Ataques cibernéticos e seus impactos na definição de conflitos armados não internacionais

Cyber attacks and their impacts on the definition of non-international armed conflicts

Bruno de Oliveira Biazatti[1]

Resumo:
A ameaça cibernética é atualmente um dos mais sérios desafios de segurança econômica, financeira, política e militar a ser enfrentado pelos Estados. Os recursos cibernéticos que tanto revolucionaram a forma dos seres humanos se comunicarem entre si, também são usados para fins militares por Estados e por grupos não estatais, podendo até configurar conflitos armados. Especificamente, um conflito armado de natureza não internacional formar-se-á quando um Estado envolve-se em hostilidades intensas contra um grupo armado não estatal organizado ou quando as hostilidades ocorrem entre dois ou mais grupos desta mesma natureza. O presente trabalho analisará os dois elementos condicionantes à existência destes conflitos (a organização interna do grupo armado e a intensidade mínima das hostilidades) à luz dos ataques cibernéticos, de forma a destacar as particularidades desses, quando comparados com os meios e métodos tradicionais de guerra, e também as dificuldades para adequá-los às normas humanitárias ora vigentes.
Palavras-chave: Ataques cibernéticos. Direito Internacional Humanitário. Conflitos armados não internacionais. Intensidade mínima de violência. Organização interna do grupo armado.

Abstract:
Currently, the cyber threat is one of the most serious challenges to economic, financial, political and military security to be faced by States. Cyber resources, which have revolutionized how human beings communicate with each other, are also applied for military purposes by States and non-State actors and they may even fulfill the amount of violence to establish an armed conflict. Specifically, an armed conflict not of an international character occurs when a State engages itself in intense hostilities against an organized non-State armed group or when intense hostilities occur between two or more organized groups. This paper will examine the two criteria to be fulfilled in order to demonstrate the existence of these conflicts in light of cyber attacks (the internal organization of the armed group and the minimum intensity of the hostilities), aiming to explain the peculiar characteristics of these attacks when faced with the traditional means and methods of warfare and the difficulties of adapting them to the existing norms of International Humanitarian Law.
Keywords: Cyber attacks. International Humanitarian Law. Non-international armed conflicts. Minimum intensity of violence. Internal organization of the armed group.

[1] Aluno de graduação em Direito na Universidade Federal de Minas Gerais (UFMG). Email: bbiazatti@gmail.com. O autor agradece à Paula Wardi Drumond Gouvêa Lana pela revisão do presente artigo.

1. Introdução

A sociedade atual cada vez mais se torna dependente de computadores e de sistemas online, não somente para o funcionamento da infraestrutura básica da vida civil, mas também na implementação de operações e sistemas militares pelas forças armadas estatais e paraestatais. Os conflitos armados da atualidade são, de forma inexorável, subordinados a elementos cibernéticos: bombas são guiados por satélites GPS, *drones* são pilotados remotamente em todo o mundo e aviões de combate e navios de guerra são hoje enormes centros de processamento de dados.

Diante disso, o espaço cibernético, que tanto facilita as interações humanas, pode também se tornar um perigo para a paz e a segurança internacionais. Sensível a essa questão, o Presidente Barack Obama, em 2009, apontou que a informatização do modo de vida atual trouxe benefícios, especialmente pelo fato de que "[...] a *World Wide Web* nos fez mais interligados do que em qualquer outro momento da história humana." (ESTADOS UNIDOS, 2009) (tradução nossa) Obama constatou ainda que os riscos advindos do espaço cibernético também são uma realidade. Ele atesta que essa "[é] a grande ironia da nossa Era da Informação. As mesmas tecnologias que nos capacitam para criar e construir também fortalecem aqueles que irão vandalizar e destruir. E esse paradoxo - visível e invisível - é algo que nós vivenciamos todos os dias." (ESTADOS UNIDOS, 2009) (tradução nossa)

Assim, a guerra cibernética é uma realidade, de forma que os operadores do Direito não podem fechar os olhos a este desafio. Como lecionam o internacionalista italiano Natalino Ronzitti (2000, p.1020) e também Antônio Augusto Cançado Trindade (2010, para.193), atual juiz brasileiro perante a Corte Internacional de Justiça (CIJ), é dever de qualquer jurista, em caso de dúvida sobre a aplicação das normas internacionais, esclarecer estas incertezas e nunca perpetuá-las, como a única maneira de efetivamente trazer justiça para o processo de resolução de litígios. Destarte, a adaptação do sistema jurídico a estas mudanças nos meios e métodos de fazer guerra se torna imperativa para assegurar a efetiva proteção dos direitos e liberdades fundamentais do ser humano, bem como dos próprios interesses e direitos dos Estados.

É esta tarefa de análise e adequação hermenêutica das normas internacionais que se trata o presente trabalho. Contudo, esse exercício de amoldamento normativo é uma empreitada muito vasta, sendo necessário realizar um corte metodológico. Nesse liame, para os propósitos do presente estudo, somente um elemento será objeto de apreciação: o conceito de conflito armado não internacional. Pretende-se analisar o elemento da organização interna

dos grupos não estatais, bem como a intensidade das operações militares, à luz do universo cibernético.

2. O Direito Internacional Humanitário e a guerra cibernética: velhas normas para novas realidades

O Direito Internacional Humanitário, também chamado de *Jus in Bello*, é um ramo do Direito Internacional Público, composto por normas que procuram limitar o uso de violência em conflitos armados. Em linhas gerais, as suas regras e princípios garantem proteção àqueles que não podem ou não mais participam diretamente das hostilidades e restringem o uso de força exclusivamente ao montante necessário para enfraquecer o poder militar do inimigo e, assim, derrotá-lo.

O Direito Internacional Humanitário se aplica, então, durante e no espaço geográfico onde ocorrem conflitos armados ou na incidência de uma ocupação militar.[2] Uma ocupação militar ocorre quando um território "[...] é efetivamente colocado sob a autoridade do exército inimigo." (VERRI, 1992, p.81) (tradução nossa) Por sua vez, segundo o Tribunal Penal Internacional para a Ex-Iugoslávia (TPIEI),[3] os conflitos armados "[...] existem sempre que há recurso de força armada entre Estados ou violência armada prolongada entre autoridades governamentais e grupos organizados ou entre estes grupos dentro de um Estado." (1995, para.70) (tradução nossa) Essa definição revela que os conflitos armados se dividem em duas espécies distintas conforme as partes beligerantes: os conflitos armados internacionais, em que dois ou mais Estados se enfrentam; e os conflitos armados não internacionais, entre forças governamentais e grupos armados não estatais ou somente entre estes grupos, desde que as hostilidades ocorram com certa intensidade e os grupos não estatais envolvidos sejam internamente organizados (TPI, 2012, para.538).

[2] Apesar do Direito Humanitário ter seu escopo de aplicação limitado aos conflitos armados e ocupações, certas regras criam obrigações aos Estados que devem ser implementadas em tempos de paz. Normalmente, essas obrigações se referem a tomada de medidas preventivas para evitar danos à população civil ou garantir o respeito às normas humanitárias durante potenciais conflitos. Para fins de ilustração, aponta-se: a disseminação geral das regras humanitárias entre os militares e civis; o dever de dar instruções especiais aos membros das forças armadas; a contratação de assessores jurídicos para aconselhar os comandantes militares; a construção de instalações militares o mais distante possível de bens e pessoas protegidas; e o dever de treinar pessoas qualificadas e assessores jurídicos em tempos de paz para que sejam operacionais durante os conflitos armados.

