CICAD.I.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

APLICABILIDADE DE REGRAS DE ENGAJAMENTO À GUERRA CIBERNÉTICA À LUZ DO DIREITO INTERNACIONAL DOS CONFLITOS ARMADOS

Ronald Felipe de Paula Santana
Pós-Graduado em Oficial de Comunicações

RESUMO: A Guerra Cibernética é um tema extremamente atual. Isso porque ainda que não caracterizado por uma guerra propriamente dita, observamos incidentes cibernéticos ocorrendo diariamente. No entanto, ainda não está muito claro quais legislações internacionais podem regular o meio ou o método de se fazer determinado ataque, levando em conta que o caminho usado para invadir um computador e roubar uma senha de banco é o mesmo usado para atacar uma rede de distribuição de energia e parar toda uma nação. A fim de determinar como preencher essa lacuna e verificar a viabilidade de se adotar regras de engajamento, foi realizada uma pesquisa aplicada, qualitativa e exploratória, baseada em uma pesquisa bibliográfica minuciosa com o intuito de subsidiar uma resposta à hipótese levantada. Fica claro o entendimento unânime acerca da aplicabilidade do Direito Internacional dos Conflitos Armados à Guerra Cibernética e completo alinhamento do Brasil e da doutrina de emprego do Exército Brasileiro com esse conjunto de normas. O país pode demonstrar seu comprometimento com a legislação internacional humanitária vigente reafirmando sua liderança regional. Isso poderá ser feito por meio da adoção de regras de engajamento.

Palavras-chave: Direito Internacional dos Conflitos Armados. Direito Internacional Humanitário. Guerra Cibernética. Regras de Engajamento.

INTRODUÇÃO

O Exército Brasileiro(EB) encontra-se em um processo de evolução, buscando o constante aperfeiçoamento de sua doutrina para uma Força Terrestre mais eficiente. Assim, pesquisas científicas na área de Operações Militares são importantes, considerando que trarão subsídios para alcançar o nível de prontidão e operacionalidade buscado.

O Direito Internacional dos Conflitos Armados (DICA) surgiu formalmente em 1864 com as Convenções de Genebra. Já o conceito de Guerra Cibernética é algo mais recente e no âmbito do Exército tem avançado exponencialmente desde 2008. Considerando que o Brasil é signatário das Convenções de Genebra e de seus protocolos adicionais, bem como outros tratados do DICA, é conveniente que se estude a possibilidade de se propor regras de engajamento para as ações de guerra cibernética.

Sendo assim, é viável que se aplique regras de engajamento à guerra cibernética considerando a legislação vigente no DICA e a doutrina de emprego do Exército Brasileiro para as operações de guerra cibernética? Será trabalhada a hipótese de que é viável que se aplique regras de engajamento que limitem os meios e métodos a serem empregados na guerra cibernética.

O objetivo geral desta pesquisa é verificar a viabilidade da aplicação de regras de engajamento à guerra cibernética no âmbito do EB, levando em consideração o Protocolo I adicional às Convenções de Genebra. Os objetivos específicos serão os seguintes: analisar a doutrina de guerra cibernética do Exército com a finalidade de determinar se é viável que se aplique regras de engajamento em consonância com o DICA; identificar a legislação humanitária internacional vigente que possa limitar as ações de guerra cibernética.

Também é importante que se apresente os principais conceitos que nortearam este trabalho. Sobre guerra cibernética, tem-se o seguinte:

> corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las. (BRASIL, 2017).

Em se tratando de DICA, o conceito é o que segue:

> na atualidade, o DICA representa um conjunto de normas de proteção dos indivíduos e bens nos conflitos armados, além de disciplinar o comportamento dos Estados em tais conflitos, no tocante aos métodos e aos meios permitidos pelo Direito na condução das hostilidades. (BRASIL, 2011).

Este estudo é de fundamental importância, uma vez que adotar regras de engajamento poderia dar uma maior expressividade internacional ao Exército Brasileiro e ao Brasil, além de se vislumbrar um entendimento mundial acerca deste tema tão atual.

