doi: 10.5102/rdi.v9i2.1755

O direito internacional humanitário e a

International humanitarian law and the emergence of cyberwar

José Pedro Teixeira Fernandes[1]

Resumo

Em O Direito Internacional Humanitário e a Emergência da Ciberguerra o autor analisa os desafios levantados pelos ataques e conflitos cibernéticos às normas de Direito Internacional Humanitário atualmente existentes. O principal objetivo do artigo é apresentar um sucinto state of the art em matéria de regulação jurídica internacional da ciberguerra. O objetivo é também discutir o conceito de ciberguerra a partir de uma abordagem estratégica e de segurança para, em seguida, analisar em que medida a regulação do DIH deverá aplicar-se a ela. A análise se assenta em uma revisão de literatura, essencialmente norte-americana, pois é aí que a reflexão sobre os seus aspectos legais se encontra mais avançada e aprofundada. A conclusão é a de que, apesar de ser líquido não estarmos perante um vazio jurídico, o enquadramento pelo DIH não está isento de dificuldades, sendo talvez a mais notória atribuição da responsabilidade em um ciberataque.

Palavras-chave: Direito Internacional Humanitário. Ciberguerra. Segurança.

Abstract

In International Humanitarian Law and the Emergence of Cyberwar, the author analyzes the challenges posed by cyberattack and cyberconflicts to the International Humanitarian Law that currently exists. Thus, the main purpose of the paper is to present a state of the art in the field of international legal regulation of cyberwar. The aim is also to address the conceptualization of cyberwar from a strategic and security perspective, then to examine at what extent the regulation of IHL should be applied. The article contains a brief review of the literature, especially of the American approach to the subject, where we can find the legal analysis more advanced. The conclusion is that despite being clear that we are not facing a legal vacuum the application of the IHL is not without difficulties. Perhaps the most notorious is the attribution of responsibility in a cyberattack.

Keywords: International Humanitarian Law. Cyberwar. Security.

* Artigo recebido em 29/12/2011
Artigo aprovado em 19/05/2012

[1] Professor auxiliar convidado na licenciatura em Ciência Política e Estudos Eleitorais da Faculdade de Ciências Sociais e Humanas da Universidade Lusófona do Porto.

1 Introdução

> [A legislação internacional sobre a] guerra é largamente reativa por natureza – uma coletânea de regulações retrospectivas modeladas nos conflitos do passado. Evoluções, e até mesmo revoluções, na forma de fazer a guerra raramente inspiram disposições legais novas ou adaptadas. Em vez disso, os assessores jurídicos e especialistas do Direito Internacional analisam as inovações na estratégia, meios e métodos de guerra sob uma lei e tradição antigas – de décadas ou até de séculos (Sean Watts).[2]

A ciberguerra é um fenômeno novo, complexo e multifacetado. Para o seu estudo, convergem, entre outras, as perspectivas tecnológica, estratégica, de segurança, política e jurídica. No seu uso mais comum, designa vagamente algum tipo de "ataque" ou "represália", intrusão ilícita em uma rede e/ou computador que ocorre usando meios informáticos, ação essa ligada ou não a conflitos políticos envolvendo atores estaduais e/ou não estaduais a uma conflitualidade cinética. O que neste artigo nos propomos efetuar é, naturalmente, um uso mais rigoroso do conceito de ciberguerra, o qual vai para além da sua utilização livre. A clareza e o rigor no uso dos conceitos são fundamentais não só para a segurança jurídica, como para a decisão política no caso de um ciberconflito envolvendo atores estaduais. Um esforço de rigor acadêmico-científico no uso dos conceitos e teorias encerra também as suas próprias dificuldades. No contexto da investigação jurídica vale a pena relembrar aqui uma reflexão efetuada no século passado pelo jurista alemão Reinhold Zippelius, que permanece inteiramente válida. Como ele fez notar, os conceitos são, na sua essência, combinações de traços comuns a vários objetos. Todavia, os aspectos comuns que pomos em evidência e incluímos neles dependem muito daquilo por que nos interessamos. Por outras palavras, os conteúdos e contornos dos conceitos estão estreitamente ligados aos objetivos de uma investigação concreta no âmbito da qual vão ser utilizados[3]. Por isso, mesmo no contexto de estudos acadêmico-científicos rigorosos, a maneira como se usa um conceito não é necessariamente coincidente. Naturalmente que isso se aplica ao estudo da ciberguerra, no qual, para além da questão conceptual, várias interrogações preliminares se colocam.

Sendo a ciberguerra uma nova dimensão da guerra, resultante de avanços tecnológicos inexistentes na altura da elaboração das normas de Direito Internacional Humanitário (DIH) e de Direito dos Conflitos Armados (DCA), em que medida pode ser regulada pelo DIH/DCA existente? Ocorrendo um determinado ciberataque, em que circunstâncias poderá ser considerado um ato de guerra? E os intervenientes numa ciberguerra devem ser tratados de forma similar aos combatentes numa guerra cinética? Quanto às ciberarmas, em que condições podem ser legalmente equiparadas a armas "físicas" e abrangidas por similares restrições às que constam no atual DIH/DCA? Em face a essas múltiplas e complexas questões, o principal objetivo deste artigo é apresentar o que usualmente se designa pelo *state of the art* em matéria de enquadramento legal da ciberguerra. Isso será feito de uma forma sucinta pelas condicionantes de espaço de uma publicação sob a forma de artigo. Assim, vamos proceder a uma revisão de literatura, sobretudo norte-americana. Como principal potência mundial e pioneira na criação da Internet, nos EUA há um interesse particular pelo uso das redes e tecnologias de informação para fins militares e de segurança. Existe também uma crescente preocupação estratégica com as vulnerabilidades que daí resultam. A reflexão jurídica sobre essas questões encontra um terreno fértil, pelo que, naturalmente, está aí mais avançada e aprofundada. O nosso intuito é identificar e avaliar alguns dos principais esforços já empreendidos nessa temática de crescente importância estratégica, de segurança, política e jurídica. Para efeito, a abordagem do artigo foi estruturada da seguinte forma: em um primeiro ponto, vamos efetuar uma breve resenha histórica sobre a origem dessa área jurídica – o DIH/DCA – e discutir a terminologia que melhor a designa. Em um segundo ponto, abordar a gênese e evolução da ideia de ciberguerra no âmbito dos estudos estratégicos e de segurança militar, e traçar uma conceptualização rigorosa dela, nomeadamente em face de outros conceitos afins. Em seguida, ocupamo-nos sucessivamente da questão da legalidade do recurso à ciberguerra, da problemática da qualificação de um ciberataque como um ataque armado e, por último, do delicado problema da atribuição de responsabilidade num ciberataque.

[2] WATTS, Sean. Combatant status and computer network attack. *Virginia Journal of International Law*, Virginia, v. 50, n.2, p. 392, 2010. (Tradução para a Língua Portuguesa efetuada pelo autor do artigo).

[3] ZIPPELIUS, Reinhold. *Filosofia do direito*. Lisboa: Quid Juris, 2010. p. 23.