[3] O Tribunal Penal Internacional para a Ex-Iugoslávia foi criado em 25 de maio de 1993, através da Resolução do Conselho de Segurança da ONU no. 827, de mesma data. Nos termos do artigo 1º de seu Estatuto, esse Tribunal tem competência criminal para julgar pessoas físicas responsáveis por graves violações do direito internacional humanitário cometidas no território da Ex-Iugoslávia (hoje corresponde aos Estados da Eslovênia, Croácia, Bósnia e Herzegovina, Sérvia, Macedônia e Montenegro), desde 1º de janeiro de 1991. A sua sede se localiza em Haia, nos Países Baixos (SCHABAS, 2007, p.11-15; CASSESE, 2003, p.335-340).

Como destacado pelo Tribunal Penal Internacional para Ruanda (TPIR),[4] meros distúrbios e tensões locais, tais como atos isolados de violência, não se enquadram na definição de conflito armado (1998, para.620). Logo, são regulados pelas leis domésticas dos Estados e pelo Direito Internacional dos Direitos Humanos.

As normas internacionais humanitárias se baseiam num equilíbrio delicado entre as ambições e necessidades militares das partes beligerantes e as considerações mínimas de humanidade (DINSTEIN, 2004, p.16). Como defendido por Michael Schmitt (2010, p.798), "[c]ada uma das [regras do Direito Internacional Humanitário] constitui um compromisso dialético entre essas duas forças opostas." (tradução nossa) Contudo, manter esse equilíbrio é uma tarefa difícil e delicada, particularmente nos conflitos armados contemporâneos, marcados por uma indefinição contínua das distinções e categorias tradicionais em que o arcabouço normativo humanitário foi concebido e sobre o qual a sua operacionalidade depende. Assim, os conflitos armados de nossos dias desafiam as definições humanitárias clássicas (MELZER, 2010, p.833).

Um destes desafios são as operações bélicas no espaço cibernético, vez que, nos dias atuais, a internet e os sistemas digitais são relevantes na condução dos conflitos armados de uma forma impensável em décadas passadas. Qualquer medida que uma parte beligerante possa tomar para neutralizar ou destruir o comando ou a infraestrutura militar eletrônica de seu inimigo, antes ou no decurso de um conflito armado, traria uma enorme vantagem.

Diante disso, constantemente, a mídia e a doutrina relatam ataques por *hackers* com a finalidade de comprometer a operacionalidade digital de governos ou grupos não estatais no campo militar. Podemos destacar, por exemplo, que durante os bombardeios da Organização do Tratado do Atlântico Norte (OTAN) no Kosovo, no final da década de 1990, os comandantes militares desta organização planejaram um ataque cibernético para inserir mensagens e alvos falsos nos sistemas *online* do comando militar de defesa aérea da Sérvia. Este ataque objetivaria limitar a capacidade sérvia em direcionar ataques com precisão contra aviões da OTAN durante a campanha aérea (KELSEY, 2008, p.1434-1435).

Em outubro de 2000, depois que três soldados israelenses foram sequestrados, *hackers* pró-Israel invadiram sites militares e políticos do grupo Hezbollah, da Autoridade Nacional Palestina e do Hamas, substituindo seu conteúdo por bandeiras e pelo hino de Israel. Em

[4] O Tribunal Penal Internacional para Ruanda foi estabelecido pelo Conselho de Segurança da ONU, através da Resolução no. 955, de 8 de novembro de 1994. Seu o objetivo é julgar e condenar aqueles que são responsáveis pelo crime de genocídio e outras violações graves do direito internacional humanitário cometidos no território de Ruanda e também os cidadãos ruandeses que cometeram esses mesmos crimes no território de Estados vizinhos, entre 1 de janeiro de 1994 e 31 de dezembro de 1994. O Tribunal tem sede em Arusha, na Tanzânia (SCHABAS, 2007, p.11-15; CASSESE, 2003, p.335-340).

resposta, *hackers* pró-Palestina derrubaram sites israelenses estratégicos, incluindo os que operavam a Bolsa de Valores de Tel Aviv e o Banco de Israel (ROSCINI, 2014, p.8).

Em 6 de setembro de 2007, Israel haqueou o sistema de defesa aérea da Síria, o desabilitando. Isso permitiu que caças daquele Estado se infiltrassem no espaço aéreo sírio sem ser detectados, a fim de bombardear uma instalação nuclear em Dayr az-Zawr, a qual se suspeitava estar sendo usada para fins militares. A operação recebeu o nome de Operação Pomar (*Operation Orchard*) e foi um completo sucesso, vez que o laboratório nuclear sírio foi destruído, sem nenhuma baixa israelense (DINNISS, 2012, p.289-290).

Mais recentemente, durante o atual conflito armado não internacional na Síria (em andamento desde março de 2011), o Exército Eletrônico Sírio, fiel ao Presidente Bashar al-Assad, realizou ataques cibernéticos contra os insurgentes, enquanto que estes fizeram o mesmo com os sistemas e sites governamentais (ROSCINI, 2010, p.7-8 e 114-115).

Assim, a humanidade presencia hoje uma nova revolução tecnológica dos armamentos e dos métodos de guerra, sendo necessário ao Direito Internacional Humanitário se adaptar a essas transformações, sob pena de expor o indivíduo a abusos intoleráveis. Diante desse paradigma de mudanças, Cançado Trindade esclarece que "[...] mais do que uma época de transformações, vivemos uma verdadeira transformação de época [...]" (2006, p.426). Nessa mutação paradigmática, percebe-se "[...] que o avanço científico e tecnológico paradoxalmente tem gerado uma crescente vulnerabilidade dos seres humanos face às novas ameaças do mundo exterior." (CANÇADO TRINDADE, 2006, p.426). Este jurista sustenta que nem o Estado, nem outras formas de organização política, social e econômica, podem se eximir do dever "[...] de tomar medidas de proteção redobrada dos seres humanos, particularmente em meio às incertezas, contradições e perplexidades desta transformação de época que testemunhamos e vivemos" (CANÇADO TRINDADE, 2006, p.426).

A fim de enfrentar estes desafios ao sistema jurídico, deve-se reafirmar, com ainda mais vigor, os direitos da pessoa humana. Nesse liame, Cançado Trindade leciona que

> [n]unca, como em nossos dias, se tem propugnado com tanta convicção por uma visão integral dos direitos humanos, a permear todas as áreas da atividade humana (civil, política, econômica, social e cultural). Nunca, como na atualidade, se tem insistido tanto nas vinculações da proteção do ser humano com a própria construção da paz e do desenvolvimento humano. Nunca, como no presente, se tem avançado com tanta firmeza uma concepção tão ampla da própria proteção, a abarcar a prevenção e a solução durável ou permanente dos problemas de direitos humanos (2006, p.426).

In fine, afirma-se que o avanço tecnológico, apesar de suas vantagens inegáveis, pode ser prejudicial à proteção dos seres humanos, especialmente em conflitos armados, tendo em

vista que os institutos legais estabelecidos para a proteção da humanidade podem se tornar obsoletos. Surge, assim, a necessidade de (re)avaliar o arcabouço jurídico humanitário à luz do uso de recursos cibernéticos no contexto de conflitos.

Nesse prisma, nota-se que o sistema jurídico não é estático, de forma a adaptar-se às condições atuais de vida e à evolução das normas internacionais, bastando à comunidade jurídica realizar tais adequações (CIJ, 2009, para.64). Passa-se agora a analisar tais mudanças de circunstâncias, as aplicando à definição de conflito armado não internacional.

3. Os elementos legais para a caracterização de um conflito armado não internacional e a guerra cibernética

3.1. Aspectos gerais sobre os conflitos armados não internacionais

A primeira vez que os conflitos armados não internacionais foram mencionados expressamente em um tratado internacional humanitário foi em 12 de agosto de 1949, no Artigo 3º Comum às Quatro Convenções de Genebra[5]. Gary D. Solis chega a afirmar que este dispositivo é a "inovação mais significativa" destas convenções (2010, p.97) (tradução nossa). Todavia, a definição encontrada no Artigo 3º Comum é muito simples e abrangente, se reduzindo a uma mera referência negativa a um "conflito armado que não apresente um caráter internacional".