1 METODOLOGIA

Levando em consideração o problema apresentado, com o viés de atingir o objetivo que foi proposto, desde o mês de março de 2018, quando iniciada as pesquisas, foi feita uma abordagem qualitativa, estudando particularidades do tema abordado, buscando tendências, pensamentos ou opiniões acerca do tema, realizando observações.

A pesquisa foi de natureza aplicada, uma vez que não se buscou criar um conhecimento novo, mas sim, o estudo de pesquisas já existentes, que pudessem resultar em algo mais palpável, de fácil manipulação por parte de outros pesquisadores em uma oportunidade futura.

Desde seu início, essa pesquisa se caracterizou como exploratória quanto ao seu objetivo, uma vez que se iniciou com um minucioso levantamento bibliográfico com a finalidade de aperfeiçoar ideias já existentes sobre o assunto.

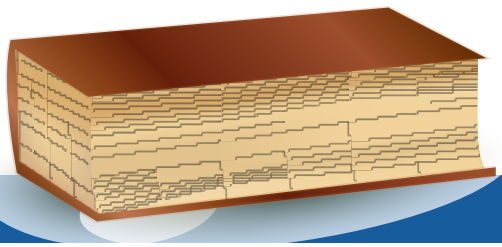
Isso conduziu este trabalho a uma pesquisa bibliográfica e após leitura analítica da literatura selecionada e fichamento das informações mais relevantes e pertinentes, chegar a conclusão desejada ao fim do mês de maio.

Foram feitas algumas visitas ao Comando de Defesa Cibernética, na segunda e terceira semanas de abril, com o intuito de coletar dados mais minuciosos. Diversos materiais foram disponibilizados, no entanto, alguns se revestem de um certo sigilo, considerando que, ainda, estão em fase de estudo doutrinário para posterior emprego pela Força Terrestre ou, até mesmo, pelas demais Forças Armadas. Isso limitou, de certa forma, a pesquisa, inviabilizando o emprego de outros instrumentos como entrevistas ou questionários.

Há uma vasta literatura que fala isoladamente sobre regra de engajamento ou guerra cibernética ou Direito Internacional dos Conflitos Armados. Entretanto, pouco foi encontrado ligando a guerra cibernética e o DICA e nada foi encontrado ligando essas três palavras-chave, que norteiam essa pesquisa.

Sendo assim, o artigo faz exatamente essa ligação, analisando o que motivou o Exército a voltar suas vistas para o setor cibernético, a doutrina de emprego decorrente disso e a interação com a legislação internacional humanitária.

Explorou-se a importância do DICA e do nosso país em respeitar essas normas, bem como qual a relação existente entre o DICA e a guerra cibernética que nos permitisse de alguma forma adotar regras de engajamento, considerando legislações que pudessem limitar os métodos e meios pelos quais nosso país poderia levar a cabo um ataque cibernético e assim, confirmar a hipótese apresentada.



2 RESULTADOS E DISCUSSÕES

2.1 O SETOR CIBERNÉTICO E O EXÉRCITO BRASILEIRO

O setor cibernético vem crescendo exponencialmente, sobretudo neste início de século. O governo brasileiro, atento às novas demandas tecnológicas, elaborou a Estratégia Nacional de Defesa(END). Este documento determina que os setores estratégicos espacial, nuclear e cibernético são essenciais para a defesa nacional e devem ser fortalecidos (BRASIL, 2008).

Em 2009, diretriz do Ministério da Defesa(MD) determinou que o setor cibernético ficaria sob coordenação do Exército e ainda destacou o fato de não haver qualquer tipo de tratado e controle internacional acerca deste setor (BRASIL, 2009).

Seguindo essa determinação, em 2010, foi criado o Centro de Defesa Cibernética(CDCiber), para fazer a coordenação e integração dos esforços da defesa cibernética. Posteriormente, foi criado o Comando de Defesa Cibernética (Com D Ciber), sendo um Comando Operacional Conjunto que dentre outras, possui a missão de planejar, orientar e controlar as atividades doutrinárias no âmbito do Sistema de Defesa Cibernética.

Reafirmando a importância do setor para o Exército, O Livro Branco de Defesa Nacional destacou que uma das capacidades consideradas prioritárias para consolidação da Força é a atuação no espaço cibernético com liberdade de ação (BRASIL, 2012).