2 Direito internacional humanitário ou direito dos conflitos armados?

Antes de mais nada, importa esclarecer uma questão terminológica: Direito Internacional Humanitário ou Direito dos Conflitos Armados? A dúvida surge quanto a saber se ambas as designações podem ser consideradas sinônimas, ou, em caso de resposta negativa, qual deverá ser usada preferencialmente pelo seu maior rigor na designação do domínio jurídico em causa. Sobre essa questão terminológica, o jurista francês Michel Deyra sustenta que, apesar de as Nações Unidas utilizarem preferencialmente a expressão Direito dos Conflitos Armados, a designação de Direito Internacional Humanitário é a mais adequada. O argumento utilizado é o de que as disposições que integram essa área do Direito são, essencialmente, uma transposição das preocupações de ordem moral e humanitária. Além disso, acrescenta o autor que "a expressão direito da guerra encontra-se atualmente abandonada a partir do momento em que caducou o conceito do estado de beligerância, ou, pelo menos, desde a adopção do princípio da proibição do recurso à força".[4] Idêntica posição é adotada por Marco Sassòli, Antoine Bouvier e Anne Quintin em uma publicação efetuada pelo Comité Internacional da Cruz Vermelha, em que dão preferência à designação Direito Internacional Humanitário. Esses juristas recordam que o referido ramo do Direito Internacional Público começou a desenvolver "[...] numa altura em que o uso da força era entendido como uma forma legal das relações internacionais, quando os Estados não estavam proibidos de travar a guerra"[5] – ou seja, quando o *jus ad bellum* era um recurso "normal" dos Estados. Um papel pioneiro na criação de uma consciência coletiva internacional, impulsionadora de regulação jurídica nessa área, deve-se a um suíço do século XIX, Henry Durant. Este foi também o principal fundador da Cruz Vermelha Internacional (1863), em Genebra. Em um pequeno, mas influente livro, *Uma Memória de Solferino*[6], relatou os acontecimentos que marcaram decisivamente o rumo da sua vida e o levaram a impulsionar o movimento internacional humanitário. Todavia, como Sassòli, Bouvier e Quintin sublinham, a situação na atualidade é substancialmente diferente daquela na qual se deu o nascimento do DIH, pela ação pioneira de Henry Durant. Hoje, o uso da força entre os Estados "é proibido por uma regra peremptória do Direito Internacional" – o *jus ad bellum* transformou-se num *jus contra bellum*. Exceções legais são admitidas apenas "[...] no caso da defesa individual ou coletiva baseada em resoluções do Conselho de Segurança das Nações Unidas e, sem dúvida, no caso do direito dos povos à autodeterminação (guerras de libertação nacional)".[7]

Dentro de uma linha similar, Robert Kolb e Richard Hyde[8] explicam que a origem de duas diferentes terminologias está intrinsecamente ligada à evolução histórica dessa área do Direito Internacional (Público). Em primeiro lugar, surgiu o termo mais antigo – "lei da guerra" – ou leis da guerra. "Um equivalente destes termos será a frequentemente usada expressão neolatina *jus in bello*, que significa literalmente lei na guerra". Posteriormente, foi cunhada a designação Direito dos Conflitos Armados, que se tornou de utilização corrente a partir da entrada em vigor das quatro Convenções de Genebra

[4] DEYRA, Michel. *Direito internacional humanitário.* Lisboa: Procuradoria-Geral da República/Gabinete de Documentação e Direito Comparado, 2001. p. 15.

[5] SASSÒLI, Marco; BOUVIER, Antoine; QUINTIN, Anne. *How does Law Protect in War? Outline of International Humanitarian Law*. 3. ed., Genebra: International Committee of the Red Cross, 2001. v. 1. p. 14.

[6] A batalha de Solferino, ocorrida na Lombardia, opôs, no Verão de 1859, as tropas da Sardenha-Piemonte em coligação com a França, às tropas do Império Austríaco o qual, na época, governava grande parte do Norte de Itália. Esta sangrenta batalha, uma das várias campanhas militares que precederam a unificação italiana de 1861, envolveu mais de 200.000 soldados, originando alguns milhares de mortos e feridos de ambos os lados. Henry Durant encontrava-se numa cidade próxima do local de confronto militar devido a uma deslocação por motivos de negócios ao Norte de Itália. Assim, acabou por observar pessoalmente o terrível sofrimento dos soldados feridos e abandonados no campo de batalha por falta de assistência e meios médicos de tratamento. Em termos mais gerais, o contexto deste acontecimento era uma de uma Europa em plena transformação, pela ação conjugada das revoluções liberais e nacionalistas e da revolução industrial. Ambos os movimentos estavam transformando profundamente o panorama econômico e social e a forma de fazer a guerra. Quanto a esta última, a guerra, estava se transformando numa atividade cada vez mais mortífera, pelos avanços tecnológicos da indústria de armamento. Ver: DURANT, Henry. A memory of Solferino. Genebra: International Committee of the Red Cross, 1986.

[7] SASSÒLI; BOUVIER; QUINTIN, op. cit. p. ?

[8] KOLB, Robert; HYDE, Richard. An introduction to the International Law of Armed Conflicts. Oxford-Portland: Hart Publishing, 2008. p. 16.

(1949). Estas, no seu artigo 2º – o qual é de teor comum –, usam a expressão "conflito armado".[9] O termo foi introduzido com o intuito de aumentar o número de conflitos cobertos pelas normas que regulam a ação do Estado nessa área. Antes das Convenções de Genebra, a declaração de "estado de guerra" regia a aplicação das normas da lei da guerra, não cobrindo todas as situações de fato de combate. Dependia, antes, da escolha livre, potencialmente arbitrária, de um Estado, de se considerar em guerra com outro. O termo "conflito armado" superou esse problema na medida em que passou a abranger todas as formas *de* fato de combate, independentemente de elas serem formalmente qualificadas como guerra, ou não, pelos Estados envolvidos. Assim, a terminologia "Direito dos Conflitos Armados" expressa uma mudança da cobertura legal, que passa da "guerra" para o "conflito armado". Tal mudança tornou claro que as regras que protegem as vítimas e limitam os meios e os métodos de combate são aplicáveis a todas as situações nas quais as hostilidades factualmente têm lugar e não ficam limitadas às guerras formalmente declaradas.[10] Por último, mais recentemente, surgiu o termo Direito Internacional Humanitário. A sua origem encontra-se estreitamente ligada ao movimento da Cruz Vermelha, a qual, de forma pioneira, o usou para descrever o conteúdo essencial da moderna lei da guerra, tal como expressa nas Convenções de Genebra. Enquanto o foco das Convenções de Haia de 1899 e 1907

> [...] foram os meios e os métodos de combate dos beligerantes, as Convenções de Genebra deslocaram o foco para a proteção das vítimas da guerra, tais como o pessoal militar ferido e doente, os prisioneiros de guerra e os civis. As enormes e generalizadas atrocidades cometidas pelas Potências do Eixo durante a II Guerra Mundial, contra os prisioneiros e civis, foram as razões desta mudança.[11]

Quer dizer, descontadas algumas nuances,[12] essas duas terminologias são essencialmente coincidentes. Pelas razões explicadas, Direito Internacional Humanitário é a terminologia mais frequentemente usada, pelo que vai ser também aquela que usaremos ao longo deste trabalho. Em termos de objeto de estudo, pode ser definido como o ramo do Direito Internacional que limita o uso da violência nos conflitos armados, mediante várias formas: i) poupando aqueles que não participam nas hostilidades ou deixaram de participar diretamente delas; ii) limitando a violência ao montante necessário para atingir o objetivo do conflito, o qual apenas pode ser – independentemente das causas pelas quais se luta –, enfraquecer o potencial militar do inimigo. O DIH integra um conjunto de normas convencionais – baseadas em acordos ou tratados concluídos entre os Estados, ou de origem consuetudinária – assentes nos costumes internacionais –, as quais têm por objetivo específico regular juridicamente as situações que surgem no decurso de conflitos armados internacionais. Essa definição leva-nos aos princípios básicos do DIH, que assentam em: i) distinção entre civis e militares; ii) proibição de atacar aqueles que estão fora de combate; iii) proibição de infligir sofrimentos desnecessários; e iv) principio da necessidade e princípio da proporcionalidade no uso da força.[13]

[9] Por exemplo, o artigo 2º da Convenção (I) de Genebra para Melhorar a Situação dos Feridos e Doentes das Forças Armadas em Campanha, tem o seguinte teor (a ênfase em negrito é de nossa autoria): "Além das disposições que devem entrar em vigor desde o tempo de paz, a presente Convenção aplicar-se-á em caso de guerra declarada ou de qualquer outro conflito armado que possa surgir entre duas ou mais das Altas Partes contratantes, mesmo que o estado de guerra não seja reconhecido por uma delas […]". Disponível em: <http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhuniversais/dih-conv-I-12-08-1949.html - capII>. Acesso em: 8 nov. 2011.

