LUIZ ARTUR RODRIGUES NUNES

GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL:

Aplicabilidade do Jus ad Bellum e do Jus in Bello

Trabalho de Conclusão de Curso - Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia.

Orientador: Professor Doutor Eduardo Santiago Spiller

Rio de Janeiro
2015

C2015 ESG

_____
Assinatura do autor

Biblioteca General Cordeiro de Farias

Nunes, Luiz Artur Rodrigues.
Guerra Cibernética e o Direito Internacional : Aplicabilidade do Jus ad Bellum e do Jus in Bello / Contra-Almirante (FN) Luiz Artur Rodrigues Nunes. - Rio de Janeiro : ESG, 2015.

60 f.: il.

Orientador: Professor Doutor Eduardo Santiago Spiller.
Trabalho de Conclusão de Curso – Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia (CAEPE), 2015.

1. Direito. 2. Direito Internacional. 3. DICA. I.Título.

AGRADECIMENTOS

Inicio agradecendo ao meu orientador, Professor Doutor Eduardo Santiago Spiller que, além de prover uma orientação precisa e oportuna, que me permitiu lapidar este trabalho, me incentivou e motivou em todas as fases de sua elaboração.

Agradeço, também, à fraterna convivência com a turma Destinos do Brasil, sem dúvida a melhor turma do CAEPE. A integração entre seus componentes e o clima de amizade e cooperação foram primordiais para a tranquilidade na execução deste e dos demais trabalhos pertinentes ao Curso.

E termino com um agradecimento especial pela compreensão, apoio e tolerância de minha família em face das prolongadas horas dedicadas a esta monografia. Sem o amor incondicional de minha esposa Fernanda e de meus filhos este trabalho não seria possível.

RESUMO

A área militar, uma ramificação da área social, visto que a guerra, em seu conceito Clausewitiziano, nada mais é do que o enfrentamento violento de vontades, tem sua evolução intimamente ligada às transformações e inovações científico-tecnológicas, cuja evolução se deu de forma vertiginosa, a partir do século passado, levando-nos à era digital. O avanço tecnológico que gerou oportunidade de crescimento e desenvolvimento se apresentou, ao mesmo tempo, como uma vulnerabilidade nos tempos atuais. A sociedade, que se tornou cada vez mais dependente desse mundo "on-line", passa a viver diuturnamente sob a ameaça de um ataque cibernético, que pode se dar com os mais diversos fins, como o roubo de dados ou a corrupção de sistemas, entre outros. O mundo passa a conviver com a possibilidade de hostilidades entre Estados no ciberespaço, ou seja, uma Guerra Cibernética. Tal fato, aliado à sofisticação crescente do arsenal cibernético, faz surgir o risco de que os efeitos provenientes de um ataque cibernético, com potencial cada vez mais adverso, sejam percebidos em todo um país. Nesse sentido, cabe buscar o enquadramento da Guerra Cibernética no ordenamento jurídico internacional, de modo a limitar seus efeitos, a exemplo do que ocorre em um conflito armado tradicional. Destarte, o presente trabalho busca, inicialmente, analisar os conceitos e características relacionados à Guerra Cibernética, para formação de uma base conceitual, de modo a possibilitar a posterior análise de sua aplicabilidade e enquadramento frente aos conceitos do Jus ad Bellum e do Jus in Bello.

Palavras chave: Guerra Cibernética, Direito Internacional dos Conflitos Armados, Direito Internacional Humanitário, Jus ad Bellum, Jus in Bello.

ABSTRACT

War, as a Clausewitzian concept, is no more than the violent clash of opposing wills. The military field, responsible for the study of this specific social behavior, showed large development in the last century in face of the spike on scientific and technological advances wich led us to the digital era. The enhancing capabilities of technology and its innovations also revealed to be dangerous, posing possible threats nowadays. Society, which has become increasingly more dependable on an online world, is now vulnerable to hazards that cyber attacks might impose, like data theft and corruption of systems. Our world now lives with the very real possibility of hostilities between States in the cyberspace, a cyberwarfare. This fact allied with an ever growing and sophisticated cyber-arsenal, may have very real and dangerous effects that could be felt by an entire country. Hence the importance of framing cybernetic warfare in the International Legal Order, in order to limit its effects, as it is the case with every armed conflict. The present work intents to firstly analyze concepts and characteristics related to cyberwar, in order to establish a conceptual basis, enabling a later analysis on its applicability and framing with the concepts of Jus ad Bellum and Jus in Bello.

Keywords: Ciberwarfare, Law of Armed Conflicts, International Humanitarian Law, Jus ad Bellum, Jus in Bello.

LISTA DE ABREVIATURAS E SIGLAS

C2	Comando e Controle
CICV	Comitê Internacional da Cruz Vermelha
CIJ	Corte Internacional de Justiça
DICA	Direito Internacional dos Conflitos Armados
DIH	Direito Internacional Humanitário
ONU	Organização das Nações Unidas
STIC2	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
TCIAI	Tribunal Criminal Internacional para a Antiga Iugoslávia
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
VANT	Veículo Aéreo Não Tripulado

SUMÁRIO

1 INTRODUÇÃO

Vivemos em um mundo em constante evolução. O homem, dotado de curiosidade nata e grande engenhosidade, é o motor dessa contínua transformação, que se processa em várias áreas afetas ao seu cotidiano e que são interdependentes, como as expressões do poder nacional: a psicossocial, a política, a econômica, a militar e, sobretudo, a científico-tecnológica. Esta última ganha dimensão e se destaca por possuir a capacidade de influenciar e alavancar tanto as demais, como a si própria.

Nesse diapasão, observou-se um avanço vertiginoso da tecnologia no século passado. Usando-se como referência o primeiro computador, na década de 1940, o ENIAC, que pesava trinta toneladas e ocupava 180 metros quadrados, os computadores se tornaram populares, pessoais e cada vez menores, até chegar aos "smart phones" do Século XXI, pesando apenas alguns gramas e superando em muito a capacidade computacional do primeiro computador eletrônico digital.

Durante esse mesmo período, os computadores passaram a operar em redes, de modo a poder compartilhar dados e, fruto de necessidades militares, surge a ARPANET, considerada a precursora da Internet, cujo desenvolvimento foi fomentado pelo Departamento de Defesa norte-americano, no auge da Guerra Fria. Surge, então, a Internet na década de 1980 e o mundo não seria mais o mesmo. O mundo passou a ser digital (NUNES, 2010).

Distâncias foram encurtadas, informações passaram a trafegar em quantidades cada vez maiores e tempos menores. Tudo isso permitiu maior fluidez nas relações pessoais e institucionais, transcendendo as fronteiras físicas dos Estados. "O mundo como um todo passou a estar à distância de um clique do mouse, em alusão à facilidade de acesso à informação. O mundo se tornou mais integrado e o planeta transformou-se em uma aldeia global" (NUNES, 2010).

Toda uma sorte de dados passa a trafegar em rede, interconectados ao mundo "on-line". Hoje, vários serviços, como o bancário e o controle de infraestruturas críticas[1], dependem de recursos computacionais e, assim como as mais diversas formas de interação eletrônica disponíveis ao homem moderno, estão de alguma forma ao alcance de todos por intermédio da Internet.

[1] Ver Glossário.

O avanço tecnológico que gerou oportunidade de crescimento e desenvolvimento se apresentou, ao mesmo tempo, como uma vulnerabilidade nos tempos atuais. A facilidade de acesso à informação e aos sistemas que a gerenciam trouxe, também, novos riscos relacionados à exposição virtual a que todos se submetem.

Surge, então, uma miríade de programas maliciosos, os “malware”, que iniciam como uma simples experiência de laboratório e evoluem até chegar a complexas armas cibernéticas. Uma síntese de sua evolução pode ser vista na Tabela 1.

1971	CREEPER - primeiro programa viral autorreplicante, foi escrito por Bob Thomas. Este vírus infectava computadores rodando o sistema operacional Telex e se espalhou via a ARPANET. Não causava dano, apenas apresentava uma mensagem na tela do computador infectado.
1981	ELK CLONER - vírus escrito para sistemas Apple II, causou a primeira infecção em larga escala.
1986	THE BRAIN - também conhecido como “Pakistani Flu”, vírus que infectava o setor de “boot”, foi o primeiro a infectar computadores tipo IBM-PC e causou uma epidemia global.
1988	MORRIS WORM - infectava sistemas rodando BSD Unix, foi o primeiro “worm” a se espalhar extensivamente.
1992	MICHELANGELO - causou grande preocupação devido à previsão de que infectaria milhões de computadores. Danos reais foram mínimos.
2003	SQL SLAMMER - também conhecido como “Saphire worm”, trata-se de um worm que atacava vulnerabilidades do Microsoft SQL, foi o worm de mais rápida propagação, impactando a Internet em apenas 15 minutos.
2010	STUXNET - primeiro worm a atacar sistemas SCADA (supervisory control and data acquisition).
2011	DUQU - worm relacionado ao stuxnet, porém sem possuir efeito destrutivo. Destinava-se a recolher informações.
2012	FLAME - na verdade foi um precursor do stuxnet que passou despercebido, usado em ciberespionagem contra o Iran.

Tabela 1 - Marcos históricos de programas maliciosos (KUSHNER, 2013)

A tecnologia se renova e evolui em um ritmo superior às soluções de segurança no ambiente cibernético, expondo novas tecnologias e sistemas de informação emergentes à exploração de suas vulnerabilidades. E o homem, dotado de imperfeições éticas e morais, logo descobriu como perpetrar ilícitos nesse novo mundo digital.

Exemplo do aumento exponencial das vulnerabilidades a que estamos expostos, o número de incidentes cibernéticos reportados no ano de 2014 em todo o mundo aumentou 48% em relação ao ano anterior, alcançando a marca de 42,8 milhões de incidentes, ou seja, 117.339 ataques por dia ao longo de todo o ano (GLOBAL, 2014).

A sociedade, que se torna cada vez mais dependente desse mundo “on-line”, passa a viver diuturnamente sob a ameaça de um ataque cibernético, que pode se dar com os mais diversos fins, como o roubo de dados ou a corrupção de sistemas, entre outros, e o mundo convive com a possibilidade de hostilidades entre Estados no ciberespaço, ou seja, uma guerra cibernética (NUNES, 2010).

Segundo Jastram e Quintin (2011), a guerra cibernética é a concepção bélica de desenvolvimento mais revolucionário desde o aparecimento do armamento nuclear, indo muito além de outras novidades tecnológicas, como os veículos aéreos não tripulados (VANT) - comumente chamados de “drones”.

Durante a primeira década do século atual, puderam ser observados vários incidentes cibernéticos que, se não chegaram a se configurar como ataques no contexto de uma guerra cibernética, ao menos tiveram grande repercussão e, pode-se dizer, constituíram os mais graves até então conhecidos, havendo sido dirigidos contra a Estônia, em 2007, e os eventos ocorridos simultaneamente à invasão russa na Geórgia, em 2008. Além desses, houve o ataque realizado pelo “stuxnet”, um marco em termos de sofisticação e efeitos de uma arma cibernética, que destruiu parte das centrífugas iranianas de enriquecimento de urânio localizadas em Natanz, constituindo-se na primeira arma cibernética a causar efeitos no mundo real. Waxman (2011) sugere que o “stuxnet” foi utilizado para causar danos ao programa nuclear iraniano em substituição a uma operação militar convencional.

A gravidade do tema é apresentada pelo Journal of Law and Cyber Warfare:

> Os ataques cibernéticos surgiram, sem dúvida, como um dos mais graves desafios à segurança nacional e internacional no Século XXI e tornaram-se

> o armamento da guerra fria dos dias atuais, ao qual governos e forças armadas precisam reagir rapidamente[2] (CYBER, 2013, tradução nossa).

Lewis (2011) relata que pelo menos cinco países possuem capacidades cibernéticas avançadas, com potencial de realizar ataques destrutivos, e que outros trinta têm intenção de alcançar tais capacidades. Como comparação, ele argumenta que em 1914 apenas poucos países possuíam aeronaves militares e que dez anos após a maioria dos países já possuía tal capacidade. Ao tomarmos em conta esse fato histórico, não há como negar que o número de países com alguma capacidade de ataque cibernético crescerá consideravelmente nos próximos anos.

O caso da Geórgia, citado anteriormente, sugere que este tipo de operação, em que um ataque cibernético precede o desenvolvimento de operações militares convencionais, passará a ser a tendência dos conflitos armados atuais (DAVIS, 2014; GILL, DUCHEINE, 2013). Mas seu uso não se restringirá aos momentos iniciais de um conflito. Assim como outros sistemas de armas, ele será empregado ao longo de toda uma operação militar, podendo, até mesmo, vir a substituir o emprego de armas convencionais.

Com a possibilidade cada vez mais presente da ocorrência de conflitos envolvendo a guerra cibernética, aliada à sofisticação crescente do arsenal cibernético e à interconectividade presente no ciberespaço, surge o risco de que os efeitos provenientes de um ataque cibernético, com potencial cada vez mais adverso, sejam sentidos em todo um país. Destarte, cabe buscar o enquadramento da guerra cibernética no ordenamento jurídico internacional, de modo a limitar seus efeitos, a exemplo do que ocorre em um conflito armado tradicional.

Como o potencial militar da guerra cibernética está na infância de sua aplicação, é de fundamental importância verificar a aplicabilidade do Direito Internacional dos Conflitos Armados (DICA) às operações cibernéticas desenvolvidas no contexto de um conflito armado. Tal importância é expressa nas palavras de Anne Quintin, que declara: “é difícil estimar as consequências agora, mas não podemos nos dar ao luxo de aguardar até que seja tarde demais para prevenir os piores cenários”[3] (JASTRAN e QUINTIN, 2011, tradução nossa).

---

[2] Cyber-attacks have undoubtedly emerged as one of most serious national and international security challenges we face in the 21st century, and have become the modern-day Cold War weaponry to which governments and militaries need to react, rapidly.

[3] The consequences are difficult to assess now, but we cannot afford to wait until it is too late to prevent worst-case scenarios.

Nesse sentido, a guerra cibernética poderá ensejar novas interpretações do DICA, a formulação de novas regras adicionais ou mesmo uma nova legislação que venha a regular a condução cibernética dos conflitos armados. Entretanto, o presente trabalho buscará apenas analisar a aplicabilidade dos principais preceitos insculpidos no DICA à guerra cibernética.

Como ponto de partida, o segundo capítulo abordará os conceitos relacionados à guerra cibernética. Buscará não somente uma definição, mas apresentar suas principais características e alguns preceitos acerca de seu ambiente operacional - o espaço cibernético, peças fundamentais para a formação de uma base conceitual, de modo a prover um entendimento comum sobre este tema, atual e complexo, cuja unanimidade existe apenas no sentido de identificar que não existe um conceito comum.

A partir da fundamentação teórica apresentada, o terceiro capítulo abordará aspectos legais relacionados ao Direito Internacional dos Conflitos Armados, que tem como suas fontes o direito internacional consuetudinário, as Convenções de Haia e de Genebra e seus Protocolos Adicionais. Tratará, também, do *Jus ad Bellum*, usando para tal a Carta das Nações Unidas como fonte. Nesse capitulo, será verificado, inicialmente, o enquadramento da guerra cibernética a esses preceitos, momento em que serão analisados os parâmetros que caracterizam o “uso da força” e o “ataque armado”. Em sequência, será analisada a aplicabilidade dos princípios do *Jus in Bello*, também conhecido como Direito Internacional Humanitário (DIH), à guerra cibernética.

