doutoral Heather Harrison Dinniss[110], notadamente ao afirmar que:

> [...] o patamar de um ataque armado conduzido por um ataque de rede de computadores deve ser estabelecido em conformidade com o direito internacional atual que regula o direito à legítima defesa. Um Estado está autorizado a responder em legítima defesa quando ele é vítima de um ataque de rede de computadores causando danos à propriedade ou pessoas em dimensão e efeitos suficientes para elevá-lo além do equivamente a um incidente de fronteira.

O posicionamento de que tal força armada não precisa ser necessariamente cinética já havia sido verberado pela Corte Internacional de Justiça, no parecer consultivo sobre a Legalidade da Ameaça ou Uso de Armas Nucleares (originalmente denominado de *Legality of the Threat or Use of Nuclear Weapons*). Naquela ocasião, a Corte foi consultada para se pronunciar sobre a eventual violação de armas nucleares, distintamente diante da radioatividade que sucede a sua utilização – e que, muito embora possa causar danos físicos, não é necessariamente cinética –, à proibição do uso da força, bem como se sua utilização configuraria a forma mais grave de ataque armado. Em parecer, fora veiculado o entendimento que as normas que proscrevem os atos belicosos "se aplicam a qualquer uso da força, independentemente das armas utilizadas" [111], restando cristalino que, caso um ataque cibernético seja considerado uso da força, por sua dimensão e efeitos, poderá ser considerado como um ataque armado. O exemplo prático do Conselheiro Geral do Departamento de Defesa dos Estados Unidos auxilia na compreensão e elucidação de como seria um ataque cibernético que alcançaria o patamar de um ataque armado, veja-se:

> [...] se um ataque de rede de computadores coordenado derruba o sistema de controle de tráfego aéreo nacional junto com seus sistemas financeiro e bancário, e de utilidades públicas, e abre comportas de diversas represas, resultando num alagamento geral que causa mortes civis e danos à propriedade generalizados, é possível que ninguém iria contestar que a nação vitimada se ela concluísse que foi vítima de um ataque armado, ou de um ato equivalente a um ataque armado.[112]

---

[110] Tradução livre do original, que verbera: "[…] *the threshold for an armed attack conducted by a computer network attack must be set in line with current international law regulating the right of self-defence. A state is therefore permitted to respond in self defence when it is victim of a computer network attack causing damage to property or persons of suficient scale and effect to elevate it beyond the equivalent of a frontier incident*". DINNISS, Heather Harrison. *Cyber warfare and the law of war*. New York: Cambridge University Press, 2012, p. 81.

[111] CORTE INTERNACIONAL DE JUSTIÇA. *Legality of the Threat or Use of Nuclear Weapons*. Parecer consultivo de 8 de julho de 1996. ICJ Reports n. 679. p. 244, § 38, e p. 263, § 96.

[112] Tradução livre do original, que verbera: "[...] *if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and*

É inconteste, portanto, a possibilidade do ataque cibernético ser considerado um ataque armado. Contudo, "o significado de 'ataque armado' permanence controverso […]. Com a escassez de dedicação ao assunto além de uma resolução na Assembléia Geral, parece que a questão sera avaliada com base em cada caso concreto"[113]. Assim, a análise do alcançe aos requisitos de dimensão e efeitos ainda é intrincada no âmbito das redes de computadores e, conforme aduziu o professor Daniel Ryan, da Universidade de Defesa Nacional dos Estados Unidos, "nós não sabemos quando ou se o ataque cibernético alcança o patamar de um 'ataque armado'"[114].

Esclarecido o escopo do conceito de ataque armado no direito internacional, passa-se à análise detida do conceito de ataque cibernético.

3.2.3 O conceito de ataque cibernético

O Manual de *Tallinn* explana que "ataque cibernético" é todo evento que ocasiona mortes ou causa dano a objetos[115]. Aqui não se pretende estudar o conceito de ataque cibernético como ataque armado no direito internacional, uma vez que o estudo desse instituto só seria relevante para legitimar o uso da força no âmbito da ONU.

Utiliza-se, aqui, o conceito de ataque cibernético como utilizado na prática das relações internacionais, compreendendo operações realizadas por meio da *internet*.

---

opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack". ESTADOS UNIDOS. *An Assessment of International Legal Issues in Information Operations*. Departamento de Defesa dos Estados Unidos, 1999, p. 18. Disponível em: <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf>. Acesso em: 11.mai.2016.

[113] Tradução livre do original, que verbera: "*The meaning of 'armed attack' remains controversial* […]. *Short of a dedicated resolution on the subject from the General Assembly, it appears that the question will be assessed on a case by case basis*". BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p. 749.

[114] Tradução livre do original, que verbera: "*We don't know when or if a cyberattack rises to the level of an 'armed attack'*". GJELTEN, Tom. *Extending the Law of War to Cyberspace*. NPR, edição de 22.set.2010. Disponível em: <http://www.npr.org/templates/story/story.php?storyId=130023318>. Acesso em: 11.mai.2016.

[115] ORGANIZAÇÃO DO TRATADO DA AMÉRICA DO NORTE. Grupo de Especialistas Internacionais. Tallinn Manual on the International Law Applicable to Cyber Warfare (Editor geral Michael N. Schmitt). 1. ed. New York: Cambridge University Press, 2013, p. 106.

Essas operações podem ter intensidades altas, assim compreendidos aqueles que podem vir a causar danos a pessoas ou objetos, bem aqueles considerados de baixa intensidade, como, por exemplo, ataques que obstam o acesso a serviços prestados por meio da *internet* momentaneamente.

O professor Jack Goldsmith, da Universidade de Harvard, afirmou que:

> Se as nações não sabem quais são as regras, todos os tipos de problemas acidentais podem surgir [...]. Uma nação pode fazer algo que outra nação recebe como um ato de guerra, mesmo quando a primeira nação não pretendia que fosse um ato de guerra.[116]

Vê-se, portanto, que para se configurar um ataque cibernético para o contexto do Manual de Tallinn, é necessário que haja uma operação cibernética que cause danos a pessoas ou objetos. Qualquer operação conduzida pela internet que não alcance esse critério não será considerada um ataque cibernético para os fins do aludido Manual.

Infere-se, portanto, que o que os Estados utilizam como retórica denominando de "ataque cibernético" são, na verdade, operações cibernéticas conduzidas pelos Estados. Como se infere da filosofia de Ludwig Witgenstein[117]:

> O homem possui a capacidade de construir linguagens com as quais pode expressar qualquer sentido sem ter nenhuma noção de como e do que significa cada palavra. – Tal como se fala sem se saber como os sons individuais são produzidos.
>
> [...]
>
> A linguagem mascara o pensamento. E tanto assim que da forma exterior da roupa não se pode deduzir a forma do pensamento mascarado; porque a forma exterior da roupa é concebida não para deixar reconhecer a forma do corpo, mas para fins inteiramente diferentes.

Assim, resta cristalino que os Estados subvertem o conceito de ataque cibernético, adequando-os a todos os tipos de operação. Da análise do Manual de Tallinn, somente podem ser considerados ataques cibernéticos as operações conduzidas pela *internet* que causam danos a objetos ou a pessoas.

---

[116] Tradução livre do original, que verbera: "*If nations don't know what the rules are, all sorts of accidental problems might arise* [...]*. One nation might do something that another nation takes to be an act of war, even when the first nation did not intend it to be an act of war*". GJELTEN, Tom. *Extending the Law of War to Cyberspace*. NPR, edição de 22.set.2010. Disponível em: <http://www.npr.org/templates/story/story.php?storyId=130023318>. Acesso em: 11.mai.2016.

[117] WITTGENSTEIN, Ludwig. *Tratado filosófico*. 2. ed. Lisboa: Fundação Caloste Gulbenkian, 1995, p. 52.

4 RESPONSABILIDADE INTERNACIONAL DOS ESTADOS

A ideia primaz de responsabilidade é que aquele que causou dano, cometendo ato ilícito, deverá responder pelos prejuízos causados.

Nas “relações internacionais assim como em outras relações sociais, a violação da esfera jurídica de um sujeito de direito por outro cria responsabilidade em forma e alcance determinados pelo sistema jurídico aplicável“[118]. Essa transgressão, quando considerada ilegal, tem incidência e consequências jurídicas determinadas pelo que se convencionou chamar de direito da responsabilidade internacional[119].

No âmbito internacional, ação ou omissão contrárias às obrigações de um Estado lhe atribui responsabilidade[120]. É esse, em síntese, o escopo da responsabilidade internacional – instituto que se aplica igualmente aos Estados, sujeitos primários de direito internacional, bem como às organizações internacionais[121]. Tal entendimento restou incontroverso no julgamento, pela Corte Internacional da Justiça, do caso *Reparation for Injuries Suffered in the Service of the United Nations*[122].

Para os fins propostos nesse trabalho, faz-se imperiosa a análise precípua da responsabilidade internacional dos principais sujeitos do Direito Internacional: os Estados. Contudo, algumas considerações acerca do instituto às organizações internacionais serão salutares para a melhor compreensão do tema.

Não se tem, no Direito Internacional, uma autoridade central da qual emanam as normas e que imponha seu poder coercitivo para evitar seu descumprimento. Na sociedade internacional, incumbe aos Estados (e demais sujeitos de direito) responderem àqueles que infringem as regras vigentes, de modo que a eficácia do

---

[118] Tradução livre do original, em inglês, que verbera “*In international relations, the invasion of the legal interest of one subject of the law by another creates responsibility in a form and to an extent determined by the applicable legal system.* [...]”, vide BROWNLIE, Ian; CRAWFORD, James. *Brownlie’s Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p.539.

[119] JANIS, Mark Weston. *An Introduction to International Law*. 4. ed. New York: Aspen Publishers, 2003, 189.

[120] BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011, p.239 *et seq*.

[121] REZEK, Francisco. *Direito Internacional Público: curso elementar*. 14. ed. São Paulo: Saraiva, 2013, p.321.

[122] CORTE INTERNACIONAL DE JUSTIÇA. *Reparation for Injuries Suffered in the Service of the United Nations*. Parecer consultivo de 11 de abril de 1949. ICJ Reports n. 17, p. 184-185.

âmbito jurídico internacional está estritamente relacionada com o instituto da responsabilidade internacional[123].

Desse modo, "A responsabilidade internacional visa, portanto, a contribuir para a aplicação prática das normas internacionais e a promover a eventual reparação dos prejuízos sofridos pelos sujeitos de Direito Internacional"[124].

O aludido instituto, diante da ausência de norma positiva cogente em vigor, caracteriza-se por ser consuetudinário, não somente através da difundida prática estatal mas considerando, principalmente, sua natureza política[125].

Até os idos de 2001, poucas regras existiam regulando a responsabilidade internacional, de modo que não se desenvolvia um estudo expressivo do instituto[126]. Contudo, desde 2001, com o trabalho desenvolvido pela Comissão de Direito Internacional (CDI) da Organização das Nações Unidas (ONU) – que tem servido como diretriz internacional acerca do tema – a construção doutrinária acerca do tema vem ganhando crescente relevo[127].