Posteriormente, à luz dos muitos conflitos pós-1949,[6] o Comitê Internacional da Cruz Vermelha[7] convocou uma conferência diplomática internacional realizada em Genebra, entre 1973 e 1977, com o objetivo de modernizar e aperfeiçoar as normas do Direito Internacional Humanitário. A conferência aprovou dois protocolos adicionais às Convenções de Genebra de 1949: um específico para regular conflitos armados internacionais, o 1º Protocolo Adicional

[5] As Convenções de Genebra são quatro tratados independentes adotados na Conferência de Paz de Genebra, em 1949, por iniciativa do Comitê Internacional da Cruz Vermelha. A primeira convenção lida com a proteção dos doentes e feridos em batalhas terrestres; a segunda protege doentes, feridos e náufragos em conflitos navais; a terceira regula os direitos dos prisioneiros de guerra; e a quarta protege os civis durante as hostilidades e ocupações. Destaca-se que o artigo 3º é idêntico nesses quatro instrumentos, daí a expressão "Artigo 3º Comum".

[6] Podemos apontar como exemplos: Guerra Indo-Paquistanesa (1947-1948), Guerra da Coreia (1950 - 1953), Guerra Civil do Laos (1953 - 1975), Guerra da Argélia (1954 - 1962), Guerra do Vietnã (1955 - 1975), Guerra do Canal de Suez (1956), Guerra de Independência da Eritreia (1961-1991), as Guerra Coloniais Portuguesas (1961 - 1975), Guerra Civil na Colômbia (1964 - presente), Guerra de Independência da Namíbia (1966 - 1988), Guerra Indo-Paquistanesa de 1965 (1965), Guerra dos Seis Dias (1967), Guerra Civil do Camboja (1967 - 1975), Segunda Ocupação da República Dominicana (1965 - 1966), Guerra Indo-Paquistanesa de 1971 (1971), Guerra do Yom Kipur (1973) e a Guerra Civil Angolana (1975 - 2002).

[7] O Comitê Internacional da Cruz Vermelha é uma instituição privada fundada em 24 de junho de 1863, com sede em Genebra, na Suíça. Ela foi criada pelo comerciante Henry Dunant, depois dele ter testemunhado os horrores da Batalha de Solferino, no norte da Itália. As atividades do Comitê são caracterizadas por imparcialidade, neutralidade e independência, de forma a fornecer ajuda humanitária a todos os necessitados, independente da parte beligerante a favor da qual lutavam.

de 1977, e outro cujo objeto são os conflitos armados não internacionais, o 2º Protocolo Adicional de 1977.

O artigo 1º do 2º Protocolo Adicional define o âmbito de aplicação material desse tratado e, para tanto, lista os elementos condicionantes à existência de conflitos armados não internacionais que serão regulados especificamente por este Protocolo. São eles: não ser um conflito armado sob o âmbito de aplicação do 1º Protocolo Adicional; o conflito deve ocorrer no território de uma Alta Parte Contratante; as hostilidades devem necessariamente ter as forças armadas do Estado signatário como parte; como outra parte beligerante podem figurar forças armadas dissidentes ou grupos armados organizados, desde que estes grupos estejam sob a chefia de um comando responsável, exerçam controle efetivo sobre uma parte do território do Estado contratante, sejam capazes de executar operações militares contínuas e organizadas e tenham o aparato estrutural e institucional necessário para implementar as regras e princípios codificados no 2º Protocolo Adicional.

Percebe-se que o âmbito de aplicação do 2º Protocolo é muito mais restrito que o Artigo 3º Comum. Para tanto, os Estados presentes na Conferência de Genebra deixaram claro que aquele tratado, o 2º Protocolo, visa "[...] desenvolver e completar o artigo 3º comum às Convenções de 12 de agosto de 1949, sem modificar as suas condições de aplicação atuais" (CICV, 1987, para.4457) (grifo e tradução nossos). Diante disso, conflitos com um nível baixo de intensidade e que não preenchem as características exigidas pelo 2º Protocolo Adicional ainda são regulados pelo Artigo 3º Comum. Isso explica porque conflitos onde o grupo não estatal envolvido não controla parte do território ou quando o conflito não possui a participação de forças armadas oficiais de um Estado parte do 2º Protocolo Adicional não estão sujeitos à aplicação desse tratado, mas estão sob a autoridade do Artigo 3º Comum.

Em resumo, o Artigo 3º Comum contém uma existência autônoma, ou seja, a sua aplicabilidade não é limitada ou afetada pelo campo de aplicação material do 2º Protocolo Adicional. Essa arquitetura normativa tem o propósito de impedir que qualquer redução no nível de proteção garantida pelo Artigo 3º Comum seja imposta pelas partes beligerantes. Como defendido por Jean Pictet, "[...] o escopo de aplicação do artigo 3º deve ser o mais amplo possível." (1952, p.36) (tradução nossa)

No presente trabalho será aplicada a definição de conflito armado presente no Artigo 3º Comum. Essa escolha se justifica no fato deste conceito ser mais genérico, de forma a alcançar todos os conflitos não internacionais. Ademais, até a data do presente trabalho,

vários Estados ainda não ratificaram o 2º Protocolo Adicional[8] e há incerteza se as disposições deste tratado refletem costume.

Para este fim, adotar-se-á a definição concebida pelo TPIEI e que já foi mencionada acima: "[...] existem [conflitos armados não internacionais] sempre que há [...] violência armada prolongada entre autoridades governamentais e grupos organizados ou entre estes grupos dentro de um Estado" (TPIEI, 1995, para.70) (tradução nossa). Este conceito foi escolhido por estar codificado no artigo 8º, §2º, alínea "f" do Estatuto de Roma do Tribunal Penal Internacional (TPI)[9] e ser frequentemente adotado na literatura humanitarista[10] e também na jurisprudência de outras cortes internacionais[11].

A definição adotada pelo TPIEI demonstra que os conflitos armados não internacionais possuem dois elementos: **(3.2)** a organização interna do grupo armado e **(3.3)** a intensidade mínima do uso da força.

3.2 A organização interna do grupo armado

Para que se configure um conflito armado de caráter não internacional, a parte beligerante composta por forças não estatais precisa ter um nível mínimo de organização interna, de forma a lhe dar condições para realizar atos militares de forma intensa e planejada. Contudo, tendo em vista que o grau exato de organização dos grupos não está estabelecido na lei internacional, não é razoável exigir padrões extremamente rígidos (SASSOLI, 2007, p.56). Diante disso, o nível organizacional não precisa ser similar àquele encontrado na estrutura de comando das forças armadas oficiais dos Estados. Na verdade, exigi-se apenas uma cadeia hierárquica de comando minimamente estruturada e a capacidade de realizar operações militares coordenadas (TPIEI, 2005, para.129; OTAN, 2013, p.88).

No *Caso Promotor v. Ljube Boškoski e Johan Tarčulovski*, o TPIEI descreveu os fatores a se considerar quando da análise da organização do grupo não estatal, os classificando em cinco grupos (2008, paras.199-203). Os primeiros são os fatores que indicam uma estrutura hierárquica interna, tais como a presença de um alto comando responsável pelas

[8] Tais como Estados Unidos, Tailândia, Turquia, México, Índia, Paquistão, Malásia, Indonésia, Angola, Irã, Azerbeijão, Iraque, Síria, Papua Nova Guiné, Sri Lanka, Vietnã e outros.

[9] O Tribunal Penal Internacional é a primeira jurisdição internacional criminal permanente, sendo estabelecido em 1º de julho 2002, depois do depósito do sexagésimo instrumento de ratificação ou adesão de seu Estatuto, em 11 de abril do mesmo ano. A sua função é investigar, julgar e condenar pessoas físicas que cometeram crimes de guerra, crimes contra a humanidade, genocídio e crimes de agressão, apesar da jurisdição da corte sobre esse último estar suspensa. O Brasil ratificou o Estatuto em 20 de junho de 2002, sendo o 69º Estado a fazê-lo. Por fim, destaca-se que, na data da presente publicação, o TPI tinha 123 membros.