Finalizando, os principais e mais importantes aspectos do presente estudo serão sintetizados em uma breve conclusão, consolidando, assim, a visão do autor sobre o enquadramento da guerra cibernética frente aos conceitos do *Jus ad Bellum* e do *Jus in Bello*, razão de ser do presente trabalho.

2 ENTENDENDO A GUERRA CIBERNÉTICA

2.1 DEFINIÇÃO DE GUERRA CIBERNÉTICA

Atualmente, quase todo e qualquer incidente cibernético é chamado de ataque cibernético, ou mesmo chega-se a falar em guerra cibernética, com a consequente tendência em se vulgarizar tal terminologia. A crescente presença dos Estados no espaço cibernético e as atividades dos atores não estatais, incluindo entidades comerciais, criminosos cibernéticos e grupos terroristas, tornam o ciberespaço um ambiente cada vez mais complexo. As ações desses atores combinam toda a sorte de atividades, como crime, espionagem e ações militares, de modo que, frequentemente, esses elementos são indistinguíveis ao usuário comum do ciberespaço (NUNES, 2010).

Inicialmente, deve-se entender a guerra cibernética como sendo as ações desenvolvidas entre dois ou mais Estados no ciberespaço, no desenrolar de um conflito. Destarte, para diferenciar a guerra cibernética dos demais incidentes que diuturnamente ocorrem no ciberespaço e estabelecer uma linguagem de uso comum, as demais atividades desenvolvidas por atores não estatais, com potencial de dano à informação no ciberespaço, devem ser tratadas como incidentes cibernéticos.

Nunes (2010) propôs uma definição formal às várias ações desenvolvidas na guerra cibernética:

Ações Ofensivas de Guerra Cibernética: ações realizadas por meio de redes de computadores para interromper, negar, degradar/corromper ou destruir a informação contida em computadores, redes e/ou sistemas de tecnologia da informação (TI) inimigos;

Ações Defensivas de Guerra Cibernética: ações realizadas por meio de redes de computadores para proteger, monitorar, analisar, detectar e responder à atividade não autorizada em computadores e/ou redes, de modo a garantir o uso continuado e a inviolabilidade dos nossos sistemas de TI;

Ações de Exploração de Guerra Cibernética: ações realizadas por meio de redes de computadores para a obtenção de informações sobre as vulnerabilidades dos sistemas de TI do inimigo, ou para a coleta de dados contidos nesses sistemas.

Ao sintetizar os conceitos acima elencados, Nunes chegou à definição para Guerra Cibernética:

> São as ações ofensivas, defensivas e de exploração realizadas por meio de sistemas de informação e de redes de computadores, destinadas a interromper, negar, corromper, destruir ou acessar as informações contidas nos sistemas de TI inimigos e, ao mesmo tempo, garantir o uso continuado e a inviolabilidade dos nossos sistemas de TI (NUNES, 2010).

Na realidade, as Ações Ofensivas de Guerra Cibernética definidas acima tratam-se do que passaremos a chamar de Ataques Cibernéticos.

Corroborando as definições anteriores, temos que o Ministério da Defesa brasileiro define atualmente guerra cibernética como:

> Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² [Comando e Controle] do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar (BRASIL, 2014).

No entender daquele Ministério, a guerra cibernética compreende as ações cibernéticas, que envolvem as ferramentas de tecnologia da informação e comunicações (TIC) para desestabilizar ou tirar proveito dos sistemas de tecnologia da informação e comunicações e comando e controle (STIC2) do oponente e defender os próprios STIC2. As ações cibernéticas englobam o ataque cibernético; a proteção cibernética; e a exploração cibernética (BRASIL, 2014).

O ataque cibernético, por sua vez, compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente (BRASIL, 2014).

Ao analisar as definições apresentadas acima, pode-se dizer que são similares. Entretanto, a definição aportada por Nunes é, a princípio, completa, pois inclui o escopo defensivo em seu propósito, além do exploratório e ofensivo, o que não é observado na definição do Ministério da Defesa brasileiro, apesar de esta última conter referência às operações militares. Ocorre que ambas as definições encontram-se desatualizadas.

O lançamento do stuxnet, descoberto em 2010, quebrou um paradigma associado às características da guerra cibernética. A partir de então, o mundo foi testemunha de que era possível causar danos no mundo físico-real a partir de uma arma cibernética. Conforme declaração do ex-chefe da Central Intelligence Agency, Michael V. Hayden (apud NGUYEN, 2013), enquanto os ataques anteriores

possuíam efeitos limitados a outros computadores, stuxnet foi o primeiro ataque cibernético de maior envergadura utilizado para produzir destruição física.

No domínio cibernético, um ataque está limitado a alterar a estrutura de um determinado programa ou fornecer dados errados a um programa. Assim, o objetivo de primeiro nível de um ataque será alterar um programa ou manipular dados. Porém o objetivo principal poderá ser causar um efeito físico no mundo real. Nesse diapasão, Nguyen (2013) considera os meios cibernéticos, os computadores inimigos por exemplo, como instrumentos de ataque em vez dos objetivos propriamente ditos. Logo, o alvo de um ataque cibernético a uma rede de computadores será, frequentemente, o equipamento físico que possui uma estreita ligação, via domínio cibernético, àquela rede.

Assim, o termo ataque cibernético pode subentender o uso da Tecnologia da Informação e Comunicações (TIC) como arma cibernética, com o adjetivo “cibernético” caracterizando o modo de ataque, do mesmo modo que no termo ataque aéreo o adjetivo “aéreo“ denota o uso de aeronaves para a execução de uma operação militar. Nesse sentido, o ataque cibernético é um instrumento ou método de ataque, um armamento ou capacidade que é utilizada para levar a efeito um determinado propósito (NGUYEN, 2013).

Tal assertiva reforça a caracterização da guerra cibernética como um sistema de armas, em apoio a uma campanha militar. Ou seja, ela por si só não possui efeito decisivo, porém contribui, junto a outros sistemas de armas, para a consecução do objetivo final de uma campanha militar.

Voltando ao ponto fulcral da questão analisada, tem-se que as definições de guerra cibernética apresentadas acima apresentam uma lacuna no que diz respeito à capacidade de um ataque cibernético poder fazer-se efetivo no mundo real. Em ambas as definições tal possibilidade é negligenciada.

Assim, de modo a corrigir tal deficiência, este autor apresenta a seguinte definição para as ações ofensivas cibernéticas ou ataque cibernético: são as ações realizadas por meio de redes de computadores para interromper, negar, degradar, corromper ou destruir a informação ou sistemas computacionais contidos em computadores, redes e/ou sistemas de tecnologia da informação (TI) inimigos, bem como destruir ou causar danos a equipamentos físicos controlados por sistemas de TI inimigos.

Por conseguinte, tem-se a definição atualizada para guerra cibernética, que são as ações ofensivas, defensivas e de exploração realizadas por meio de sistemas de informação e de redes de computadores, destinadas a interromper, negar, corromper, destruir ou acessar as informações contidas nos sistemas de TI inimigos, bem como destruir ou causar danos a equipamentos físicos controlados por sistemas de TI inimigos e, ao mesmo tempo, garantir o uso continuado e a inviolabilidade dos nossos sistemas de TI.

2.2 O AMBIENTE OPERACIONAL DA GUERRA CIBERNÉTICA

O espaço cibernético, ou ciberespaço, como também é conhecido, é o palco onde se desenvolvem todas as ações cibernéticas, sendo seu ambiente operacional por excelência. Atualmente, o espaço cibernético é considerado como um dos cinco domínios operacionais, juntamente com o marítimo, o terrestre, o aéreo e o espacial, estando, na realidade, presente em todos os demais (NUNES, 2010; BRASIL, 2014).

2.2.1 Definição de espaço cibernético

Mas o que vem a ser o espaço cibernético? Como tudo relacionado ao adjetivo “cibernético”, não há unanimidade sobre a definição de espaço cibernético, ou ciberespaço, existindo mais de vinte e oito diferentes significados para o termo (KRAMER, 2009).

Na visão norte-americana o “ciberespaço é um sistema de sistemas no qual sistemas menores e variados compõem a estrutura como um todo”[4] (ESTADOS UNIDOS DA AMÉRICA, 2014).

Há, portanto, necessidade de apresentar uma definição que deverá servir como orientadora para o restante do trabalho.

Inicialmente, tem-se ciberespaço definido como sendo o “espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas” (BRASIL, 2014).

Apesar de simples e, em certa medida, esclarecedora, a definição apresentada acima não deixa clara uma das principais características do espaço

[4] Cyberspace is a system of systems in that many small and diverse systems comprise the structure as a whole.

cibernético e que, portanto, deve, de algum modo, estar presente em sua definição. Trata-se da interatividade.

A mesma definição aporta um critério questionável, ao incluir a possibilidade de dispositivos computacionais não conectados em rede fazerem parte do espaço cibernético, pois tal fato vai de encontro à noção de interatividade. Corroborando a argumentação deste autor, Libicki (2009) afirma que a transferência bidirecional de informações é o melhor marco referencial para a definição de ciberespaço.

Nesse sentido, tem-se, ainda, que o "espaço cibernético é um ambiente criado e mantido com o propósito de facilitar o uso e a exploração da informação, a interação humana e a intercomunicação"[5] (ESTADOS UNIDOS DA AMÉRICA, 2014).

Dessa forma, apresenta-se uma segunda definição, em que tal deficiência é contornada, onde ciberespaço é a parcela integrante do ambiente da informação caracterizada pelo uso interativo dos espectros eletrônico e eletromagnético para criar, armazenar, modificar, trocar e explorar a informação, por meio de tecnologias da informação e comunicações em redes interdependentes e interconectadas (NUNES, 2010).

2.2.2 Características do espaço cibernético

Conforme observado por diversos trabalhos e autores – Estados Unidos da América (2014); Kramer (2009); Rattray (2009); Kuehl (2009); Parks e Duggan (2001); Boleng, Schweitzer e Gibson (2008) – o espaço cibernético é um ambiente artificial construído pelo homem, sujeito a constantes modificações, sendo, portanto, imperfeito.

O ciberespaço é, por conseguinte:

> […] um ambiente onde novas capacidades e habilidades são desenvolvidas, as quais são por ele incorporadas e assim por diante, como em um moto contínuo, em que sua retroalimentação o regenera tornando-o algo novo em sua composição. Logo, o ciberespaço não se trata de um domínio coerente e encontra-se em constante evolução, por meio da contribuição independente e descentralizada de diversos atores, cada qual com sua própria capacidade e motivação (NUNES, 2010).

Segundo Parks e Duggan (2001), a artificialidade do espaço cibernético confere uma dose de instabilidade, na qual software e hardware falham ou geram

[5] Cyberspace is an environment created and maintained for the purpose of facilitating the use and exploitation of information, human interaction, and intercommunication.

resultados inesperados. Como consequência, na guerra cibernética, os resultados dos ataques nem sempre serão os mesmos e haverá a possibilidade de alteração de desempenho dos meios cibernéticos, além de que a "geografia" do próprio ambiente estará em mutação, como alerta Rattray (2009).

Em face de seu caráter artificial, Parks e Duggan (2001) argumentam que o ciberespaço é construído e controlado pelo homem e suas ferramentas, não havendo parte do ciberespaço que não esteja sob o controle de alguém. Tal assertiva é corroborada por Lewis (2009), que considera que o ciberespaço não é algo livre como o alto-mar, pois existe um controle soberano sobre cada uma das redes que poderão ser utilizadas por uma arma cibernética para atingir seu alvo – mesmo que esse controle ocorra por apenas alguns milissegundos. Segundo Lewis, "não existe momento em que um conjunto de bits que se move de um computador a outro não esteja situado em uma rede que pertença a alguém e que esteja fisicamente localizada em um Estado soberano"[6] (LEWIS, 2009, tradução nossa).

Entretanto, há limites a esse controle, não se aplicando, portanto, aos conceitos militares de supremacia e de superioridade, pois, conforme expressado por Rattray (2009), não se pode controlar o ciberespaço no mesmo nível em que se controlam os ambientes terrestre, marítimo, aéreo e, até mesmo, espacial. Tal assertiva é confirmada por Kramer (2009), o qual sugere que se tal capacidade fosse possível os Estados Unidos já teriam se livrado dos ataques cibernéticos a que estão sujeitos diuturnamente.

Existem duas características próprias do espaço cibernético que, unidas, o diferenciam de todos os demais domínios operacionais.

> A primeira diz respeito à inexistência de fronteiras no ciberespaço, o que vale dizer que não existem distâncias, ou seja, uma ação executada no Brasil pode ter consequências em qualquer parte do globo. Sendo assim, não há necessidade de contiguidade física entre oponentes para execução de ações de guerra cibernética. A segunda refere-se ao fato de que sempre haverá um usuário conectado ao ciberespaço (NUNES, 2010).

Em consonância com tais características, tem-se que enquanto as repercussões do que acontece nos campos de batalha tradicionais podem gerar efeitos sociais e políticos em todo o mundo, os impactos físicos estarão limitados àquele espaço. A inclusão do espaço cibernético como um novo domínio torna toda a estrutura operacional ainda mais complexa e complicada, elevando um campo de

[6] There is no moment when a collection of bits moving from one computer to another is not actually on a network that someone owns and that is physically located in a sovereign state.

batalha limitado fisicamente a um nível global, ou seja, sem barreiras físicas (ESTADOS UNIDOS DA AMÉRICA, 2014).

Um dos pontos mais marcantes do espaço cibernético diz respeito à possibilidade de ocultação, ou seja, de anonimato. Identidades são facilmente ocultadas e, até mesmo, trocadas, o que possibilita fazer com que a autoria de um ataque pareça ser proveniente de outro ator, que poderá estar fisicamente localizado em qualquer lugar, literalmente. Esta característica é de extrema importância às ações de exploração levadas a cabo antes do início do conflito, entretanto configura-se, também, como a fonte de um dos maiores problemas enfrentados na atualidade para a definição de uma resposta a um ataque cibernético: a atribuição de sua autoria.

Poder-se-ia argumentar que no transcurso de um conflito armado este problema estaria minimizado, pois um ataque seria inicialmente atribuído ao inimigo. Ocorre, porém, que outros atores poderão intervir no conflito com ações cibernéticas independentes, com ou sem a aquiescência de quaisquer das partes envolvidas. Da mesma forma, podem ocorrer ataques cibernéticos envolvendo Estados neutros ou aliados de uma das partes, como aqueles dirigidos contra as comunicações entre esses atores e um dos contendores. Tais fatos tornam o problema da atribuição relevante, cabendo, ainda, ressaltar que ele poderá estar presente em período de crises.

2.3 CARACTERÍSTICAS DA GUERRA CIBERNÉTICA

De modo a melhor compreender o fenômeno “guerra cibernética”, faz-se necessário recorrer às suas principais características, a partir das quais poder-se-á conhecer, principalmente, o comportamento de um ataque cibernético.