4.1 PROJETO DE ARTIGOS DA ONU

Visando normatizar a responsabilidade dos Estados em decorrência de atos que acarretem no descumprimento de suas obrigações internacionais, a CDI adotou três principais documentos. São eles: o Projeto (*draft*) de Artigos sobre Responsabilidade Internacional do Estado por Atos Internacionalmente Ilícitos de 2001[128], os Artigos

---

123 MAZZUOLI, Valério de Oliveira. *Curso de Direito Internacional Público*. 7. ed. São Paulo: Revista dos Tribunais, 2013, p.586.
124 PORTELA, Paulo Henrique Gonçalves. *Direito Internacional Público e Privado*. 5. ed. Salvador: JusPodivm, 2013, p. 382.
125 SILVA, Roberto Luiz. *Direito Internacional Público*.4. ed. Belo Horizonte: Del Rey, 2014, p.355.
126 HARRIS, David. *Cases and Materials on International Law*. 7. ed. London: Sweet & Maxwell, 2010, p. 421.
127 BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p.539.
128 COMISSÃO DE DIREITO INTERNACIONAL. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.

sobre Proteção Diplomática de 2006 e o Projeto de Artigos sobre Responsabilidade das Organizações Internacionais de 2011[129].

É pacífico que os trabalhos da CDI resultaram em um grande avanço da responsabilidade internacional como um instituto do Direito Internacional[130], servindo de influência não somente para a doutrina, como para tribunais internacionais (a exemplo da Corte Internacional de Justiça)[131].

O trabalho mais relevante da CDI para o desenvolvimento do instituto é o Projeto de Artigos sobre Responsabilidade Internacional do Estado por Atos Internacionalmente Ilícitos de 2001 (eventualmente denominado de *draft*, ou projeto, eis que o texto ainda não fora oficialmente adotado). Trata-se de instrumento de primaz importância para o direito internacional, dotando-o de maior rigor jurídico, na medida em que confere eficácia às normas que estabelecem obrigações para os Estados[132].

Incumbe, aqui, expor alguns dos assuntos tratados no *draft*, tais como, *inter alia*, os elementos da responsabilidade internacional, a caracterização do descumprimento de obrigações internacionais ensejadoras de responsabilidade, a questão da atribuição e as excludentes de responsabilidade internacional.

4.2 CONCEITO DE RESPONSABILIDADE INTERNACIONAL

Fundamenta-se a responsabilidade internacional dos Estados, precipuamente, em dois pilares, quais sejam, “o dever do cumprir as obrigações internacionais livremente avençadas e a obrigação de não causar dano a outrem”[133].

---

[129] BROWNLIE, Ian; CRAWFORD, James. *Brownlie’s Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p.539.
[130] HARRIS, David. *Cases and Materials on International Law*. 7. ed. London: Sweet & Maxwell, 2010, p. 421.
[131] MAZZUOLI, Valério de Oliveira. *Curso de Direito Internacional Público*. 7. ed. São Paulo: Revista dos Tribunais, 2013, p.588.
[132] RESENDE, Ranieri Lima. Responsabilidade dos estados por atos internacionalmente ilícitos: perspectivas atuais. *Revista da Faculdade de Direito de Minas Gerais*. Belo Horizonte: Nova Fase, n. 45, jul./dez., 2004, p. 343 *et seq*. Disponível em: < http://www.direito.ufmg.br/revista/index.php/revista/article/viewFile/1299/1231>. Acesso em: 22 nov. 2015.
[133] PORTELA, Paulo Henrique Gonçalves. *Direito Internacional Público e Privado*. 5. ed. Salvador: JusPodivm, 2013, p. 382.

O artigo 1º do Projeto (*draft*) de Artigos sobre Responsabilidade Internacional do Estado por Atos Internacionalmente Ilícitos de 2001, documento não cogente que constitui diretriz internacionalmente aceita sobre o tema, estabelece o princípio geral de que "todo ato internacionalmente ilícito de um Estado acarreta na responsabilidade internacional daquele Estado"[134].

Em igual sentido se estabeleceram os precedentes internacionais. O juiz Max Huber, atuando como árbitro exclusivo da reclamação submetida quanto à *Spanish Zone of Morocco*[135], ressaltou que:

> Responsabilidade é o corolário necessário de um direito. Todos os direitos de caráter internacional envolvem responsabilidade internacional. Responsabilidade resulta no dever de reparação se um a obrigação em questão não é cumprida .

É de muito proveito à explanação do instituto a manifestação da Corte Permanente de Justiça Internacional, no julgamento do caso *Chorzów Factory*, ao asseverar que "é um princípio do direito internacional, e até mesmo uma maior concepção do direito, que qualquer violação de um compromisso envolve uma obrigação de reparação" [136].

Percebe-se, destarte, que a responsabilidade internacional é traduzida pelo dever do Estado que pratica um ato internacionalmente ilícito em favor daqueles aos quais a obrigação inadimplida é devida[137].

4.3 CARACTERÍSTICAS

---

[134] Tradução livre do original, em inglês, que estabelece que "*Every internationally wrongful act of a State entails the international responsibility of that State*", vide COMISSÃO DE DIREITO INTERNACIONAL. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.

[135] Na decisão arbitral, fora asseverado que a "*responsibility is the necessary corollary of a right. All rights of an international character involve international responsibility. Responsibility results in the duty to make reparation if the obligation in question is not met*", vide COMISSÃO DE JURISTAS INTERNACIONAIS (através do árbitro exclusivo apontado para o caso, o juiz Max Huber). *Spanish Zone of Morocco* (Grã Bretanha *v*. Espanha). Decisão de 1925. 2 Reports of International Arbitral Awards 615.

[136] Isso se infere da decisão da Corte Permanente, notadamente ao asseverar que "*it is a principle of international law, and even a greater conception of law, that any breach of an engagement involves an obligation to make reparation*", vide CORTE PERMANENTE DE JUSTIÇA INTERNACIONAL. *Chorzów Factory Case*. Julgamento de 13 de setembro de 1928. PCIJ Series A n. 17.

[137] REZEK, Francisco. *Direito Internacional Público: curso elementar*. 14. ed. São Paulo: Saraiva, 2013, p.321.

A partir do estudo da responsabilidade internacional, observa-se pacificamente quatro características do instituto.

De plano, a responsabilidade internacional é tida como um meio de concretização da ideia de justiça, no sentido que impele os sujeitos de direito ao cumprimento das obrigações livremente assumidas. Isso ocorre na medida em que, ao determinar a reparação pelo prejuízo causado ou, eventualmente, determinar a sanções de cunho compensatório, escorado nas normas de responsabilidade internacional, cuja finalidade precípua é de desestimular a conduta ilícita[138], os Estados tendem a refrear o inadimplemento.

Outra característica é o seu caráter institucional. Isto é observando quando os Estados e as organizações internacionais respondem pelos atos praticados por seus funcionários ou particulares com os quais tenham concorrido. Contudo, há uma tendência – sobretudo doutrinária – de aceitação da responsabilidade internacional das pessoas naturais[139], já que:

> [...] os indivíduos não podem ser ignorados como atores do direito internacional, na medida em que lhe são imputados fatos ilícitos internacionais (vide o Tribunal Penal Internacional) e o direito de acesso a contenciosos internacionais, como a Corte Interamericana de Direitos Humanos, criada pelo Pacto de San José da Costa Rica, esgotados os recursos no âmbito interno, por meio da Comissão Interamericana de Direitos Humanos da Organização dos Estados Americanos. [140]

Vê-se, ainda, que responsabilidade internacional atende a uma finalidade eminentemente reparatória, isto é, busca-se a cessação do dano, sua reparação ao *statu quo ante* e, quando este não for possível, a compensação[141]. Difere, portanto, de uma ideia de punição, no sentido de castigar o Estado através de normas semelhantes às penais[142].

Por fim, a principal fonte normativa do instituto é o costume, consubstanciado pela difundida prática estatal e o *opinio juris* – a crença de que a atividade estatal é

---

[138] BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011, p.244.
[139] Nesse sentido entendem, por exemplo, CASELLA, Paulo Borba; ACCIOLY, Hildebrando Accioly; SILVA, Geraldo Eulálio do Nascimento e. *Manual de Direito Internacional Público*. 20. ed. São Paulo: Saraiva, 2012, p. 396 *et seq*.
[140] BORGES, Thiago Carvalho. *Op. cit.*, 2011, p.195.
[141] GUERRA, Sidney. *Curso de Direito Internacional Público*. 7. ed. São Paulo: Saraiva, 2013, p. 167.
[142] REZEK, Francisco. *Direito Internacional Público: curso elementar*. 14. ed. São Paulo: Saraiva, 2013, p.338.

juridicamente obrigatória[143]. Não obstante, a normatização do instituto é amplamente ventilada em outros meios, e há diversos tratados gerais no âmbito da ONU sobre o assunto, bem como tratados multilaterais elaborados pelos sujeitos de direito internacional[144].

Dá-se bastante relevo ao Projeto (*draft*) de Artigos sobre Responsabilidade Internacional do Estado por Atos Internacionalmente Ilícitos elaborado pela Comissão de Direito Internacional, sendo este amplamente utilizado pela sua crescente autoridade como expressão do direito consuetudinário acerca da responsabilidade internacional[145].

Demonstradas as quatro características da responsabilidade internacional (meio de concretização de um ideal de justiça, atribuição institucional, finalidade reparatória e regras predominantemente consuetudinárias), impende analisar os elementos constitutivos do instituto.

4.4 ELEMENTOS CONSTITUTIVOS

O artigo 2º do *draft* estabelece que um ato é internacionalmente ilícito quando a conduta (ação ou omissão) é atribuível ao Estado e constitui uma violação de uma obrigação internacional daquele Estado[146].

Sem óbice ao exposto, parte relevante da doutrina internacionalista afirma que a responsabilidade internacional do Estado é constituída por três elementos, quais sejam, o descumprimento de uma obrigação internacional (designado por alguns como ato internacionalmente ilícito), a ocorrência de prejuízo ou dano e a atribuição

---

[143] SHAW, Malcolm Nathan. *International Law*. 5. ed. Cambridge: Cambridge University Press, 2003, p. 80.
[144] BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011, p. 240.
[145] BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p.540.
[146] O art. 2º do texto original verbera que "*There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State*" vide COMISSÃO DE DIREITO INTERNACIONAL. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.

do evento danoso a um Estado[147]. Compartilham desse entendimento os célebres professores Malcolm Nathan Shaw[148] e Antonio Cassese[149].

Contudo, tal entendimento não se assemelha abalizado com a moderna doutrina da responsabilidade internacional do Estado. Com efeito, a própria Comissão de Direito Internacional que elaborou os Artigos sobre Responsabilidade Internacional asseverou que o dano não é um elemento necessário, uma vez que ele depende da obrigação que fora desrespeitada[150]. Por exemplo, se a violação for à proibição do uso da força, é provável que tenha havido dano material haja vista que este terá que ter alcançado dimensão e efeitos suficientes para se tornar internacionalmente ilícito. Mas se a obrigação malferida for uma cláusula contratual que não enseje nenhum prejuízo material ou moral, ainda assim, poderá haver a responsabilidade pelo descumprimento obrigacional atribuível ao Estado descumpridor. Assim entendia o saudoso professor Ian Brownlie, em obra que fora atualizada pelo jurista australiano James Richard Crawford[151], que desde fevereiro de 2015 é um dos juízes da Corte Internacional de Justiça[152].

