# Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil

## Cyber war, threats to critical infrastructure and Brazil's cyber defense

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 103-131
DOI: 10.26792/RBED.v7n2.2020.75178
ISSN 2358-3932

**DANIELLE JACON AYRES PINTO**
**JÉSSICA MARIA GRASSI**

## INTRODUÇÃO

Nos conflitos contemporâneos os meios não-tradicionais de ataque têm evoluído constantemente, isso se deve a busca constante pelo distanciamento do soldado do *front* de batalha e da automação cada vez mais acentuada da guerra. Nessa perspectiva, o espaço cibernético vem nos últimos anos tornando-se cenário central da dinâmica securitária dos Estados tanto interna como externamente. Infraestruturas críticas, tanto as ligadas ao setor privado quanto as do setor público, passaram a ser alvo principal de uma nova maneira de violência, que apesar de não ser direta, causa danos efetivamente sérios a sociedade e aos Estados. A partir da relevância dessa temática nos dias atuais, um questionamento central que surge e motiva o desenvolvimento deste artigo é: de que forma esses novos moldes e dinâmicas ligadas aos recursos cibernéticos poderiam ser compreendidos diante de um potencial cenário de ciberguerra?

Para analisar tal questão, este estudo corrobora a maioria dos debates acadêmicos nessa seara que afirmam que uma verdadeira ciberguerra ainda não existiu. Apesar do uso do ciberespaço em conflitos, dos crescentes ataques cibernéticos e das preocupações futuras quanto ao seu desenvolvi-

1 **Danielle Jacon Ayres Pinto** — Coordenadora da Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina – UFSC. Pós-Doutora em Ciências Militares na Escola de Comando e Estado-Maior do Exército – ECEME, Doutora em Ciência Política, na linha de Política Internacional, pela UNICAMP. Vice-Presidente da ABED - gestão 2020-2022. Líder do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea - GEPPIC.
2 **Jéssica Maria Grassi** — Doutoranda em Relações Internacionais na Universidade Federal de Santa Catarina – UFSC e Bolsista da CAPES. Mestra em Integração Contemporânea da América Latina pela Universidade Federal da Integração Latino-Americana – UNILA. Pesquisadora do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea – GEPPIC.

mento, a materialização da guerra movida por esse recurso de poder digital ainda é uma nebulosa na realidade da política internacional.

No entanto, os atores estatais já pensam em estratégias específicas para lidar com esse fenômeno tanto numa dinâmica defensiva e resiliente, como ofensiva. Entre os fatores que poderiam permitir uma retaliação imediata e legítima a um ciberataque, levando a uma guerra cibernética, elenca-se a possibilidade concreta e precisa de identificação do ator agressor, a regulamentação dos comportamentos no ciberespaço dando ao Estados a capacidade de demarcar seus limites soberanos e a delimitação das ações legais e sanções possíveis ao transgressor para que possam assim responder com atos repressivos aos atores que venham lhe atacar intencionalmente e ferir sua soberania no espaço cibernético. Já na ordem defensiva e resiliente a proposta é aumentar a segurança efetiva de seus aparatos tecnológicos das infraestruturas críticas e planejar maneiras rápidas e eficazes de colocar a funcionar novamente as infraestruturas estratégicas atacadas de forma a não gerar pânico na sociedade e debilidades prolongadas no serviço afetado.

Frente a esse cenário, com a emergência dessas novas dinâmicas, ao observarmos o Brasil vemos que ele é um dos países que mais sofre ataques cibernéticos no mundo — e o que mais sofre ataques cibernéticos na América Latina. Essa realidade demonstra a importância de se investigar como o país vem inserindo a temática na sua política de defesa e como lida com as possibilidades estabelecidas nesse novo espaço de atuação e com as vulnerabilidades crescentes diante do aperfeiçoamento tecnológico, principalmente no sentido de estabelecer meios eficazes de segurança de suas infraestruturas críticas. Desse modo, este estudo pensa ser importante entender como o Brasil vem construindo sua ação na esfera da defesa cibernética e da segurança de suas infraestruturas críticas para entender suas pretensões estratégicas em relação a uma possível ciberguerra.

Portanto, o objetivo da pesquisa é discutir sobre os novos moldes de atuação estabelecidos diante de ações ofensivas e defensivas no ciberespaço de modo a compreender algumas dinâmicas envolvidas diante das potencialidades de cenários de ciberguerra. A partir disso, serão investigadas as ações que têm sido tomadas pelo Brasil no âmbito de seus documentos sobre defesa nacional para enfrentar essa nova ameaça.