Assim, serão apresentadas somente aquelas características consideradas relevantes e que, somadas aos conceitos já apresentados sobre a própria guerra cibernética e seu ambiente operacional, o espaço cibernético, permitirão a análise e o entendimento posteriormente, quando serão verificadas a adequabilidade e a aplicabilidade dos preceitos legais relacionados aos conflitos armados.

2.3.1 Temporalidade dos efeitos do ataque cibernético

Os efeitos diretos, ou de primeiro nível, são aqueles que se fazem sentir diretamente sobre os sistemas de TI atacados. Os efeitos indiretos, ou de segundo nível, são aqueles causados a partir da interrupção ou alteração do sistema de TI, ou seja, a partir dos efeitos de primeiro nível. Segundo Nguyen (2013), os verdadeiros efeitos buscados ao efetuar-se um ataque cibernético são os indiretos.

Os efeitos diretos são temporários, podendo ser revertidos, a partir do momento em que os ataques sejam descobertos, em um período de tempo que, dependendo da capacidade tecnológica de defesa cibernética, o tipo de vulnerabilidade explorada e a sofisticação da arma empregada, poderá variar de minutos a semanas. Entretanto, como afirma Nguyen (2013), os efeitos indiretos de um ataque são geralmente irreversíveis.

Tomando-se o stuxnet como exemplo, tem-se que os efeitos de primeiro nível foram as alterações realizadas no sistema de controle, de modo a permitir que as centrífugas ultrapassassem o limite de rotações considerado seguro, ao mesmo tempo em que apresentasse ao supervisor desse sistema parâmetros normais de operação. O efeito de segundo nível, e real propósito do ataque, foi a destruição das centrífugas.

Pode-se pensar no emprego militar, a partir da experiência do stuxnet ao imaginar-se como alvo do ataque um sistema de radares, só que, em vez de centrífugas, o efeito de segundo nível seria provocado nas antenas desse sistema.

2.3.2 Imprevisibilidade dos efeitos do ataque cibernético

Inicialmente, deve-se destacar que um ataque cibernético pode produzir uma série de efeitos em cadeia, com consequências imprevisíveis e distintas em cada um de seus níveis. Tal imprevisibilidade é fruto da mutabilidade do ciberespaço e, também, de erros humanos.

Ou seja, “as ações no espaço cibernético podem não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados” (BRASIL, 2014).

Kostadinov (2014) argumenta que a precisão é prerrogativa de ataques cibernéticos de alta sofisticação. Além disso, por outro lado, devido a motivos escusos ou a erros tecnológicos ou humanos, um ataque pode facilmente sair de

controle e “transformar-se em uma avalanche indiscriminada, varrendo tudo em seu caminho”.

Como exemplo, Kostadinov (2014) cita que um ataque cibernético contra uma rede elétrica que alimenta o sistema de comando e controle inimigo poderá gerar um blackout prolongado e atingir uma série de sistemas da infraestrutura civil, cujos efeitos em cadeia poderão ser: ocorrência de doenças relacionadas à deficiência nos sistemas de tratamento de esgoto e de purificação da água; aumento do número de acidentes de trânsito devido à falha do sistema de semáforos; e a morte imediata de civis inocentes devido à falha de sistemas de suporte à vida em centros de emergência médica.

Um exemplo real de imprevisibilidade é encontrado no caso do “stuxnet”. A despeito de possuir um desenho altamente complexo e discricionário e ser executado com grande precaução, após ser exaustivamente testado em réplicas das centrífugas iranianas, o stuxnet não estava livre do risco de erros em seu código. Considerada a arma cibernética mais sofisticada e precisa já detectada e analisada, sendo também a primeira a causar destruição física, um erro de programação permitiu que ele se espalhasse livremente pela internet, infectando mais de 90 mil sistemas em vários países, incluindo vários equipamentos da empresa americana Chevron. (NGUYEN, 2013; CLAYTON, 2010; DICKEY, SCHNEIDERMAN, DEHGHANPISHEH, 2010; SANGER, 2012; KUSHNER, 2013; JASTRAM, QUINTIN, 2011).

Há que se ter em mente que a interconectividade inerente ao ciberespaço torna difícil a predição do dano colateral. Não há fronteiras limitando o tráfego de dados. Uma simples linha de código de uma ferramenta utilizada em uma ação cibernética, seja ela de exploração, ofensiva ou mesmo defensiva, poderá causar danos não intencionais a sistemas situados a grandes distâncias do alvo verdadeiro (NUNES, 2010).

2.3.3 Presença de não combatentes no espaço cibernético

O espaço cibernético, domínio onde a guerra cibernética se desenvolve, possui uma característica que o torna peculiar em relação ao campo de batalha das operações militares convencionais. No ciberespaço, onde inexistem barreiras físicas e sempre haverá alguém conectado, não estarão presentes apenas combatentes,

mas, também, civis não combatentes de todas as nacionalidades, extrapolando as nações em conflito e envolvendo nações aliadas e neutras (NUNES, 2010).

Destarte, combatentes estarão conectados a não combatentes e um ataque a um alvo legítimo poderá, inevitavelmente, causar danos a um Estado neutro. Em termos práticos, tal fato implica a aplicabilidade e o sucesso de um ataque cibernético, que necessitará de um profundo esforço de inteligência, de modo a proporcionar conhecimento acerca das redes-alvo e de suas conexões a outras redes e, assim, aumentar a probabilidade de que apenas os alvos planejados sejam afetados (LEWIS, 2009).

Até este ponto buscou-se formar uma base conceitual acerca da guerra cibernética, abrangendo seus principais aspectos e introduzindo o leitor ao tema, de modo a possibilitar a fundamentação teórica necessária à análise legal quanto à aplicabilidade do *jus ad bellum* e do *jus in bello*, que, a partir de agora, será a tônica do presente trabalho.

3 ANÁLISE LEGAL

Jastram e Quintin (2011), ao analisarem os temas cibernéticos em geral, argumentam que a dificuldade de caracterização da maioria das atividades hostis que ocorrem no ciberespaço como ações de guerra colocam em dúvida a aplicabilidade do Direito Internacional dos Conflitos Armados (DICA), inquietação recorrente entre os estudiosos do assunto, até agora não superada.

Conforme observado durante a construção de um conceito para guerra cibernética no início do capítulo anterior, a assertiva acima trata fenômenos distintos sob uma mesma ótica e mistura ações desenvolvidas no escopo de uma guerra cibernética com os demais incidentes que diuturnamente se manifestam no espaço cibernético. Atividades criminais e de espionagem não constituem atos de guerra. Deve-se manter o foco da análise aos cenários presentes em um conflito armado, sobretudo ao se analisar os princípios do *jus in bello*, pois o DIH se aplica apenas nesses casos (INTERNATIONAL COMMITTEE OF THE RED CROSS, 2013; JARDIM, 2006).

Na visão de Schmitt (2012), os princípios do DIH são aplicáveis sempre que um ataque cibernético puder ser atribuído a um Estado, algo que vá além de um simples e esporádico incidente e possua o propósito de causar morte, ferimento, danos ou destruição, mesmo que forças armadas não estejam sendo empregadas em seu sentido clássico.

Tal assertiva se mostra coerente, uma vez que toda aplicação de força por um Estado, em seu uso legal, deverá observar os princípios do DIH. Note-se, também, que, como visto no capítulo anterior, um ataque cibernético poderá ser realizado como medida preparatória a um ataque por forças convencionais.

Portanto, faz-se mister ter em mente que atividades cibernéticas hostis levadas a cabo, direta ou indiretamente, por atores estatais também ocorrem em tempo de paz. Estas devem respeitar o DIH e possuem especial relevância no trato do *jus ad bellum*, pois podem constituir transgressões à proibição do uso da força ou, até mesmo, ensejar o direito de legítima defesa.

3.1 A GUERRA CIBERNÉTICA E O *JUS AD BELLUM*

A aplicação do DICA à guerra cibernética só poderá ocorrer após o prévio enquadramento legal do uso da força por um Estado, que deve ser realizado no contexto do *jus ad bellum*, ou seja, as normas e procedimentos que estabelecem quando um Estado poderá, ou não, fazer o uso legítimo da força como instrumento da resolução de controvérsias com outro ator estatal (GRAHAM, 2010; NGUYEN, 2013).

No contexto do *jus ad bellum*, dois conceitos avultam de importância na análise a ser realizada com relação à guerra cibernética. São eles: “uso da força” e “ataque armado”. O primeiro é relevante para a correta interpretação do Inciso 4 do Artigo 2º da Carta das Nações Unidas (Carta da ONU):

> 4. Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas (NAÇÕES UNIDAS, 1945).

Tal provisão proíbe tanto a ameaça quanto o uso da força por um Estado. Entretanto existem duas exceções a esta regra, consubstanciadas na própria Carta da ONU. A primeira encontra-se insculpida no Artigo 39, que prevê a possibilidade do uso da força por meio de autorização do Conselho de Segurança. A segunda depende diretamente do entendimento do que vem a ser ataque armado, pois possibilita o uso da força em caso de legítima defesa, conforme estabelecido no Artigo 51:

> 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 pêlos [sic] 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 tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais (NAÇÕES UNIDAS, 1945).

O recurso ao ataque cibernético por parte dos Estados, no curso de um conflito interestatal, excede as noções jurídicas tradicionais sobre o uso da força. A Carta da ONU foi redigida e adotada em uma época em que os Estados infligiam

dano físico a seus adversários por meio de ataques cinéticos[7]. Segundo Nguyen (2013), embora a Carta não defina claramente o que vem a ser “uso da força” ou “ataque armado”, o costume internacional e a jurisprudência da Corte Internacional de Justiça (CIJ) trouxeram clareza sobre sua aplicação com respeito aos modos utilizados em uma guerra tradicional, como bombardeio aéreo, assalto terrestre, uso de mísseis etc. Porém, ao trasladar-se ao campo dos ataques cibernéticos, nota-se a falta de uma orientação normativa positiva e de prática internacional sobre o assunto, fatos que obscurecem os limites interpretativos.

Tem-se, portanto, os conceitos de “uso da força” e “ataque armado” como questões fundamentais para a análise do *jus ad bellum*, que, como salienta Nguyen (2013), não são sinônimos e carecem de uma boa definição.

3.1.1 Uso da força

Como visto anteriormente, o termo “uso da força” está diretamente vinculado ao Inciso 4 do Artigo 2º da Carta da ONU, que proíbe não só sua aplicação, mas sua ameaça. Fica claro, então, que se trata de instrumento que visa a limitar o recurso à violência em tempo de paz. Sua relevância no presente estudo se prende ao fato de que se faz necessário conhecer o limite, além do qual uma ação levada a cabo no espaço cibernético seria considerada ilegal, de modo a ter-se a exata noção sobre o enquadramento jurídico das atividades desenvolvidas no ciberespaço, seja para sua execução, bem como para a análise de ações cibernéticas sofridas por um Estado.

Segundo Waxman (2011), alguns Estados, além de vários especialistas em direito internacional, argumentam que a proibição contida no Artigo 2º da Carta da ONU se aplica a uma categoria de coerção mais ampla do que apenas à força militar.

Shakelford (2009), por sua vez, argumenta que o termo “força” poderia ser interpretado de acordo com o escopo da Carta da ONU e que, embora seja um tema que gere divergências, pode-se afirmar que “força” não se restringe apenas ao uso de armamentos militares, em sua acepção cinética. O que importa nesta análise, diz Shakelford, são os efeitos que se busca alcançar e não os meios utilizados.

[7] A utilização do termo cinético foi escolhida para diferenciar as formas de ataque, pois remete à ideia de movimento físico, logo pertencente ao mundo real, em contraposição ao cibernético. O termo “convencional” deixou de ser usado em vista do armamento nuclear, que não se enquadra como convencional, porém se adequa como cinético.

O próprio Brasil tentou incluir, junto à ONU, a forma de coerção econômica na redação daquele artigo. No entanto, esta interpretação ampliada não ganhou adesão e a iniciativa brasileira não teve sucesso, prevalecendo a interpretação mais restritiva, limitada ao uso de meios militares (MELZER, 2011; NGUYEN, 2013).

Tal posição é reforçada por Gervais (2012), que, além de mencionar a exclusão explícita da coerção econômica, aduz que os instrumentos diplomáticos e ideológicos foram implicitamente excluídos da redação, concluindo que, desse modo, os redatores da Carta da ONU sinalizaram que a interpretação do uso da força, para aplicação do Artigo 2º, tem como foco apenas os armamentos militares.

Por sua vez, Melzer (2011) cita que a Corte Internacional de Justiça (CIJ), ao tratar da ameaça ou uso de armamento nuclear, estabeleceu que a proibição contida no Artigo 2º da Carta da ONU se aplica a qualquer uso da força, independente do armamento empregado. Mas, mesmo nesse caso, pode-se perceber que a interpretação permanece focada no uso de armamentos militares. O que a CIJ faz é apenas declarar que o uso de qualquer armamento, seja ele convencional ou nuclear, configura o uso da força.

Tendo em vista as argumentações apresentadas, pode-se dizer que as ações de guerra cibernética cujos efeitos são equivalentes ao uso de armamentos cinéticos podem facilmente ser enquadradas no Artigo 2º da Carta da ONU, no que diz respeito à proibição da ameaça ou uso da força. Entretanto, quando se trata de ações de guerra cibernética cujos efeitos não se façam sentir no mundo físico, o mesmo não acontece.

Tal assertiva é corroborada por Melzer (2011), para quem as ações de guerra cibernética, geralmente enquadradas em uma zona cinzenta entre a força militar tradicional e outras formas de coerção, simplesmente não foram antecipadas pelos redatores da Carta da ONU e, desde então, nem a prática estatal ou a jurisprudência internacional foram capazes de prover um critério claro a respeito do limite a partir do qual as ações que não causem morte, ferimento ou destruição devem ser consideradas proibidas à luz do disposto no Inciso 4, do Artigo 2º da Carta da ONU.

De modo a buscar preencher esse vazio conceitual, vários modelos foram criados para definição do limiar de uso da força, sendo que os tradicionalmente utilizados se baseiam nas seguintes abordagens: instrumento utilizado para o ataque; alvo atacado; e efeito sobre o alvo. Ocorre que tais modelos possuem

fragilidades teóricas e práticas, conforme demonstrado por Nguyen (2013) e Waxman (2011).

Outro modelo muito aceito foi proposto por Michael Schmitt (apud WINGFIELD, 2009), que consiste na quantificação de sete fatores, de modo a qualificar qualquer tipo de operação em um espectro que vai desde o permitido ao proibido:

- Gravidade, ou seja, o número de mortes e o nível de danos ocasionados;
- Imediatismo, que busca analisar a rapidez com que os efeitos do ataque foram sentidos e o período em que perduraram;
- Diretividade, que se refere à relação de causa e efeito;
- Penetração, que verifica se a ação envolveu a entrada física no território do país-alvo;
- Mensurabilidade, que analisa se os efeitos podem ser quantificados e se podem ser separados dos efeitos de outras ações realizadas em paralelo;
- Legitimidade Presumível, que verifica se a ação empreendida possui aceitação no seio da comunidade internacional, por meio do direito consuetudinário; e
- Responsabilidade, que trata se o ato é direta ou indiretamente atribuível a determinado ator/Estado e se há declaração de autoria.