Também da análise do artigo 2 dos Artigos sobre Responsabilidade do Estado por Atos Internacionalmente ilícitos, nota-se que não se exige o elemento dano para a configuração da responsabilidade. Somente se requer a presença conjunta de duas circunstâncias para que isso ocorra: ato em descumprimento obrigacional e atribuição deste a um Estado.

Cumpre salientar, de logo, que o ato ilícito é consubstanciado no descumprimento de uma obrigação internacional. Isso ganha relevo no sentido de que as normas e obrigações consideradas no momento de aferir a idoneidade do ato são aquelas de

---

147 MAZZUOLI, Valério de Oliveira. *Curso de Direito Internacional Público*. 7. ed. São Paulo: Revista dos Tribunais, 2013, p.594.
148 SHAW, Malcolm Nathan. *International Law*. 5. ed. Cambridge: Cambridge University Press, 2003, p. 696.
149 CASSESE, Antonio. *International law*. 2. ed. New York: Oxford University Press, 2005, p. 246.
150 COMISSÃO DE DIREITO INTERNACIONAL. *Commentaries to the Articles on Responsibility of States for Internationally Wrongful Acts*. Yearbook of the International Law Commission, vol. II, Part Two, 2001, p. 36, artigo 2, comentário n. 9.
151 BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p. 540.
152 Vide informação veiculada no site da Corte Internacional de Justiça, disponível em: <http://www.icj-cij.org/court/index.php?p1=1&p2=2&p3=1&judge=200>.

direito internacional (e não de direito interno)[153]. Como leciona o internacionalista Thiago Carvalho Borges, “a referência da ilicitude é a norma de direito internacional, consubstanciada em uma regra consuetudinária ou tratadística ou em princípio”[154].

Ademais, é ponderoso que haja um liame entre a conduta violadora do direito e um sujeito de direito internacional, eis que deste vínculo decorrerá a responsabilidade. Esse elemento é denominado imputabilidade ou nexo de causalidade pela doutrina (muito embora a terminologia utilizada pelo *draft* seja “atribuição”). Desse modo:

> A ação ou omissão ilícita deve ser imputada a pessoas de direito internacional: Estado ou Organização Internacional. Será, entretanto, indireta a responsabilidade do Estado nos casos em que um ente subordinado, como um Estado federado, for o causador do dano. [...][155]

O Projeto (*draft*) de Artigos sobre Responsabilidade Internacional do Estado por Atos Internacionalmente Ilícitos, em seu artigo 2º, “a”, estabelece como um dos elementos essenciais para configuração de um ato internacionalmente ilícito ser este “atribuível ao Estado sob o direito internacional”[156].

Nos comentários aos Artigos, a Comissão de Direito Internacional asseverou que a questão da atribuição é essencialmente normativa, mormente ao estabelecer que a atribuição de conduta ao Estado como um sujeito de direito internacional é baseado no critério determinado pelo direito internacional e não no mero reconhecimento de um vínculo de causalidade fática[157].

Os critérios para se atribuir a conduta a um Estado estão elencados nos artigos 4 ao 11, todos insertos no capítulo II do instrumento normativo. À exceção dos artigos 4, 5 e 8, todos os demais artigos possuem previsões bem específicas, não suscitando muita controvérsia sobre sua aplicação. Esses artigos verberam, em síntese, que condutas de órgãos colocados à disposição por outro Estado serão atribuíveis que utilizou da entidade de sujeito alheio para realizar o ato (artigo 6), que serão imputáveis as condutas realizadas por pessoas que assemelhem empoderadas para a realização do ato, mesmo que elas hajam com excesso de autoridade ou em

---

153 REZEK, Francisco. *Direito Internacional Público: curso elementar*. 14. ed. São Paulo: Saraiva, 2013, p.323.
154 BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011, p.239.
155 *Ibidem*, *Loc. cit*.
156 *Cf*. Nota de rodapé 24.
157 COMISSÃO DE DIREITO INTERNACIONAL. *Commentaries to the Articles on Responsibility of States for Internationally Wrongful Acts*. Yearbook of the International Law Commission, vol. II, Part Two, 2001, p. 35, artigo 2, comentário n. 6.

contrariedade às instruções (artigo 7) ou mesmo na ausência ou negligência das autoridades oficiais (artigo 9), que as condutas realizadas por movimentos insurgentes ou que suceda o governo anterior será atribuível àquele Estado (artigo 10) e, caso qualquer Estado reconheça e adote a conduta como sendo sua, mesmo que não a tenha perpetrado, lhe será atribuída a responsabilidade (artigo 11). A análise do presente trabalho se direciona mais detidamente aos artigos 4, 5 e 8, uma vez que estes possuem controversa aplicação e notório relevo aos eventos ocorridos no âmbito cibernético.

Frise-se, de logo, que a Comissão de Direito Internacional assentou que:

> [...] o termo "atribuição" é usado para denotar a operação de ligar uma dada ação ou omissão a um Estado. Na prática internacional e decisões judiciais, o termo "imputação" também é utilizado. Mas o termo "atribuição" afasta qualquer sugestão de que o processo jurídico de conexão da conduta ao Estado é uma ficção, ou que a conduta em questão é "realmente" de outro alguém.[158]

Com efeito, o artigo 4 dos Artigos estabelece que "a conduta de qualquer órgão do Estado deve ser considerada como um ato daquele Estado sob o direito internacional"[159]. Esse excerto foi reproduzido à exatidão pela Corte Internacional de Justiça, que considerou a norma como de caráter costumeiro e bem estabelecida no direito internacional, no parecer consultivo do caso relativo à *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*[160]. Em resposta à crescente proliferação de entidades paraestatais na condução de atos ilícitos dos Estados[161], artigo 5 dos Artigos sobre Responsabilidade Internacional dispôs que "a conduta de uma pessoa ou entidade que não é um órgão do Estado sob o artigo 4, mas que está empoderada pela lei

---

[158] Tradução livre do original, que verbera: "[...] *the term "attribution" is used to denote the operation of attaching a given action or omission to a State. In international practice and judicial decisions, the term "imputation" is also used. But the term "attribution" avoids any suggestion that the legal process of connecting conduct to the State is a fiction, or that the conduct in question is "really" that of someone else*". COMISSÃO DE DIREITO INTERNACIONAL. *Commentaries to the Articles on Responsibility of States for Internationally Wrongful Acts*. Yearbook of the International Law Commission, vol. II, Part Two, 2001, p. 36, artigo 2, comentário n. 12.

[159] O artigo 4 do texto original verbera que "*The conduct of any State organ shall be considered an act of that State under international law*" vide COMISSÃO DE DIREITO INTERNACIONAL. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.

[160] CORTE INTERNACIONAL DE JUSTIÇA. *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*. Parecer consultivo de 29 de abril de 1999. ICJ Reports n. 726, p. 87, § 62.

[161] SHAW, Malcolm Nathan. *International Law*. 5. ed. Cambridge: Cambridge University Press, 2003, p. 702.

daquele Estado para exercer elementos de autoridade governamental, devem ser considerados um ado do Estado sob o direito internacional"[162]. Sobre o aludido dispositivo, Malcolm Nathan Shaw leciona que:

> Essa norma é destinada, *inter alia*, a abranger a situação de corporações privatizadas que retêm certas funções públicas ou regulatórias. Exemplos da aplicação desse artigo podem incluir a conduta de empresas de segurança privada autorizadas a atuar como guardas prisionais, ou quando empresas aéreas privadas ou estatais exercem certos controles imigratórios, ou em relação em relação a uma companhia ferroviária à qual certos poderes de polícia foram conferidos. [163]

Já o artigo 8 dos Artigos elaborados pela Comissão de Direito Internacional estabelecem a atribuição com base na direção e controle sobre a condução do ato delituoso, ao verberar que:

> A conduta de uma pessoa ou grupo de pessoas deve ser considerada um ato de um Estado sob o direito internacional se a pessoa ou grupo de pessoas está, de fato, agindo com base em instruções, ou sob a direção e controle, daquele Estado ao conduzir a conduta.[164]

A estudo desse dispositivo, e sua relevância no direito internacional público, é impulsionada pelos divergentes julgamentos dos casos acerca das *Military and Paramilitary Activities in and against Nicaragua* e do caso *The Prosecutor v. Duško Tadic*[165]. Enquanto naquele se estabeleceu, para fins de se imputar a conduta ao Estado, que a direção e controle devem ser "efetivas"[166], neste quedou consignado que apenas seria necessário um controle "genérico"[167].

---

[162] O artigo 5 do texto original verbera que "*The conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law*" vide COMISSÃO DE DIREITO INTERNACIONAL. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.

[163] Tradução livre do original, que verbera: "*This provision is intended inter alia to cover the situation of privatised corporations which retain certain public or regulatory functions. Examples of the application of this article might include the conduct of private security firms authorised to act as prison guards or where private or state-owned airlines exercise certain immigration controls or with regard to a railway company to which certain police powers have been granted*". SHAW, Malcolm Nathan. *International Law*. 5. ed. Cambridge: Cambridge University Press, 2003, p. 702.

[164] O artigo 8 do texto original verbera que "*The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct*" vide *COMISSÃO DE DIREITO INTERNACIONAL. Op. cit.*, 2001.

[165] SHAW, Malcolm Nathan. *International Law*. 5. ed. Cambridge: Cambridge University Press, 2003, p. 704-705.

[166] CORTE INTERNACIONAL DE JUSTIÇA. *Case concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. Estados Unidos). Decisão de mérito de 1986. ICJ Reports n. 520, p. 64-65, § 115.

[167] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the

Veja-se, nas seguintes linhas, as causas que podem excluir a responsabilidade internacional pela elisão da ilicitude prevista nos Artigos formulados pela Comissão de Direito Internacional da ONU.

4.5 EXCLUDENTES DA RESPONSABILIDADE INTERNACIONAL

Por vezes, ações que constituiriam um ilícito se praticadas pelos Estados não são consideradas violadoras do direito internacional em decorrência de circunstâncias que eximem o sujeito perpetrador do ato da responsabilidade internacional. De acordo com o abalizado magistério de Valério de Oliveira Mazzuoli, "merecem destaque o consentimento do Estado, a legítima defesa, as contramedidas, a prescrição liberatória, o caso fortuito e força maior, o estado de necessidade e a renúncia do indivíduo lesado"[168].

O consentimento válido do Estado que fora vítima do dano causado pela conduta de outro exclui a responsabilidade deste, nos termos do art. 20 do *draft*[169]. "O exemplo mais comum é o tipo de situação onde tropas de um Estado são enviadas para outro a pedido deste"[170].