[10] Cf.: MILANOVIC, 2007, p.382; PAULUS e VASHAKMADZE, 2009, p.106-107; RADIN, 2013, p.710-711; ASSOCIAÇÃO DE DIREITO INTERNACIONAL, 2010, p.14-15.

[11] Cf.: TPI, 2012, para.533; TPI, 2009, para.59; TPI, 2008, para.9; TPIR, 1998, para.619.

nomeações e instruções aos comandantes, redação e divulgação interna de regulamentos, organização e fornecimento de armamentos, autorização de operações militares, delegação de tarefas aos membros do grupo, emissão de declarações e comunicados políticos e recebimento de relatórios redigidos por unidades operacionais sob a sua esfera de comando; a atribuição de um porta-voz oficial; a existência de uma sede; e a emissão de regulamentos internos estabelecendo postos de comando e os deveres dos comandantes e subcomandantes de uma unidade, pelotão ou esquadrão, criando uma cadeia de hierarquia militar entre os vários níveis de comandantes (TPIEI, 2008, para.199).

O segundo grupo são os fatores que indicam a capacidade do grupo de realizar operações militares de forma organizada, tais como a habilidade para determinar uma estratégia militar unificada; a capacidade de conduzir operações militares em larga escala; a competência para administrar territórios ocupados; e a cooperação entre as unidades operacionais, a fim de coordenar suas ações e disseminar de forma eficaz as ordens de comando (TPIEI, 2008, para.200).

Em terceiro lugar estão os fatores que indicam um nível mínimo de logística, tais como a capacidade de recrutar novos membros; fornecimento de treinamento militar; organização da aquisição e distribuição de armamentos; fornecimento e uso de uniformes; e a existência de equipamentos de comunicação entre a sede e as unidades ou entre as unidades (TPIEI, 2008, para.201).

A quarta classe são os fatores que determinam se o grupo possui um nível mínimo de disciplina e capacidade para implementar obrigações humanitárias, tais como a existência de regulamentos internos e sua efetiva disseminação entre os membros; estabelecimento de mecanismos disciplinares e punitivos; e a formação militar adequada (TPIEI, 2008, para.202).

Por fim, o TPIEI apontou os fatores que indicam que o grupo armado é capaz de falar com uma só voz, tais como a sua capacidade de agir em nome de seus membros em negociações políticas com representantes de organizações internacionais, países estrangeiros ou partes beligerantes inimigas; e sua capacidade de negociar e celebrar acordos de cessar-fogo ou acordos de paz (TPIEI, 2008, para.203).

Estes elementos são meramente exemplificativos e não precisam ser exauridos cumulativamente pelo grupo em questão. Deve ser feita uma análise de cada situação concreta, na qual a presença de somente alguns dos critérios *supra* já seria suficiente para demonstrar a organização do grupo.

O critério da organização deve ser entendido, assim, como o elemento de coesão interna e hierarquia da parte beligerante não estatal. Em outras palavras, o grupo deve ser articulado e coordenado o suficiente para ser identificado de fato como um grupo e não como

se seus atos fossem perpetrados por indivíduos de forma isolada e esporádica. A organização visa permitir que a outra parte beligerante seja capaz de identificar claramente os membros do grupo, de forma a evitar ataques contra alvos equivocados, especialmente contra a população civil.

Assim, *hackers* que atuam isoladamente, ainda que para alcançar o mesmo propósito, não podem ser considerados membros de um grupo organizado. Carece a eles o elemento de unidade hierárquica e estrutura que a organização interna demanda. Com isso, ataques cibernéticos que são coletivos meramente porque os seus perpetradores os executam de forma paralela para atingir um objetivo comum, mas sem qualquer liderança, não podem ser considerados organizados (MELZER, 2011, p.24; SCHMITT, 2012, p.255).

Questiona-se, ainda, se atos militares cibernéticos realizados por um grupo de indivíduos de forma conjunta, instigados por um líder comum, mas sem qualquer conexão ou coordenação permanente entre si, podem configurar um grupo organizado. Imagine uma situação onde um indivíduo, através de redes sociais e emails, agenda um horário específico para que os interessados, que ele nunca teve contato antes, inclusive *online*, e que provavelmente nunca conhecerá pessoalmente, realizem um ataque conforme as suas instruções, que serão enviadas previamente e também durante a execução dos ataques. Seria a situação de uma entidade digital com nome, símbolo distintivo e líder próprios e reconhecidos, mas que não possui membros fixos. Para cada operação feita por essa entidade, um certo número de *hackers* voluntariamente segue os comandos desse líder e atua coletivamente para implementar as operações planejadas. Assim que as operações terminam, aqueles que participaram dela não mais tem contato com o líder, podendo atuar em outra operação futura ou não. Ainda que essas operações ocorram conforme as instruções deste suposto comandante, a organização exige muito mais do que isso. Aquela situação descreve um mero conjunto de indivíduos, que, de forma esporádica, realizam ataques cibernéticos sob às ordens de um terceiro. O critério da organização demanda que um certo número de indivíduos esteja permanentemente subordinado e à disposição do seu comandante, formando a força perene e estável do grupo.

Todavia, é possível formar grupos organizados na internet. Seria o caso de um grupo identificável, com estrutura de liderança estabelecida e com membros fixos. Nesse contexto, o(s) comandante(s) do grupo atuaria(m) na coordenação e emissão de ordens, identificação de alvos para os ataques, distribuição de ferramentas para realizar tais ataques, estabelecimento de métodos para encontrar pontos de defesa vulneráveis no inimigo e análise dos dados resultantes das operações militares, a fim de verificar a necessidade de novos atos ofensivos para destruir o alvo. Isso demonstra que o grupo atua de forma coordenada internamente,

sendo um indício de sua organização (OTAN, 2013, p.89). Essas funções e comandos podem ser todos emitidos e realizados via comunicação eletrônica, tornando possível a existência de grupos organizados no ciberespaço.

O mero fato dos membros nunca terem se encontrado fisicamente não prejudica o caráter organizado do grupo. Como exposto no parágrafo anterior, a coordenação operacional, bem como a realização dos próprios ataques, pode ser articulada totalmente *online*, sendo dispensável o encontro físico dos membros, muitas vezes, residentes em diversos Estados diferentes.

Uma discussão relevante se refere à capacidade do grupo de impor regras humanitárias aos seus membros. De fato, este é um critério adotado no artigo 1º do 2º Protocolo Adicional de 1977 como condição de existência de um grupo armado não estatal que estaria sujeito aos direitos e deveres desse tratado. Diante disso, certos autores, incluindo Michael N. Schmitt (2012, p.257) e Cordula Droege (2012, p.550-551), apresentam este elemento como grande entrave ao exaurimento da condição de organização do grupo. Segundo eles, devido à inexistência de contato físico entre o comandante e seus subordinados ou entre os próprios subordinados, seria muito difícil ou impossível que um comandante fosse capaz de implementar sanções por violações de normas humanitárias no contexto de um grupo formado exclusivamente *online.*

De fato, não se pode negar que as lideranças de grupos armados cibernéticos dificilmente terão meios idôneos para estabelecer um aparato punitivo eficaz contra membros que transgridem normas humanitárias. A falta de contato físico entre eles torna esse parâmetro praticamente inatingível na esfera cibernética. Contudo, ao usar esse fato para negar a existência de grupos armados cibernéticos, Schmitt e Droege não apresentam uma conclusão aceitável. Isso porque a aplicação do regime jurídico do Artigo 3º Comum não exige um grau tão elevado e sofisticado de organização. O texto desse dispositivo é simplesmente silente quanto ao dever de estabelecer uma estrutura capaz de implementar normas humanitárias. Com isso, não se pode condicionar a aplicação desse artigo à existência de tão rigoroso parâmetro organizacional.