Ocorre que Nguyen (2013) não só critica a proposta de Schmitt, mas a desconstrói, demonstrando que seu resultado é facilmente manipulável, ao apresentar duas análises antagônicas para os ataques de negação de serviço[8] sofridos pela Estônia, em 2007, provando que os sete critérios podem ser manipulados para atender aos interesses geopolíticos daquele que realiza a análise.

Nguyen (2013) apresenta, então, uma proposta de modelo em que o uso da força fica configurado quando há a intenção de causar danos a sistemas físicos monitorados ou controlados por computadores. A grande questão envolvendo tal modelo reside na dificuldade em se caracterizar fielmente qual a intenção de um ataque cibernético. Seria necessário um esforço incalculável de inteligência e de engenharia reversa, levando-se em conta a tecnologia atualmente disponível. Ademais, conforme apresentado no capítulo anterior, a guerra cibernética e o ciberespaço possuem características que em muito dificultam tal análise, como a

[8] Ver glossário.

imprevisibilidade dos efeitos do ataque cibernético. Como assegurar, então, o levantamento confiável acerca da intenção de um ataque? Essa é uma questão que ainda não pode ser respondida.

Tem-se, portanto, que nenhum dos modelos apresentados está isento de falhas, sejam elas por questões teórico-práticas, sejam por incapacidade tecnológica. Torna-se clara, assim, a profunda dificuldade de se formular um modelo ou padrão que venha a satisfazer todos os requisitos para o correto enquadramento legal, devido, principalmente, à subjetividade intrínseca ao tema em lide, pois se tratam de eventos que ocorrem em um ambiente virtual ou, no máximo, a nível cognitivo. O fato de não haver correspondência no mundo real o torna, praticamente, imensurável e inqualificável. Consequentemente, surge a dificuldade de aceitação global de tais modelos, em vista da existência de diferentes visões e interesses no concerto internacional de nações.

Destarte, este autor propõe uma abordagem tradicional, coerente com o costume internacional e a visão dominante entre os Estados membros da ONU de que a proibição do uso da força se aplica a atos de violência armada, uma vez que a própria Carta da ONU, em seu preâmbulo, estabelece que “a força armada não será usada, a não ser no interesse comum” (NAÇÕES UNIDAS, 1945).

Portanto, com a finalidade de enquadramento na proibição insculpida no Inciso 4, do Artigo 2º da Carta da ONU, no que diz respeito ao uso da força, deve ser utilizado o critério de equivalência de efeitos, ou seja, ações de guerra cibernética cujos efeitos são equivalentes ao uso de armamentos cinéticos e que causem danos a objetos materiais ou estruturas físicas, bem como morte ou sofrimento a pessoas.

Nesse diapasão, faz-se mister ressaltar que, além do dano físico ou destruição, a perda de funcionalidade de um objeto também configura “dano”. Segundo o Comitê Internacional da Cruz Vermelha (CICV), se um objeto foi inutilizado, não há relevância em como isso ocorreu, se por meios cinéticos ou por meio de uma ação de guerra cibernética (INTERNATIONAL COMMITTEE OF THE RED CROSS, 2013). Na prática, tal interpretação é de grande importância à correta aplicação dos princípios contidos no DIH, pois, caso não fosse adotada, um ataque cibernético dirigido contra uma rede de computadores de uso civil que a tornasse inoperante não seria alcançado pela proibição de ataque a pessoas e objetos civis.

A inclusão do conceito de inutilização de um objeto ou, em outros termos, sua neutralização, se faz mister, também, por possibilitar o enquadramento de uso ilegal da força para aqueles ataques cibernéticos dirigidos contra a infraestrutura crítica de um Estado, devido ao sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade que poderiam advir como consequência de tais ataques.

3.1.2 Ataque armado

Conforme já citado anteriormente, o uso do direito de legítima defesa por um Estado, de acordo com o prescrito no Artigo 51 da Carta da ONU, depende diretamente da exata compreensão do que se entende por “ataque armado”.

Mais ainda, torna-se fundamental trasladar-se esse conceito à guerra cibernética, pois, segundo Padmanabhan, “é razoável assumir que Estados possam usar a força contra aqueles envolvidos em tais ataques [cibernéticos] no futuro e, de fato, os Estados Unidos expressamente reservaram o direito de assim fazê-lo”[9] (PADMANABHAN, 2013, tradução nossa).

Entretanto, a Carta da ONU é omissa com relação à definição daquele termo. Ao pesquisar-se outras fontes, tem-se que o Protocolo Adicional às Convenções de Genebra de 1949, relativo à Proteção das Vítimas dos Conflitos Armados de Caráter Internacional (Protocolo I), apresenta, no Inciso 1 do Artigo 49, a seguinte definição: “entende-se por “ataques” o ato de violência contra o adversário, sejam ofensivos ou defensivos” (JARDIM, 2006). Nesse sentido, Jastram e Quintin (2011) argumentam que o termo “atos de violência” tem sido interpretado no sentido de aplicação da força física.

Gill e Ducheine (2013), baseando-se na jurisprudência internacional e no direito consuetudinário, corroboram a noção de “ato violento” contida no Protocolo I e concluem que um “ataque armado” consiste no uso de força originada de fora do território do Estado atacado, que ultrapasse o nível de um incidente armado isolado e de pequena escala, dirigido contra o território ou meios militares em águas internacionais, espaço aéreo internacional ou legalmente presentes no território de outro Estado, ou, ainda, em certas ocasiões, dirigido contra seus nacionais localizados no exterior.

---

[9] It is reasonable to assume that States may wish to use force in the future against those involved in such attacks, and indeed the United States has expressly reserved the right to do so.

Outro conceito é apresentado por Gervais (2012), para quem a prática consuetudinária sugere que, de acordo com noções convencionais de “força”, até mesmo ataques de pequena escala, sejam eles aéreos, navais ou de artilharia, qualificam-se como um “ataque armado”, ressalvando a necessidade de que sejam capazes de resultar em destruição de propriedades ou perda de vidas humanas. Observa-se com esta ressalva a inclusão de uma maior discricionariedade que faz com que, dentro desta conotação, um ataque com mísseis que atingisse uma região despovoada, embora denote uso ilegal da força, em contradição com o Artigo 2º da Carta da ONU, não seja suficiente para acionar o direito de legítima defesa contido no Artigo 51.

Tem-se, portanto, a partir da consolidação das visões abordadas, que o conceito de ataque armado envolve o uso da força como um ato violento, contra alvos específicos e com um nível tal que resulte em danos físicos ou destruição a objetos e/ou cause morte ou ferimento a pessoas.

A partir desse conceito, pode-se chegar, então, a uma qualificação objetiva quanto ao enquadramento do ataque cibernético como um ataque armado, que ocorrerá sempre que as ações cibernéticas causarem danos físicos a pessoas ou objetos. Esta argumentação é de ampla aceitação e é corroborada por estudiosos do tema, como Jastram e Quintin (2011), Shackelford (2009), Lewis (2011), Gill e Ducheine (2013), Gervais (2012), Banks (2013) e Schmitt (2012).

Há, ainda, outra abordagem, chamada de “escala e efeitos”, baseada em decisão da CIJ no julgamento do Caso Nicarágua[10], na qual aquela Corte declarou que, com base nesses parâmetros, nem todo uso da força atinge o limiar que caracteriza um ataque armado. Tal padrão foi adotado em documento produzido pelo Centro de Excelência de Defesa Cibernética da OTAN, o Manual de Tallinn do Direito Internacional aplicado à guerra cibernética, que teve como seu editor Schmitt (2013), o qual interpreta o termo “escala e efeitos” como fatores quantitativos e qualitativos a serem analisados para determinar se uma ação de guerra cibernética se qualifica como uso da força ou ataque armado.

No caso em questão, este autor considera que a abordagem do Manual de Tallinn corrobora a visão apresentada, sendo o nível de violência equivalente aos

[10] Julgamento na CIJ das Atividades Militares e Paramilitares desenvolvidas contra a Nicarágua (Nicarágua x Estados Unidos da América).

fatores quantitativos ou à escala; e o dano material ou a pessoas como o fator qualitativo, ou seja, o efeito propriamente dito.

Outrossim, há uma corrente que defende a noção de que, mesmo na ausência de ferimento ou dano físico, um ataque cibernético poderia constituir um ataque armado quando dirigido contra a infraestrutura crítica de um Estado. Porém não existe consenso a esse respeito.

Gill e Ducheine (2013) defendem tal ponto de vista, argumentando que, devido ao potencial do ataque cibernético de incapacitar severamente a habilidade de um Estado em efetuar e garantir algumas funções essenciais ou debilitar gravemente sua estabilidade econômica, social e política por um período prolongado, um ataque contra a infraestrutura crítica de um Estado deve ser considerada como um ataque armado. Outro a defender esta excepcionalidade é o Manual de Tallinn que, diferentemente de Gill e Ducheine, não considera os fatores econômicos, ou seja, ataques ao sistema financeiro, uma vez que, conforme visto no item anterior, as formas de coerção econômica não foram consideradas como “uso da força”.

Por sua vez, Nguyen (2013) rejeita essa visão por considerá-la perigosa e demasiadamente extensiva, argumentando que, assumindo haver uma atribuição adequada de sua autoria, qualquer ação cibernética contra os sistemas de controle de uma infraestrutura crítica, incluindo a espionagem, permitiria a um Estado responder com o uso defensivo da força, independentemente dos efeitos reais do ataque. Nguyen (2013) pondera, ainda, que, embora essa abordagem reflita a importância das infraestruturas críticas à segurança nacional e as sérias implicações de um ataque cibernético sobre as mesmas, ela assume que qualquer penetração em seu sistema de controle denotaria uma intenção hostil e, citando a doutrina estadunidense de legítima defesa preventiva - a Doutrina “Caroline” -, ensejaria a necessidade de legítima defesa imediata.

Vê-se, portanto, que há riscos de se escalar o nível de violência ao se adotar tal abordagem, tendo em vista, principalmente, a facilidade em se confundir ações de espionagem com a fase inicial de um ataque cibernético, que consiste na penetração dos sistemas. Na realidade, tais ações são indistinguíveis, pois o que as diferencia reside em uma esfera além do espaço cibernético, pertence ao campo cognitivo: a intenção. Baseado no risco inerente às infraestruturas críticas decorrente de uma penetração em seus sistemas de controle, independentemente

da dualidade intencional existente, alguns Estados podem não considerar prudente aguardar o desenrolar das ações para comprovar que se trata realmente de um ataque e optar por uma ação de legítima defesa preventiva. Tal acionar incorre, inicialmente, em dois problemas. O primeiro diz respeito em se adotar uma conduta ainda não consolidada internacionalmente como prática estatal. O segundo, no risco em se fazer uso ilegal da força, ensejando, pois, a condenação internacional e possibilitando o nascedouro ou o agravamento de crises. Destarte, este autor entende que, enquanto não houver, ao menos, consenso internacional a favor da legítima defesa preventiva, não se pode utilizar o critério de caracterizar-se um ataque cibernético a uma infraestrutura crítica como um ataque armado.

Do mesmo modo, há discordâncias relativas à caracterização da "neutralização" como um ataque. Favoravelmente a essa posição, Jastram e Quintin (2011) argumentam que o Artigo 52 do Protocolo I, que trata da limitação dos ataques estritamente aos objetivos militares, possibilita tal interpretação ao referir-se à neutralização de um objetivo.

Há que se ter em mente que, em termos militares, a neutralização não constitui uma ação operacional como o ataque, mas, sim, um dos efeitos que se pode buscar ao se atacar um objetivo. Esse o motivo pelo qual o Artigo 52 do Protocolo I a cita juntamente com os termos "destruição" e "captura", outros efeitos que se pode obter. Existe todo um leque de opções de efeitos sobre um objetivo disponíveis a quem realiza um ataque, variando, de uma forma simplificada, desde a "inquietação", passando pela própria "neutralização", até chegar à "destruição". Essa variação é função, principalmente, do nível de força, logo violência, empregado.

Como já tratado anteriormente, ao consolidarem-se as visões dos autores estudados, concluiu-se que há a necessidade de aplicação da violência acima de um determinado nível para caracterização de um ataque armado, de tal modo que, em termos objetivos, tal limite foi fixado como sendo o limiar de danos físicos. Sendo assim, um ataque cibernético, cujo efeito desejado sobre o alvo seja a neutralização, só poderá ser considerado como um ataque armado caso ocorram "efeitos físicos" que acarretem dano material ou ferimento a pessoas.

3.1.2.1 O problema da Atribuição

Tratou-se, até o momento, de se entender o que, em termos de ações de guerra cibernética, caracteriza um ataque armado. Entretanto, para que se possa

recorrer à excepcionalidade de emprego da força contida no Artigo 51 da Carta da ONU, faz-se necessário conhecer contra quem vamos nos defender. Tal assertiva pode parecer óbvia e desnecessária, à luz do que se está acostumado a vivenciar e fruto das visões históricas acerca dos conflitos armados já ocorridos e, mesmo, da prática estatal ao se aplicar tal dispositivo, uma vez que todas essas experiências se deram no campo “cinético”.

Contudo, em uma visão que pode ser considerada como de consenso internacional e corroborada por especialistas como Waxman (2011), Shackelford (2009), Kostadinov (2014), Melzer (2011), Crowley e Gerstein (2014), Gervais (2012), Banks (2013) e Graham (2010), determinar a autoria de um ataque cibernético é um processo difícil e, invariavelmente, de longa duração.

Ao trasladar-se ao campo virtual do espaço cibernético, a atribuição de autoria de um ataque transforma-se em um problema complexo e de difícil solução, conforme abordado quando se tratou das características daquele espaço. A capacidade de anonimato e de mascaramento, passando-se por outra identidade, são características do ciberespaço em que se originam tal problema. Dado o avanço tecnológico estar usualmente disponível a ambos os lados, a solução desse problema dependerá de massivo investimento e grande esforço estatal para o aprimoramento de seus sistemas de forense computacional[11].

Segundo Banks (2013), um dos aspectos mais desafiantes na busca de regulamentação da guerra cibernética diz respeito à atribuição oportuna. Além da possibilidade de ocultação de seu autor, um ataque cibernético pode ocorrer em vários estágios ao longo do tempo, iniciando-se com a infiltração nos sistemas por um ou vários computadores localizados em diferentes locais, seguido pela transferência de um código malicioso para, enfim, a qualquer tempo, manifestar seus efeitos. A questão que se coloca, então, é: quando ocorreu o ataque?

Na visão deste autor, de modo a diferenciar o estágio de infiltração de um ataque de uma ação de exploração, o ataque se caracteriza quando o código malicioso - a arma cibernética propriamente dita - é transferido para o sistema alvo. Nesse ponto, entretanto, não está caracterizado o ataque armado, que só ocorrerá quando seus efeitos se manifestarem. E, muitas das vezes, o ataque propriamente dito somente é percebido após a manifestação de seus efeitos. Tal fato, aliado ao

[11] Ver glossário.

lapso de tempo que pode haver transcorrido desde que a arma cibernética foi inserida no sistema alvo até sua efetiva ativação, dificulta ainda mais o problema da atribuição de sua autoria.