[10] KOLB, Robert; HYDE, Richard. *An introduction to the international law of armed conflicts*. Oxford-Portland: Hart Publishing, 2008.

[11] Ibidem, p.16-17.

[12] Ibidem, p. 20. Ver também: SASSÒLI; BOUVIER; QUINTIN, 2001, p. 14.

[13] Esta definição de Direito Internacional Humanitário encontra-se na 3ª edição de How Does Law Protect in War, uma publicação efetuada pelo Comité Internacional da Cruz Vermelha de Genebra, da autoria de Marco Sassòli, Antoine Bouvier e Anne Quintin, How Does Law Protect in War*? v. 1,* Outline of International Humanitarian Law, 3. ed., Genebra: International Committee of the Red Cross, 2001, p.1. Similar definição é avançada no manual introdutório ao Direito Internacional Humanitário de KOLB, Robert; HYDE, Richard. *An Introduction to the international law of armed conflicts*. Oxford-Portland: Hart Publishing, 2008. p. 15-16.

Tabela 1: As Fontes do Direito Internacional Humanitário (DIH)

Fonte	Título	Data	Nº Artigos
Convenção de Genebra	Melhoria da Condição dos Feridos no Campo de Batalha	1864	10
II Conferência de Haia	Leis e Costumes da Guerra em Terra	1899	60 (55 em Anexo)
IV Conferência de Haia	Leis e Costumes da Guerra em Terra	1907	64 (56 em Anexo)
Protocolo de Genebra	Para a Proibição do Uso na Guerra de Gás Asfixiante e dos Métodos de Guerra Bacteriológica	1928	___
I Convenção de Genebra	Para Melhoria das Condições dos Feridos e Doentes das Forças Armadas no Terreno	1864 (revista em 1949)	77 (13 em Anexo)
II Convenção de Genebra	Para Melhoria das Condições dos Feridos, Doentes e Náufragos das Forças Armadas no Mar	1949	63
III Convenção de Genebra	Relativa ao Tratamento dos Prisioneiros de Guerra	1929 (revista em 1949)	143
IV Convenção de Genebra	Relativa à Proteção de Civis em Tempo de Guerra	1949	180 (21 em Anexo)
Convenção de Genebra	Proibindo o Desenvolvimento, Produção e Armazenamento de Armas Bacteriológicas e Tóxicas e sobre a sua Destruição	1975	15
Protocolo I	Relativa à Proteção das Vítimas de Conflitos Armados Internacionais (amplia a definição dos mesmos às guerras de libertação nacional)	1977	102
Protocolo II	Relativa à Proteção das Vítimas de Conflitos Armados Não Internacionais (completa o art.º 3 comum as quatro Convenções de Genebra)	1977	28
Protocolo III	Relativa à Adoção de um Emblema Adicional Distintivo	2005	17

Fonte: EASTWEST INSTITUTE. Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace, 2011. p. 13 (adaptação).

Conforme já referido, o DIH desenvolveu-se por várias fases ligadas a períodos marcantes da evolução europeia e mundial. As regras mais antigas do DIH, também designadas pelo Direito de Haia, surgiram entre finais do século XIX e início do século XX. Contêm essencialmente princípios legais aplicáveis à condução de operações militares. A maior parte das suas disposições encontra-se nas Convenções de Haia de 1899 (revistas em 1907) – daí a designação por Direito de Haia –, existindo também disposições relevantes no seu âmbito que se encontram no Protocolo I Adicional às Convenções de Genebra (1949), que contêm regras sobre os direitos e deveres dos militares participantes na conduta das operações militares e limita os meios que podem ser usados para infligir danos ao inimigo. Tais regras jurídicas procuram articular as necessidades militares das partes em conflito, com princípios fundamentais de humanidade e de dignidade humana.

Uma segunda fase de evolução ocorreu a partir de meados do século XX e é consequência direta das tragédias militares da primeira metade do século passado, sobretudo da II Guerra Mundial. Aqui se inserem as quatro Convenções de Genebra (1949) para a proteção das vítimas de guerra às quais acrescem dois Protocolos Adicionais (1977). Essas convenções internacionais – também conhecidas como Direito de Genebra, são o conjunto jurídico mais volumoso do DIH, perfazendo aproximadamente seiscentos artigos. Esse normativo foi elaborado, como, aliás, os próprios títulos das quatro convenções sugerem, com o objetivo primordial de dar proteção às vítimas de guerra. Incluem-se no âmbito do Direito de Genebra, quer os civis que não participam em ações militares, quer os militares que estão fora de operações de combate.

A essas duas fases de evolução do DIH podemos eventualmente acrescentar ainda uma terceira, a mais recente historicamente, ligada às atividades da Organização das Nações Unidas (ONU) – a que, por vezes, chama-se Direito de Nova Iorque, por alusão à sede da organização. O início dessa fase pode datar-se da segunda metade

da década de 60, sobretudo devido à ação da Assembleia Geral das Nações Unidas nessa área. O seu marco simbólico foi a Resolução 2444 (XXIII), adotada em 1968 sob o título "Respeito dos Direitos Humanos em período de conflito armado". No seu âmbito, surgiram também resoluções sobre a questão do uso legítimo da força efetuada por movimentos de autodeterminação nacional (guerras de libertação nacional) e foram dados impulsos à interdição ou limitação do uso de determinados tipos de armamento.

3 A emergência da ciberguerra nos conflitos internacionais

No início dos anos 90 do século passado, em *Ciberwar is Coming!* (1993), John Arquilla e David Ronfeldt procuraram traçar os contornos de uma futurista "ciberguerra" (*cyberwar*). Esses dois norte-americanos da *Rand Corporation* integram o grupo dos pioneiros que anteciparam a evolução do ciberespaço para um novo terreno de batalha dos conflitos internacionais, paralelamente aos tradicionalmente existentes: terra, mar e ar. Estávamos, então, nos primórdios da sociedade em rede[14] tal como hoje a conhecemos, em termos de uso da Internet, da Web, de comunicações móveis e de outras tecnologias digitais. Para clarificar a sua conceptualização, os autores procuraram destrinçar o conceito de ciberguerra de outros próximos, nomeadamente da infoguerra" (*netwar*). Quanto a esta última, a infoguerra, foi definida como:

> [...] um conflito relacionado com a informação a um grande nível, entre Estados ou sociedades. Significa tentar desarticular, danificar ou modificar o que uma população "sabe", ou pensa que sabe, sobre ela própria e o mundo à sua volta. A infoguerra pode focalizar-se na opinião pública, ou da elite, ou de ambas. Pode envolver medidas de diplomacia pública, propaganda e campanhas psicológicas, subversão cultural e política, induzir em engano ou interferir com os *media* locais, infiltrações em redes de computadores e bases de dados e esforços para promover movimentos dissidentes e de oposição através das redes de computadores.[15]

Uma vez clarificado esse conceito afim, Arquilla e Ronfeldt procuraram definir o conceito de ciberguerra propriamente dito. Na sua ótica, ela se refere a:

> [...] conduzir e preparar para conduzir, operações militares de acordo com os princípios da informação [...] Esta forma de guerra pode envolver diversas tecnologias – nomeadamente C3I[16]; recolha de informação, posicionamento e identificação de amigos ou inimigos (IFF)[17]; e sistemas de armas "inteligentes" – para dar apenas alguns exemplos. Pode também envolver interferência electrónica, falseamento, sobrecarga e intrusão nos circuitos de informação e comunicação de um adversário. [...] Poderá também implicar o desenvolvimento de novas doutrinas sobre o tipo de forças necessárias, onde e como deslocá-las, e saber o quê e como atacar no lado do inimigo. Como e onde posicionar determinados tipos de computadores e sensores relacionados, redes, bases de dados, etc., pode-se tornar tão importante como a questão que costumava ser efetuada sobre deslocação de bombardeiros e as suas funções de suporte. A ciberguerra pode também ter implicações para a integração dos aspectos políticos e psicológicos com os aspectos militares de fazer a guerra.[18]

Importa relembrar que esta conceptualização data de 1993, em uma altura na qual, como já referimos, a Internet e sociedade em rede estavam a dar os primeiros passos e era difícil discernir a evolução futura. Daí que Arquilla e Ronfeldt tenham sido também bastante cautelosos na sua formulação prospectiva. Na publicação original, eles faziam notar o seguinte[...] como inovação na forma de fazer a guerra, antecipamos que a ciberguerra pode ser para o século XXI o que a *blitzkrieg* foi para o século XX. Mas, por agora, também acreditamos que o conceito é demasiado especulativo para uma definição precisa".[19] O conceito de ciberguerra, tal como definido por Arquilla e Ronfeldt, tornou-se influente pelo prestígio dos autores e da Rand Corporation à qual estão ligados, bem como pelo seu carácter pioneiro e "futurista". Tal como ocorreu frequentemente no século XX, com muitas inovações em diferentes domínios, o conceito projetou-se rapidamente para fora dos EUA, interessando, em primeira linha, aos meios estratégico-militares de diferentes países.

[14] Ver, entre outros: CASTELLS, Manuel. *A sociedade em rede*. Lisboa: Fundação Calouste Gulbenkian, 2002. v. 1.

[15] ARQUILLA, John; RONFELDT, David. Cyberwar is Coming! (Ed.). In: *Athena's Camp:* preparing for conflict in the information age. Santa Monica CA: Rand Corp, 1997. p. 23. (Reedição do artigo originalmente publicado na *Comparative Strategy,* v. 12, n. 2, 1993).

[16] Communications, Command, Control and Intelligence.

[17] Identification-Friend-or-Foe.

[18] ARQUILLA; RONFELDT, op. cit., p. 30-31.

[19] ARQUILLA; RONFELDT, 1997. p. 31.

Nesse domínio, marcado frequentemente por avanços tecnológicos espetaculares em curtos espaços de tempo, naturalmente que há outros desenvolvimentos relevantes que importa tê-los em conta. Nos últimos anos, em especial desde os conflitos da Estônia (2007) e da Geórgia (2008) com a Rússia, tem-se assistido a um crescente interesse pela questão dos ciberataques e a uma maior sofisticação das abordagens teóricas. De fato, esses conflitos serviram, de alguma forma, de terreno de ensaio para uma nova dimensão deles, ligada ao ciberespaço. Quanto a este último, o ciberespaço, não existe um consenso sobre o que ele abrange (ou deve abranger) exatamente. Uma possível definição é a utilizada pelo governo norte-americano, que o caracteriza como "[...] a rede de infraestruturas de tecnologias de informação interdependentes que inclui a Internet, redes de telecomunicações, sistemas computacionais e processadores e controladores embebidos em indústrias críticas".[20]

Paralelamente, em termos de desenvolvimentos teóricos, constatou-se o aparecimento crescente de análises mais aprofundadas e apuradas, quer da parte dos meios militares e de segurança, quer de organizações internacionais, de *think tanks*, de acadêmicos ou de outros interessados. Nesse contexto, diferentes conceptualizações de ciberguerra surgiram também. Destaca-se, aqui, a proposta pelo *Institute for Advanced Study of Information Warfare* dos EUA. Tal instituição norte-americana define a ciberguerra como "[...] o uso ofensivo e defensivo da informação e dos sistemas de informação para negar, explorar, corromper, ou destruir a informação de um adversário, processos baseados na informação, sistemas de informação e redes baseadas em computadores, enquanto se protegem as próprias. Tais ações são projetadas para atingir vantagens sobre adversários militares".[21] Recentemente, Peter Sommer e Ian Brow, em um relatório elaborado no âmbito da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), intitulado *Reducing Systemic Cybersecurity Risk* (2011), passaram em revista alguns dos usos mais correntes do termo ciberguerra. E referem que, no âmbito do pensamento sobre segurança e estratégia, é frequente encontrarmos o termo utilizado no sentido de "uma guerra conduzida substancialmente no ciberespaço ou no domínio virtual". Aqueles que partilham de tal concepção "[...] têm frequentemente em mente que as ciberguerras tendem a ser muito similares às guerras convencionais" pelo que idênticas doutrinas de retaliação ou dissuasão poderão ser aplicadas. Todavia, Sommer e Brown consideram que é mais fácil e adequado definir "ciberguerra", se os critérios aplicáveis ao conceito forem similares aos utilizados para qualquer guerra convencional ou "cinética".[22]

4 A questão da legalidade (*jus ad bellum*) do recurso à ciberguerra

Uma primeira questão jurídica levanta-se no caso da ciberguerra: será que os Estados podem recorrer a ela em um quadro de legalidade em face do Direito Internacional? Sendo um fenômeno recente, posterior à concepção das normas legais internacionais que regulam o uso da força, as quais são anteriores à era da Internet, poderíamos ser levados a pensar que existe um vazio jurídico. Na realidade, não é exatamente assim. É constatável a existência de divergências sobre a questão de saber se as inúmeras questões legais levantadas pela ciberguerra podem ser integralmente resolvidas no quadro da atual legalidade internacional. Para alguns, elas se beneficiariam da criação de um tratado internacional específico, ou, pelo menos, de um acordo internacional que estendesse – com novas disposições concretas –, as Convenções de Genebra e de Haia ao ciberespaço[23]. A discussão sobre as eventuais vantagens dessa solução exorbita dos objetivos limitados da nossa análise, restrita ao quadro legal atualmente existente. No entanto, não podemos deixar de

[20] Ver: GOVERNO DOS ESTADOS UNIDOS DA AMÉRICA, *Cyberspace policy review.* Assuring a trusted and resilient information and communications infrastructure. p. 1. Disponível em: <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf**>.** Acesso em: 1 dez. 2011. Ver também: *A national security presidential directive 54/homeland security presidential directive 23* (NSPD-54/HSPD-23), dos EUA. Disponível em: <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>**.** Acesso em: 01 dez. 2012.

[21] Citado em: SINKS, Michael**.** *Cyberwarfare and international law Maxwell*: Air Command and Staff College/Air University, 2010. p. 5. (Research Report Submitted to the Faculty in Partial Fulfillment of the Graduation Requirements).