Além disso, tendo em vista a relevância dos trabalhos preparatórios de um tratado para sua interpretação, *mister* notar que uma proposta inicial do Artigo 3º asseverava que um grupo só estaria protegido por este dispositivo se tivesse "[...] os meios para fazer respeitar a Convenção e as outras leis e costumes da guerra" (PICTET, 1952, p.45) (tradução nossa). Esta proposta foi abertamente rejeitada, pois tornaria a aplicação da proteção humanitária a estes grupos muito difícil, o que aumentaria a crueldade nas hostilidades (PICTET, 1952, p.46).

A maioria das delegações presentes na Conferência de Paz de Genebra, depois de muito embate, aceitou a proposta que consistia em adotar uma definição ampla e abrangente de conflito armado não internacional no Artigo 3º Comum. Optou-se por não descrever os elementos caracterizadores dessa espécie de conflito armado e, ao invés disso, detalhar quais os direitos e deveres que aquele dispositivo asseguraria (PICTET, 1952, p.46-48). Assim, não se deve fazer qualquer interpretação restritiva do Artigo 3º Comum no tocante à definição de conflitos armados não internacionais, sob pena de indevidamente diminuir o seu escopo protetivo.

A exigência de uma estrutura punitiva instituída dentro do grupo já foi analisada pelo TPIEI no caso *Promotor v. Fatmir Limaj*. Nesse processo, a defesa de Fatmir Limaj alegou que "[...] uma parte de um conflito deve ser capaz de aplicar o direito internacional humanitário e, no mínimo, deve possuir: uma compreensão básica dos princípios estabelecidos no Artigo 3º Comum, uma capacidade de disseminar regras humanitárias e um método sancionatório contra violações" (TPIEI, 2005b, para.88) (tradução nossa).

Entretanto, o TPIEI inequivocamente rechaçou essa linha de argumentação. Atestou-se que o propósito de exigir um nível mínimo de organização interna visa simplesmente separar os conflitos armados das insurreições desorganizadas e volúveis, dos atos criminosos executados em quadrilha e das atividades terroristas. O critério da organização não pode jamais ser usado para privar certos grupos e seus membros da proteção assegurada pelo Artigo 3º Comum através da exigência de critérios organizacionais excessivamente rigorosos. "Assim, somente um pouco de organização pelas partes já é suficiente para atestar a existência de um conflito armado" (TPIEI, 2005b, para.89) (tradução nossa).

O TPIEI se deparou novamente com essa questão em 2008, no caso *Promotor v. Ljube Boskoski e Johan Tarculovski*, e em cujo julgamento o precedente do caso *Fatmir Limaj* foi repetido. O TPIEI foi consideravelmente incisivo, fazendo menção expressa aos critérios rejeitados nos trabalhos preparatórios do Artigo 3º Comum (TPIEI, 2008, para.197). O TPIEI deixou claro também que a existência de um instrumento de sanção contra os membros infratores do grupo é um "critério conveniente" e não juridicamente mandatório para a configuração de um conflito armado. *In fine*, estabeleceu-se que o critério de organização a ser adotado é: "[...] a liderança do grupo deve, no mínimo, ter a capacidade de exercer algum controle sobre seus membros para que as obrigações básicas do Artigo Comum 3º das Convenções de Genebra possam ser implementadas" (2008, para.196) (tradução nossa).

Com isso, a simples existência de uma liderança *online* capaz de disseminar ordens de ataques a seus subordinados e esses comandos estarem em conformidade com as normas

humanitárias já é suficiente para configurar o elemento de organização, independentemente do efetivo respeito dessas ordens pelos membros do grupo. Em outras palavras:

> [...] desde que o grupo armado possua a capacidade organizacional de cumprir com as obrigações do direito internacional humanitário, a existência de um padrão de violações das leis humanitárias não necessariamente indica que o grupo não possui o nível de organização necessário para ser um grupo em um conflito armado. [O TPIEI] não pode simplesmente inferir uma falta de organização do grupo armado em razão do fato de que o direito internacional humanitário foi frequentemente violado pelos seus membros. Na análise deste elemento, [o TPIEI] precisa examinar como os ataques foram planejados e executados - ou seja [...] se eles eram principalmente o resultado de uma estratégia militar imposta por aqueles que lideram o grupo ou se eles foram perpetrados pelos membros do grupo de uma forma que eles mesmos decidiram como agir (TPIEI, 2008, para.205) (tradução nossa).

Afirma-se, em sede doutrinária, que a análise da organização dos grupos não estatais depende de elementos futuros a serem estabelecidos pela prática estatal ainda por vir (DROEGE, 2012, p.551). De fato, concorremos que ainda há certa precariedade de informações nesta área, mas a criação de grupos e instituições organizadas para fins militares especialmente cibernéticos já é uma realidade em diversos países. Destaca-se o *U.S. Cyber Command*, criado em 23 de junho de 2009, pelo então Secretário de Defesa dos Estados Unidos, Robert Michael Gates. Apesar de mais notório, ele não é o único. A Colômbia, em 2013, criou o *Grupo de Respuesta a Emergencias Cibernéticas de Colombia* e o *Comando Conjunto Cibernético*. Um exemplo notável é a Coreia do Norte, que apesar de sua pobreza e isolamento, tem feito pesados investimentos para manter uma unidade militar cibernética sofisticada, a Unidade 121, que opera no território chinês, devido ao limitado número de conexões de internet no território norte-coreano (ROSCINI, 2014, p.10).

Além destes, outros Estados, incluindo Austrália, Canadá, Coreia do Sul, Estônia, França, Alemanha, Índia, Irã, Israel, Itália, Quênia, Mianmar, Holanda, Nigéria, Paquistão, China, Polônia, Rússia, Suécia, Taiwan, Turquia, Reino Unido e República Tcheca, já estabeleceram unidades militares cibernéticas próprias ou demonstraram publicamente a sua intenção de criá-las no futuro breve (CARR, 2011, p.243-262; ROSCINI, 2014, p.10). O Brasil não fica de fora dessa lista. Em 2010, por ordem do Comando do Exército brasileiro, criou-se o Centro de Defesa Cibernética, responsável por coordenar toda a rede de defesa cibernética no país, incluindo o Comando de Defesa Cibernética e a Escola Nacional de Defesa Cibernética (BRASIL, 2010, p.7-8; BRASIL, 2014, Seção 1, nº 208).

Assim, há um movimento global de militarização e institucionalização do espaço cibernético. Seria ilógico acreditar que grupos armados não estatais, frequentemente dotados de sofisticada articulação e organização internas e imenso potencial econômico e financeiro, não estariam a fazer o mesmo. Há precedentes que ilustram a atuação de grupos não estatais

no campo cibernético. Em 1998, os guerrilheiros do grupo armado Tigres de Liberação do Tamil Eelam[12] interromperam a comunicação das embaixadas do Sri Lanka, enviando um volume maciço de e-mails às mesmas. Durante o ataque, as embaixadas receberam cerca de 800 e-mails por dia ao longo de duas semanas. As mensagens eram todas semelhantes e diziam: "*Nós somos os Tigres Negros da Internet e estamos fazendo isso para interromper suas comunicações*." (tradução nossa)[13] Autoridades cingalesas caracterizaram esse incidente como o primeiro ataque cibernético por grupos não estatais a ser perpetrado contra os sistemas informáticos oficiais de um Estado (DENNING, 2000).

Em 7 de janeiro de 2015, pelo menos três sites oficiais do governo alemão, incluindo o da Chancelaria Federal (*Bundeskanzleramt*) e o do Parlamento Alemão (*Bundestag*), ficaram inacessíveis por horas devido a um ataque cibernético realizado pelo *Cyber Berkut*, um grupo de *hackers* pró-Rússia originário do leste da Ucrânia. Em troca do retorno da normalidade dos *websites*, o grupo exigiu que a Alemanha interrompesse seu apoio financeiro e político ao governo de Kiev (MARTIN e KIRSCHBAUM, 2015).