Além dos aspectos técnicos, Waxman (2011) cita que existem questões jurisdicionais que agravam ainda mais o problema da atribuição, ao limitarem a competência de um Estado de investigar além de suas fronteiras físicas. Uma vez mais fica evidente a limitação imposta, ainda que indiretamente, pelas características do ciberespaço, posto que não existem fronteiras naquele domínio e o fluxo de dados pertinente a um ataque cibernético pode percorrer livremente variadas trajetórias ao longo do território de diversos Estados.

Considerando-se que o problema primário da atribuição foi solucionado e se chegou a um responsável pelo ataque, cabe, então, realizar uma análise de cunho legal, de modo a verificar se existe responsabilidade por parte de um Estado, ou de um ator não estatal. Tal análise tem sua relevância ao permitir elencar e dosar, efetiva e legalmente, as ações de legítima defesa a serem desencadeadas pelo Estado vítima do ataque.

De acordo com o direito internacional, uma ação pode ser atribuída a um Estado, quando esta é executada por pessoas ou entidades agindo como seu representante ou com autorização ou endosso daquele Estado. Tais pessoas ou entidades são chamadas de agentes estatais. Nesse escopo encontram-se os membros das forças armadas e das diversas agências estatais, além de elementos privados contratados pelo Estado. Aqueles que não se encontram em tais situações, ou seja, cuja ligação a um determinado Estado seja insuficiente para comprometer sua responsabilidade legal internacional, são descritos como atores não estatais (MELZER, 2011).

Shakelford (2009) chama a atenção para o fato de que, devido à natureza clandestina do espaço cibernético, os Estados podem facilmente incitar grupos civis a executar ataques cibernéticos, ocultando sua participação e, portanto, escapando à responsabilidade pelos atos desenvolvidos por aqueles grupos.

Entretanto, conforme codificado pela Minuta de Artigos sobre a Responsabilidade dos Estados por Atos Internacionalmente Ilegais (Artigos sobre a Responsabilidade dos Estados), da Comissão de Direito Internacional da ONU, que foi oficialmente reconhecida pela Assembleia Geral daquela organização, qualquer violação de uma obrigação internacional de um Estado para com outros resultará em

sua responsabilização internacional. Tal violação pode ser resultante de determinada ação estatal ou, ainda mais importante, por sua falha em agir (GRAHAM, 2010).

Graham (2010), por sua vez, infere que a responsabilidade estatal pode ser atribuída fruto da falha de um Estado em cumprir com sua obrigação internacional de evitar que seu território seja utilizado como base por atores não estatais, para execução de ataque contra outros Estados.

Nesse sentido, o Manual de Tallinn oferece uma regra sobre o controle da infraestrutura cibernética, intimamente ligada à responsabilidade estatal, que estabelece: “Um Estado não deve permitir conscientemente que a infraestrutura cibernética localizada em seu território ou sob seu controle governamental exclusivo seja utilizada para atos que afetem de modo adverso e ilegal outros Estados”[12] (SCHMITT, 2013, tradução nossa).

Tal regra se aplica quando o Estado possui real conhecimento dos atos em questão, como, por exemplo, órgãos desse Estado (tais como agências de inteligência) detectaram um ataque cibernético originado de seu território, ou se o Estado recebeu informação crível (como do Estado atacado) de que um ataque cibernético está em curso a partir de seu território. O não cumprimento dessa regra, segundo aquele manual, possibilita ao Estado atacado responder proporcionalmente (SCHMITT, 2013).

Conclui-se, portanto, que apesar de alguns Estados buscarem utilizar atores não estatais para a realização de ataques cibernéticos, a partir do próprio território, é factível atribuir-se a responsabilidade desses ataques àqueles Estados, com base na interpretação da norma internacional de responsabilidade estatal, insculpida nos Artigos sobre a Responsabilidade dos Estados.

No entanto, nem sempre os grupos utilizados por Estados agirão a partir de seu território. Nesse caso, a norma de Responsabilidade dos Estados torna-se ineficaz.

Ocorre que, como nos ensinam Banks (2013), Melzer (2011), Graham (2010) e Shakelford (2009), tal fato pode ser analisado a partir dos julgamentos do

[12] A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.

Caso Nicarágua e do Caso Tadic[13]. No julgamento do Caso Nicarágua, em 1986, ainda que os Estados Unidos da América (EUA) tivessem financiado, organizado, treinado e equipado os rebeldes “Contras” em uma luta para derrubar o governo nicaraguense, a CIJ não considerou os EUA responsáveis pelas ações daquele grupo. Segundo aquela Corte, um Estado não pode ser considerado legalmente responsável pelas ações de atores não estatais, a não ser que possuam o controle efetivo das operações militares e paramilitares no curso das quais as violações foram cometidas.

Por outro lado, no julgamento do Caso Tadic, em 1999, o Tribunal Criminal Internacional para a Antiga Iugoslávia (TCIAI) decidiu que um Estado pode ser considerado responsável pelas ações de um grupo militarizado quando aquele Estado coordenar ou auxiliar o planejamento geral das atividades militares do grupo em questão. Segundo Graham (2010), tal fato marcou uma mudança de interpretação legal, passando do teste de “controle efetivo” para o de “controle global” de atores não estatais por um Estado, com o fim de se atribuir a responsabilidade estatal.

Destarte, para fins de enquadramento da guerra cibernética, este autor sugere a adoção do “padrão Tadic” ou de “controle global”, para a definição da responsabilidade estatal sobre as ações de atores não estatais executadas fora do território do Estado.

Resolvida a questão da responsabilidade estatal, resta verificar qual seria a possibilidade de resposta por parte de um Estado em face de um ataque cibernético atribuído unicamente a atores não estatais. Verifica-se, fruto do costume internacional, que tal questão constitui uma prática já consolidada, como nos apresenta Michael Gervais:

> A prática e o costume demonstram que Estados podem responder - e respondem - com o uso da força contra atores não estatais. A resposta internacional aos ataques de 11 de setembro sofridos pelos Estados Unidos validou este princípio do direito consuetudinário internacional. Após 11 de setembro, o Conselho de Segurança aprovou a resolução 1368, que reafirmou o “direito inerente” de os Estados Unidos responderem em legítima defesa, de acordo com o Artigo 51 da Carta da ONU. Semanas após, quando ficou claro que os ataques de 11 de setembro foram executados por atores não estatais, os Estados Unidos ainda assim receberam apoio quase universal, incluindo o apoio do Conselho de

[13] O Caso Tadic foi conduzido pelo Tribunal Criminal Internacional para a Antiga Iugoslávia.

> Segurança, quando invocou seu direito de responder em legítima defesa[14] (GERVAIS, 2012, tradução nossa).

Por fim, apesar de cobertos todos os aspectos pertinentes ao ataque armado, incluindo o problema de atribuição, faz-se mister abordar como um Estado poderia responder a uma ação cibernética que não alcance o limiar de um ataque armado, como, por exemplo, um ataque cibernético que cause um distúrbio econômico, mas nenhum dano físico. Sobre tal tema, Banks (2013) esclarece que, nesse caso, estaria caracterizada uma violação à norma internacional de não intervenção, permitindo ao Estado vítima agir em reciprocidade com a mesma forma de violação. De acordo com os Artigos sobre a Responsabilidade dos Estados, as contramedidas devem ser dirigidas ao Estado responsável pelo ato ilegal prévio e devem ser temporária e instrumentalmente conduzidas, de modo a induzir o Estado infrator a cessar tal violação.

Gervais (2012), contudo, adverte que um Estado não pode responder imediatamente, após ser atribuída a responsabilidade estatal por um ataque cibernético, com base nos Artigos sobre a Responsabilidade dos Estados. Preferivelmente, o Estado vítima deve requerer que o ofensor sujeite-se às suas obrigações legais internacionais, utilizando-se das contramedidas apenas caso a violação persista.

Embora a doutrina de contramedidas seja adequada à resposta àqueles ataques cibernéticos que não constituam um ataque armado, a demora em se determinar a atribuição de tais ataques poderá limitar sua utilidade. Ademais, deve-se ter em conta que a resposta não constitua um uso ilegal da força, o que contrariaria o Artigo 2 da Carta da ONU (BANKS, 2013).

---

[14] Yet custom and practice demonstrate that states can—and do—respond with force to non-state actors. The international response to the 9/11 attacks on the United States validated this principle of customary international law. After 9/11, the Security Council passed Resolution 1368, which reaffirmed the “inherent right” of the United States to respond in self-defense in accordance with Article 51 of the UN Charter.106 Weeks later, when it was clear that non state actors had committed the 9/11 attacks, the United States still received nearly universal support, including from the Security Council, when it invoked its right to respond in self-defense.

3.2 A GUERRA CIBERNÉTICA E O *JUS IN BELLO*

Após analisarem-se as hipóteses em que o emprego da força é legitimado, resta observar que tal emprego deverá obedecer a um corpo normativo que rege a condução das hostilidades durante um conflito armado, visando minimizar o sofrimento desnecessário. Tal corpo normativo, o *Jus in Bello*, é conhecido como o Direito Internacional dos Conflitos Armados (DICA) ou, ainda, Direito Internacional Humanitário (DIH), que pode ser assim compreendido:

> Assim, se entenderá por Direito Internacional Humanitário (DIH) o corpo de normas internacionais, de origens convencional ou consuetudinário, especificamente aplicável aos conflitos armados, internacionais ou não-internacionais [sic], e que limita, por razões humanitárias, o direito das partes em conflito de escolher livremente os métodos e os meios utilizados na guerra, ou que protege às pessoas e aos bens afetados, ou que possam ser afetados pelo conflito (SWINARSKI, 1989).

O DICA, aplicado exclusivamente em situações de conflito armado, busca, então, regular o uso da força entre as partes beligerantes e moderar suas consequências. A existência de regras claras sobre como operar em um campo de batalha, ou no espaço cibernético, confere ordem à guerra e proteção aos não combatentes. Ambos os contendores devem possuir a confiança de que estão combatendo segundo o mesmo código de conduta, pois a falta de tal confiança levaria a uma escalada paranóica da violência, aumentando ainda mais os riscos aos não combatentes (GERVAIS, 2012; MELZER, 2011, SHACKELFORD, 2009).

Assim, sempre que uma ação cibernética atribuída a uma das partes beligerantes for destinada a causar dano ao adversário, seja ao causar morte, danos físicos ou destruição, ou, ainda, ao afetar diretamente suas operações ou capacidades militares, tais ações serão qualificadas como hostilidades e estarão sujeitas às restrições impostas pelo DICA à escolha e ao uso de meios e métodos de guerra (MELZER, 2011).

Tem-se, pois, que os princípios tradicionais do DICA se aplicam à guerra cibernética, desde que essas ações estejam propriamente caracterizadas como operações militares (KOSTADINOV, 2014; WINGFIELD, 2009).

Reforçando tal posição, o Protocolo I brindou uma norma genérica o bastante para abarcar toda e qualquer tecnologia vindoura, ao prever a obrigação de avaliarem-se novas armas, incluindo o arsenal cibernético, quanto ao seu

enquadramento total ou parcial ao DICA. Assim, fica patente a aplicabilidade do *jus in bello* à guerra cibernética, conforme estabelecido no Artigo 36:

> Quando uma Alta Parte Contratante estude, desenvolva, adquira ou adote uma nova arma, ou novos meios ou métodos de combate, terá a obrigação de verificar se seu emprego, em certas condições ou em todas as circunstâncias, estaria proibido pelo presente Protocolo ou por qualquer outra norma de direito internacional aplicável a essa Alta Parte Contratante (JARDIM, 2006).

Contudo, embora os ataques representem a forma predominante na condução das operações de combate, seria impreciso assumir que as ações cibernéticas que não se equivalem a um ataque armado não estejam sujeitas às normas do DICA. A aplicabilidade das restrições impostas pelo DIH na condução das ações cibernéticas dependerá apenas em seu enquadramento como parte das hostilidades, ou seja, como parte da campanha militar como um todo, e não em sua qualificação como um ataque armado (MELZER, 2011).

Nesse sentido, a CICV vê a guerra cibernética com grande preocupação, devido à vulnerabilidade das redes e sistemas de TI e o custo humanitário potencial dos ataques cibernéticos. Quando uma rede de computadores de um Estado é atacada, existe o risco de que civis sejam privados de serviços essenciais básicos, como água potável, cuidados médicos e eletricidade (INTERNATIONAL COMMITTEE OF THE RED CROSS, 2013).

Assim, qualquer mal causado à população civil por motivos relacionados ao conflito, incluindo o simples aborrecimento ou inconveniência decorrentes de uma ação cibernética, deve ser considerada como parte das hostilidades militares, despertando a pertinente aplicação do DIH (MELZER, 2011).

Desse modo, ao constatar-se a aplicabilidade do *jus in bello* à guerra cibernética, tem-se que toda e qualquer ação cibernética deve observar os princípios do DIH, que, em última análise, norteiam sua execução. No escopo deste trabalho, são abordados os seguintes princípios: necessidade militar, distinção, proporcionalidade, humanidade, neutralidade e perfídia.

3.2.1 Princípio da Necessidade Militar

O princípio da necessidade militar, também conhecido como objetivo militar, estabelece que “em todo conflito armado, o uso da força deve corresponder à vantagem militar que se pretende obter. As necessidades militares não justificam

condutas desumanas, tampouco atividades que sejam proibidas pelo DICA" (BRASIL, 2011).

Há, pois, uma restrição ao uso da força, que só poderá ser empregada contra alvos que constituam objetivos militares válidos. Assim, tem-se que a base para o princípio da necessidade militar é encontrada no Inciso 2°, do Artigo 52 do Protocolo I:

> 2. Os ataques limitar-se-ão estritamente aos objetivos militares. No que concerne aos bens, os objetivos militares se limitam àqueles objetos que por sua natureza, localização, finalidade ou utilização contribuam eficazmente para a ação militar ou cuja destruição total ou parcial, captura ou neutralização, ofereça nas circunstâncias do caso presente uma vantagem militar definida (JARDIM, 2006).

Para Kostadinov (2014) e Gervais (2012), dentre os princípios do DIH, a noção de necessidade militar possui um papel central, pois consideram que este último possui uma precedência temporal sobre os demais, que buscam equilibrar, por meio de limites de caráter humanitário, essa necessidade de tomar armas para vencer. Consequentemente, um ato cibernético hostil deverá ser analisado inicialmente sob a ótica da necessidade militar para, depois, ser verificada sua conformidade com os demais princípios do DIH.

Atualmente, as forças armadas usam sistemas computadorizados em várias plataformas de armas e em seus sistemas de comando e controle, cobrindo praticamente todo o escopo de suas operações. Logo, oferecem alvos compensadores a ataques cibernéticos que, dirigidos contra os sistemas de TI militares do inimigo, satisfazem a condição de necessidade militar, em virtude do emprego exclusivamente militar dos sistemas alvo.