[22] SOMMER, Peter; BROWN, Ian. *Reducing systemic cybersecurity risk*. Paris: OECD/IFP-International Future Program Department, 2011. p. 13. (Project on "Future Global Shocks")

[23] Ver a proposta do EASTWEST INSTITUTE. *Working towards rules for governing cyber conflic.:* endering the Geneva and Hague Conventions in Cyberspace. Nova Iorque: The EastWest Institute, 2011.

assinalar que existe um obstáculo político antecipável à via de um direito convencional *ex novo*: os múltiplos e divergentes interesses das grandes potências tornam difícil o consenso internacional necessário a um tratado desse tipo. Além disso, conforme já referimos, existem soluções no quadro jurídico atual. Se estivermos perante um ato de ciberguerra, este poderá, verificando-se certos requisitos, ser considerado similar a um ato de guerra cinética, ou seja, ao uso da força física – efetuaremos essa discussão com detalhe mais à frente. Como veremos também melhor, não parece existir nenhum motivo válido para não serem aqui aplicadas as normas de Direito Internacional atualmente existentes.[24]

Em matéria de legalidade do uso da força no plano internacional, as disposições mais relevantes encontram-se na Carta das Nações Unidas.[25] Esse documento contém um princípio geral de proibição do recurso à guerra, expressão de um *jus contra bellum*, ou seja, da tendência para a ilegalização dela como modo de solução de conflitos internacionais, iniciada no pós-Guerra com a Sociedade das Nações (1919) e o Pacto Briand-Kellog(1928).[26] Atente-se no teor do artigo 2º nº 4 da Carta:

> Os membros deverão abster-se nas suas relações internacionais de recorrer à ameaça ou ao uso da força, quer que seja contra a integridade territorial ou a independência política de um Estado, quer seja de qualquer outro modo incompatível com os objetivos das Nações Unidas.

Todavia, importa recordar que a proibição geral contida no supramencionado artigo é matizada por duas exceções admitidas pela própria Carta. A primeira exceção está contida no artigo 39º, conjugado com os artigos 41º e 42º, e se refere às ações autorizadas pelo Conselho de Segurança, que poderão, se necessário, incluir o recurso à força:

> O Conselho de Segurança determinará a existência de qualquer ameaça à paz, ruptura da paz ou ato de agressão e fará recomendações ou decidirá que medidas deverão ser tomadas de acordo com os artigos 41º e 42º, a fim de manter ou restabelecer a paz e a segurança internacionais.

A segunda exceção encontra-se vertida no artigo 51º e se refere à admissibilidade (legalidade) do direito de legítima defesa, individual ou coletiva:

> Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva, no caso de ocorrer um ataque armado 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 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 momento, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais.

Em face deste dispositivo, o Conselho de Segurança terá poder para autorizar os Estados a recorrerem a ações de ciberguerra? É inquestionável que esse órgão da ONU tem competência para autorizar os Estados-Membros a recorrerem ao uso da força ou outras medidas contra outros Estados. Todavia, isso só poderá ser feito, como determina o artigo 39º, quando as ações de um Estado constituem uma ameaça à paz, ruptura da paz ou ato de agressão:

> O Conselho de Segurança determinará a existência de qualquer ameaça à paz, ruptura da paz ou cato de agressão e fará recomendações ou decidirá que medidas deverão ser tomadas de acordo com os artigos 41º e 42º, a fim de manter ou restabelecer a paz e a segurança internacionais.

Ressalte-se também que, como faz notar David Graham, a experiência internacional de várias décadas tem mostrado grandes dificuldades na aplicação do dispositivo deste artigo:

> A maioria das decisões apenas chega após extensas e morosas deliberações, e, mesmo então, estão sujeitas ao veto de qualquer membro permanentes do Conselho de Segurança. Assim, dada a natureza nebulosa e com *nuances* dos ciberataques e a incerteza de saber como o Con-

[24] Nesse mesmo sentido ver: DROEGE, Cordula. No legal vacuum in cyber space. (Entrevista, 16/08/2011). Disponível em: <http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>>. Acesso em: 6 dez. 2011. Ver também LEWIS, James. *A note on the laws of war in cyberspace.* Disponível em: <http://csis.org/publication/note-laws-war-cyberspace>. Acesso em: 6 dez. 2011.

[25] Ver Carta das NAÇÕES UNIDAS. In: Gabinete de documentação e direito comparado, direitos humanos. Instrumentos e textos universais. Disponível em: http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhuniversais/onu-carta.htm.>. Acesso em: 14 nov. 2011. .

[26] Sobre o pacto Briand-Kellog, ver, entre outros, FERNANDES, Paulo Jorge. *1928 – Pacto Briand-Kellog:* a Europa da utopia. Janus, 2008. Disponível em: <http://www.janusonline.pt/2008/2008_2_8.html>. Acesso em: 14 nov. 2011.

> selho de Segurança irá responder aos mesmos de forma atempada, parece válido assumir que um Estado escolherá lidar com os ciberataques através do exercício do seu direito de legítima defesa.[27]

O direito de um Estado adotar medidas de legítima defesa existia já, sob outras formas, no Direito Internacional pré-existente à Carta das Nações Unidas. Basicamente, o artigo 51º reafirma o entendimento anterior, em matéria de costume internacional, ou seja, no Direito Internacional Consuetudinário (DIC), no qual era reconhecido o direito dos Estados sobreviverem na comunidade internacional. Assim, para a análise do conceito de legítima defesa, é necessário olhar não só para as disposições do artigo 51º da Carta, como para as disposições do DIC. No entanto, como faz notar David Graham, isso não impede a existência de um sólido consenso sobre o assunto. Na realidade, embora diferentes teorias sempre tenham existido sobre o tipo de ações que constituem "ataques armados", um Estado, sem qualquer dúvida, possui um direito simultaneamente intrínseco e derivado da Carta, de adotar uma resposta "apropriada" a esse ataque. A dúvida aqui consiste em saber o que constitui uma legítima defesa apropriada. A resposta é que uma legítima defesa em respeito da legalidade internacional "terá de respeitar dois alicerces fundamentais do DIC: a 'necessidade' e a 'proporcionalidade'". Um Estado preenche o requisito da "necessidade" quando se torna evidente que, "[...] sob as circunstâncias prevalecentes, o Estado não pode obter uma razoável resolução de um diferendo através de meios pacíficos". Quanto à "proporcionalidade", requer que um Estado "[...] limite as ações de legítima defesa à quantidade de força necessária para deter um ataque em curso ou um futuro ataque. A observância deste último princípio está obviamente dependente da particular situação factual".[28]

5 A problemática da qualificação de um ciberataque como um ataque armado

Em que circunstâncias um ciberataque, ou uma série de ciberataques, poderão ser qualificados como um ataque armado? Note-se que essa qualificação é fundamental, pois, só com ela poderá ser invocado o direito de legítima de defesa de um Estado, incluindo a possibilidade de recurso legal ao uso da força. Segundo Sommer e Brown, os já referidos autores do estudo da OCDE sobre o risco da ciberguerra, para se decidir se um ato deve, ou não, ser qualificado como ciberguerra, deverá submeter-se ao teste para verificar se pode ser considerado "equivalente" a um ataque convencional no seu objetivo, intensidade e duração. Sommer e Brown fazem notar ainda que a

> Carta das Nações Unidas requer uma justificação para a adoção de contra-medidas por aqueles que afirmam ter sido atacados. No essencial, a vítima deve ser capaz de produzir provas fidedignas sobre quem a atacou – algo nem sempre fácil como mostraremos em seguida – e sobre os efeitos dos ataques sobre o seu território e população. O objetivo das contra-medidas deverá ser forçar o Estado atacante a acatar as suas obrigações nos termos da Carta das Nações Unidas.[29]

Importa notar que a qualificação legal de um ciberataque, como um ataque armado, enfrenta, à partida, uma dificuldade devido à não definição do termo "ataque armado" em qualquer tratado internacional. Há, todavia, em termos doutrinários, desenvolvimentos teóricos relevantes que podem ajudar nessa delicada questão. Um consenso interpretativo decorre à volta dos critérios avançados pelo jurista suíço, Jean Pictet, o qual foi o principal redator técnico do texto das Convenções de Genebra de 1949. Em face do(s) artigo(s) 2º das quatro Convenções de Genebra, o uso da força será considerado um ataque armado quando passar o teste do "escopo, duração e intensidade suficiente".[30] Todavia, o problema é que, quer os Estados, quer os juristas especializados em Direito Internacional, interpretam de forma diferente esse teste. Apesar dessa dificuldade, como assinala também David Graham[31],

> [...] ao longo do tempo certos instrumentos internacionais evoluíram, o que facilitou a aplicação dos critérios de Jean Pictet. O instrumento

[27] GRAHAM, David. Cyber threats and the law of war. *Journal of National Security Law and Policy,* v. 4, n. 1, p. 88-89, 2010.