O exercício de reação a um ataque armado, real ou iminente, constitui um meio válido de uso da força, eis que utilizado para garantir a soberania do Estado – o que se denomina de legítima defesa. Muito embora a proibição do uso da força seja um princípio veiculado na Carta da ONU, distintamente em seu artigo 2, parágrafo 4º, o direito inerente aos Estados de se protegerem de ataques armados faz parte do sistema de proteção destes, como previsto no art. 51 do mesmo instrumento, de

---

Former Yugoslavia since 1991. *The Prosecutor v. Duško Tadic Case*. Julgamento de 15 de julho de 1999. Case n. IT-94-1-A, p. 49-72, §§ 120 *et seq*.

[168] MAZZUOLI, Valério de Oliveira. *Curso de Direito Internacional Público*. 7. ed. São Paulo: Revista dos Tribunais, 2013, p.610.

[169] O art. 20 do documento original estabelece que "*Valid consent by a State to the commission of a given act by another State precludes the wrongfulness of that act in relation to the former State to the extent that the act remains within the limits of that consent*" vide COMISSÃO DE DIREITO INTERNACIONAL. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.

[170] Tradução livre do original, que verbera: "*The most common example of this kind of situation is where troops from one state are sent to another at the request of the latter*". SHAW, Malcolm Nathan. *International Law*. 5. ed. Cambridge: Cambridge University Press, 2003, p. 707.

modo que o exercício do direito de legítima defesa não constitui violação aos princípios da Carta, como a Corte Internacional de Justiça afirmou no caso *Legality of the Threat or Use of Nuclear Weapons*[171].

São valiosas as insignes lições do internacionalista Thiago Carvalho Borges[172] acerca das contramedidas, veja-se:

> A ordem internacional admite ainda a prática de *represálias* com caráter de legítima defesa, como sendo adoção de medidas internacionalmente ilícitas como forma de revidar medidas ilícitas adotadas por outro Estado, não envolvendo uso da força e não havendo meio lícito eficiente para combater os danos sofridos. São também chamadas de *contramedidas*.

Acerca das contramedidas, se pronunciou a Corte Internacional de Justiça no julgamento do caso relativo ao projeto *Gabčíkovo-Nagymaros*, estabelecendo as condições que devem ser atendidas para que tais "represálias" estejam em consonância com o direito internacional público, veja-se:

> Para que seja justificável, a contramedida deve atender a certas condições [...]. Em primeiro lugar, ela deve ser realizada em resposta a um ato internacionalmente ilícito prévio de outro Estado e deve ser direcionado contra esse Estado [...]. Segundo, o Estado prejudicado deve ter invocado o Estado comitente do ato ilícito para que ele interrompa a conduta indevida ou realize reparação em razão desta [...]. Na visão da Corte, uma importante consideração é que os efeitos de uma contramedida devem ser proporcionais ao prejuízo sofrido, levando em consideração os direitos em questão [...]. Seu propósito deve ser de induzir o Estado violador a cumprir com suas obrigações sob o direito internacional e [...] a medida deverá ser, então, reversível.[173]

A prescrição liberatória tem gênese na inércia daquele que fora prejudicado pelo evento danoso em agir, fazendo-o perder o direito de reclamar por aquele dano oriundo de ato ilícito. Diante da ausência de parâmetro universal para que se extirpe

---

[171] CORTE INTERNACIONAL DE JUSTIÇA. *Legality of the Threat or Use of Nuclear Weapons*. Parecer consultivo de 8 de julho de 1996. ICJ Reports n. 679. p. 244, § 38, e p. 263, § 96.

[172] BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011, p.243.

[173] Tradução livre do original, que verbera: "In order to be justifiable, a countermeasure must meet certain conditions [...] In the first place it must be taken in response to a previous international wrongful act of another state and must be directed against that state [...]. Secondly, the injured state must have called upon the state committing the wrongful act to discontinue its wrongful conduct or to make reparation for it [...]. In the view of the Court, an important consideration is that the effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question [...] its purpose must be to induce the wrongdoing state to comply with its obligations under international law, and [...] the measure must therefore be reversible". CORTE INTERNACIONAL DE JUSTIÇA. *Case Concerning the Gabcikovo-Nagymaros Project* (Hungria v. Eslováquia). Julgamento de 25 de setembro de 1997. ICJ Reports n. 692, p. 55-57, §§ 83-88.

o aludido direito, o lapso temporal e a forma da inércia deverão ser regulamentados em tratado[174].

Quanto ao caso fortuito e a força maior, impende assinalar o ensinamento de Valério de Oliveira Mazzuoli[175], notadamente ao afirmar que:

> A ilicitude de um ato estatal contrário a uma obrigação internacional não será causa de responsabilização do Estado caso o ato ilícito praticado tenha sido consequência de um evento externo irresistível ou imprevisto, fora do controle do Estado, que tornou materialmente impossível ao Estado agir em conformidade com a obrigação assumida.

Infere-se, assim, que o Estado não responderá quando um acontecimento exterior e imprevisto resulta na impossibilidade de cumprir uma obrigação. Contudo, a força maior não será causa excludente de ilicitude quando o evento danoso derivar, no todo ou em parte, da conduta do próprio Estado[176].

O estado de necessidade consiste na ação promovida com o fito em remover perigo iminente, causando dano a outros Estado. Conforme o teor do artigo 25 do *draft*[177], para a exclusão da responsabilidade, a conduta deve ser o único meio hábil para a salvaguarda dos interesses e enquanto a ação não pode obstar seriamente os direitos do outro Estado. “Embora se reconheça a sua condição de excludente de ilicitude, é discutida internacionalmente a possibilidade de se excluir a responsabilidade do Estado que age para remover perigo iminente, causando danos a outros Estados”[178].

---

174 PORTELA, Paulo Henrique Gonçalves. *Direito Internacional Público e Privado*. 5. ed. Salvador: JusPodivm, 2013, p. 392.

175 MAZZUOLI, Valério de Oliveira. *Curso de Direito Internacional Público*. 7. ed. São Paulo: Revista dos Tribunais, 2013, p.612.

176 ALBUQUERQUE, Roberto Chacon de. A responsabilidade dos estados pela prática de ilícitos internacionais. *Revista da Faculdade de Direito da Universidade de São Paulo*. São Paulo: USP, v. 97, jan. 2002, p. 456. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67557>. Acesso em: 22 nov. 2015.

177 O art. 25 do texto original verbera que “[...]*Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act: (a) Is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) Does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.* [...]” vide COMISSÃO DE DIREITO INTERNACIONAL. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.

178 BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011, p. 243.

Portanto, a lesão de bem jurídico de outrem para salvaguardar o próprio constitui conduta realizada em estado de necessidade, excluindo-se a responsabilidade internacional do sujeito que a perpetrou[179].

Exauridas as hipóteses de excludente de responsabilidade internacional previstas no Projeto (*draft*) de Artigos sobre Responsabilidade Internacional do Estado por Atos Internacionalmente Ilícitos, cumpre apontar mais uma ocasião na qual a construção de parte da doutrina entende haver uma mitigação do instituto: a renúncia do indivíduo lesado.

Para os adeptos do aludido entendimento, um particular poderia renunciar à proteção, pela via diplomática, contatando previamente o governo estrangeiro interessado em se utilizar do instituto[180].

[179] PORTELA, Paulo Henrique Gonçalves. *Direito Internacional Público e Privado*. 5. ed. Salvador: JusPodivm, 2013, p. 392.
[180] MAZZUOLI, Valério de Oliveira. *Curso de Direito Internacional Público*. 7. ed. São Paulo: Revista dos Tribunais, 2013, p.612.

5 APLICABILIDADE DAS NORMAS SOBRE RESPONSABILIDADE INTERNACIONAL AOS ATAQUES CIBERNÉTICOS

Restou consignado, da análise do capítulo anterior[181], que o escopo da responsabilidade internacional dos Estados deriva da necessidade de imputar uma ação ou omissão violadora de uma obrigação validamente estabelecida a um sujeito de direito internacional, que irá sofrer as consequências do inadimplemento. Não obstante, para que tais normas sejam aplicáveis aos Estados, é necessário que a conduta ilícita seja composta de elementos subjetivos e objetivos, sem os quais não há que se falar em responsabilidade[182].

Há de se anotar, de plano, que tal critério objetivo e subjetivo da responsabilidade internacional, para os fins deste trabalho, não analisa a culpa do agente na aferição da causalidade entre o ato e o dano. É verdade que o aludido instituto pode ser dividido em responsabilidade subjetiva (ou por culpa) e responsabilidade objetiva (ou sem culpa), tal como na responsabilidade civil[183]. Contudo, a despeito da relevância de tal divisão, ela não está abrangida na presente proposta, haja vista que essa se debruça sobre os elementos objetivos (que versam sobre o descumprimento obrigacional) e subjetivos (aqueles relacionados à atribuição da conduta a um ou mais Estados) dispostos nos Artigos sobre Responsabilidade do Estado por Atos Internacionalmente Ilícitos, que refletem o consagrado posicionamento jurisprudencial[184].

O objeto da responsabilidade internacional será sempre relacionado à inconsistência da conduta (ou omissão) de um Estado a uma obrigação internacional[185]. Já o elemento subjetivo será a imputabilidade dessa conduta ao Estado[186]. Embora sua aplicabilidade no direito internacional seja patente, o problema exsurge da dificuldade de se aplicar esses elementos imprescindíveis ao âmbito cibernético,

---

[181] Capítulo 4, sobre Responsabilidade Internacional dos Estados.
[182] CASSESE, Antonio. *International law*. 2. ed. New York: Oxford University Press, 2005, p. 245.
[183] BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011, p. 240.
[184] BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p. 542.
[185] CASSESE, Antonio. *Op. cit.*, 2005, p. 251.
[186] *Ibidem*, p. 246.

notadamente diante da dificuldade de se atribuir uma operação conduzida por meio de redes de computadores a um agente específico[187].

Será analisada, nas seguintes linhas, a aplicabilidade genérica das normas sobre responsabilidade internacional dos Estados aos ataques cibernéticos, perpassando pela análise da incidência dos elementos objetivos e subjetivos do instituto, notadamente no que concerne à possível ilicitude das operações conduzidas por meio da *internet* e a dificultosa – e crucial – questão da atribuição.

5.1 APLICABILIDADE GENÉRICA DAS NORMAS SOBRE RESPONSABILIDADE INTERNACIONAL AOS ATAQUES CIBERNÉTICOS

Consoante já fora aduzido[188], a disciplina jurídica internacional acerca da responsabilidade internacional dos Estados se pauta nos Artigos de Responsabilidade do Estado por Atos Internacionalmente Ilícitos de 2001, elaborados pela Comissão de Direito Internacional (CDI) da Organização das Nações Unidas (ONU), para abalizar a juridicidade do instituto[189]. O artigo 1, que estabelece princípios gerais, verbera que "todo ato internacionalmente ilícito de um Estado acarreta na responsabilidade internacional daquele Estado"[190].