Entretanto, há outros fatores a ponderar, o que pode tornar complexa a determinação da vantagem militar. Gervais (2012) argumenta que a complexidade dos sistemas de TI gera desafios ao cálculo da necessidade militar, fato esse que limita os ataques cibernéticos cujas vantagens militares sejam indeterminadas, uma vez que nem sempre será possível prever todos os efeitos indiretos de um ataque. E como visto anteriormente, são os efeitos de segundo nível que normalmente se busca alcançar. Ademais, não se pode esquecer da característica de imprevisibilidade dos efeitos do ataque cibernético que, por si só, poderá ofuscar toda e qualquer vantagem militar vislumbrada.

Ocorre que o grande desafio imposto ao ataque cibernético é que sua "vantagem militar definida" somente pode ser comprovada após a realização do

ataque e apenas no caso de o mesmo obter sucesso, em vista, principalmente, da busca por efeitos secundários que efetivamente suprirão o efeito desejado do ataque e que, invariavelmente, não são facilmente antecipados. Assim, uma análise anterior à execução do ataque poderá levar a uma conclusão diferente. Por tal motivo, Gervais (2012) sugere a criação de um registro que possibilite armazenar toda a informação disponível sobre o alvo, antes do ataque, de modo a viabilizar sua defesa perante possíveis questionamentos.

Por fim, tem-se que a avaliação de um ataque cibernético quanto à observância ao princípio da necessidade militar é um exercício que deverá ser realizado caso a caso, conforme apontado por Gervais (2012), de modo análogo aos ataques cinéticos, o que demandará um esforço continuado de inteligência e profundo conhecimento acerca das relações de interconectividade e interdependência entre os vários sistemas existentes que poderão ser afetados pelo ataque.

3.2.2 Princípio da Distinção

O princípio da distinção requer que as partes beligerantes diferenciem combatentes e civis não combatentes, assim como objetivos militares e bens de caráter civil. Tanto os não combatentes como os bens de caráter civil são protegidos contra os ataques, não podendo ser, também, objetos de represália (BRASIL, 2011).

Tal norma está explicitada no Artigo 48 do Protocolo I:

> De forma a assegurar respeito e proteção à população civil e aos bens de caráter civil, as Partes em conflito deverão sempre fazer distinção entre a população civil e os combatentes, entre os bens de caráter civil e os objetivos militares e, em consequência, dirigirão suas operações unicamente contra os objetivos militares (JARDIM, 2006).

Em que pese o conceito de distinção entre combatentes e a população civil ser claro na teoria, sua aplicação prática pode tornar-se nebulosa e complexa no contexto das ações de guerra cibernética, onde os alvos estão literalmente fora das vistas de seus atacantes e onde infraestruturas interconectadas e de uso dual apoiam igualmente a usuários civis e militares, as quais poderão ser atingidas pelos efeitos secundários e, até mesmo, terciários de um ataque cibernético, com resultados totalmente imprevisíveis. Aliado a isso, tem-se a presença simultânea de combatentes e civis no ciberespaço, não sendo demais lembrar que, por suas

próprias características, inexistem barreiras físicas no espaço cibernético e tampouco seus usuários se distinguem por meio de insígnias ou uniformes.

Ou seja, mesmo que um ataque cibernético seja direcionado contra um objetivo militar, existe a possibilidade de ser impreciso a ponto de causar danos colaterais excessivos, ou mesmo não previstos inicialmente, e se tornar indiscriminado. Uma vez que uma arma cibernética é empregada, um vírus por exemplo, muitas das vezes seu operador não poderá impedir sua retransmissão subsequente, o que pode ocorrer mesmo em redes fechadas, pois o vírus pode ser transferido por meio de mídias removíveis, como um “pen drive”. Uma vez que, praticamente, quase toda infraestrutura cibernética militar depende de redes civis, um ataque contra a infraestrutura de TI militar pode se disseminar nos sistemas civis e, a partir desse ponto, causar efeitos em escala global (JASTRAM e QUINTIN, 2011; GERVAIS, 2012; SCHMITT, 2012; WINGFIELD, 2009).

Nesse sentido, Wingfield (2009) argumenta que a necessidade de distinção entre alvos militares e bens de caráter civil apresenta toda uma gama de problemas, que vão desde uma grande dependência de inteligência, passando pela necessidade de análise legal e cuidados na execução das operações, que inclui a seleção de uma arma cibernética com precisão suficiente para atacar, apenas, os alvos cibernéticos selecionados.

Esse requisito de precisão da arma cibernética já é algo factível nos dias de hoje. Como apontado por Lewis (2011), o stuxnet é um artefato cibernético de nível militar e foi uma alternativa de precisão à realização de um ataque aéreo às instalações de enriquecimento nuclear iranianas. Ele causou menos danos que um ataque aéreo e evitou efeitos colaterais adversos, como a morte de civis, em que pese um erro de programação o tenha tornado indiscriminado em seu alcance, porém sem causar a mesma sorte de efeitos destrutivos.

Tal possibilidade levou à ideia de que a guerra cibernética pode ser uma alternativa mais humana, uma vez que suas armas podem ser usadas no lugar de sua contraparte cinética para alcançar o mesmo resultado, ao mesmo tempo em que possuem menor letalidade e produzem destruição limitada. A capacidade que um ataque cibernético pode alcançar de desabilitar, neutralizar, ou mesmo destruir um determinado objetivo oferece maior discricionariedade do que um ataque cinético, característica que o torna hiperdistintivo. Nesse sentido, em várias ocasiões o

ataque cibernético será preferível à opção cinética (JASTRAM e QUINTIN, 2011; LEWIS, 2011; GERVAIS, 2012; SCHMITT, 2012, GRAHAM, 2010).

Jastram e Quintin (2011) alertam que se tem utilizado da característica de hiperdistinção para justificar o uso de ataques cibernéticos contra uma gama mais ampla de alvos, incluindo-se objetos usualmente considerados como bens de caráter civil, o que é ilegal perante o DIH. A definição de um objetivo militar independe dos meios e métodos empregados e um ataque cibernético contra bens protegidos, como é o caso daqueles de caráter civil, contraria as normas do DIH, mesmo que tal ataque não resulte em danos ou destruição.

Como observado, a distinção é um problema para a guerra cibernética, cujos alvos são usualmente de uso dual, aumentando as chances de o ataque se tornar indiscriminado, mormente devido à interconectividade inerente ao ciberespaço. Por outro lado, é possível alcançar-se a hiperdistinção por meio de códigos dedicados e especificamente moldados para o sistema-alvo, devendo-se ter em mente a necessidade de cuidado em sua execução, de modo a evitar sua dispersão indiscriminada, minimizando, assim, os efeitos colaterais indesejados.

Ao mudar-se o ponto de vista da análise para as ações defensivas, o princípio da distinção impõe outros problemas. Segundo Watts (2010), a distinção na guerra cibernética demanda mais atenção à conduta do ataque do que à aparência externa de indivíduos ou grupos que o executaram. Seu argumento é de que, em oposição ao combate convencional, em que um elemento atacado responde diretamente contra os combatentes adversários, em uma ação defensiva cibernética há a tendência em se responder aos meios e métodos do ataque, concluindo que a guerra cibernética efetivamente retira a aparência do combatente da “equação” da distinção.

Complicando ainda mais tal situação, Gervais (2012) declara que a definição de combatente pelo DIH não se adéqua ao ciberespaço, onde indivíduos não organizados podem prontamente participar em ataques cibernéticos contra uma das partes beligerantes.

Tais posicionamentos decorrem do requisito imposto pelo DIH de que os beligerantes devem se distinguir entre combatentes e não combatentes, conforme estabelecido no Inciso 3, do Artigo 44 do Protocolo I:

> 3 - Para que a proteção da população civil contra os efeitos das hostilidades seja reforçada, os combatentes devem distinguir-se da população civil quando tomarem parte num ataque ou numa operação militar preparatória de um ataque (JARDIM, 2006).

Ademais, não se pode olvidar que civis também podem tomar parte na guerra cibernética e, ao participarem diretamente das hostilidades, estarão sujeitos ao ataque, conformando alvos legítimos, conforme expresso no Inciso 3, do Artigo 51 do Protocolo I: “3. As pessoas civis gozarão da proteção outorgada por esta Seção, exceto se participarem diretamente das hostilidades e enquanto dure tal participação” (JARDIM, 2006).

De acordo com a posição oficial do CICV, a noção de “participação direta nas hostilidades” ultrapassa o conceito de ataque e inclui, não somente, o infligir de morte, ferimento ou destruição, mas, essencialmente, qualquer ato que cause um efeito adverso às operações ou capacidades militares de um dos beligerantes (MELZER, 2011).

Corroborando aquela noção, o grupo internacional de especialistas que redigiu o Manual de Tallinn chegou a três critérios cumulativos para qualificar um ato como participação direta. Primeiro, o ato deve possuir a intenção ou o efeito real de afetar negativamente as operações militares do adversário, suas capacidades, ou, ainda, infligir a morte, dano físico ou destruição material a pessoas e objetos protegidos. Porém, não há a necessidade de ocorrência de danos físicos ou materiais a pessoas ou objetos. Ou seja, ações cibernéticas que não se caracterizem como ataque armado poderão se enquadrar nesse critério desde que causem um efeito negativo ao inimigo, militarmente. Um exemplo seria uma ação cibernética que interrompesse a rede do sistema de comando e controle inimigo a nível lógico, apenas. Segundo, deve haver uma ligação causal direta entre o ato em questão e o dano pretendido ou infligido, o nexo causal. Finalmente, o ato deve ser diretamente relacionado às hostilidades, o nexo beligerante (SCHMITT, 2013).

Como já observado, qualquer ato de participação direta nas hostilidades por civis os tornam passíveis de se tornarem alvos de ataque durante o tempo em que estiverem engajados no ato em questão. Estão incluídas aí, ao menos, as ações imediatamente precedentes e subsequentes ao ato em si, como, por exemplo, os deslocamentos para a “estação de combate”, local onde estão localizados os computadores que serão efetivamente utilizados para a operação. No caso de operações cibernéticas, esse período pode ter início desde a fase de varredura do

sistema alvo na busca de vulnerabilidades, se estender durante o período das ações contra o sistema e, ainda, incluir o período durante o qual o inimigo realiza a avaliação do ataque (SCHMITT, 2013).

Um ponto de particular importância no contexto cibernético diz respeito aos efeitos retardados. Um exemplo seria a colocação de uma bomba lógica, projetada para ser ativada em um determinado ponto futuro, que poderá ocorrer após um intervalo específico de tempo, um comando do operador do ataque, ou mesmo por uma ação realizada pelo sistema-alvo. Esse, porém, é um ponto polêmico, que não encontra consenso entre os estudiosos no tema, como Gervais (2012), e que merece um estudo cuidadoso. Mesmo entre os especialistas que redigiram o Manual de Tallinn existem opiniões opostas quanto a esta situação (SCHMITT, 2013).

No caso, onde há um retardo entre a introdução da arma cibernética e o aparecimento de seus efeitos, este autor considera que não houve solução de continuidade com relação à participação direta do responsável por tal ataque, uma vez que há uma relação direta de causa e efeito entre o autor e os efeitos do ataque. Portanto, no caso da participação de civis, estes perderiam sua proteção por todo o período, desde a infiltração até a avaliação dos danos do ataque.

No que tange à participação de civis, há, ainda, uma situação particular a ser considerada. Trata-se do conceito de “levée en masse” que, de acordo com o Inciso 6, do Artigo 4º da III Convenção de Genebra, de 1949, entende-se como:

> A população de território não ocupado que, à aproximação do inimigo, pegue espontaneamente em armas para combater as tropas invasoras, sem ter tido tempo de constituir em forças armadas regulares, se carregar armas abertamente e se respeitar as leis e costumes de guerra (JARDIM, 2006).

Nesse caso, o “levée en masse” guarda o status de combatente. Logo sua atuação nas hostilidades está legitimada e, assim como qualquer combatente legal, está passível de ataque.

Melzer (2011) alerta que, enquanto essa categoria de pessoas perdeu relevância na guerra tradicional, a mesma tende a ganhar importância no contexto da guerra cibernética, que, por operar no espaço cibernético, não pressupõe invasão ou ocupação de território, possibilitando que a “levée en masse” possa operar por um período maior. Cabe salientar, também, que o ciberespaço provê um ambiente

ideal para a incitação e a coordenação de ações de defesa cibernética coletivas e espontâneas, por um grande numero de ativistas cibernéticos[15].

Ocorre que o conceito de “levée en masse” possui o requisito de “carregar armas abertamente”, cuja interpretação para seu uso no espaço cibernético desperta dúvidas quanto a sua eficácia. Inicialmente, tem-se que, como argumentado por Gervais (2012), a eficácia da maioria das armas cibernéticas tem origem em sua capacidade de permitir ao atacante penetrar nos sistemas-alvo sem ser detectado. Logo, o fato de portar armas abertamente irá expor o ataque cibernético, inviabilizando-o técnica e taticamente. Melzer (2011) argumenta que, a partir de uma perspectiva teleológica, uma solução para tal problema seria considerar este requisito como cumprido sempre que as operações cibernéticas não sejam conduzidas por meio de simulação do status de pessoas protegidas, dentro do que estaria proibido pelo conceito de perfídia.

Some-se a isso o problema da atribuição, já explorado anteriormente, em que se viu a possibilidade de mascaramento de identidades e a consequente “falsa atribuição” a computadores civis pertencentes a nacionais de Estados neutros.

3.2.3 Princípio da Proporcionalidade

O princípio da proporcionalidade visa minimizar o sofrimento humano desnecessário e, como explicitado por Brasil (2011), pressupõe que a utilização dos meios e métodos de guerra deve ser proporcional à vantagem militar concreta e direta. Nenhum alvo, mesmo que militar, deve ser atacado se os prejuízos e sofrimento forem maiores que os ganhos militares que se espera da ação.

Sua base legal está contida no Inciso 5, do Artigo 51 do protocolo I:

> 5 - Considerar-se-ão indiscriminados, entre outros, os seguintes tipos de ataque:
> b) Os ataques quando se pode prever que causarão incidentalmente mortos e ferimentos entre a população civil, ou danos a bens de caráter civil, ou ambas as coisas, e que seriam excessivos em relação à vantagem militar concreta e diretamente prevista (JARDIM, 2006).

Assim como o princípio da necessidade militar proíbe o uso excessivo de força contra combatentes, o princípio complementar de proporcionalidade limita os efeitos de um ataque sobre os não combatentes. Essa limitação é expressa como um teste de equilíbrio entre a vantagem militar “concreta e direta” prevista e as

[15] Ver glossário.

perdas civis esperadas. Quanto maior o valor de um alvo em potencial, aumenta, também, o limite de dano colateral tolerado (WINGFIELD, 2009).

Trasladando-se à esfera cibernética, é lícito afirmar que os ataques cibernéticos podem ser uma das melhores opções para minimizar o dano colateral, uma vez que, como visto ao tratar-se do princípio da distinção, os ataques cibernéticos podem ser hiperdistintivos. Dessa forma serão menos letais que seu correspondente cinético e, adicionalmente, potencialmente reversíveis. Tais características são desejáveis para a aplicação proporcional da força, sem causar um número desproporcional de baixas civis (JASTRAM e QUINTIN, 2011; GERVAIS, 2012).