[28] GRAHAM, David. Cyber threats and the law of war. *Journal of National Security Law and Policy,* v. 4, n. 1, p. 88-89, 2010. p. 89.

[29] SOMMER, Peter; BROWN, Ian. *Reducing systemic cybersecurity risk* (Project on "Future Global Shocks"). Paris: OECD/IFP-International Future Program Department, 2011. Disponível em: < http://www.oecd.org/dataoecd/3/42/46894657.pdf>. Acesso em: 1 nov. 2011. p. 30.

[30] PICTET, Jean (Ed.). *Commentary on the Geneva Conventions of 12 August 1949*. Geneva: International Committee of the Red Cross, 1958. p. 17-21. v.4. (Relative to protection of civilian persons in time of war)

[31] GRAHAM, David. Cyber threats and the law of war. *Journal of National Security Law and Policy,* v. 4, n. 1, p.88-89, 2010. p. 90.

> mais relevante nesse contexto é a resolução da Assembleia Geral das Nações Unidas definindo 'agressão".[32] Embora a resolução não contenha uma definição definitiva de ataque armado, fornece exemplos de ações estaduais que devem ser qualificadas como tal, e estes ganharam uma extensa aceitação internacional.

Todavia, como é fácil de compreender, tais avanços doutrinários e legais só por si não resolvem o problema de saber se um cibertaque pode ser considerado um ataque armado. Desde logo pela razão histórica de que, nem na altura da elaboração das Convenções de Genebra, nem na data da Resolução da Assembleia Geral das Nações Unidas, existia tecnologia que levasse à necessidade de prever explicitamente a questão. Assim, para resolver o problema, têm sido propostos essencialmente três modelos (ou abordagens), os quais pretendem "[...] facilitar os critérios do uso da força de Pictet – escopo, duração e intensidade – aplicando-os a formas não convencionais de uso da força, incluindo ciberataques".[33] Esses modelos são os seguintes:

O primeiro modelo pode ser designado como baseado numa abordagem instrumental (*instrument-based approach*). Usando este modelo, uma avaliação será efetuada com o intuito de saber se o dano provocado por um ciberataque poderia, previamente, ser apenas causado por um ataque cinético. Por exemplo, usando este modelo, um ciberataque conduzido com o objetivo de colocar fora de funcionamento uma rede elétrica seria considerado um ataque armado. (A razão dessa qualificação tem a ver com o facto de antes do desenvolvimento de cibercapacidades, a destruição de uma rede elétrica ter, tipicamente, requerido o bombardeamento desta, ou o uso de algum tipo de força cinética para obter esse resultado);

O segundo modelo pode ser designado como abordagem baseada nos efeitos (*effects-based approach*), sendo também frequentemente referido como um modelo baseado nas consequências. O critério desse modelo assenta no efeito global provocado pelo ciberataque, no(s) Estado(s) vítima(s) do mesmo. Por exemplo, de acordo com esta abordagem, a manipulação informática de dados de instituições bancárias e financeiras, afetando um determinado país, pode ser vista como um ataque informático. (Embora esta ação não tenha semelhança com um ataque cinético, o resultado global que a manipulação de informação irá causar ao bem-estar econômico do Estado vítima justificará a sua equiparação a um ataque armado).

Um terceiro e último um modelo assenta numa abordagem baseada na responsabilidade estrita (*strict liability*). Segundo essa abordagem, um ciberataque contra qualquer infraestrutura nacional crítica seria, de forma automática, considerado equiparável a um ataque armado. Tal qualificação seria justificada pelas potenciais consequências severas que podem resultar de qualquer ataque a tais sistemas de infraestruturas críticas nacionais.[34]

Apesar das diferentes leituras que esses modelos (abordagens) permitem efetuar, na qualificação de um ciberataque como ataque armado, importa realçar a sua convergência em um aspecto fundamental: verificando se certos requisitos os ciberataques podem constituir ataques armados. Todavia, quanto aos requisitos que os ciberataques devem preencher para serem qualificados como um ataque armado, eles apresentam, naturalmente, variância. Embora não exista consenso sobre qual dos modelos supradescritos é o mais adequado para resolver esse problema, parece existir, pelo menos na discussão norte-americana, uma tendência para considerar mais adequada a *effects-based approach*, ou seja, a abordagem baseada nos efeitos.[35]. Nesse contexto, são úteis os seis requisitos (ou parâmetros), delineados originalmente, em finais da década de noventa, por Michael N. Schmitt[36], para avaliar em que medida um ciberataque poderá ser considerado um ataque armado (destrinçando-o, nomeadamente, de atos de coerção econômica e/ou política):

a. gravidade (*severity*): os ataques armados

[32] Ver *Definition of agression* - General Assembly resolution 3314 (XXIX), 14 December 1974, Disponível em: <http://untreaty.un.org/cod/avl/ha/da/da.html>. Acesso em: 14 nov. 2011.

[33] GRAHAM, op. cit., p. 91.

[34] Na apresentação desses modelos, seguimos de perto a síntese efetuada por GRAHAM, 2010, p. 91.

[35] Ver: SKLEROV, Matthew. Solving the dilemma of state responses to cyberattacks: a justification for the use of active defenses against States which neglect their duty to prevent. *Military Law Revue,* v. 201, 2009. p. 56.

[36] SCHMITT, Michael. Computer network attack and the use of force in international law: thoughts on a normative framework. *Research Publication 1*: Information series, 1999. Disponível em: <http://www.dtic.mil/cgi-bin/gettrdoc?location=u2&doc=gettrdoc.pdf&ad=ada471993>. Acesso em: 5 dez. 2011. p. 18-19.

> ameaçam danos físicos e destruição da propriedade num grau muito mais elevado que outras formas de coerção;
>
> b. iminência (*immediacy*): as consequências negativas de uma ação armada ou as ameaças das mesmas geralmente ocorrem com mais rapidez do que outras formas de coerção;
>
> c. caráter direto (*directness*): as consequências de uma coerção armada estão mais diretamente ligadas ao *actus reus* (ato de culpabilidade), do que outras formas de coerção que dependem de vários fatores para atuar;
>
> d. caráter invasor (*invasivness*): na coerção aramada, o ato que provoca danos normalmente traduz-se num atravessar da fronteira nacional, enquanto que os atos de guerra econômica geralmente ocorrem fora das suas fronteiras;
>
> e. mensuralidade ou extensão (*measurability*): enquanto que as consequências de uma ação armada são geralmente fáceis de verificar (por exemplo, certo nível de destruição), as consequências de outras formas de coerção são mais difíceis de definição;
>
> f. legitimidade (*presumptive legitimacy*): na maioria dos casos, o uso da força, seja sob o prisma da lei doméstica ou da lei internacional, é presumivelmente ilegal, exceto se estivermos perante uma disposição que a permita.