Para isso, o artigo será articulado em três seções, que delimitam os objetivos específicos desta pesquisa. Em um primeiro momento serão discutidos aspectos introdutórios ao tema e delimitados os conceitos principais do âmbito da cibernética nas relações internacionais. Após, concentrar-se-á em analisar acerca da guerra cibernética, discutindo conceituações, o que poderia levar um ataque cibernético tornar-se uma ciberguerra e dificuldades de regulação de comportamentos no nível cibernético. Por fim, pre-

tende-se explorar como o Brasil vem trabalhando com as problemáticas levantadas pelo ciberespaço, com especial atenção no que diz respeito às suas infraestruturas críticas, analisando, para isso, seus principais documentos de segurança e defesa.

Utiliza-se aqui a técnica de pesquisa bibliográfica, consultando fontes secundárias como livros, artigos, teses e dissertações sobre o tema proposto, e fontes primárias, ao analisar documentos de segurança e defesa do Brasil. Além disso, caracteriza-se como uma pesquisa exploratória e qualitativa.

## O CIBERESPAÇO NO CONTEXTO DOS CONFLITOS CONTEMPORÂNEOS

A transformação contemporânea nas formas de se fazer as guerras envolve o distanciamento do embate direto em campo de batalha, utilizando-se, para isso, meios não tradicionais. É dentro deste contexto que surge o debate acerca da revolução dos assuntos militares (RAM), sendo o domínio do espaço cibernético compreendido como primordial nessa nova forma de conflito (Olson 2012; Teixeira Júnior, Vilar-Lopes, and Freitas 2017).

Nessa perspectiva, Olson (2012, 73) assevera que a guerra hodiernamente inclui ataques contra infraestruturas nacionais, como as econômicas, e recursos cibernéticos são considerados armas estratégicas para tais fins. Desse modo, enfatiza-se aqui o papel do ciberespaço nos conflitos contemporâneos. O ciberespaço, ou espaço cibernético, é definido pelo Pentágono como "o domínio global dentro do ambiente de informações que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computadores e processadores e controladores incorporados."[1] (Singer and Friedman 2014, 13, tradução nossa).

De modo simplificado, o espaço cibernético é a "rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores." (Fernandes 2012b, 12). Da mesma maneira, Singer e Friedman (2014, 13, tradução nossa) definem o ciberespaço como "o domínio das redes de computadores (e dos usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line"[2]. Os autores ainda acrescentam:

> O ciberespaço é, antes de tudo, um ambiente de informação. É composto de dados digitalizados que são criados, armazenados e, mais importante, compartilhados. Isso significa que não é apenas um lugar físico e, portanto, desafia a medição em qualquer tipo de dimensão física. Mas o ciberespaço não é puramente virtual. Ele com-

> preende os computadores que armazenam dados, além dos sistemas e infraestrutura que permitem que ele flua. Isso inclui a Internet de computadores em rede, intranets fechadas, tecnologias de celular, cabos de fibra ótica e comunicações baseadas em espaço. (Singer and Friedman 2014, 13–4, tradução nossa).[3]

No imaginário da sociedade há uma ideia de que ciberespaço e internet sejam a mesma coisa, todavia, essa ideia é errônea e quando se pensa em ciberguerra é muito importante entender essa diferença. Assim, como afirmam Lobato e Kenkel (2015, 25) "o ciberespaço e a internet não são sinônimos: o primeiro é um domínio operacional eletrônico / eletromagnético, o segundo é a rede central do domínio operacional baseada em computadores." O primeiro existe sem o segundo, mas o segundo só existe porque o primeiro existe. Assim, o ciberespaço e a sua possibilidade como cenário e recurso de guerra é algo muito mais alargado, já a internet é uma ferramenta que pode ser utilizada para um conflito, mas que ainda não teve sua efetiva dimensionalidade bélica determinada, ou mesmo, efetivamente consensualizada entre o meio acadêmico e militar.

Outro ponto relevante a se destacar é a errônea interpretação do ciberespaço como um "patrimônio global" uma vez que, da mesma forma que se divide as fronteiras físicas dos países, o ciberespaço também deve ser compreendido a partir da aplicação das noções de nacionalidade, soberania e propriedade (Singer and Friedman 2014).

Destaca-se que no mundo virtual algumas características são distintivas e trazem dificuldades no que diz respeito à segurança e à defesa, entre estas, apontam-se que os atores podem atuar anonimamente, o que dificulta o rastreamento dos ataques, a distância física não existe, as ameaças podem avançar rapidamente e ser, até mesmo, invisíveis, bem como uma ação ofensiva é relativamente mais barata, fazendo com que aquele que promova o ataque fique em uma posição mais favorecida do que o que precisa se defender (Araújo Jorge 2012; Lobato and Kenkel 2015).