Em 15 de janeiro de 2015, *hackers* ligados ao Estado Islâmico do Iraque e do Levante, um grupo armado não estatal jihadista que assumiu o controle territorial de grande parte do norte do Iraque e leste da Síria, foram capazes de invadir e assumir o controle da conta de *Twitter* do Comando Central das Forças Armadas dos Estados Unidos. O grupo postou mensagens ameaçadoras e vídeos de propaganda jihadista, bem como documentos militares sigilosos. Um dos *tweets* dizia: "*Soldados americanos, nós estamos chegando, se preparem*." (tradução nossa)[14] Em outro: "*Em nome de Alá, o Mais Gracioso, o Mais Misericordioso, o CyberCalifado continua sua CyberJihad*." (tradução nossa)[15] Este é um dos episódios de uma intensa batalha de propaganda e credibilidade que os Estados Unidos e o Estado Islâmico travam desde meados de 2014 (VINCENT, 2015).

Grupos não estatais também já demonstraram interesse em ataques cibernéticos contra instalações civis relevantes. Em 2002, durante uma operação de busca nas cavernas de Tora Bora, no Afeganistão, tropas norte americanas encontraram um *laptop* da *Al Qaeda* com informações aplicáveis a realização de ataques cibernéticos. Relatórios forenses revelaram que os usuários do computador em questão haviam frequentado *websites* com manuais de

[12] Os Tigres de Liberação do Tâmil Eelam são um grupo armado composto por membros da etnia tâmil, que luta pela independência do Tâmil Eelam, uma região localizada no nordeste do Sri Lanka. A tensão deste grupo com o Governo cingalês levou ao início da Guerra Civil do Sri Lanka (1983-2009), que chegou ao fim com a derrota dos Tigres de Liberação.
[13] O texto original dos emails em inglês é: "*We are the Internet Black Tigers and we're doing this to disrupt your communications*."
[14] O texto original do *tweet* em inglês é: "*American soldiers, we are coming, watch your back.*"
[15] O texto original do *tweet* em inglês é: "*In the name of Allah, the Most Gracious, the Most Merciful, the CyberCaliphate continues its CyberJihad*."

sabotagem, softwares e instruções de programação para sistemas operacionais de infraestruturas civis e várias outras ferramentas para invasão de sites e programas importantes (DINNISS, 2012, p.287).

Outro *laptop* foi encontrado, no mesmo ano, no escritório da *Al Qaeda* em Cabul. Neste, foram descobertas informações muito sofisticadas, incluindo um programa que criava modelos informatizados de represas com detalhes de engenharia estrutural e dados geológicos de solo, permitindo aos usuários simular ataques cibernéticos com a finalidade de destruir represas e prever os resultados lesivos destes ataques com considerável precisão (GELLMAN, 2002).

Após analisar os episódios *supra*, resta claro que grupos não estatais atuam no espaço cibernético a fim de perseguir seus interesses, inclusive através da realização de ataques digitais. Isso releva que a ameaça cibernética é uma realidade insofismável de nossos dias, tanto aos Estados, quanto para grupos privados.

3.3 A intensidade mínima dos ataques

Além do grau de organização do grupo, é necessário identificar o grau de violência que separa meros distúrbios internos dos conflitos armados não internacionais. Assim, hostilidades internas precisam atingir um certo grau mínimo de intensidade para configurar um conflito armado.

Diante da inexistência de uma definição convencional do elemento da intensidade, o direito jurisprudencial se torna uma ferramenta relevante para sua identificação. Assim, *mister* notar que o TPI (2012, para.533), o TPIEI (2004, para.336; 1998, para.59) e o TPIR (1998, para.619) já concluíram que a configuração de conflitos armados não internacionais está condicionada à existência de "violência armada prolongada." Todavia, deve ficar claro que esta expressão faz referência à intensidade da violência e não necessariamente à sua duração temporal muito extensa. Isso fica evidente no caso *Juan Carlos Abello v. Argentina* (*La Tablada)*, decidido em 1997, pela Comissão Interamericana de Direitos Humanos. Esse litígio envolvia a legalidade do contrataque pelas forças armadas da Argentina contra guerrilheiros que haviam tomado o Regimento de Infantaria de La Tablada, em Buenos Aires. O relatório da Comissão concluiu que as hostilidades entre as tropas argentinas e o grupo de guerrilheiros configuraram um conflito armado não internacional, ainda que tenham durado aproximadamente 30 horas e causado a morte de cerca de 40 pessoas (ComIADH, 1997, paras.152-156).

A expressão "violência armada prolongada", na sua acepção temporal, significa que ataques isolados não configuram conflitos armados, por mais violentos que sejam. Isso fica evidente no emblemático ataque terrorista pela *Al-Qaeda* contra o *World Trade Center* e o Pentágono, em 11 de setembro de 2001, episódio que resultou na morte de três mil pessoas. O Presidente George W. Bush chegou a classificar tais ataques como "atos de guerra." (ESTADOS UNIDOS, 2001) Apesar disso, eles não são suficientes para constituir um conflito armado. Faz-se necessário a ocorrência de hostilidades num certo intervalo de tempo, ainda que não necessariamente muito prolongado, como verificado no caso *Juan Carlos Abello v. Argentina.*

Para verificar a presença da intensidade mínima, uma série de fatores pode ser analisada *in casu*. Pode-se apontar, de forma ilustrativa, a quantidade de tropas e unidades envolvidas; a seriedade dos ataques; o tipo de armamento empregado; o tamanho da área geográfica onde os confrontos se espalham; o número de mortos e de refugiados; a extensão da destruição patrimonial; a realização de bloqueios ou cercos de cidades e a escala dos bombardeios sobre essas cidades; a existência e deslocamento da linha de frente entre as partes; a ocorrência de ocupações de territórios, cidades e aldeias; o fechamento de estradas; a promulgação de cessar-fogos ou outros acordos de paz ou trégua; o envolvimento de organizações internacionais nas negociações de paz e no monitoramento dos acordos firmados entre os beligerantes; e a atuação específica do Conselho de Segurança da ONU (TPIEI, 2005a, paras.163-168; TPIEI, 2008, paras.177-178).

Contudo, é possível que ataques exclusivamente cibernéticos alcancem o nível de intensidade necessária? Acreditamos que sim. Para compreender a tese aqui desenvolvida, um ponto inicial precisa ficar claro. Defendemos que os meios cibernéticos nada mais são do que um novo tipo de arma disponível aos agentes beligerantes e, portanto, devem ser tratados como tal. Apesar de seu uso frequente em tratados internacionais, não existe uma definição convencional do termo "arma" no Direito Internacional. Para tanto, adotar-se-á a conceituação desenvolvida pelo Departamento de Defesa dos Estados Unidos. Segundo esse, a expressão "arma" (*weapon*) descreve "[...] todos os armamentos, munições, materiais, instrumentos, mecanismos ou dispositivos que têm o efeito pretendido de ferir, danificar, destruir ou desabilitar pessoas ou materiais" (ESTADOS UNIDOS *apud* CICV, 2006, p.933) (tradução nossa).

Diante deste conceito, a natureza de um objeto como arma não é sua designação ou finalidade corriqueira, nem a sua utilização habitual, mas a intenção com o qual ele é usado, bem como os efeitos de seu emprego específico (MELZER, 2011, p.13). De forma conclusiva, Yoram Dinstein afirma que "[t]al como acontece com todas as armas conhecidas, o teste de

uma nova arma não é o quão intimidadora ela parece - ou quão engenhoso é o funcionamento do novo mecanismo -, mas quais os danos que ela é capaz de produzir" (2013, p.280) (tradução nossa). Assim, tendo em vista que recursos cibernéticos têm sido usados para fins militares com o objetivo específico de prejudicar inimigos, eles devem ser tratados como armas.