Usados conjuntamente, esses critérios permitem aos Estados ponderar os ciberataques ao longo de diferentes dimensões críticas. Importa notar que, só por si, nenhuma dessas dimensões pode ser considerada decisiva nessa qualificação. Todavia, a avaliação conjunta em todas essas dimensões contém parâmetros "suficientes para serem caracterizados como ataques armados". No futuro, talvez os seis critérios avançados por Schmitt possam constituir um padrão de avaliação dos ciberataques internacionalmente aceitos e "[...] trazer uma uniformidade aos esforços dos Estados para classificar os ciberataques". Todavia, até que eles eventualmente adquiram uma ampla aceitação internacional – o que não discernível num futuro próximo –, "[...] os Estados irão, provavelmente, classificar os ciberataques de forma diferente, consoante o seu próprio entendimento sobre os ataques armados bem como a sua concepção do interesse vital nacional".[37]

6 O problema da atribuição de responsabilidade num ciberataque

Na discussão sobre essa problemática, na qual o jurídico e o tecnológico surgem frequentemente imbricados de uma forma complexa, vamos seguir de perto a análise efetuada por Matthew J. Sklerov.[38] Um primeiro aspecto aqui a considerar são as limitações que decorrem da própria tecnologia. Tipicamente, a análise de um ciberataque será feita pelo administrador responsável pelo sistema atacado. Nessa tarefa, são normalmente utilizados programas de aviso, detecção automática e classificação dos ataques e/ou intrusões no sistema. Por sua vez, a detecção da origem do ataque pode ser feita por meio de programas automáticos ou operada diretamente pelo responsável do sistema. Tais programas podem ajudar a classificar os ciberataques como ataques armados ou usos de força menores. Podem também ajudar a avaliar em que medida os ataques tiveram origem em um Estado previamente declarado como um "santuário" para atores não estaduais envolvidos em ciberataques. Todavia, como Sklerov faz notar, mesmo com o recurso aos programas mais sofisticados de detecção, poderá não ser possível efetuar uma atribuição de um ataque totalmente isenta de erro:

> [...] limitações tecnológicas na detecção, classificação, e vestígios dos ataques, irão provavelmente complicar, ainda mais, a decisão estadual durante a análise de um ciberataque. Idealmente, os ciberataques deveriam ser fáceis de detectar, classificar e atribuir. Infelizmente, não é esse o caso.[39]

Analisando agora mais em detalhe as limitações que decorrem da própria tecnologia, vamos começar por aquelas que dizem respeito à própria detecção do ciberataque. Os programas de detecção precoce e aviso podem ajudar a capturar os ciberataques antes de eles atingirem o seu ponto culminante. Todavia, como assinala Sklerov , mesmo os melhores programas são incapazes de deter todos os ciberataques. Numa perspectiva de análise legal, as consequências são que, se, por um lado, os Estados podem ganhar tempo para analisar o ataque – uma vez que a ameaça de perigo já passou –, por outro lado, quando

[37] SKLEROV, Matthew. Solving the dilemma of state responses to cyberattacks: a justification for the use of active defenses against states which neglect their duty to prevent. *Military Law Revue*, v. 201, p. 1-85, 2009. Disponível em: <http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/201-fall-2009.pdf>>. Acesso em: 08 nov. 2011. p. 57-58.

[38] SKLEROV, Matthew. Solving the dilemma of state responses to cyberattacks: a justification for the use of active defenses against states which neglect their duty to prevent. *Military Law Revue*, v. 201, p. 1-85, 2009. Disponível em: <http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/201-fall-2009.pdf>>. Acesso em: 08 nov. 2011. p. 73.

[39] Ibidem, p. 74.

mais tempo decorrer desde o final do ataque, mais difícil se torna reconstituir a sua origem. Quanto às limitações na classificação de um ataque – as quais, nesse contexto, são até mais importantes que as relacionadas com a detecção –, resultam, por sua vez, de constrangimentos de vária ordem. A situação mais simples de qualificar ocorre quando um ciberataque em curso já causou danos sérios, invasivos e mensuráveis. Nessa hipótese, pode, com segurança, ser considerado um ataque armado, mesmo que ainda esteja a decorrer. Mas esse é apenas o caso mais líquido. Pode acontecer que um ciberataque não tenha provocado danos sérios, invasivos e mensuráveis. Ainda de acordo com Sklerov, então será necessário:

> [...] olhar para o imediatismo de futuros danos, para determinar em que medida um ataque deverá ser classificado como um ataque armado iminente. [Todavia] dada a velocidade extremamente rápida a que os códigos dos computadores podem ser executados, tais decisões serão muito difíceis de concretizar, uma vez que o retardar do uso de defesa ativas aumenta a probabilidade de causar danos ao Estado.[40]

Para além disso, quando uma intrusão num computador é detectada, muito provavelmente o propósito do ataque será difícil de discernir enquanto não for dissecado o código do programa ou auditados os *logs* (registos de dados) da atividade do atacante. O problema é a velocidade à qual são executados os ciberataques. Ela irá forçar o administrador do sistema a atuar rapidamente para tentar discernir o objetivo do ataque, mas, provavelmente, irá perder informação crítica relevante ao qualificar corretamente.

Por último, o delicado e crucial problema de traçar a origem de um ciberataque. Desde logo, uma dificuldade surge aqui pelo fato de os ciberataques serem frequentemente conduzidos por meio de outros computadores e/ou sistemas informáticos, de modo a esconder a sua procura e esconder a sua real autoria. Depois, há a dificuldade e risco, já anteriormente mencionados, de que os programas que ajudam a traçar a autoria do ataque poderem não identificar corretamente a autoria do ataque. Esse risco de atribuição errada pode levar a que o ataque seja percebido como tendo vindo de um Estado, quando este não é o verdadeiro Estado de origem do mesmo. Todavia, apesar desse risco, no que concerne estritamente à questão legal da atribuição de responsabilidade – e abstraindo das eventuais consequências políticas –, essa não é uma dificuldade inultrapassável. Sklerov aponta as seguintes razões:

> A responsabilidade de um Estado deve ser julgada pelos factos disponíveis, mesmo se esta resulta numa atribuição errada. Primeiro, enquanto um Estado avalia uma ataque com o melhor da sua capacidade técnica e atua com boa fé face à informação disponível, este cumpre as suas obrigações internacionais. Segundo, Estados que recusam atuar em conformidade com o seu dever internacional de prevenir que o seu território seja usado para cometer ciberataques, escolheram o risco de serem considerados indiretamente responsáveis, por acidente.[41]

Quando se verifica que os ciberataques a um Estado têm origem no interior de outro Estado, este último pode, no entanto, evitar ser responsabilizado. Para o efeito, deverá ter adotado medidas afirmativas para prevenir ciberataques – tais como leis criminais severas e assegurar o seu cumprimento efetivo –, e ter uma atitude de cooperação ativa com o Estado vítima para levar os atacantes à justiça. Note-se que, em face do DIH, os ataques efetuados por atores não estaduais estão abrangidos pelo seu dispositivo, mas em circunstâncias bastante estritas. Este apenas "[...] permite aos Estados responder a tais ataques, usando a força, quando os ataques são imputáveis a um outro Estado".[42] Por outras palavras, só o poderá fazer dentro da legalidade internacional quando existe também um Estado com algum tipo de responsabilidade pelas ações dos atores não estaduais.

7 Conclusões

Os conflitos interestaduais do século XXI ocorrerão também com grande probabilidade no novo terreno do ciberespaço, tendo como alvo as redes de infraestruturas de tecnologias de informação, nomeadamente a Internet, as redes de telecomunicações e as indústrias críticas cujo funcionamento está interligado com elas.. Assim, essa nova forma de conflitualidade, designada por ciberguerra, pode ser caracterizada como a utilização, em

[40] Ibidem, p. 76.

[41] SKLEROV, Matthew. Solving the dilemma of state responses to cyberattacks: a justification for the use of active defenses against states which neglect their duty to prevent. *Military Law Revue*, v. 201, p. 1-85, 2009. Disponível em: <http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/201-fall-2009.pdf>>. Acesso em: 08 nov. 2011. p. 78.