O termo "responsabilidade internacional" se refere à criação de uma nova relação jurídica que surgirá em decorrência do cometimento de um ato internacionalmente ilícito[191]. Nesse mesmo arrimo, a Corte Permanente de Justiça Internacional

---

[187] DINNISS, Heather Harrison. *Cyber warfare and the law of war*. New York: Cambridge University Press, 2012, p. 99.
[188] No tópico 4.2, que versou sobre o Conceito de Responsabilidade Internacional.
[189] BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p. 542.
[190] Tradução livre do original, em inglês, que estabelece que "*Every internationally wrongful act of a State entails the international responsibility of that State*", vide COMISSÃO DE DIREITO INTERNACIONAL. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.
[191] COMISSÃO DE DIREITO INTERNACIONAL. *Commentaries to the Articles on Responsibility of States for Internationally Wrongful Acts*. Yearbook of the International Law Commission, vol. II, Part Two, 2001, p. 32, artigo 1, comentário n. 1.

assentou que tal relação jurídica é estabelecida "imediatamente entre as partes"[192], assim que tal conduta indevida for constatada. É importante ressaltar que:

> O Estado é responsável pelo cumprimento dos deveres que assume frente às demais nações, sejam deveres oriundos de tratados, dos costumes ou do simples fato de, voluntária ou involuntariamente, causar danos ou prejuízos a outros Estados.[193]

Note-se que essa responsabilidade não pode ser compreendida apenas no que concerne às obrigações entre as partes. No caso *Barcelona Traction*, a Corte Internacional de Justiça elaborou considerável desenvolvimento ao instituto da responsabilidade internacional, mormente por ter reconhecido que o ato indevido direcionado contra a comunidade internacional consiste em violação de uma obrigação *erga omnes*, superando a ideia de que os compromissos dos Estados deveriam ser apenas para com outros Estados, veja-se:

> [...] uma distinção essencial deve ser feita entre obrigações de um Estado em face da comunidade internacional como um todo, e aquelas surgidas *vis-à-vis* outro Estado no campo da proteção diplomática. Pela própria natureza, aquela concerne a todos os Estados. Tendo em vista a importância dos direitos envolvidos, pode se considerar que todos os Estados têm interesse na proteção deles; eles são obrigações *erga omnes*.[194]

No mesmo julgamento, a Corte afirmou que "tais obrigações decorrem, por exemplo, no direito internacional contemporâneo, da proscrição dos atos de agressão"[195]. Desse modo, considerando que a própria CIJ relaciona os conceitos de agressão e ataque armado[196], e tendo em vista que um ataque cibernético que alcance a dimensão e efeitos necessários podem ser considerados como a forma mais grave de uso da força, como fora aduzido no Capítulo 3 deste trabalho[197], é certo que as

---

[192] Tradução livre do original, que verbera: "[…] *immediately as be- tween the two States"*. CORTE PERMANENTE DE JUSTIÇA INTERNACIONAL. *Phosphates in Morocco*. Julgamento de 1938. P.C.I.J., Series A/B, n. 74, p. 28.

[193] FINKELSTEIN, Cláudio. Direito internacional. 2. ed. São Paulo: Atlas, 2013, p. 51.

[194] Tradução livre do original, que verbera: "[...] *an essential distinction should be drawn between the obligations of a State towards the international community as a whole, and those arising vis-à-vis another State in the field of diplomatic protection. By their very nature the former are the concern of all States. In view of the importance of the rights involved, all States can be held to have a legal interest in their protection; they are obligations erga omnes*". CORTE INTERNACIONAL DE JUSTIÇA. *Case concerning the Barcelona Traction, Light and Power Company, Limited*. Julgamento de 5.fev.1970. ICJ Reports n. 337, p. 32, § 33.

[195] Tradução livre do original, que verbera: "*Such obligations derive, for example, in contemporary international law, from the outlawing of acts of aggression*". CORTE INTERNACIONAL DE JUSTIÇA. *Case concerning the Barcelona Traction, Light and Power Company, Limited*. Julgamento de 5.fev.1970. ICJ Reports n. 337, p. 32, § 34.

[196] Vide CORTE INTERNACIONAL DE JUSTIÇA. *Case concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. Estados Unidos). Decisão de mérito de 1986. ICJ Reports n. 520, p. 93, § 195.

[197] Que versou sobre o Ataque Cibernético no Direito Internacional.

operações realizadas por meio de rede de computadores podem ser equiparadas à agressão. Como consecução lógica, se o recurso à agressão é proscrito, e se um ataque cibernético alcançar o patamar de uma agressão, é incontestável que tal situação ensejaria a aplicação das normas de responsabilidade internacional em consequência do descumprimento obrigacional.

Isso, frise-se, independe da tecnologia utilizada. A aplicação do instituto da responsabilidade internacional visa, como norma genérica, estabelecer regras que incidirão sobre todos os ilícitos internacionais, como se depreende das anotações de Vesa Kyyrönen[198], *verbis*:

> [...] A aplicabilidade da responsabilidade do estado não é específica por tecnologia ou ação. De fato, da perspectiva da responsabilidade do estado, essas novas tecnologias não mudam os aspectos regais como é a responsabilidade do estado. Como *lex generis*, as regras sobre responsabilidade do estado discutem que todas as ações ilícitas internacionais que são atribuíveis ao estado se inserem no escopo da doutrina.

Não obstante seja evidente a aplicabilidade genérica das normas sobre responsabilidade internacional às formas mais graves de uso da força, realizada por meio de ataque cibernético, outras operações cibernéticas de baixa intensidade também podem ensejar a violação de obrigações necessária à incidência da responsabilidade do Estado[199]. Afinal, como restou consignado na decisão arbitral do caso *Rainbow Warrior*:

> [...] os princípios gerais do Direito Internacional relativo à responsabilidade do Estado são igualmente aplicáveis no caso de violação de obrigação de tratado, uma vez que no direito internacional não há distinção entre responsabilidade delituosa e contratual, de modo que a violação do Estado a qualquer obrigação, de qualquer origem, enseja a responsabilidade do Estado e, consequentemente, o dever de reparação.[200]

---

[198] Tradução livre do original, que verbera: "[...] *The applicability of state responsibility is not technology or action specific. Indeed, from the perspective of state responsibility, these new technologies do not change general aspects of state responsibility as such. As lex generis, the state responsibility rules argue that all internationally wrongful actions which are attributable to state fall within the scope of the doctrine*". KYYRÖNEN, Vesa. *Machines Making Decisions: The Applicability of State Responsibility Doctrine in the Case of Autonomous Systems*. Helsinki: Helsingin Yliopisto, 2015, p. 34. Disponível em: <https://helda.helsinki.fi/bitstream/handle/10138/153596/Vesa%20Kyyronen%20-%20thesis%20ready.pdf?sequence=4>. Acesso em: 11.mai.2016.

[199] WATTS, Sean. Low-Intensity Cyber Operations and the Principle of Non-Intervention. In: *Cyberwar* (Ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein). New York: Oxford University Press, 2015, p. 270.

[200] Tradução livre do original, que verbera: "[...] *the general principles of International Law concerning State responsibility are equally applicable in the case of breach of treaty obligation, since in the international law field there is no distinction between contractual and tortious responsibility, so that any*

Foi nesse sentido, inclusive, que fora elaborada a regra 6 do Manual de Tallinn sobre o Direito Internacional Aplicável ao Estado de Guerra Cibernética, ao dispor que "um Estado arca com a responsabilidade jurídica internacional por uma operação cibernética que lhe seja atribuível e que constitua violação a uma obrigação internacional"[201].

Desse modo, diante do teor das aludidas normas gerais da responsabilidade do Estado e da interpretação jurisprudencial, no contexto do direito internacional público, não se vislumbra motivo para obstar a incidência delas às condutas realizadas por meio de redes de computadores, haja vista que estas podem violar a esfera jurídica de outro sujeito de direito internacional. Afastar a incidência dessas normas seria chancelar o inadimplemento de outras normas vigentes no âmbito internacional. São aplicáveis, portanto, as normas de responsabilidade internacional do Estado aos ataques cibernéticos.

Impende analisar, a seguir, os elementos objetivos e subjetivos do instituto, individualmente.

5.2 O ATAQUE CIBERNÉTICO COMO UM ATO INTERNACIONALMENTE ILÍCITO

As normas sobre responsabilidade do Estado, sobretudo aquelas concernentes aos princípios gerais, trazem a premissa de que é necessário o descumprimento obrigacional consubstanciado em um ato ilícito para que o sujeito de direito internacional seja internacionalmente responsabilizado[202].

---

violation by a State of any obligation, of whatever origin, gives rise to State responsibility and consequently, to the duty of reparation". ORGANIZAÇÃO DAS NAÇÕES UNIDAS *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior affair*. UNRIAA, vol. XX, Sales n. E/F.93.V.3, 1990, p. 215, § 75.

[201] Tradução livre do original, que verbera: "*A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation*". ORGANIZAÇÃO DO TRATADO DA AMÉRICA DO NORTE. Grupo de Especialistas Internacionais. Tallinn Manual on the International Law Applicable to Cyber Warfare (Editor geral Michael N. Schmitt). 1. ed. New York: Cambridge University Press, 2013, p. 29.

[202] COMISSÃO DE DIREITO INTERNACIONAL. *Commentaries to the Articles on Responsibility of States for Internationally Wrongful Acts*. Yearbook of the International Law Commission, vol. II, Part Two, 2001, p. 32.

É nesse contexto que são observados os elementos objetivos do instituto. O professor Antonio Cassese os subdivide em inconsistência de uma conduta em relação a uma obrigação internacional e em configuração do dano, seja ele material ou moral[203].

Faz-se imperioso, de plano, analisar se é necessária a observância de dano para que surja a responsabilidade internacional. O artigo 2 dos Artigos sobre Responsabilidade do Estado estabelece dois elementos para que se configure um ato internacionalmente ilícito, quais sejam, uma ação ou omissão que constitui violação a uma obrigação internacional e a atribuição da referida conduta ao Estado sob o direito internacional[204]. Não se observa, entre as exigências, a necessidade de que haja dano para a configuração do ilícito internacional. Tal "omissão" no texto da norma foi proposital, como se observa dos comentários da própria Comissão de Direito Internacional que elaborou o projeto dos artigos, veja-se:

> Algumas vezes é dito que responsabilidade internacional não é atrelada à conduta de um Estado em desrespeito a suas obrigações sem que elementos adicionais existam, em particular, "dano" a outro Estado. Mas se esses elementos são necessários depende do conteúdo da obrigação primária, e não há regra geral a esse respeito. Por exemplo, a obrigação sob um tratado de promulgar uma lei uniforme é violada pela falha em promulgar aquela lei, e não é necessário que o outro Estado parte aponte para nenhum dano específico que ele tenha sofrido em razão dessa falha. Se uma obrigação particular é violada imediatamente sobre a falha em agir por parte do Estado responsável, ou se algum evento adicional deve ocorrer, depende do conteúdo e interpretação da obrigação primária e não pode ser determinado em abstrato.[205]

---

[203] CASSESE, Antonio. *International law*. 2. ed. New York: Oxford University Press, 2005, p. 246.

[204] O texto original do artigo 2 verbera que "*Article 2. Elements of an internationally wrongful act of a State. There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obliga- tion of the State.*", vide COMISSÃO DE DIREITO INTERNACIONAL. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.