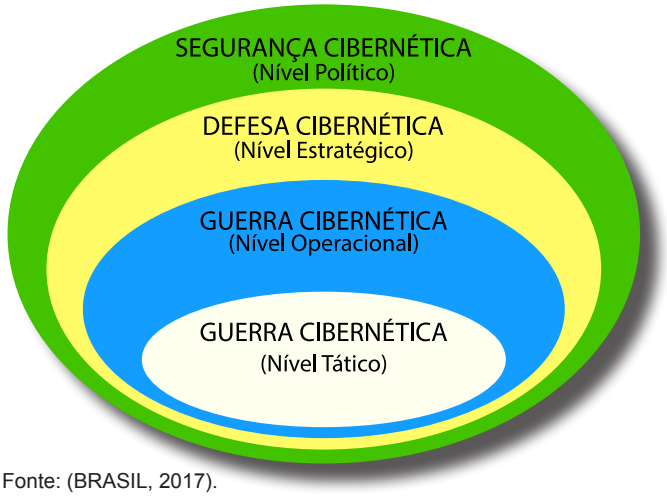
2.2 A GUERRA CIBERNÉTICA: PRINCIPAIS CONCEITOS E ASPECTOS DOUTRINÁRIOS

Já foi exposto sinteticamente o principal conceito de guerra cibernética, aquele encontrado no Manual EB70-MC-10.232: Guerra Cibernética, que hoje é utilizado pelo Exército. No entanto, Nunes (2015) dá uma maior amplitude a este conceito:

> 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 apud NUNES, 2015).

Segundo o MD, as ações no espaço cibernético não se encerram no EB, uma vez que se dividem de acordo com os níveis de decisão. A guerra cibernética se insere nos níveis operacionais e táticos, e é no nível tático que se insere a Força Terrestre, como vemos na figura abaixo:

FIGURA 1 Níveis de decisão



Fonte: (BRASIL, 2017).

No nível tático, o Sistema de Guerra Cibernética do Exército(SGCEx) precisa ter determinadas capacidades operativas que são a proteção cibernética, a exploração cibernética e o ataque cibernético, sendo este último, o que mais interessa ao escopo deste trabalho e tem a seguinte definição:

> Já o **Ataque Cibernético** é mais agressivo e, por intermédio dele, o atacante conseguirá derrubar ou corromper total ou parcialmente redes de dados e sistemas do oponente, danificar equipamentos e dispositivos ou destruir bancos de dados e informações relevantes, podendo para isso, fazer ou não uso de técnicas de invasão. (GOMES et al., 2016, grifo do autor).

No entanto, este ataque cibernético não deve ser feito de maneira aleatória, ne-

cessita estudo prévio que determine uma Lista de Alvos Cibernéticos (LIA Ciber) e uma Lista Priorizada de Alvos Cibernéticos (LIPA Ciber) (BRASIL, 2017).

Ainda sobre esses possíveis alvos, tem-se o que segue:

> A estrutura de guerra Cibernética da FTC pode, também, realizar tarefas ofensivas para negar serviço ou prejudicar o funcionamento das infraestruturas críticas do oponente localizadas no interior de sua zona de ação. (BRASIL, 2017).

Há um aspecto importante a ser destacado, daquilo que consta em Brasil (2017), que diz que "O ataque cibernético deve ser consistente com o arcabouço legal e normativo vigente".

2.3 O DICA E A LIMITAÇÃO DOS MEIOS E MÉTODOS

Nem sempre foi possível resolver situações controversas entre estados de maneira amistosa, através do diálogo, recorrendo-se muitas vezes à combates sangrentos, em guerras que por vezes se estenderam por longos anos. No entanto, uma constante se observa até os dias de hoje: o sofrimento que a guerra trás para as partes envolvidas.

Foi pensando nisso que em 1864 as Convenções de Genebra foram assinadas inicialmente por 16 países, inspirada nas propostas feitas por Henry Dunant em seu livro Memórias de Solferino, onde ele descreve as atrocidades da Batalha de Solferino e propõe normas que viriam a melhorar as condições das vítimas das Guerras.