[42] Ibidem, p. 42.

termos ofensivos ou defensivos, dos sistemas de informação e comunicação, para negar, corromper ou destruir a informação de um adversário, atacando os sistemas de informação e comunicação e as redes baseadas em computadores, as quais podem suportar o funcionamento de infraestruturas militares e/ou civis.

Apesar da crescente importância dessa temática, uma análise jurídica dela enfrenta a dificuldade prévia de nem os conceitos de ciberespaço, nem de ciberguerra, serem objeto de um consenso internacional, nem integrarem qualquer texto jurídico de Direito Internacional. Todavia, não estamos perante um vazio jurídico como poderia parecer à primeira vista. Não existe qualquer motivo válido para não serem aqui aplicadas as normas de DIH atualmente existentes. Naturalmente que o enquadramento legal da ciberguerra não está isento de dificuldades como, aliás, não está também a própria guerra cinética – uma parte significativa das dificuldades advém daí.

A qualificação legal de um ciberataque, como um ataque armado, enfrenta, à partida, a dificuldade da não definição do conceito de ataque armado no âmbito do DIH ou de qualquer outro texto legal. Contudo, esta é uma dificuldade resolúvel recorrendo à interpretação doutrinária e ao acervo de jurisprudência sobre a aplicação do DIH. Existe, pelo menos na discussão norte-americana, uma tendência para usar a chamada *effects-based approach*, ou seja, a abordagem baseada nos efeitos, para resolver esse problema. Complementarmente, parece ser útil e adequada a transposição, para um ciberataque, dos requisitos delineados originalmente por Michael N. Schmitt, o que permitirá determinar, no caso de verificação conjunta, a sua qualificação legal como um ataque armado.

Por último – e aqui reside uma diferença relevante em face da aplicação do DIH à guerra cinética –, constatou-se a existência de um problema delicado na atribuição da responsabilidade em um ciberataque. Isso ocorre devido ao risco significativo de atribuição errada. Desde logo, esse risco resulta do fato de não existir nenhuma tecnologia que permita a atribuição da sua autoria de forma totalmente isenta de erro. A consequência é que o ciberataque pode ser percebido como tendo proveniência em um determinado Estado, quando este não foi a verdadeira origem dele.. Esse delicado problema interliga-se com outro bastante nebuloso, que é o dos ciberataques empreendidos por atores não estaduais contra um Estado diferente daquele onde estão localizados. Em termos estritamente jurídicos, o DIH contempla essa situação no seu dispositivo, embora em moldes bastante estritos. Para uma resposta do Estado atingido envolvendo o uso da força, é requisito de legalidade a origem dos ataques num "Estado-santuário", ou seja, de alguma forma responsável pelas ações dos atores não estaduais. Todavia, o escasso acervo de casos até agora existentes mostra também, pelas razões já apontadas, dificuldade em efetuar essa atribuição. A essa situação não é estranho o fato de a ciberguerra estar numa fase inicial de contornos pouco definidos. Isso torna a tarefa de resolução das múltiplas questões jurídicas que levanta um desafio em grande parte em aberto para os juristas de Direito Internacional. No entanto, tais dificuldades parecem poder ser razoavelmente solúveis, com maior ou menor esforço de interpretação e adaptação, no quadro dos princípios e normas do atual DIH.

Referências

ARQUILLA, John; RONFELDT, David (Ed.). Cyberwar is Coming! In: *Athena's Camp:* preparing for conflict in the information age. Santa Monica: Rand Corp, 1997. (Reedição do artigo originalmente publicado na Comparative Strategy, v. 12, n. 2, 1993).

ARQUILLA, John; RONFELDT, David (Ed.). *Networks and netwars:* the future of terror, crime, and militancy. Santa Monica: Rand Corp, 2002.

CASTELLS, Manuel. *A sociedade em rede*. Lisboa: Fundação Calouste Gulbenkian, 2002. v. 1

COMITÉ INTERNACIONAL DA CRUZ VERMELHA. As Convenções de Genebra de 1949 e seus Protocolos Adicionais. Disponível em: <http://www.icrc.org/por/war-and-law/treaties-customary-law/geneva-conventions/index.jsp>. Acesso em: 8 nov. 2011.

DEYRA, Michel. *Direito Internacional Humanitário*. Lisboa: Procuradoria-Geral da República/Gabinete de Documentação e Direito Comparado, 2001.

DROEGE, Cordula. *No legal vacuum in cyber space.* Disponível em: <http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>. Acesso em: 6 dez. 2011.

DURANT, Henry. *A memory of Solferino*. Genebra: International Committee of the Red Cross, 1986. Disponível em: <http://www.icrc.org/eng/resources/documents/publication/p0361.htm>. Acesso em: 07 nov. 2011.

EASTWEST INSTITUTE. *Working towards rules for governing cyber conflict*: rendering the Geneva and hague conventions in cyberspace. Nova Iorque: The EastWest Institute, 2011.

FERNANDES, Paulo Jorge. *1928 – Pacto Briand-Kellog*: a Europa da utopia. Janus 2008. Disponível em: <http://www.janusonline.pt/2008/2008_2_8.html>. Acesso em: 14 nov. 2011.

GRAHAM, David. Cyber threats and the law of war. *Journal of National Security Law and Policy,* v. 4, n. 1, p.88-89, mês? 2010.

KOLB, Robert; HYDE, Richard. *An introduction to the international law of armed conflicts*. Oxford-Portland: Hart Publishing, 2008.

LEWIS, James. *A note on the laws of war in cyberspace*. Disponível em: <http://csis.org/publication/note-laws-war-cyberspace>. Acesso em: 6 dez. 2011.

SASSÒLI, Marco; BOUVIER, Antoine; QUINTIN, Anne. *How does law protect in war?* Outline of International Humanitarian Law. 3. ed. Genebra: International Committee of the Red Cross, 2001. v. 1 Disponível em: <http://www.icrc.org/eng/resources/documents/publication/p0739.htm>. Acesso em: 7 nov. 2011.

SCHMITT, Michael. Computer network attack and the use of force in international law: thoughts on a normative framework. *Research Publication 1*: Information series, 1999. Disponível em: <http://www.dtic.mil/cgi-bin/gettrdoc?location=u2&doc=gettrdoc.pdf&ad=ada471993>. Acesso em: 5 dez. 2011.

SINKS, Michael. *Cyber warfare and international law*. Maxwell: Air Command and Staff College/Air University, 2010. (Research report submitted to the faculty in partial fulfillment of the graduation requirements)

SOMMER, Peter; BROWN, Ian. *Reducing systemic cybersecurity risk* (Project on "Future Global Shocks"). Paris: OECD/IFP-International Future Program Department, 2011. Disponível em: < http://www.oecd.org/dataoecd/3/42/46894657.pdf>. Acesso em: 1 nov. 2011.

SKLEROV, Matthew. Solving the dilemma of state responses to cyberattacks: a justification for the use of active defenses against states which neglect their duty to prevent. *Military Law Revue,* v. 201, p. 1-85, 2009. Disponível em: <http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/201-fall-2009.pdf>>. Acesso em: 08 nov. 2011.

PICTET, Jean (Ed.). *Commentary on the Geneva Conventions of 12 August 1949*. Geneva: International Committee of the Red Cross, 1958. (IV Relative to Protection of Civilian Persons in Time of War).

TIKK, Eneken; TALIHÄRM, Anna-Maria. *International cyber security:* legal e policy considerations. Tallinn: CCDCOE Publications, 2010.

TIKK, Eneken; KASKA, Kadri; VIHUL, Liis. *International cyber incidents:* legal considerations. Tallin: CCDCOE Publications, 2010.

ZIPPELIUS, Reinhold. *Filosofia do direito*. Lisboa: Quid Juris, 2010.

WATTS, Sean. Combatant status and computer network attack. *Virginia Journal of International Law*, v. 50, n. 2, 2010.