Ainda assim, por vezes esse princípio é negligenciado. Schmitt (2012) aponta três modos em que o princípio da proporcionalidade é frequentemente violado: quando não se tem conhecimento completo sobre o que está sendo atacado; a inabilidade de moldar com precisão a quantidade de força aplicada no alvo; e a inabilidade em realizar um ataque “cirúrgico”, ou seja, atingir precisamente o ponto desejado. Em que pese a possibilidade de hiperdistinção, tais questões são ainda mais importantes e possuem aplicação no espaço cibernético, onde é extremamente difícil distinguir um código de programação em um computador que controla a distribuição de energia elétrica para um sistema de armas, como, por exemplo, um sistema de radar de alerta antecipado - no caso um alvo legítimo -, de um código que controla o fornecimento de energia elétrica a um hospital.

No espaço cibernético, o princípio de proporcionalidade, assim como o da distinção, exige maior fidelidade e detalhamento por parte dos esforços de inteligência.

3.2.4 Princípio da Humanidade

Também conhecido como princípio da precaução, o princípio da humanidade proíbe que se provoque sofrimento às pessoas e destruição de propriedades, se tais atos não forem necessários para obrigar o inimigo a se render. Destarte, são proibidos ataques exclusivamente contra civis, o que não impede a ocorrência de danos colaterais a bens e pessoas, mas todas as precauções devem ser tomadas para mitigá-los (BRASIL, 2011).

Uma vez mais, o ataque cibernético oferece um método preferível por permitir atingir o mesmo efeito com menor letalidade e destruição do que o ataque

cinético. Um exemplo desse tipo de aplicação seria a neutralização de um sistema radar por meio de ações cibernéticas, fato que pouparia vidas em ambos os lados do conflito, provando, assim, ser um método de guerra mais humano (KOSTADINOV, 2014; JASTRAM e QUINTIN, 2011).

Pode-se argumentar que o princípio da precaução impõe a obrigação de se escolher os meios e métodos menos letais para se alcançar os objetivos militares. E o ataque cibernético poderá, em certas ocasiões, ser esta opção. Entretanto, as armas cibernéticas são ferramentas perecíveis. Uma vez utilizadas, serão, invariavelmente, ineficazes para um segundo ataque, uma vez que as defesas cibernéticas inimigas estarão robustecidas, ao se conhecer os meios e métodos do ataque, e as vulnerabilidades exploradas serão reparadas. Logo, as armas cibernéticas serão reservadas para aplicações especiais, principalmente aquelas mais distintivas, ou seja, criadas especificamente para um determinado alvo ou que explorem determinada vulnerabilidade. Desse modo, simplesmente porque é possível usar uma capacidade cibernética para reduzir o dano colateral não significa que esta opção deverá ser a escolhida.

3.2.5 Princípio da Neutralidade

O princípio da neutralidade tem sua origem nas Convenções de Haia, que estabelecem os direitos dos Estados neutros e a obrigação de não interferirem no conflito; e a obrigação das partes beligerantes de respeitar a inviolabilidade dos Estados neutros.

De acordo com o princípio da neutralidade, em uma situação de conflito armado internacional, um Estado neutro é obrigado a prevenir que seu território seja utilizado por quaisquer das partes beligerantes, noção que pode ser interpretada para incluir o espaço cibernético em tal proibição. Contudo, a infraestrutura do ciberespaço se estende globalmente e é incomparável com qualquer noção de território. A forma como os dados se movem, dado o método de comunicação distribuída e os fundamentos de chaveamento de pacotes de dados nos quais a internet está baseada, garantem a imprevisibilidade do roteamento que a informação, seja ela legítima ou maliciosa, perfaz ao trafegar na rede até seu destino final. Segundo o protocolo da rede, a informação tomará a rota mais curta para seu destino, seja aquela qual for, dependendo apenas das condições em tempo-real de cada nó de rede. A impossibilidade de prever qual caminho uma arma cibernética irá

tomar, somada à necessidade de prevenir a utilização de seu território, faz com que a única forma de um Estado neutro atuar seja cortando todo o tráfego da internet em seu país, isolando-o ciberneticamente do mundo. Contudo, tal requisito torna-se impraticável (MELZER, 2011; GERVAIS, 2012; KOSTADINOV, 2014).

Como visto, a análise da neutralidade no contexto cibernético torna-se complexa, em vista, principalmente, das características do ciberespaço. O uso da infraestrutura de telecomunicações de um Estado neutro como um canal para o ataque cibernético não é uma violação óbvia à soberania daquele Estado, da mesma forma que um sobrevoo não autorizado por aeronave militar o seria. Em suma, o espaço cibernético corrompeu a conexão entre território e soberania (SHACKELFORD, 2009; KOSTADINOV, 2014).

O princípio da neutralidade estabelece, ainda, que as partes beligerantes devem respeitar a inviolabilidade dos territórios neutros e são proibidas de movimentar tropas e suprimentos de guerra, o que inclui munição de qualquer tipo, através o território de um Estado neutro. A Convenção de Haia estipula, também, que os Estados neutros não precisam proibir ou restringir o uso por parte dos beligerantes dos cabos telegráficos e de telefonia, bem como da infraestrutura de telegrafia sem fio, pertencentes ao Estado ou a seus nacionais, desde que aplique a mesma política a todas as partes indistintamente. Tal fato é de particular interesse à guerra cibernética, pois, como visto, o roteamento da informação não pode ser controlado, de modo a evitar o trânsito pela infraestrutura de telecomunicações de Estados neutros. Entretanto, aquela Convenção exige que os Estados neutros proíbam as partes beligerantes: construir infraestrutura própria em seu território para comunicação com suas forças militares; e utilizar, para fins militares, qualquer instalação desse tipo estabelecida pelo Estado beligerante antes do início das hostilidades (MELZER, 2011; KOSTADINOV, 2014).

Destarte, pode-se afirmar que um Estado neutro deverá impedir a condução de ações cibernéticas a partir de seu território, ao mesmo tempo em que não obstruirá o roteamento de dados provenientes das partes beligerantes, através de sua infraestrutura de telecomunicações.

3.2.6 Princípio de proibição da Perfídia

A deslealdade, quando se trata de perfídia, existe quando a vítima possui uma razão incontestável para confiar no atacante. A perfídia envolve um ato voltado

a convencer o inimigo de que o ator em questão possui direito à proteção especial de acordo com o DICA, com a intenção de trair sua confiança. Por outro lado, os ardis ou estratagemas são planejados para iludir o inimigo, como, por exemplo, levando-o a ser negligente ou a escolher uma determinada linha de ação (WINGFIELD, 2009).

O princípio de proibição da perfídia encontra-se insculpido no Artigo 37 do Protocolo I:

> 1 - É proibido matar, ferir ou capturar um adversário valendo-se de meios pérfidos. Constituirão perfídia os atos que, apelando para a boa fé de um adversário e com a intenção de atraiçoá-lo, deem a entender a este que tem direito à proteção, ou que está obrigado a concedê-la, em conformidade com as normas de direito internacional aplicáveis nos conflitos armados. São exemplos de perfídia os seguintes atos:
>
> a) Simular a intenção de negociar sob uma bandeira de armistício ou de rendição;
>
> b) Simular incapacidade por ferimentos ou enfermidade;
>
> c) Simular a condição de pessoa civil, não combatente; e
>
> d) Simular que possui condição de proteção, pelo uso de sinais, emblemas ou uniformes das Nações Unidas ou de Estados neutros ou de outros Estados que não sejam Partes em conflito.
>
> 2 - Os estratagemas não são proibidos. Constituem estratagemas os atos que têm por objeto induzir a erro um adversário ou fazer com que este cometa imprudências, porém que não infrinjam nenhuma norma do direito internacional aplicável aos conflitos armados, nem sejam pérfidos já que não apelam para a boa fé de um adversário com respeito à proteção prevista nesse direito. São exemplos de estratagemas os seguintes atos: a camuflagem, os engodos, as operações simuladas e as informações falsas (JARDIM, 2006).

No contexto da guerra cibernética, os atacantes disfarçam seus ataques, fazendo seus códigos passarem por pedidos de informação inocentes, e escondem suas identidades que, muitas das vezes, são manipuladas para parecerem como civis. Por tais motivos, estudiosos como Shakelford (2009), Gervais (2012) e Rowe (2013) consideram tais medidas como perfídia.

Rowe (2013) define a perfídia cibernética como o mascaramento de código malicioso que se faz passar por um software comum. De acordo com essa visão, o “stuxnet” pode ser considerado um exemplo de perfídia cibernética, que pode ser identificada sempre que um *malware* simular a condição de um *software* civil, como parte das operações militares.

Rowe (2013) argumenta que a confiança é a principal vítima da perfídia. Se não existir confiança nas Partes neutras, nos símbolos e situações protegidas, não

haverá intenção do uso desses elementos em sua finalidade pretendida. Até esse ponto seu argumento está correto e, pode-se dizer, é universalmente aceito. Ocorre que, trasladando-o ao campo cibernético, Rowe (2013) defende a tese de que os ataques cibernéticos corrompem a confiança a nível lógico, ou seja, um código malicioso trai a confiança do sistema operacional de modo a ganhar acesso ao sistema-alvo.

Segundo Pictet (1987), a definição de perfídia constante no Protocolo I está baseada em três elementos: a conquista da confiança do adversário; a intenção de trair essa confiança (elemento subjetivo); e a existência de proteção conferida pelo DIH (elemento objetivo). O Manual de Tallinn agrega um quarto elemento: a morte ou o ferimento do adversário. Tal argumento está contido logo no início do Artigo 37, que define perfídia, onde também há a proibição da captura do adversário.

Em que pese todo o avanço das TIC experimentado pelo ser humano, esse e todo tema envolvendo o campo cibernético é algo, ainda, muito novo. Some-se a isso a rapidez da evolução de tais tecnologias, que faz com que o homem reaja a esse fenômeno de diferentes formas. Como consequência, tem-se que sua correta e completa compreensão é, em muito, dificultada.

Nesse sentido, cabe ressaltar que a interpretação de confiança a nível lógico utilizada por Rowe não pode ser confundida com a confiança que deve existir entre as partes em um conflito. Tratam-se de campos distintos. Em um deles, o lógico, a “confiança” é burlada por uma sequência de abertura e fechamento de chaves, em analogia ao que ocorre em nível mais baixo de processamento lógico, representando os estados dos bits de valor “zero” e “um”. Trata-se do simples funcionamento de uma máquina lógica. Por sua vez, a confiança entre as partes em conflito pertence ao campo cognitivo, é o sentimento de boa fé que se deposita em seu semelhante. Esta é a confiança de que trata a proibição da perfídia. A simples alteração de um código por um *malware* não interfere com a confiança de uma das partes, pois não a alcançará a nível cognitivo. Na situação apresentada por Rowe, uma máquina foi enganada, não um combatente. Logo, não há como se falar em perfídia.

No que concerne à simulação da condição de não combatente, ou seja, de pessoa civil, tem-se que, na realidade, o atacante não a utiliza para ganhar a confiança de seu adversário. Ela é usada mais como uma forma de cortina de fumaça, mascarando sua identidade e protegendo-o contra as ações defensivas do inimigo, após o ataque ter sido executado. Por esse motivo não se deve concordar

com o enquadramento genérico da perfídia cibernética que, na prática, tornaria toda a guerra cibernética ilegal perante o DICA.

Portanto, este autor considera que a perfídia cibernética ocorrerá sempre que a ação cibernética comprometer a confiança do adversário a nível cognitivo e, corroborado por Kostadinov (2014), Schmitt (2013) e Melzer (2011), tendo como base os comentários de Pictet (1987), estará limitada aos casos em que houver morte, ferimento ou captura.

A perfídia cibernética pode ser exemplificada, então, pelo envio de um e-mail, pretensamente de origem do CICV, convidando o inimigo a uma reunião com um representante daquele órgão, ou outro indicando a intenção de rendição, mas que, na verdade, buscam levar as forças inimigas a uma emboscada.

Deve-se ressaltar que tal definição exclui dos casos de perfídia cibernética aqueles relacionados à ocorrência de danos físicos ou destruição, uma vez que tais efeitos não se enquadram no estabelecido pelo Artigo 37 do Protocolo I. Entretanto, cabe destacar que o uso de emblemas reconhecidos, como o distintivo da Cruz Vermelha ou o das Nações Unidas; e o uso de símbolos de nacionalidade, como bandeiras, insígnias e uniformes de outros Estados, sejam neutros ou beligerantes, são expressamente proibidos em qualquer situação, conforme estabelecido nos Artigos 38 e 39 do Protocolo I, respectivamente. Desse modo, mesmo que a ação cibernética não resulte em perfídia, ao utilizar-se de quaisquer desses símbolos protegidos estará caracterizada sua ilegalidade perante o DIH.

4 CONSIDERAÇÕES FINAIS

Ao longo deste trabalho, pôde-se observar a grande complexidade que envolve todos os temas pertinentes à área cibernética. A cada dia as tecnologias da informação e comunicações evoluem, exigindo um grande esforço de especialistas em todos os níveis para que se mantenham atualizados. E essa velocidade de evolução contribui, muitas das vezes, para que tais fenômenos não sejam compreendidos em sua totalidade.

Tais fatos fazem com que os estudos sobre o assunto sigam diferentes vieses. E no que tange à análise sobre o enquadramento da guerra cibernética aos preceitos do direito internacional não é diferente, como foi comprovado pela diversidade de pontos de vista encontrados na literatura utilizada, que contribuíram para uma análise mais apurada sobre o tema em lide.

Assim, sem ter a pretensão de ser uma obra definitiva, o presente trabalho buscou, respeitando a obra de vários especialistas no assunto, pacificar alguns pontos conflitantes e trazer à consideração do leitor o ponto de vista do autor.

O primeiro aspecto a ser ressaltado diz respeito à aplicabilidade das normas do *jus ad bellum* e do *jus in bello* à guerra cibernética. A esse respeito, deve-se lembrar, inicialmente, que as ações de guerra cibernética fazem parte de uma campanha militar e devem ser contextualizadas como um sistema de armas de apoio a essa campanha e, como tal, podem e devem ser submetidas às normas internacionais aplicáveis aos conflitos armados.

Ao tratar da análise da adequação da guerra cibernética ao *jus ad bellum*, o estudo deparou-se com a necessidade de conceituar as expressões “uso da força” e “ataque armado” dentro do contexto cibernético. Assim, chegou-se à conclusão de que o uso da força se caracteriza quando os efeitos de uma ação cibernética causam danos a objetos materiais ou estruturas físicas, bem como morte ou sofrimento a pessoas, estando englobado no conceito de dano a neutralização lógica do objeto, não se restringindo ao dano físico ou destruição.

Já a interpretação do conceito de ataque armado foi mais restritiva, uma vez que sua ocorrência pressupõe o direito de legítima defesa por parte do Estado vítima do ataque. Nesse contexto, o ataque armado ocorrerá sempre que as ações cibernéticas causarem morte ou ferimento a pessoas ou danos físicos a objetos.