Abaixo, no quadro 1, pode-se ver a síntese dos principais conceitos utilizados quando se trata do ciberespaço nas relações internacionais.

Quadro 1
Principais conceitos relacionados à cibernética
nas relações internacionais

| Termo | Autor | Definição |
|---|---|---|
| Cibernética | Ministério da Defesa (2015, 62) | "Termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais." |
| ***Cyberspace* / Ciberespaço / Espaço cibernético** | Fernandes (2012b, 12) | "[...] rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores." |
| | Singer e Friedman (2014, 13) | "[...] o domínio das redes de computadores (e dos usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line. [...] não é apenas um lugar físico [...] não é puramente virtual." |
| | Ministério da Defesa (2015, 106) | "Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas." |

*(Continua)*

*(Continuação)*

| Termo | Autor | Definição |
|---|---|---|
| ***Cyberpower* / Ciberpoder / Poder cibernético** | Nye Jr. (2011, 123) | "[...] um conjunto de recursos relacionados a criação, controle e comunicação da informação eletrônica e computacional — infraestrutura, redes, software e habilidades humanas. Isso inclui não apenas a Internet de computadores em rede, mas também Intranets, tecnologias móveis e comunicações espaciais."[4] |
| | Ministério da Defesa (2015, 211) | "Capacidade de utilizar o Espaço Cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder". |
| ***Software Power*** | Vilar-Lopes (2016, 98) | "[...] a capacidade político-estratégica de que dispõem Estados para intervir na política internacional ou externa de outro Estado via utilização de software." |
| ***Cyberdefense* / Ciberdefesa / Defesa cibernética** | Oliveira *et al.* (2017, 13). | "[...] ato de defender o sistema crítico das TICs [Tecnologias de Informação e Comunicação] de um Estado", além de englobar "as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país." |
| | Ministério da Defesa (2015, 85) | "Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente." |

*(Continua)*

*(Continuação)*

| Termo | Autor | Definição |
|---|---|---|
| ***Cybersecurity* / Cibersegurança / Segurança cibernética** | Oliveira *et al.* (2017, 14). | "[...] aborda questões políticas, gestão de riscos, melhores práticas de garantia e tecnologias usadas para proteger o ambiente cibernético de um país e suas organizações. De forma mais direta, a segurança cibernética trata de temas relacionados à segurança pública." |
| | Ministério da Defesa (2015, 249) | "Arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas." |
| ***Ciberthreats* / Ciberameaça / Ameaça cibernética** | Ministério da Defesa (2015, 27) | "Causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse." |
| ***Cyber-attack* / Ciberataque / Ataque cibernético** | Gandhi *et al.* (2011, 29) | "[...] qualquer ato de um *insider* ou *outsider* que compromete as expectativas de segurança de um indivíduo, organização ou nação."[5] |
| | Lobato e Kenkel (2015, 27) | "[...] uma ação humana que explora as vulnerabilidades da esfera virtual, conseguindo prejudicar os sistemas informacionais ou mesmo, à luz da dependência on-line da vida moderna, da vida diária material."[6] |
| | Ministério da Defesa (2015, 39) | "Ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais em dispositivos e redes computacionais e de comunicações do oponente." |
| ***Cyberhacktivism ou Cybervandalism* / Ciber-hacktivismo ou Cibervandalismo** | Cavelty (2010, 01) | "[...] envolve modificação virtual ou destruição de conteúdo, por exemplo, invadir websites ou desativar um servidor por sobrecarga de dados. [...] os efeitos de tais incidentes são limitados no tempo e relativamente inofensivos."[7] |
| ***Cyberterrorism* / Ciberterrorismo / Terrorismo cibernético** | Curran, Concannon e McKeever (2008, 01) | "[...] é um ataque premeditado e politicamente motivado contra informações, sistemas de computadores, programas de computador e dados que resultam em violência contra alvos não combatentes por parte de grupos subnacionais ou agentes clandestinos."[8] |

*(Continua)*

*(Continuação)*

| Termo | Autor | Definição |
|---|---|---|
| **Resiliência cibernética** | Ministério da Defesa (2015, 241) | "Capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa." |
| ***Cyberwar* / Ciberguerra / Guerra cibernética** | Ministério da Defesa (2015, 134) | "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. Compreende ações 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. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC." |

Fonte: quadro elaborado pelas autoras

No Quadro 1 é possível perceber a complexa lista de conceitos que permeiam a dimensão cibernética na área da defesa e como tais definições são elementos essenciais para compreender as estratégias dos Estados quando pensam essa nova seara como um meio para a existência da guerra. Assim, tomando como ponto de partida os diferentes conceitos apresentados, este estudo irá concentrar-se mais enfaticamente acerca da percepção de guerra cibernética, também denominada de ciberguerra, e sua aplicação nas relações internacionais.