Com o passar dos anos, mais países inclusive o Brasil, aderiram às convenções e seus protocolos adicionais e demais tratados correlacionados:

> O Estado Brasileiro possui significativa predisposição em acatar as normas do Direito Internacional. O País ratificou ou aderiu a aproximadamente cinqüenta tratados multilaterais relacionados à proteção de pessoas e bens e à proibição de armas de destruição em massa. (BRASIL, 2011).

Assim, o Brasil promulgou por meio de decreto os protocolos adicionais às Convenções de Genebra, e especial destaque damos aos artigos 35 e 36 do protocolo I:

> **Artigo 35** – Regras fundamentais
>
> 1. Em qualquer conflito armado, o direito de as Partes em conflito escolherem os métodos ou os meios de guerra não é ilimitado.
>
> 2. É proibido utilizar armas, projéteis e materiais, assim como métodos de guerra de natureza a causar danos supérfluos ou sofrimento desnecessário.
>
> 3. É proibido utilizar métodos ou meios de guerra concebidos para causar, ou que se possa presumir que irão causar, danos extensos, duradouros e graves ao meio ambiente natural.
>
> **Artigo 36** — Armas novas
>
> Durante o estudo, preparação ou aquisição de uma nova arma, de novos meios ou de um novo método de guerra, uma Alta Parte contratante tem a obrigação de determinar se sua utilização seria proibida, em algumas ou em todas as circunstâncias pelas disposições do presente Protocolo ou por qualquer outra regra de direito internacional aplicável a essa Alta Parte contratante. (BRASIL, 1993).

Ainda que não exista no DICA ou Direito Internacional Humanitário(DIH) legislação específica que limite a maneira de conduzir a Guerra Cibernética por meio de um ataque a determinado Estado, se observarmos os artigos citados, vemos que não podemos atacar alvos de maneira irrestrita, sem preocupação com danos colaterais a cidadãos ou até mesmo ao meio ambiente. E ainda temos a obrigação de estabelecer regras limitando ações no ato de desenvolver novos métodos, técnicas e armas.

2.4 PRINCIPAIS CASOS DE ATAQUES CIBERNÉTICOS

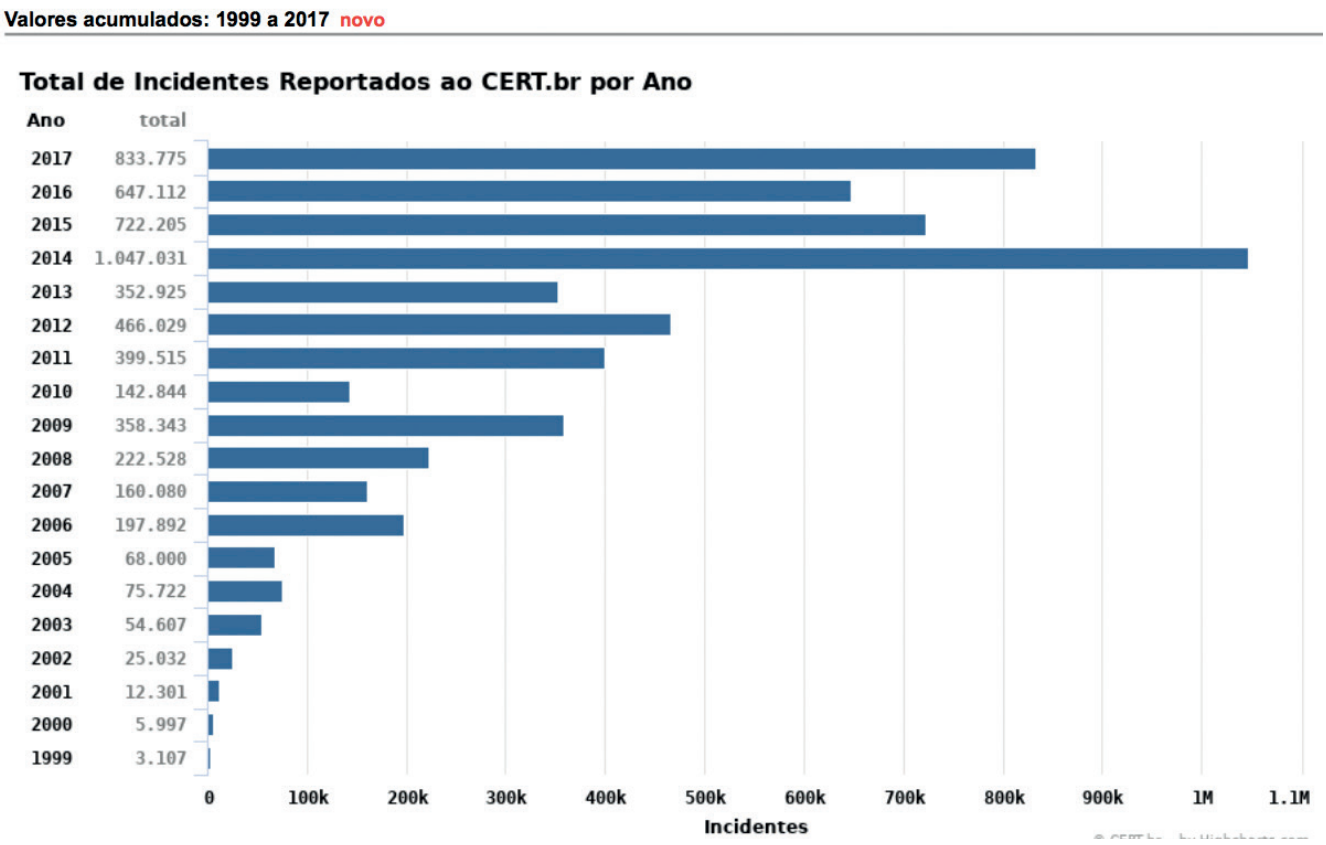
A atribuição de responsabilidade seja a Estados ou indivíduos fica dificultada pela ação de hackers que apesar de possuírem uma nacionalidade específica, não necessariamente atuam a mando de um País. Abaixo, no QUADRO 1, vemos uma síntese da evolução dos malwares, que caracterizam uma das formas de ataque por parte desses hackers:

QUADRO 1 Evolução histórica dos malware

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 efetio destrutivo. Destinava-se a recolher informações.
2012	FLAME - na verdade foi um precursor do stuxnet que passou despercebido, usado em ciberespionagem contra o iran.

Fonte: (KUSHNER, 2013 apud NUNES, 2015).

GRÁFICO 1 Incidentes por ano no Brasil



Fonte: CERT.br.

Ataques acontecem diariamente no espaço cibernético, muitas vezes sendo de menor gravidade e geralmente não se caracterizam como de um Estado contra outro. No gráfico acima vemos o número crescente de ataques ou incidentes ocorridos no Brasil des-

de 1999, o que corrobora a posição de destaque do país como um dos mais atingidos por ataques.

Quando fazemos esta comparação entre ataques ou incidentes, Nunes (2015), diz o seguinte:

> 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 (...).

É possível, ainda, observar na figura 2 um dos principais casos de ataques cibernéticos, através do malware Stuxnet, que "foi projetado para infectar sistemas industriais, no caso as centrífugas nucleares iranianas". (PONTE PINHEIRO, 2013).

Podemos ainda citar o ataque NotPetya, atribuído a Rússia e direcionado ao setor financeiro e energético da Ucrânia e que se estendeu por outros países da Europa, mostrando desrespeito com a soberania ucraniana.

Usinas nucleares, sistemas de controle de ferrovias, de tráfego aéreo, de fornecimento de energia são exemplos de infraestruturas críticas que se atacadas, podem causar sérios efeitos colaterais que vão além da vantagem militar, trazendo prejuízo para a população devido a seu impacto social, econômico e político. O Direito Internacional Humanitário é perfeitamente aplicável a este tipo de ação.

2.5 A APLICABILIDADE DO DIH PARA A GUERRA CIBERNÉTICA

Para Schimitt (2012), o espaço cibernético não é uma zona sem lei e os princípios da Lei Internacional são aplicáveis a esta área. Este mesmo autor foi o editor e o diretor da equipe que escreveu o Manual de Tallinn:

> O manual de Tallinn, que recebeu este nome em homenagem à capital da Estônia, local onde foi compilado, foi desenvolvido a pedido do Centro de Excelência em Defesa Cibernética Colaborativa da OTAN e aplica regras de comportamento de campos de batalha reais à internet. Seu objetivo é mostrar que uma guerra no mundo virtual pode se tornar real e, sendo assim, suas ações têm que ser submetidas às mesmas normas internacionais que regulam os combates nos campos de batalha. (GOMES et al., 2016).