Um ponto importante abordado durante a análise do ataque armado foi a atribuição de responsabilidade estatal pela ação de terceiros, que foi dividida em duas abordagens. A primeira utiliza o estatuído pelos Artigos sobre a Responsabilidade dos Estados para estabelecer que a responsabilidade estatal pode ser atribuída, fruto da falha de um Estado em cumprir com sua obrigação internacional de evitar que seu território seja utilizado como base por atores não estatais, para execução de ataques cibernéticos contra outros Estados. A segunda abordagem tem sua eficácia quando os grupos utilizados pelos Estados agem a partir do território de outro Estado. Nesse caso, deve-se adotar o “padrão Tadic”, ou de controle global, baseado na decisão do Tribunal Criminal Internacional para a Antiga Iugoslávia, que decidiu que um Estado pode ser considerado responsável pelas ações de um grupo militarizado quando aquele Estado coordenar ou auxiliar o planejamento geral das atividades militares do grupo em questão.

No que tange ao *jus in bello*, ou DIH, constatou-se sua plena aplicabilidade à guerra cibernética, devendo toda e qualquer ação cibernética observar seus princípios, que, em última análise, nortearão sua execução.

O grande desafio imposto pelo DIH à guerra cibernética é o de garantir que os ataques sejam direcionados apenas contra objetivos militares legítimos, poupando a população civil e os bens de caráter civil das partes beligerantes, bem como os Estados neutros e toda a infraestrutura civil a nível mundial. Entretanto o espaço cibernético é único e global. Não existem fronteiras ou subdivisões segregando determinada classe de usuários. Nele encontram-se civis, militares, usuários corporativos, governamentais etc., convivendo simultaneamente em um ambiente interconectado e mutante. Portanto, a possibilidade de hiperdistinção que pode ser aplicada a uma ação cibernética torna-se uma opção para a aplicação dos princípios do DIH.

Contudo, adotar tal opção requer um grande esforço em várias áreas, que deve ser iniciado desde os tempos de paz, em virtude do tempo necessário ao desenvolvimento da expertise e ferramentas necessárias para se alcançar a hiperdistinção. Há que se ter em mente que seu desenvolvimento demandará o aporte de recursos financeiros consideráveis e a mobilização de recursos humanos altamente qualificados.

Acerca do material consultado para a realização deste trabalho, considero relevante destacar a obra produzida por iniciativa da OTAN, que foi lançada em

2013 e que aborda de maneira extensiva o tema: o Manual de Tallinn sobre o direito internacional aplicável à guerra cibernética, que nada mais é do que um compêndio interpretativo sobre as normas do *jus ad bellum* e do *jus in bello*. Em que pese esse manual apresentar interpretações controversas, como pôde ser visto no presente estudo, o simples fato de buscar consolidar toda a norma a respeito da guerra cibernética em uma única publicação torna o Manual de Tallinn uma fonte de consulta indispensável, podendo, até mesmo, servir como ponto de partida para a criação de uma nova legislação sobre o assunto. Destarte, cabe a sugestão para que o Manual de Tallinn seja analisado integralmente por todos aqueles que, de algum modo estejam ligados à condução das ações da guerra cibernética.

Por fim, faz-se mister ressaltar que as fontes do *jus ad bellum* e do *jus in bello* carecem de atualização, tendo em vista a natural evolução tecnológica que levou de arrasto toda uma nova doutrina militar, mudando a forma de se fazer a guerra. Tal fato torna-se ainda mais importante e urgente em face da existência de diferentes interpretações sobre o tema no contexto cibernético.

Portanto, assim como foram criados protocolos adicionais e convenções específicas sobre certos tipos de armas, urge a necessidade de que uma nova legislação internacional venha a disciplinar a condução da guerra cibernética.

Desse modo, recomendo que este tema seja permanentemente revisto e, até mesmo, ampliado, por meio do detalhamento de suas partes, sugerindo que seja aplicado a futuros estudos desta Escola, ou, mesmo, como tema de outros trabalhos de conclusão de curso.

REFERÊNCIAS

BANKS, William. The role of counterterrorism law in shaping ad bellum norms for cyber warfare. **International Law Studies**, EUA, v. 89, p. 157-197, 2013. Disponível em: <https://www.usnwc.edu/getattachment/50b19368-bbba-4cd8-980b-bd81d1c67245/Banks.aspx>. Acesso em 27 abr. 2015.

BOLENG, Jeff; SCHWEITZER, Dennis; GIBSON, David S. **Developing Cyber Warriors**. EUA: U.S. Air Force Academy, 2008. Disponível em: <http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/boleng2008a.pdf>. Acesso em: 15 mar. 2015.

BRASIL. Ministério da Defesa. Estado-Maior Cionjunto das Forças Armadas. **Doutrina militar de defesa cibernética**. 1. ed. Brasília, 2014. MD31-M-07.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. Chefia de Preparo e Emprego. **Manual de emprego do direito internacional dos conflitos armados (DICA) nas Forças Armadas**. 1. ed. Brasília, 2011. MD34-M-03.

CLAYTON, Mark. Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant? **CS Monitor**, EUA, 21 Sept. 2010. Disponível em: <http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant>. Acesso em: 6 maio 2015.

CROWLEY, Michael; GERSTEIN, Josh. **No rules of cyber war**: U.S. in uncharted waters with ‘proportionate response’ on hack attacks. EUA, 23 Dec. 2014. Disponível em: <http://www.politico.com/story/2014/12/no-rules-of-cyber-war-113785.html#ixzz3Mpg0I9pq>. Acesso em: 14 maio 2015.

CYBER warfare: the modern cold war. **Journal of Law and Cyber Warfare**, EUA, 16 Dec. 2013. Disponível em: <<http://www.jlcw.org/cyber-warfare-modern-cold-war/>. Acesso em: 14 maio 2015.

DAVIS, Paul K. **Deterrence, influence, cyber attack, and cyberwar**. EUA: RAND National Security Research Division, June. 2014. 26 p. Disponível em: <http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1049/RAND_WR1049.pdf>. Acesso em: 27 abr. 2015.

DICKEY, Christopher; SCHNEIDERMAN, R. M.; DEHGHANPISHEH, Babak. The covert war against Iran's nuclear program. **Newsweek**, EUA, 13 Dec. 2010. Disponível em: <http://www.newsweek.com/covert-war-against-irans-nuclear-program-69083>. Acesso em: 6 maio 2015.

ESCOLA SUPERIOR DE GUERRA (Brasil). **Manual para elaboração do Trabalho de Conclusão de Curso:** monografia. Rio de Janeiro, 2015.

ESTADOS UNIDOS DA AMÉRICA. Department of the Army. **FM 3-38**: Cyber electromagnetic activities. 2014.

GERVAIS, Michael. Cyber attacks and the laws of war. **Berkeley Journal of International Law**, EUA, v. 30, n. 2, p. 525-579, 2012. Disponível em: <http://scholarship.law.berkeley.edu/bjil/vol30/iss2/6>. Acesso em: 10 maio 2015.

GILL Terry D.; DUCHEINE, Paul A. L. Anticipatory self-defense in the cyber context. **International Law Studies**, EUA, v. 89, p. 438-471, 2013. Disponível em: <https://www.usnwc.edu/getattachment/f041ec70-19af-4df4-bf59-be73ec0fe493/Anticipatory-Self-Defense-in-the-Cyber-Context.aspx>. Acesso em 27 abr. 2015.

GLOBAL state of information security survey: 2015 results by industry. *PWC*. EUA, 2014. Disponível em: <http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#>. Acesso em: 15 maio 2015.

GRAHAM, David E. Cyber threats and the law of war. **Journal of National Security Law & Policy**, EUA, v. 4, p. 87-102, 2010. Disponível em: < http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf>. Acesso em: 29 abr. 2015

INTERNATIONAL COMMITTEE OF THE RED CROSS. **What limits does the law of war impose on cyber attacks?** Genebra, 28 June 2013. Disponível em: <https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm>. Acesso em: 14 maio 2015.

JARDIM, Tarciso Dal Maso. **O Brasil e o direito internacional dos conflitos armados**. t. 1. Porto Alegre: Sergio Antonio Fabris Editor, 2006.

JASTRAM, Kate; QUINTIN, Anne. The internet in bello: cyber war law, ethics & policy. In: CYBERWARFARE SEMINAR, 2011, Berkeley. **Proceedings**… Berkeley, 2011. Disponível em: < https://www.law.berkeley.edu/files/cyberwarfare_seminar--summary_032612.pdf>. Acesso em: 5 abr. 2015.

KOSTADINOV, Dimitar. **Jus in cyber bello:** how the law of armed conflict regulates cyber attacks. EUA, 10 Apr. 2014. Disponível em: <http://resources.infosecinstitute.com/jus-cyber-bello-law-armed-conflict-regulates-cyber-attacks-part/>. Acesso em: 7 maio 2015.

KRAMER, Franklin D. Cyberpower and National Security: policy recommendations for a strategic framework. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. **Cyberpower and National Security**. 1. ed. Dulles, EUA: National Defense University Press and Potomac Books, 2009. cap. 1, p. 3-23.

KUEHL, Daniel T. From cyberspace to cyber power: defining the problem. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. **Cyberpower and National Security**. 1. ed. Dulles, EUA: National Defense University Press and Potomac Books, 2009. cap. 2, p. 24-42.

KUSHNER, David. **The real story of stuxnet**: how Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program. EUA, 26 Feb. 2013. Disponível em: <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>. Acesso em: 7 maio 2015.

LEWIS, James A. **Cyber attacks, real or imagined, and cyber war**. Washington, EUA: Center for Strategic and International Studies, 11 July, 2011. Disponível em: <http://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war>. Acesso em: 7 maio 2015.

LEWIS, A. James. **The korean cyber attacks and their implications for cyber conflict**. Washington, EUA: Center for Strategic and International Studies, 2009. Disponível em: <http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf>. Acesso em: 29 maio 2015.

LIBICKI, Martin C. Military cyberpower. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. **Cyberpower and National Security**. 1. ed. Dulles, EUA: National Defense University Press and Potomac Books, 2009. cap. 11, p. 275-284.

MELZER, N. **Cyberwarfare and international law**. Genebra, Suiça: United Nations Institute for Disarmament Research, 2011. Disponível em: <http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>. Acesso em: 8 maio 2015.

NAÇÕES UNIDAS. **Carta das Nações Unidas**. São Francisco, EUA, 1945.

NGUYEN, Reese. Navigating jus ad bellum in the age of cyber warfare. **California Law Review**, v. 101, n. 4, p. 1079-1129, 2013. Disponível em: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4210&context=californialawreview>. Acesso em: 10 mar. 2015.

NUNES, Luiz Artur Rodrigues. **Guerra cibernética:** está a MB preparada para enfrentá-la? 2010. 108 f. Monografia (Curso de Política e Estratégia Marítimas) - Escola de Guerra Naval, Rio de Janeiro, 2010.

PADMANABHAN, Vijay M. Cyber warriors and the jus in bello. **International Law Studies**, EUA, v. 89, p. 288-308, 2013. Disponível em: < https://www.usnwc.edu/getattachment/c5edcbe9-991e-4a28-a4d8-2e1eafd972bf/Cyber-Warriors-in-the-Jus-in-Bello.aspx>. Acesso em 27 abr. 2015.

PARKS, Raymon C.; DUGGAN, David P. Principles of cyber-warfare. In: **Proceedings of the IEEE Workshop on Information Assurance**, West Point, NY-EUA, p 122 – 125, 2001. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.1478&rep=rep1&type=pdf>. Acesso em: 15 mar. 2015.

PICTET, Jean et al. **Commentary on the additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949**. Genebra, Suíça: Martinus Nijhoff Publishers. 1987. 1625 p.

RATTRAY, Gregory J. An environmental approach to understanding cyberpower. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. **Cyberpower and National Security**. 1. ed. Dulles, EUA: National Defense University Press and Potomac Books, 2009. cap. 10, p. 253-274.

ROWE, Neil C. Cyber perfidy. In: EVANS, N. **Routledge handbook of war and ethics**. EUA: US Naval Postgraduate School, 2013, cap. 29. Disponível em: <http://faculty.nps.edu/ncrowe/cyberperfidy.htm>. Acesso em: 13 maio 2015.

SANGER, David E. Obama order sped up wave of cyberattacks against Iran. **New York Times**, EUA, 1 June 2012. Disponível em: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&>. Acesso em 6 maio 2015.

SHACKELFORD, Scott J. From nuclear war to net war: analogizing cyber attacks in international law. **Berkeley Journal of International Law**. v. 27, n. 1, p. 192-251, 2009. Disponível em: <http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7>. Acesso em: 15 abr. 2015.

SCHMITT, Michael N (Ed.). **Tallinn manual on the international law applicable to cyber warfare**. Cambridge, Reino Unido: Cambridge University Press, 2013. 282 p.

SCHMITT, Michael N. Wired warfare: computer network attack and jus in bello. **International Review of the Red Cross**, Suíça, v. 84, n. 846, p. 365-399, June, 2012. Disponível em: <https://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf>. Acesso em: 7 maio 2015.

SWINARSKI, Christophe. As Convenções de Genebra como sistema de proteção internacional da pessoa humana. In: TRINDADE, Augusto C. et al. **Direito internacional humanitário**. Brasília: Instituto de Pesquisa de Relações Internacionais, 1989. p. 53-74.

WATTS, Sean. Combatant status and computer network attack. **Virginia Journal of International Law**, EUA, v. 50, n. 2, p. 392-447, 2010. Disponível em: <http://ssrn.com/abstract=1460680>. Acesso em: 27 abr. 2015.

WAXMAN, Matthew C. Cyber-attacks and the use of force: back to the future of article 2(4). **The Yale Journal of International Law**, New Haven, EUA, v. 36, p. 421-459, 2011. Disponível em: <http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf>. Acesso em: 10 abr. 2015.

WINGFIELD, Thomas C. International law and information operations. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. **Cyberpower and national security**. 1. ed. Dulles, EUA: National Defense University Press and Potomac Books, 2009. cap. 22, p. 525-542

GLOSSÁRIO

ATIVISMO CIBERNÉTICO: Conhecido também por seu nome em inglês – hacktivism, é entendido como a manipulação da informação digital a fim de promover uma mudança política ou social. Os atos de ativismo cibernético buscam resultados similares aos obtidos pelo ativismo regular ou atos de desobediência civil, por meio de ataques de negação de serviço ou protestos efetuados via alteração de sítios da Internet.

FORENSE COMPUTACIONAL: É o emprego de técnicas e de procedimentos para aquisição, preservação, identificação, extração, restauração, análise e documentação de provas computacionais armazenadas em mídias eletrônicas, a fim de atender demandas administrativas, jurídicas ou judiciais.

INFRAESTRUTURA CRÍTICA - instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

MALWARE: Termo proveniente da fusão das palavras “malicious software”, é também conhecido por código malicioso e consiste de um software – programa de computador – destinado a se infiltrar em um sistema de TI alheio, de forma não consentida, com o intuito de assumir seu controle, causar algum dano ou subtrair informações. Os vírus de computador, worms, cavalos de Tróia – trojan horses – e spywares são exemplos de malware.

NEGAÇÃO DE SERVIÇO (Denial of Service – DoS): Um ataque de negação de serviço busca paralisar o acesso aos serviços de TI saturando-os com um alto volume de requisições. O sucesso dessa prática está no volume de requisições, e não na sua natureza, de forma que é muito difícil preveni-lo.