[205] Tradução livre do original, que verbera: "*It is sometimes said that international responsibility is not engaged by conduct of a State in disregard of its obligations unless some further element exists, in particular, "damage" to another State. But whether such elements are required depends on the content of the primary obligation, and there is no general rule in this respect. For example, the obligation under a treaty to enact a uniform law is breached by the failure to enact the law, and it is not necessary for another State party to point to any specific damage it has suffered by reason of that failure. Whether a particular obligation is breached forthwith upon a failure to act on the part of the responsible State, or whether some further event must occur, depends on the content and interpretation of the primary obligation and cannot be determined in the abstract*". COMISSÃO DE DIREITO INTERNACIONAL. *Commentaries to the Articles on Responsibility of States for Internationally Wrongful Acts*. Yearbook of the International Law Commission, vol. II, Part Two, 2001, p. 36, artigo 2, comentário n. 9.

Nota-se, desse modo, que não há a aludida exigência da ocorrência de dano para que se configure um ato internacionalmente ilícito. Como bem anotado pela Comissão de Direito Internacional, isso dependerá da obrigação primária – as quais, caso desrespeitadas, dão ensejo à responsabilidade[206] – de modo que se for estabelecida uma obrigação que não vislumbra nenhuma ocorrência de dano com o inadimplemento, o seu descumprimento dará azo à responsabilidade independentemente da demonstração de acontecimento danoso. Exemplificando no contexto cibernético, caso dois países acordassem entre si que um não poderia usar falsear a identidade do endereço de IP de um sistema de computadores inserto no território do outro, e essa obrigação fosse desrespeitada por uma das partes, o Estado violado não teria que comprovar nenhum dano para responsabilizar a sua contra-parte, notadamente se a obrigação primária não exige qualquer prejuízo efetivo.

Superada a discussão sobre a (des)necessidade da existência de dano para que haja um ato internacionalmente ilícito, impende examinar o cerne de sua configuração – o descumprimento obrigacional. Como aduz Antonio Cassese[207]:

> Para que a conduta de um Estado seja inconsistente com uma obrigação internacional, ela deve ser contrária a uma obrigação ligada àquele Estado a partir de uma regra ou princípio de direito internacional aplicável, qualquer que seja a natureza da obrigação violada.

No âmbito cibernético, um ato ilícito pode decorrer da violação de diversas normas de direito internacional. Pode-se, por exemplo, malferir a Carta das Nações Unidas (*e.g.* fazendo uso da força por meio de redes de computadores sem autorização do Conselho de Segurança ou ação em legítima defesa), as leis dos conflitos armados previstas no direito humanitário internacional (*e.g.* conduzir um ataque, tal como previsto nas Convenções de Genebra de 1949, contra a população civil, e não contra o adversário, por meio da *internet*), bem como outras obrigações que não envolvam necessariamente algum conflito, como a violação do direito do mar ou ao

---

[206] BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p. 540.

[207] Tradução livre do original, que verbera: "*For the conduct of a State to be inconsistent with an international obligation, it must be contrary to an obligation stemming for that State from an applicable rule or principle of international law, whatever the nature of the obligation breached*". CASSESE, Antonio. *International law*. 2. ed. New York: Oxford University Press, 2005, p. 251.

princípio da não-intervenção[208]. Isso é o que estabelece o próprio Manual de Tallinn sobre o Direito Internacional Aplicável ao Estado de Guerra Cibernética, que traz, como exemplo hábil a ilustrar a situação, que "[...] um navio de guerra de um Estado é proibido de conduzir operações cibernéticas que são adversas aos interesses da nação costeira enquanto estiver em passagem inocente" [209], de modo que a realização de tais operações nesse contexto consistiria em violação de obrigação idônea a dar azo à responsabilidade internacional.

Demonstrado o escopo do elemento objetivo da responsabilidade internacional por ataques cibernéticos, cumpre discorrer acerca da questão mais controversa de sua configuração: a dificuldade de atribuição das contudas aos verdadeiros agentes perpetradores do ato no âmbito dos sistemas interconectados de computadores.

5.3 A QUESTÃO CRUCIAL DA ATRIBUIÇÃO DE ATAQUES CIBERNÉTICOS AOS ESTADOS

Em acepção geral, a atribuição de uma violação de dever aos Estados deve decorrer de ação ou omissão perpetrados por um (ou mais) de seus órgãos ou agentes[210].

Ocorre que, no âmbito cibernético, a atribuição de um ato ilícito a um Estado é muito difícil de ser demonstrada. Isso pois, devido à complexidade dos sistemas de informação, é possível alterar ou disfarçar o registro de onde aquele ato teria sido originado, obstando a identificação do real perpetrador do ato.

É o que acontece, por exemplo, quando um *hacker* utiliza um endereço de IP que não condiz com sua localização geográfica, fazendo parecer que estava situado em outro lugar. A depender da sofisticação do ataque e da habilidade técnica do agressor, será inviável descobrir a real localidade de origem do ato.

---

[208] ORGANIZAÇÃO DO TRATADO DA AMÉRICA DO NORTE. Grupo de Especialistas Internacionais. Tallinn Manual on the International Law Applicable to Cyber Warfare (Editor geral Michael N. Schmitt). 1. ed. New York: Cambridge University Press, 2013, p. 29-30.

[209] Tradução livre do original, que verbera: "*As an example, a warship of one State is prohibited from conducting cyber operations that are adverse to the coastal nation's interests while in innocent passage*". *Ibidem*, p. 30.

[210] BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012, p.542.

Nesse sentido, os abalizados ensinamentos de Scott Shackelford acerca do tema demonstram claramente as dificuldades da questão da atribuição quanto aos ataques cibernéticos, o que se consubstancia através do seguinte excerto:

> […] atribuição é difícil porque os agressores podem marcar suas identidades, se dispersando pelas plataformas e jurisdições. Isso pode ser feito por causa de pelo menos três razões: a primeira é conceitual, a segunda é técnica, e a terceira é legal. Conceitualmente, atribuição significa diferentes coisas para diferentes pessoas. Para alguns, ela pode significar apenas identificar um endereço de IP; para outras, um estado ou uma organização; e para outras, um ser humano com uma causa. Tecnicamente, ataques sofisticados por *hackers* instruídos, quer seja privado ou patrocinado pelo governo, são difíceis de rastrear conclusivamente até sua fonte. A ciência de rastrear ataques cibernéticos tem sido um tanto quanto devagar de desenvolver em parte por causa do TCP/IP. Se um IP com um pacote de dados pode ser apanhado ou forjado no meio do caminho, se torna mais difícil de rastreá-lo até sua fonte. Desse modo, enquanto em teoria é possível localizar o endereço de IP de agressores cibernéticos e usar essas informações para identificar *hackers* individuais, *hackers* sofisticados podem redirecionar ou confundir os programas feitos para encontrá-los. Igualmente, se um *hacker* está usando uma *botnet* para conduzir os ataques, o processo de rastreamento dos pacotes de dados do IP se torna muito mais complexo e moroso[211].

Depreende-se, da análise do excerto acima, que a questão da atribuição por ataques cibernéticos perpassa três dificuldades, quais sejam, a conceitual, a técnica e a legal.

A conceitual está relacionada ao conceito que se dá à atribuição no âmbito cibernético. Não parece ter solução absoluta para a questão, todavia, a aferição do liame de um determinado evento a um estado será feita casuisticamente, sempre atentando para o que estabelece o Projeto (*draft*) de Artigos sobre Responsabilidade Internacional do Estado por Atos Internacionalmente Ilícitos, em seu capítulo II, artigos 4 a 11.

---

[211] O texto original verbera que "*[...] attribution is difficult because attackers can mark their identities, dispersing themselves across platforms and jurisdictions. This may be done because of at least three reasons: the first is conceptual, the second is technical, and the third is legal. Conceptually, attribution means different things to different people. To some, it might just mean identifying an IP address; to others, a state or an organization; and to others, a human being with a motive. Technically, sophisticated attacks by knowledgeable hackers, whether private or state sponsored, are difficult to trace definitively to their source. The science of tracing cyber attacks has been somewhat slow to develop in part because of TCP/IP. If an IP is packet can be grabbed or spoofed mid-route, it becomes more difficult to trace it back to where it actually began. Thus, whereas in theory it is possible to locate the IP address of cyber attackers and use that information to identify individual hackers, sophisticated hackers are able to re-route or otherwise confuse programs designed to locate them. Similarly, if a hacker is using botnet to carry out attacks, the process of tracing IP packets becomes much more involved and time consuming*". SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014, p. 146.

Já a dificuldade técnica exige aprofundamento acadêmico e doutrinário, não se afastando a importância de educar todos os cidadãos, haja vista que a conexão – sobretudo através da *internet* – do mundo moderno vulnerabiliza a todos os que acessam a informação pela via cibernética.

Sob o enfoque legal, o principal óbice encontrado na questão da atribuição de um ataque cibernético a um estado está na insuficiência das normas vigentes em se aplicarem aos modernos paradigmas trazidos pelo avanço tecnológico. Todavia, não se deve olvidar de buscar uma evolução normativa, criando normas que sejam tecnicamente condizentes com o âmbito cibernético, a fim de abarcar um maior número de situações.

A Corte Internacional de Justiça já afirmou, no julgamento do caso *Military and Paramilitary Activities in and against Nicaragua*, muito antes da era da informação e desenvolvimento cibernético, que a primeira medida a ser tomada é determinar quais fatos são relevantes ao caso, mas que "o problema não é o processo jurídico de imputação de um ato a um Estado em particular, com vistas ao estabelecimento da responsabilidade, mas o processo anterior de rastrear as provas matérias da identidade do perpetrador"[212].

Essa visão tem notória relevância quando se percebe que dificuldade de determinar quem foi o agente que realizou a conduta ilícita não é um estorvo enfrentado apenas no âmbito da *internet*. Nesse mesmo arrimo, os Estados Unidos declararam, em sua manifestação submetida ao Secretário-Geral da ONU sobre os estudos acerca dos desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional, que esses problemas "simplesmente refletem os desafios [...] que já existem em muitos outros contextos"[213].

---

[212] Tradução livre do original, que verbera: "*The problem is [...] not the legal process of imputing the act to a particular State for the purpose of establishing responsibility, but the prior process of tracing material proof of the identity of the perpetrator*". CORTE INTERNACIONAL DE JUSTIÇA. *Case concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. Estados Unidos). Decisão de mérito de 1986. ICJ Reports n. 520, p. 38-39, § 57.

[213] Tradução livre do original, que verbera: "*they simply reflect the challenges [...] that already exists in many contexts*". ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Developments in the Field of Information and Telecommunications in the Context of International Security*, *Study series n. 33*. UN Doc A/66/152, 2011, p. 36. Disponível em: <http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf>. Acesso em: 4.mai.2016.

Não obstante, os ataques realizados por meio de sistemas de informação trazem novas situações em que o avanço tecnológico e jurídico não viabiliza, de forma segura e confiável, a localização ou identificação do indivíduo perpetrador do aludido ataque, sendo inegável que esses desafios de atribuição são "particularmente evidentes no espaço cibernético, onde identificar quem está por trás de uma operação cibernética apresenta problemas técnicos significativos"[214].