O Comitê Internacional da Cruz Vermelha (CICV) acata com entusiasmo o que fala o Manual de Tallinn, além de nos remeter ao Protocolo I adicional às Convenções de Genebra:

> Avaliar a legalidade de novas armas é do interesse de todos os Estados, já que isso ajudará a assegurar que as suas forças armadas ajam em conformidade com suas obrigações internacionais. O artigo 36 do Protocolo I, de 1977, adicional às Convenções de Genebra exige que cada Estado-Parte se certifique que de que quaisquer novas armas que utilize ou considere utilizar cumpram com as regras de DIH, outro ponto proficuamente recordado pelo Manual de Tallinn. (INTERNATIONAL COMMITTEE OF THE RED CROSS, 2013, tradução nossa).

O Manual propõe 95 regras baseadas em leis internacionais consideradas aplicáveis no ato de disciplinar as ações de guerra cibernética. Ainda que tenha sido preparado a pedido da OTAN, não se trata de um tratado ou tampouco tem poder vinculativo, ou seja, nem mesmo os países membros da OTAN adotaram essas proposições como regras de engajamento ou atribuíram-na um valor legal, dando obrigatoriedade a seu cumprimento.

Ao falarmos de regras de engajamento, cabe ressaltar seu significado, uma vez que por meio dessas regras temos a possibilidade de limitar as ações de guerra cibernética:

> Caracteriza-se por série de instruções pré-definidas que orientam o emprego das unidades que se encontram na zona de operações, consentindo ou limitando determinados tipos de comportamento, em particular o uso da força, a fim de permitir atingir os objetivos políticos e militares estabelecidos pelas autoridades

> responsáveis. Dizem respeito a preparação e à forma de condução tática dos combates e engajamentos, descrevendo ações individuais e coletivas, incluindo as ações defensivas e de pronta resposta. (BRASIL, 2018).

Schimitt (2013) cita ainda no manual, qual o entendimento que os Estados Unidos têm acerca da aplicabilidade do DICA à guerra cibernética:

> O desenvolvimento de normas para a conduta do Estado no ciberespaço não requer uma reinvenção do direito internacional consuetudinário, nem torna obsoletas as normas internacionais existentes. As normas internacionais de longa data que orientam o comportamento do estado – em tempos de paz e conflito – também se aplicam no ciberespaço. (WHITE HOUSE CYBER STRATEGY, apud SCHIMITT, 2013, tradução nossa).

É pertinente ressaltar que dentro das estruturas criadas a partir da Estratégia Nacional de Defesa e diretrizes decorrentes, o Comando de Defesa Cibernética é a organização que tem a possibilidade de realizar estudos a fim de se estabelecer Regras de Engajamento para Guerra Cibernética. De acordo com pesquisas realizadas, têm sido feito análises doutrinárias neste sentido.

CONCLUSÕES

Ficou claro nesta pesquisa a importância que o governo brasileiro tem dado às questões que envolvem o setor cibernético, sobretudo a partir de 2008 com a criação da Estratégia Nacional de Defesa e desde então vemos uma sequência de ações e medidas que proporcionaram avanços significativos nesta área.

Uma vez atribuído ao Exército Brasileiro a coordenação das atividades neste setor, surgiram algumas organizações militares e iniciou-se o desenvolvimento de uma doutrina que viabilizasse o emprego da Força Terrestre não só para o ataque cibernético, mas também para defesa cibernética, considerando que o EB se insere no nível tático.

Por vezes, menos danosos à população de uma maneira geral, vimos que é grande a quantidade de incidentes cibernéticos que ocorrem no Brasil. É extremamente positivo que pensemos em como nos defender de tais situações que em dado momento, pode vir a se caracterizar como um verdadeiro ataque cibernético contra nossa soberania, como alguns que citamos neste trabalho.

E quando pensamos em ataques, não consideramos somente aqueles feitos contra nós, mas também o ataque a infraestruturas críticas da força oponente. Contudo, esse ataque não acontece de maneira irrestrita, havendo a necessidade de se estabelecer previamente uma lista de alvos a serem atacados.