Portanto, para averiguar a intensidade para fins de configuração de um conflito armado, a natureza cibernética do ataque é irrelevante, pois a utilização de qualquer dispositivo, mecanismo ou instrumento que resulte na perda de vidas humanas ou destruição de patrimônio pode ser classificado como uso de força militar, inclusive meios cibernéticos (MELZER, 2011, p.13; ROSCINI, 2010, p.114-115). Considerando que ataques cibernéticos podem ser tão danosos quanto ataques realizados com o uso de força tradicional, não há nenhuma razão para acreditar que operações cibernéticas que podem provocar as mesmas consequências violentas que as operações militares tradicionais não possam alcançar a intensidade mínima.

Diante disso, aponta-se como exemplos de ataques cibernéticos que claramente configuram exemplos de uso de força com considerável intensidade: mortes causadas pela desativação de aparelhos em hospitais; uma extensa interrupção da rede de energia elétrica (apagão), criando consideráveis repercussões deletérias; o desligamento de computadores que controlam obras hidráulicas e barragens, gerando inundações em áreas habitadas; queda de aeronaves devido ao mau funcionamento provocado nos sistemas de navegação; e o colapso de uma usina nuclear, levando à liberação de materiais radioativos em áreas povoadas (DINSTEIN, 2002, p.105).

Como exemplo real a citar, temos o ataque ocorrido contra a instalação nuclear de Natanz, no Irã. Entre 2009 e 2010, um vírus de computador chamado "*Stuxnet*" foi disseminado contra as centrífugas nucleares de Natanz, que foram adquiridas ilicitamente pelo governo iraniano com o propósito de enriquecer urânio para a fabricação de armas nucleares. O *Stuxnet* é uma arma muito sofisticada, que controla e desabilita centrífugas da marca *Siemens*, através da indução de oscilações drásticas na frequência de rotação dos rotores das centrífugas, as sobrecarregando e, assim, as desativando. Nenhum Estado assumiu a responsabilidade pelos ataques, mas há indícios de que o vírus foi produzido e lançado pelos Estados Unidos e Israel (O'CONNELL, 2012, p.194; WAXMAN, 2013, p.119).

Apesar do Irã ter negado veementemente a ocorrência de tais ataques, o *Stuxnet* foi desastroso ao programa nuclear deste país, desabilitando cerca de um quinto das centrífugas nucleares em Natanz. Analistas especulam que o retardo nas operações de enriquecimento de

urânio no Irã resultou num atraso de vários anos no programa de desenvolvimento de armas nucleares do país (NGUYEN, 2013, p.1082).

Diante do exposto, um método comparativo se revela eficiente para averiguar a existência do elemento da intensidade. A autoridade competente deve se questionar se os efeitos dos ataques cibernéticos *in casu* são equivalentes aos efeitos de possíveis ataques tradicionais naquelas mesmas condições. Em outras palavras, se no lugar daqueles ataques cibernéticos, ataques com força tradicional tivessem ocorrido, com efeitos precisamente iguais, as circunstâncias poderiam ser definidas como um conflito armado? Acredita-se que essa é a pergunta que o agente decisório deve se fazer.

Sabendo quais as condições razoáveis que podem alcançar a intensidade mínima para configurar um conflito armado, passemos às circunstâncias que dificilmente satisfariam este critério. Primeiramente, meros ataques cibernéticos isolados não configuram a intensidade necessária, ainda que provoquem danos materiais ao alvo atacado. Deve haver um conjunto de ataques coordenados e coletivos para que a magnitude e amplitude demandada sejam alcançadas (OTAN, 2013, p.86; SCHMITT, 2012, p.258).

Em segundo lugar, ataques cibernéticos, ainda que executados de forma maciça, não podem chegar à intensidade mínima quando não produzem danos materiais efetivos e amplos. São as consequências no mundo cinemático (material) das operações cibernéticas que são graves o suficiente para alcançar a intensidade necessária. Ataques sem qualquer destruição patrimonial física não são suficientes (DROEGE, 2012, p.551). Nesse prisma, a mera coleta não autorizada de informações, a interrupção das comunicações ou a emissão de ordens falsas para forças inimigas, sozinhos, não chegam à intensidade demandada.

Por fim, destaca-se que não é a intenção do autor propor um limite certo e preciso entre a força que possui intensidade mínima e aquela que não alcança o nível exigido. Até porque este limite supostamente inequívoco é impossível de ser descrito. Deve-se realizar uma análise caso a caso adotando os critérios identificados na prática estatal, na doutrina e no direito jurisprudencial.

4. Conclusão

Desde meados do século passado, o aparato jurídico-tecnológico relevante aos conflitos armados modificou consideravelmente. A mais nova mudança de paradigma que desafia os institutos e definições internacionais humanitárias vigentes é a aplicação de recursos cibernéticos para fins militares, tanto por Estados, quanto por grupos não estatais.

Através da análise dos conflitos armados não internacionais à luz desses elementos cibernéticos, destacou-se no decorrer do presente trabalho que os elementos da organização interna dos grupos armados e a intensidade mínima das hostilidades por eles perpetradas também podem ser exauridos no campo cibernético. Grupos não estatais podem se organizar através de uma estrutura de liderança e comando exclusivamente *online*, sem qualquer contato físico entre seus membros. Além disso, devido aos efeitos destrutivos que os ataques cibernéticos podem produzir no mundo físico/cinemático, o elemento da intensidade das hostilidades também pode ser exaurido por meio de operações militares digitais.

Diante de todo o exposto, não se deve negar ou até mesmo subestimar o poder militar e a capacidade estratégica e organizacional de grupos não estatais, que possuem agora todo o espaço cibernético como campo de batalha para perseguir seus interesses. Da mesma forma, não se pode esquecer que a própria funcionalidade da nossa sociedade é, hoje, amplamente dependente de recursos cibernéticos. Serviços críticos à coletividade, tais como geração, transmissão e distribuição de eletricidade, transportes, serviços financeiros, comércio eletrônico, abastecimento de água, saúde pública e distribuição de alimentos, são todos condicionados ao perfeito funcionamento de sistemas operacionais informatizados.

Os interesses mais valiosos aos Estados, pelos quais eles se engajavam em guerras no passado para proteger, hoje são outros e muitos deles se relacionam com a segurança cibernética. Assim, ataques por grupos armados não estatais contra tais interesses essenciais devem ser tratados com grande seriedade por juristas e estadistas, especialmente para evitar o sofrimento das populações civis.

5. Referências

ASSOCIAÇÃO DE DIREITO INTERNACIONAL. *Final Report on the Meaning of Armed Conflict in International Law*, The Hague Conference, Committee on the Use of Force, Chair: Mary Ellen O'Connell, 2010.

BRASIL. *Portaria nº 666*, de 4 de agosto de 2010, Comandante do Exército, Boletim do Exército nº 31/2010, Brasília/DF, 6 de agosto de 2010.

_____. *Portaria Normativa nº 2.777/MD*, de 27 de outubro de 2014, Diário Oficial da União.

CANÇADO TRINDADE, Antônio Augusto. "Desafios e Conquistas do Direito Internacional dos Direitos Humanos no Início do século XXI", *XXXIII Curso de Direito Internacional Organizado*, Comissão Jurídica Interamericana da OEA, Rio de Janeiro, 2006, 407-490.

_____. *Separate Opinion to the Pulp Mills on the River Uruguay* (Argentina v. Uruguay), [2010] ICJ Rep.14.

CARR, Jeffrey. *Inside Cyber Warfare*, 2ª ed., Sebastopol: O'Reilly Media, 2011.