Com efeito, o conjunto de dificuldades exposto demonstra a necessidade de se desenvolver normas específicas regulando a questão dos ataques cibernéticos no plano internacional. Recorrendo à jurisprudência internacional, notadamente à dicotomia entre as razões do caso *Military and Paramilitary Activities in and against Nicaragua* e do caso *The Prosecutor v. Duško Tadic*, se afigura mais abalizado que se utilize o critério deste, que exige apenas que o controle seja "genérico"[215], em detrimento daquela *ratio* que determina que o controle seja "efetivo"[216].

Diante da complexidade da atribuição no âmbito cibernético, é ponderoso que se utilize das disposições vigentes, ainda que sem total subsunção ao fato, para evitar que os atos ilícitos cometidos sejam propiciados, por ausência de coerção repressiva.

---

[214] Tradução livre do original, que verbera: "*It is indeniable, however, that these challenges are particularly evident in cyberspace, where identifying who is behind a cyber operation presents significant technical problems*". ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. In: *Cyberwar* (Ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein). New York: Oxford University Press, 2015, p. 215.

[215] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991. *The Prosecutor v. Duško Tadic Case*. Julgamento de 15 de julho de 1999. Case n. IT-94-1-A, p. 49-72, §§ 120 *et seq*.

[216] CORTE INTERNACIONAL DE JUSTIÇA. *Case concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. Estados Unidos). Decisão de mérito de 1986. ICJ Reports n. 520, p. 64-65, § 115.

6 CONCLUSÃO

Ante a análise de todas as razões expostas no presente trabalho, infere-se que as normas de responsabilidade internacional se aplicam a todos os atos que sejam considerados internacionalmente ilícitos, em decorrência de uma violação a uma obrigação validamente estabelecida. Em cumulação a este critério, é necessário que sejam alcançados os critérios de imputabilidade daquela conduta de inadimplência a um determinado sujeito de direito internacional.

Assim como violações à proibição do uso da força na forma cinética, ou qualquer outro inadimplemento de obrigação internacional, é possível que uma conduta realizada por meio de uma rede de computadores seja considerada contrária a uma obrigação validamente estabelecida. Destarte, infere-se que não há qualquer óbice para se admitir, de forma genérica, a aplicabilidade das normas sobre responsabilidade internacional ao âmbito cibernético.

Desse modo, é patente que um ataque cibernético pode ser considerando como um ato ilícito, basta que ele viole a esfera jurídica de outro Estado. Isso pode ser facilmente observado quando do ataque cibernético resultar dano, mas também pode ser aferível no momento em que a soberania de outro sujeito originário de direito internacional restar malferida.

Há de se atentar que para que haja o preenchimento dos requisitos da responsabilidade internacional do estado estabelecida nos Artigos sobre Responsabilidade formulados pela Comissão de Direito Internacional, a atribuição deve ser preenchida na forma prevista naquele instrumento normativo. Este é um elemento de caracterização muito difícil no âmbito cibernético. Grande parte da estrutura normativa do direito internacional fora elaborada para operações realizadas de forma cinética, e é necessária a evolução interpretativa da norma para que se adeque aos ataques cibernéticos.

Os ataques cibernéticos não devem permanecer em um campo cinzento. Não deve ser permitido que o descumprimento de uma obrigação em detrimento a um direito alheio não tenha consequência em razão de um vazio normativo – alegado por aqueles que acreditam não haver aplicabilidade das normas sobre responsabilidade internacional aos ataques cibernéticos. Assim, todos os artigos dos Artigos sobre

Responsabilidade do Estado por Atos Internacionalmente Ilícitos devem ser aplicados aos ataques cibernéticos.

Ainda assim, reside uma dificultosa questão quanto àqueles atos que assemelham ser do estado. É verdade que a complexidade dos sistemas de informação viabiliza falsear a origem do ataque cibernético, sendo inseguro se atribuir a conduta a um estado sem bases fáticas – e, portanto, probatórias – firmes. Aqueles atos em que seja constatado o exercício da autoridade governamental. De fato, é bem complexa a localização do atual perpetrador do ato. O desenvolvimento da estrutura da *internet* priorizou celeridade e inovações tecnológicas em detrimento da segurança e da rastreabilidade do real usuário do serviço pela *internet*.

A questão pode ser solucionada pela interpretação normativa realizada por famosos julgamentos do direito internacional. Enquanto o *Nicaragua Case* exige a observância do "controle efetivo", o *Tadic Case* exige o "controle genérico". Em razão das dificuldades técnicas de se provar a atribuição do Estado por ataques cibernéticos realizados com exercício de autoridade governamental, e considerando o regime excessivamente alto de ônus da prova exigido pelo parâmetro adotado na corrente do "controle efetivo", parece razoável e em consonância com a disciplina jurídico-normativa do direito internacional a adoção do padrão de "controle genérico" para a atribuição de ataques cibernéticos aos Estados.

Contudo, para se obstar que o Estado seja penalizado pelo fardo excessivo de assegurar que sua infraestrutura cibernética não será utilizada para afetar outros, deve ser levada em consideração, ainda, as ações do Estado supostamente perpetrador do ataque cibernético em amenizar o dano causado, ou auxiliar na localização do real perpetrador, após realizado o ataque.

Assim, caso observados os elementos exigidos nos Artigos sobre Responsabilidade do Estado por Atos Internacionalmente Ilícitos nos ataques cibernéticos, quais sejam, o descumprimento de obrigação e a atribuição aos Estados, estes seriam responsabilizados da mesma forma que se tivessem realizado a conduta ilícita da forma cinética. É inconteste, portanto, a aplicabilidade das normas sobre responsabilidade internacional aos ataques cibernéticos, desde quesses sejam atribuíveis a Estados.

Não obstante, determinar quem é responsável pelo ataque cibernético é apenas um dos passos necessários para se alcançar a segurança cibernética. É necessário tomar medidas para se desenvolver a infraestrutura cibernética e torná-la mais segura. Isso deverá ser desenvolvido não somente com avanços jurídicos, mas, sobretudo, ampliando a segurança da infraestrutura da *internet*, e criando meios técnicos para que o real perpetrador do ato seja identificado.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. A responsabilidade dos estados pela prática de ilícitos internacionais. *Revista da Faculdade de Direito da Universidade de São Paulo*. São Paulo: USP, v. 97, jan. 2002. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67557>. Acesso em: 22 nov. 2015.

ARENG, Liina. International Cyber Crisis Management And Conflict Resolution Mechanisms. In: *Peacetime Regime for State Activities in CyberSpace* (Ed. Katharina Ziolkowski). Tallinn: NATO CCD COE Publication, 2013.

BORGES, Thiago Carvalho. *Curso de Direito Internacional Público e Direito Comunitário*. São Paulo: Atlas, 2011.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Livro verde: segurança cibernética no Brasil* (organização Claudia Canongia e Raphael Mandarino Junior). Brasília: GSIPR/SE/DSIC, 2010.

BROWNLIE, Ian; CRAWFORD, James. *Brownlie's Principles of Public International Law*. 8. ed. Oxford: Oxford University Press, 2012.

CASELLA, Paulo Borba; ACCIOLY, Hildebrando Accioly; SILVA, Geraldo Eulálio do Nascimento e. *Manual de Direito Internacional Público*. 20. ed. São Paulo: Saraiva, 2012.

CASSESE, Antonio. *International law*. 2. ed. New York: Oxford University Press, 2005.

CERF Vinton G.; KAHN Robert E. *A Protocol for Packet Network Intercommunication*. IEEE Transactions on Communications. Vol. Com-22, No. 5, May 1974, p. 1.

_____. *IP Denial-of-Service Attacks*. CERT Advisory CA-1997-28. 1997. Disponível em:<http://www.cert.org/historical/advisories/CA-1997-28.cfm>. Acesso em: 25.abr.2016.

_____. *TCP SYN Flooding and IP Spoofing Attacks*. CERT Advisory CA-1996-21. 1996. Disponível em:<http://www.cert.org/historical/advisories/CA-1996-21.cfm>. Acesso em: 25.abr.2016.

COMISSÃO DE DIREITO INTERNACIONAL. *Commentaries to the Articles on Responsibility of States for Internationally Wrongful Acts*. Yearbook of the International Law Commission, vol. II, Part Two, 2001.

_____. *Draft articles on Responsibility of States for Internationally Wrongful Acts*. Documentos oficiais da Assembléia Geral da ONU, 56ª sessão. Suplemento n. 10 (A/56/10). New York, 2001.

COMISSÃO DE JURISTAS INTERNACIONAIS (através do árbitro exclusivo apontado para o caso, o juiz Max Huber). *Spanish Zone of Morocco* (Grã Bretanha *v*. Espanha). Decisão de 1925. 2 Reports of International Arbitral Awards 615.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. Comentários de 1987 do Comitê Internacional da Cruz Vermelha às disposições do Protocolo Adicional I às Convenções de Genebra de 1949. Disponível em: <https://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F5EA0CB6C1075C59C12563CD004345C3>. Acesso em: 9.mai.2016.

CONRAD, David. *Towards Improving DNS Security, Stability, and Resiliency*. Internet Society, 2012. Disponível em: <http://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf>. Acesso em: 27.abr.2016.

CONSTANTIN, Lucian. *Computer Trojan Horse Steals Credit Card Details From Hotel Reception Software*. *PC World Australia*, 19.abr.2012. Disponível em: <http://www.pcworld.com/article/254030/computer_trojan_horse_steals_credit_card_details_from_hotel_reception_software.html>. Acesso em: 8.mai.2016.

CORTE INTERNACIONAL DE JUSTIÇA. *Case concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. Estados Unidos). Decisão de mérito de 1986. ICJ Reports n. 520.

_____. *Case concerning the Barcelona Traction, Light and Power Company, Limited*. Julgamento de 5.fev.1970. ICJ Reports n. 337.

_____. *Case Concerning the Gabcikovo-Nagymaros Project* (Hungria v. Eslováquia). Julgamento de 25 de setembro de 1997. ICJ Reports n. 692.

_____. *Competence of the General Assembly for the Admission of a State to the United Nations*. Parecer consultivo de 3 de março de 1950. ICJ Reports n. 33.

_____. *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*. Parecer consultivo de 29 de abril de 1999. ICJ Reports n. 726.

_____. *Legality of the Threat or Use of Nuclear Weapons*. Parecer consultivo de 8 de julho de 1996. ICJ Reports n. 679.

_____. *Oil Platforms* (República Islâmica do Irã v. Estados Unidos da América). Julgamento de 6 de novembro de 2003. ICJ Reports n. 876.

_____. *Reparation for Injuries Suffered in the Service of the United Nations*. Parecer consultivo de 11 de abril de 1949. ICJ Reports n. 17.

CORTE PERMANENTE DE JUSTIÇA INTERNACIONAL. *Chorzów Factory Case*. Julgamento de 13 de setembro de 1928. PCIJ Series A n. 17.