Esta lista deve considerar o alcance dos danos causados por estes ataques. Ataques a sistemas de controle de tráfego aéreo, a usinas hidrelétricas, sistemas de controle de usinas de nuclear ou de redes de distribuição de energia, podem em um primeiro momento parecerem como um alvo militarmente compensador. Mas não podemos considerar apenas o valor militar desses alvos pois podem afetar serviços básicos utilizados por não combatentes, afetando o controle de voos comerciais, fornecimento de energia para hospitais e escolas, água potável, circulação de transporte público, entre outros. Esses danos colaterais não são aceitáveis e devem ser evitados ao máximo.

Resta sabido também que os ataques devem levar em consideração o arcabouço legal vigente, e isso nos remete ao Protocolo I adicional às Convenções de Genebra que de maneira tácita afirma que devemos limitar os meios e métodos utilizados em combate e devemos ao criar uma arma, técnica ou método, limitar a forma de emprego. O Comitê Internacional da Cruz Vermelha corrobora esse entendimento.

Cabe destacar também a grande contribuição do Manual de Tallinn que juntando a experiência de especialistas, propôs regras que garantem a aplicabilidade do DICA à Guer-

ra Cibernética.

Vale lembrar que pouco mais de 200 anos atrás, foi o livro de Henry Dunant que apresentou proposições que dariam origem ao primeiro conjunto de normas não consuetudinárias, que tinham poder vinculativo para as nações que assinaram as Convenções de Genebra. O mesmo pode acontecer com o Manual de Tallinn, podendo ser usado como um marco inicial ou até mesmo como uma referência, tanto pela Organização das Nações Unidas(ONU) quanto pelos países membros da OTAN.

Ora, se considerarmos que o Brasil acata essas normas do Direito Internacional, o Exército deveria considerar também essas normas no sentido de limitar os meios e métodos para a Guerra Cibernética.

As hipóteses de emprego (HE) de nossas Forças Armadas são diversas, no entanto, considerando os compromissos firmados internacionalmente pelo Brasil e que a própria doutrina determina que o ataque cibernético deve ser consistente com o arcabouço legal vigente, considero viável que se estabeleça regras de engajamento que tenham uma aplicação geral, em qualquer HE, limitando os meios e métodos utilizados para realizar um possível ataque num contexto de uma Guerra Cibernética. Isso permitiria que na fase de planejamento só se levantasse a possibilidade de atacar alvos que nos trariam estritamente a vantagem militar, auxiliando o decisor na tomada da melhor linha de ação e proporcionando uma melhor consciência situacional.

Tais regras ainda não são empregadas de maneira ostensiva por outros países que possuem notório saber no setor cibernético. Isso fica claro quando vemos ataques acontecendo com uma certa frequência e sua autoria sendo atribuída a países como a Rússia e os Estados Unidos.

Desde 2009 o próprio MD reconheceu que não há qualquer tratado internacional acerca deste setor. Sendo assim, o estabelecimento destas regras de engajamento por parte de nossas Forças Armadas traria um grande avanço para a área das operações militares, potencializando nosso reconhecimento internacional, o comprometimento entre as Forças e possivelmente nos alçando à vanguarda no que concerne à cibernética e ao respeito ao Direito Internacional Humanitário, reafirmando inclusive nossa liderança regional.

É extremamente importante que se prossiga nos estudos relacionados a este tema e até mesmo que outros pesquisadores brasileiros proponham regras de engajamento coerentes com nossa doutrina de emprego de guerra cibernética.

APPLICABILITY OF RULES OF ENGAGEMENT TO CYBER WARFARE UNDER THE INTERNATIONAL LAW OF ARMED CONFLICTS

Abstract. Cyber warfare is an extremely topical subject. This is because even though not characterized by a war itself, we observe cyber incidents occurring daily. However, it is still not very clear which international laws can regulate the means or method of making a particular attack, taking into account that the mean used to invade a computer and steal a bank password is the same used to attack a power distribution network and stop a whole nation. In order to determine how to fill this gap and verify the feasibility of adopting rules of engagement, an applied, qualitative and exploratory research was carried out, based on a thorough bibliographical survey with the intention of subsidizing a response to hypothesis raised. It is clear unanimous understanding of the applicability of the international law of armed conflicts to the cyber war and complete alignment of Brazil and the doctrine of employment of the Brazilian Army with this set of standards. The country can demonstrate its commitment to the existing humanitarian international legislation and its regional leadership. This can be done by adopting rules of engagement.