CASSESE, Antonio. *International Criminal Court*, Oxford: Oxford University Press, 2003.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS (ComIADH). *Juan Carlos Abella v. Argentina (La Tablada)*, Case 11.137, Report Nº 55/97, Inter-American Comission on Human Rights, 18 November 1997.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA (CICV). "Commentaries to the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977", *International Committee of Red Cross*, Geneva, 1987. Disponível em: <https://www.icrc.org/applic/ihl/ihl.nsf/INTRO/475?OpenDocument>. Acesso em: 30.02.2015.

_____. "A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977", *International Review of Red Cross*, Vol.88, No.864, 2006, 931-956.

CORTE INTERNACIONAL DE JUSTIÇA (CIJ). *Dispute regarding Navigational and Related Rights* (Costa Rica v. Nicaragua), [2009] ICJ Rep.213.

DENNING, Dorothy. "Cyberterrorism: The Logic Bomb versus the Truck Bomb", *Global Dialogue***,** Vol.2, No.4, 2000. Disponível em: <http://www.worlddialogue.org/content.php?id=111>. Acesso em: 13.06.2015.

DINNISS, Heather Harrison. *Cyber Warfare and the Laws of War*, Cambridge: Cambridge University Press, 2012.

DINSTEIN, Yoram. *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge: Cambridge University Press, 2004.

_____. "Computer Network Attacks and Self-Defense", *International Law Studies*, Vol.76, 2002, 100-119.

_____. "Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference", *International Law Studies*, Vol.86, 2013, 276-287.

DROEGE, Cordula. "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross*, Vol. 94, No.886, 2012, pp.533-578.

ESTADOS UNIDOS. *Remarks by the President In Photo Opportunity with the National Security Team*, The White House, Office of the Press Secretary, 12 September 2001. Disponível em: <http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010912-4.html>. Acesso em: 20.01.2015.

_____. *Remarks by the President on Securing our Nation's Cyber Infrastructure*, The White House, Office of the Press Secretary, 29 May 2009. Disponível em: <https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>. Acesso em: 22.01.2015.

GELLMAN, Barton. "Cyber-Attacks by Al Qaeda Feared", *The Washington Post***,** 27 June 27 2002. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html>. Acesso em: 02.02.2015.

KELSEY, Jeffrey. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", *Michigan Law Review*, Vol.106, 2008, 1427-1451.

MARTIN, Michelle e KIRSCHBAUM, Erik. "Pro-Russian group claims cyber attack on German government websites", *Reuters***,** 7 January 2015. Disponível em: <http://www.reuters.com/article/2015/01/07/us-germany-cyberattack-idUSKBN0KG15320150107>. Acesso em: 13.06.2015.

MELZER, Nils. Keeping the balance between military necessity and Humanity: a response to four critiques of the ICRC's interpretive guidance on the notion of direct participation in hostilities", *New York University Journal of International Law and Politics*, vol.42, No. 831, 2010, 831-916.

_____. "Cyberwarfare and International Law", *United Nations Institute for Disarmament Research Resources*, Geneva, 2011.

MILANOVIC, Marko. "Lessons for human rights and humanitarian law in the war on terror: comparing Hamdan and the Israeli Targeted Killings case", *International Review of the Red Cross*, Vol.89, No.866, 2007, 373-393.

NGUYEN, Reese. "Navigating Jus Ad Bellum in the Age of Cyber Warfare", *California Law Review*, vol.,101, no.4, 2013, 1079-1129.

O'CONNELL, Mary Ellen. "Cyber Security without Cyber War", *Journal of Conflict & Security Law*, Vol. 17, No. 2, 2012, 187–209.

ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE (OTAN). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, International Group of Experts, NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press, 2013.

PAULUS, Andreas e VASHAKMADZE, Mindia. "Asymmetrical war and the notion of armed conflict – a tentative conceptualization", *International Review of the Red Cross*, Vol.91, No.873, 2009, 95-125.

PICTET, Jean. *I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field with Commentaries*, Geneva: ICRC, 1952.

RADIN, Sasha. "Global Armed Conflict? The Threshold of Extraterritorial Non-International Armed Conflicts", *International Law Studies*, vol.89, 2013, 696-743.

RONZITTI, Natalino. "Is the Non Liquet of the Final Report by the Committee Established to Review the NATO Bombing against the Federal Republic of Yugoslavia Acceptable?", *International Review of Red Cross*, No.840, 2000, 1017.

ROSCINI, Marco. "World Wide Warfare - 'Jus Ad Bellum' and the Use of Cyber Force", *Max Planck Yearbook of United Nations Law*, Vol.14, 2010, 85-130.

_____. *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press, 2014.

SASSOLI, Marco. "The Implementation of International Humanitarian Law: Current and Inherent Challenges", *Yearbook of International Humanitarian Law*, vol.10, 2007, p.45-73.

SCHABAS, Willian. *An Introduction to the International Criminal Court*, 3ª ed., Cambridge: Cambridge University Press, 2007.

SCHMITT, Michael. "Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance", *Virginia Journal of International Law*, vol. 50, No. 4, 2010, 795-839.

_____. "Classification of Cyber Conflict", *Journal of Conflict & Security Law*, Vol. 17, No. 2, 2012, 245–260.

SOLIS, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War*, New York: Cambridge University Press, 2010.

TRIBUNAL PENAL INTERNACIONAL (TPI). *Prosecutor v. Jean-Pierre Bemba Bombo, Warrant of Arrest for Jean-Pierre Bemba Gombo*, ICC, Pre-Trial Chamber III, Case no. ICC-01/05-01/08, 23 May 2008.

_____. *Prosecutor v. Omar Hassan Ahmad Al Bashir, Warrant of Arrest for Omar Hassan Ahmad Al Bashir*, ICC, Pre-Trial Chamber I, Case no. ICC-02/05-01/09, 4 March 2009.

_____. *Prosecutor v. Thomas Lubanga Dyilo***,** Judgment, ICC, Trial Chamber I, Case n. ICC-01/04-01/06, 14 March 2012.

TRIBUNAL PENAL INTERNACIONAL PARA A EX-IUGOSLÁVIA (TPIEI). *Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*, ICTY, Appeals Chamber, Case No. IT-94-1-T, 10 August 1995.

_____. *Prosecutor v. Anto Furundžija*, Judgment, ICTY, Trial Chamber, Case No. IT-95-17/I-T, 10 December 1998.

_____. *Prosecutor v. Dario Kordić e Mario Čerkez*, Judgment, ICTY, Appeals Chamber, Case No. IT-95-14/2-A, 17 December 2004.

_____. *Prosecutor v. Miroslav Kvoćka and others*, Judgment, ICTY, Appeals Chamber, Case No. IT-98-30/1-A, 28 February 2005.

_____. *Prosecutor v. Sefer Halilović*, Judgment, ICTY, Trial Chamber I, Section A, Case No. IT-01-48-T, 16 November 2005[2005a].

_____. *Prosecutor v. Fatmir Limaj and others*, Judgment, ICTY, Trial Chamber, Case n. IT-03-66-T, 30 November 2005[2005b].

_____. *Prosecutor v. Ljube Boskoski and Johan Tarculovski*, Judgment, ICTY, Trial Chamber, Case n. IT-04-82-T, 10 July 2008.

TRIBUNAL PENAL INTERNACIONAL PARA RUANDA (TPIR). *Prosecutor v. Jean-Paul Akayesu***,** Judgment, Trial Chamber, Case No. ICTR-96-4-T, 2 September 1998.

VERRI, Pietro. *Dictionary of the International Law of Armed Conflict*, Geneva: ICRC, 1992.

VINCENT, Michael. "US Central Command Twitter and YouTube feeds hacked by people claiming to be Islamic State supporters, *ABC News*, 12 January 2015. Disponível em: <http://www.abc.net.au/news/2015-01-13/us-central-command-twitter-feed-hacked-by-is-supporters/6013522>. Acesso em: 12.06.2015.

WAXMAN, Matthew. "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions", *International Law Studies*, Vol.89, 2013, 109-122.