_____. *Phosphates in Morocco*. Julgamento de 1938. P.C.I.J., Series A/B, n. 74.

CUPA, Basil. Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware). In: WEBSTER, C. William R.; CLAVELL, Gemma Galdon; ZURAWSKI, Nils; BOERSMA, Kees; SÁGVÁRI, Bence; BACKMAN, Christel; LELEUX, Charles (Editores). *Living in Surveillance Societies: 'The State of Surveillance'*. Barcelona: COST, 2012. Disponível em: <http://www.zora.uzh.ch/81157/1/Cupa_Living_in_Surveillance_Societies_2012.pdf>. Acesso em: 8.mai.2016.

DAVIES, Joe. TCP/IP Fundamentals for Windows In *Microsoft TechNet*. Chapter 2 – Architectural Overview of the TCP/IP Protocol Suite. 2. ed. 2007. Disponível em: <https://technet.microsoft.com/en-us/library/bb726993.aspx#EGAA>. Acesso em 19.abr.2016.

DINNISS, Heather Harrison. *Cyber warfare and the law of war*. New York: Cambridge University Press, 2012.

ESTADOS UNIDOS. Glossário disponibilizado no sítio eletrônico do Departamento de Segurança Nacional dos Estados Unidos. Disponível em: <https://niccs.us-cert.gov/glossary#letter_m>. Acesso em 22 nov. 2015.

_____. *An Assessment of International Legal Issues in Information Operations*. Departamento de Defesa dos Estados Unidos, 1999. Disponível em: <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf>. Acesso em: 11.mai.2016.

_____. Departamento de Defesa Nacional. *The National Strategy to Secure Cyberspace*. Washington: US Department of Homeland Security 2003. Disponível em: <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>. Acesso em 5.mai.2016.

_____. Federal Trade Commission. *Monitoring Software on Your PC: Spyware, Adware, and Other Software*. Washington: Federal Trade Commission, 2005. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf>. Acesso em: 8.mai.2016.

FALL, Kevin R.; STEVENS, W. Richard. *TCP/IP Illustrated, volume 1*. 2. ed. Michigan: Addison-Wesley, 2012.

FINKELSTEIN, Cláudio. Direito internacional. 2. ed. São Paulo: Atlas, 2013.

FRANÇA. Tratado Geral de Renúncia à Guerra de 1929 (Pacto Kellogg-Briand). Disponível em: <https://www.uni-marburg.de/icwc/dateien/briandkelloggpact.pdf>. Acesso em: 11.mai.2016.

GARDINER, Richard. *Treaty Interpretation*. 2. ed. New York: Oxford University Press, 2015.

GEERS, Kenneth. *Strategic Cyber Security*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2011.

GERCKE, Marco. Cybercrime, Terrorist Use of the Internet and Cyberwarfare: The Importance of Clear Distinction. *In*: VOICA, Dan-Radu (Editor). *Trends and Developments in Contemporary Terrorism*. Amsterdam: IOS Press, 2012.

GJELTEN, Tom. *Extending the Law of War to Cyberspace*. NPR, edição de 22.set.2010. Disponível em: <http://www.npr.org/templates/story/story.php?storyId=130023318>. Acesso em: 11.mai.2016.

GONT, Fernando. *Security assessment of the internet protocol*. United Kingdom's Centre for Protection of the National Infrastructure. 2008. Disponível em: < http://web.archive.org/web/20100211145721/http://www.cpni.gov.uk/Docs/InternetProtocol.pdf>. Acesso em: 25.abr.2016.

GUERRA, Sidney. *Curso de Direito Internacional Público*. 7. ed. São Paulo: Saraiva, 2013.

HARRIS, David. *Cases and Materials on International Law*. 7. ed. London: Sweet & Maxwell, 2010.

INSTITUTO INTERNACIONAL DE DIREITO HUMANITÁRIO. Manual de Sanremo sobre o Direito Internacional Aplicável aos Conflitos Armados no Mar de 1994. Disponível em: <http://assets.cambridge.org/97805215/58648/excerpt/9780521558648_excerpt.pdf>. Acesso em: 9.mai.2016.

JANIS, Mark Weston. *An Introduction to International Law*. 4. ed. New York: Aspen Publishers, 2003.

KUHN, Rick; SRIRAM, Kotikalapudi; MONTGOMERY, Doug. *Border Gateway Protocol Security: Recommendations of the National Institute of Standards and Technology*. Gaithersburg: US National Institute of Standards and Technology, 2007. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf>. Acesso em 5.mai.2016.

KYYRÖNEN, Vesa. *Machines Making Decisions: The Applicability of State Responsibility Doctrine in the Case of Autonomous Systems*. Helsinki: Helsingin Yliopisto, 2015. Disponível em: <https://helda.helsinki.fi/bitstream/handle/10138/153596/Vesa%20Kyyronen%20-%20thesis%20ready.pdf?sequence=4>. Acesso em: 11.mai.2016.

LANDWEHR, Carl E.; BULL, Alan R.; MCDERMOTT, John P.; CHOI, William S. . *A Taxonomy of Computer Program Security Flaws, with Examples*. ACM Computing Surverys, 26,3, 1994. Disponível em: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA465587>. Acesso em: 7.mai.2016.

LIPSON, Howard F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. Pittsburgh: Carnegie Mellon Software Engineering Institute, 2002. Disponível em: <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408853>. Acesso em: 22 nov. 2015.

MAZZUOLI, Valério de Oliveira. *Curso de Direito Internacional Público*. 7. ed. São Paulo: Revista dos Tribunais, 2013.

MCAFEE. McAfee Threat Glossary. Disponível em: <http://www.mcafee.com/us/threat-center/resources/threat-glossary.aspx>. Acesso em: 22 nov. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior affair*. UNRIAA, vol. XX, Sales n. E/F.93.V.3, 1990.

_____. Assembléia Geral. *Resolução n. 3314 (XXIX): Definição de Agressão*. Disponível em: <http://crimeofaggression.info/documents/6/1974_GA_RES_3314.pdf>. Acesso em: 11.mai.2016.

_____. *Carta das Nações Unidas*. 1945. Disponível em: <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>. Acesso em: 12.abr.2016.

_____. Convenção de Viena sobre o DIreito dos Tratados de 1969. Disponível em: <https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf>. Acesso em: 12.abr.2016.

_____. *Developments in the Field of Information and Telecommunications in the Context of International Security, Study series n. 33*. UN Doc A/66/152, 2011. Disponível em: <http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf>. Acesso em: 4.mai.2016.

_____. International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991. *The Prosecutor v. Duško Tadic Case*. Julgamento de 15 de julho de 1999. Case n. IT-94-1-A.

ORGANIZAÇÃO DO TRATADO DA AMÉRICA DO NORTE. Grupo de Especialistas Internacionais. Tallinn Manual on the International Law Applicable to Cyber Warfare (Editor geral Michael N. Schmitt). 1. ed. New York: Cambridge University Press, 2013.

ÖYKÜIRMAKKESEN. *The Notion of Armed Attack under the UN Charter and the Notion of International Armed Conflict – Interrelated or Distinct?*. Geneva: Geneva Academy, 2014. Disponível em: <http://www.prix-henry-dunant.org/sites/prixhd/doc/2014_IRMAKKESEN_Paper.pdf>. Acesso em: 11.mai.2016.

PORTELA, Paulo Henrique Gonçalves. *Direito Internacional Público e Privado*. 5. ed. Salvador: JusPodivm, 2013.

PROGRAMA DE PESQUISA EM POLÍTICA E CONFLITOS HUMANITÁRIOS. Manual sobre o Direito Internacional Aplicável à Guerra Aérea e por Mísseis de

2009. Disponível em: <http://ihlresearch.org/amw/HPCR%20Manual.pdf>. Acesso em: 12.mai.2016.

REKHTER, Yakov; LI, Tony. *A Border Gateway Protocol 4*. Internet Engineering Task Force (IETF) Request for Comments (RFC) 1771, 1995. Dispobível em: <https://tools.ietf.org/html/rfc1771>. Acesso em: 1º.mai.2016.

RESENDE, Ranieri Lima. Responsabilidade dos estados por atos internacionalmente ilícitos: perspectivas atuais. *Revista da Faculdade de Direito de Minas Gerais*. Belo Horizonte: Nova Fase, n. 45, jul./dez., 2004. Disponível em: < http://www.direito.ufmg.br/revista/index.php/revista/article/viewFile/1299/1231>. Acesso em: 22 nov. 2015.

REZEK, Francisco. *Direito Internacional Público: curso elementar*. 14. ed. São Paulo: Saraiva, 2013.

ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. In: *Cyberwar* (Ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein). New York: Oxford University Press, 2015.

ROWLAND, Craig. *Covert Channels in the TCP/IP Protocol Suite*. First Monday Journal, 1997, Volume 2, Number 5. Disponível em: <http://www.firstmonday.org/issues/issue2_5/rowland/>. Acesso em: 25.abr.2016.

SAMANI, Raj; PAGET, François. *Cybercrime exposed: cybercrime-as-a-service*. Santa Clara: McAfee, 2013. Disponível em <http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf>. Acesso em: 7.mai.2016.

SCHMITT, Michael N. *"Attack" as a Term of Art in International Law: The Cyber Operations Context*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012.

SHACKELFORD, Scott J. *Managing cyber attacks in international law, business, and relations: in search of cyber peace*. New York: Cambridge University Press, 2014.

SHAW, Malcolm Nathan. *International Law*. 5. ed. Cambridge: Cambridge University Press, 2003.

SILVA, Roberto Luiz. *Direito Internacional Público*.4. ed. Belo Horizonte: Del Rey, 2014.

STALLINGS, William; BROWN, Lawrie. *Computer Security: Principles and Practice*. 3. ed. New Jersey: Pearson, 2015.

SYMANTEC. Glossário da empresa Norton by Symantec. Disponível em: <http://us.norton.com/security_response/glossary/define.jsp?letter=t&word=trojan-horse>. Acesso em: 7.mai.2016.

TERRY, Douglas B.; PAINTER, Mark; RIGGLE, David W.; ZHOU, Songnian. *The Berkeley Internet Name Domain Server*. Computer Systems Research Group, 1984.

Disponível em: <http://www.eecs.berkeley.edu/Pubs/TechRpts/1984/CSD-84-182.pdf>. Acesso em: 26.abr.2016.

WALKER, Paul A. *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*. American University-Washington College of Law. National Security Law Brief, vol. 1, iss. 1, 2011. Disponível em: <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1002&context=nslb>. Acesso em: 9.mai.2016.

WATTS, Sean. Low-Intensity Cyber Operations and the Principle of Non-Intervention. In: *Cyberwar* (Ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein). New York: Oxford University Press, 2015.

WITTGENSTEIN, Ludwig. Tratado filosófico. 2. ed. Lisboa: Fundação Caloste Gulbenkian, 1995.

WRIGHT, Cory. *Understanding Kaminsky's DNS Bug*. Linux Journal, 2008. Disponível em: <http://www.linuxjournal.com/content/understanding-kaminskys-dns-bug>. Acesso em: 02.mai.2016.