Keywords: Cyber Warfare. International Law of Armed Conflicts. International Humanitarian Law. Rules of Engagement.

REFERÊNCIAS

BRASIL. Ministério da Defesa. Exército Brasileiro. **EB70-MC-10.232: Guerra Cibernética**. 1. ed. Brasília: Estado Maior do Exército, 2017. Disponível em: <http://bdex.eb.mil.br/jspui/handle/1/631> Acesso em: 14 fevereiro

2018.

_____. Ministério da Defesa. **MD34-M-03: Manual de Emprego do Direito Internacional dos Conflitos Armados(DICA) nas Forças Armadas**. 1. ed. Brasília: Estado Maior Conjunto das Forças Armadas, 2011. Disponível em: < http://bdex.eb.mil.br/jspui/handle/123456789/140> Acesso em: 14 fevereiro 2018.

_____. DECRETO Nº 849, DE 25 DE JUNHO DE 1993. **Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados**. Brasília: Presidência da República (Casa Civil). Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0849.htm> Acesso em: 13 março 2018.

_____. Ministério da Defesa. Exército Brasileiro. **EB20-MF-03.109 Glossário de Termos e Expressões para uso no Exército**. 5. ed. Brasília: Estado Maior do Exército, 2018.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, 2008.

_____. Presidência da República. **Livro Branco de Defesa Nacional**. Brasília, 2012.

_____. Diretriz Ministerial nº 14. **Integração e Coordenação dos Setores Estratégicos da Defesa**. Brasília: Ministério da Defesa, 2012. Disponível em: <http://www.defesa.gov.br/arquivos/File/legislacao/emcfa/portarias/0014_2009.pdf> Acesso em: 24 abril 2018.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTOS DE INCIDENTES DE SEGURANÇA NO BRASIL. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: <https://www.cert.br/stats/incidentes/> Acesso em: 02 maio 2018.

GOMES, Mauro Guedes Ferreira Mosqueira; CORDEIRO, Sandro Silva; PINHEIRO, Wallace Anacleto. **A Guerra Cibernética:** exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C2). Rio de Janeiro: RMCT Vol 33, n° 2, 2016. Disponível em: <http://rmct.ime.eb.br/arquivos/RMCT_3_tri_2016_web/RMCT_275.pdf> Acesso em: 17 abril 2018.

INTERNATIONAL COMMITTEE OF THE RED CROSS. **What limits the law of war impose on cyber attacks?** Genebra, 28 junho 2013. Disponível em: <https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm> Acesso em: 15 março 2018.

NUNES, Luiz Artur Rodrigues. **Guerra Cibernética e o Direito Internacional**: Aplicabilidade do Jus ad Bellum e o Jus in Bello. Rio de Janeiro: ESG, 2015. Disponível em: <http://www.esg.br/images/Monografias/2015/Nunes.pdf> Acesso em: 11 abril 2018.

PONTE PINHEIRO, Fábio. **A Cibernética como arma de Combate.** Rio de Janeiro: ESG, 2013. Disponível em: <http://200.143.206.219/images/Monografias/2013/PINHEIRO.pdf> Acesso em: 17 abril 2018.

SCHMITT, Michael. **Tallinn Manual on the International Law applicable to Cyber Warfare**. Cambridge. Reino Unido: Cambridge University Press, 2013.

_____. **International Law in Cyberspace:** The Koh Speech and Tallinn Manual Juxtaposed. Harvard, Estados Unidos: Harvard International Law Journal, 2012.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Possui especialização nas áreas de Operações de Paz e Operações Engenharia de Construção. Concluiu o curso Básico Paraquedista. Atualmente, exerce a função de Comandante de Companhia no 9º Batalhão de Engenharia de Construção e pode ser contatado pelo e-mail ronaldsantana88@hotmail.com.