Não há ainda um consenso entre os pesquisadores para a definição e caracterização de uma ciberguerra, existindo assim, diferentes definições com graus de abrangência e delimitações distintas para o termo. O termo tem sido frequentemente usado para descrever várias ações cibernéticas, indo desde uma campanha de cibervandalismo, ciberterrorismo e ataques cibernéticos no geral (Singer and Friedman 2014).

Mas compreender de forma mais efetiva possível esse termo, mais do que uma necessidade conceitual para erigir meios de proteção e controle no sistema internacional, é o caminho para entender com os atores internacionais o estão utilizando e perceber se o estão manipulando para que ele atenda aos seus interesses individuais.

Nesse sentido, a seção seguinte terá como objetivo discutir mais profundamente acerca do conceito e da utilização do termo guerra cibernética, assim como compreender as condições para que um ataque cibernético escale para a condição de guerra cibernética. Além disso, serão apresentadas algumas das dificuldades que imperam na regulação das ações e comportamentos internacionais no nível cibernético.

## CIBERGUERRA: ATAQUES CIBERNÉTICOS E AS AMEAÇAS ÀS INFRAESTRUTURAS CRÍTICAS

O termo ciberguerra, ou guerra cibernética, vem sendo utilizado para uma série de acontecimentos, inclusive sobrepondo-se aos termos já definidos na seção anterior, frequentemente usado para designar qualquer tipo de conflito no ciberespaço. Isso leva a uma abrangência de significados, divergências quanto a sua ocorrência e consequências e dificuldades ao lidar com as situações advindas do ciberespaço.

Frente a esse cenário, Cavelty (2010, 1, tradução nossa) aponta ser necessário uma categorização conceitual mais precisa, sendo esta "uma pré-condição indispensável para avaliar o perigo concreto e sua importância, alocar responsabilidades, implementar contramedidas preventivas e reativas e conduzir investigações criminais".[9]

Ressalta-se que, pela definição de Clausewitz (2010), a guerra segue alguns princípios: é um ato violento; tem um propósito fundamentalmente político; tem um meio sério e um fim sério; e não é apenas um ato isolado. Partindo dessa perspectiva, Rid (2013) afirma que não há ainda uma ofensa cibernética que atenda a todos esses três critérios.

> Até agora não há nenhum ato conhecido de "guerra" cibernética, quando a guerra é adequadamente definida. Isto, obviamente, não significa que não haja ofensas cibernéticas políticas. Mas todas as ofensas cibernéticas políticas conhecidas, criminosas ou não, não são crime comum nem guerra comum. Seu objetivo é subverter, espionar ou sabotar[10] (Rid 2013, 10, tradução nossa).

Deve-se levar em consideração que as novas formas de se fazer a guerra podem estar fugindo, em certa medida, dos termos postos por Clausewitz. Contudo, Singer e Friedman (2014) frisam que, independentemente do es-

paço — terra, mar, ar, ou ciberespaço —, a guerra tem essencialmente um objetivo e um modo político, o que a distingue do crime, e o elemento da violência está sempre presente.

Nye (2012, s. p.) distingue ciberataque como "uma ampla variedade de ações, que vão de simples tentativas para apagar dados até danos a websites, negação de serviço, espionagem e destruição". Enquanto a ciberguerra é designada pelo autor, de maneira ampla, como "uma ação hostil no ciberespaço cujos efeitos ampliam ou são equivalentes a uma enorme violência física."

Já Teixeira Júnior, Vilar-Lopes e Freitas (2017, 31), retratam a guerra cibernética, de maneira mais aberta, "como um estado de coisas em que o poder militar utiliza meios, estratégias e ferramentas no ciberespaço para alcançar seus objetivos". Os autores acrescentam que a guerra cibernética se caracteriza pela atuação beligerante no ambiente cibernético, buscando obter informações privilegiadas, desestabilizar ou destruir sistemas computadorizados do país alvo (Teixeira Júnior, Vilar-Lopes, and Freitas 2017).

A guerra cibernética estratégica é compreendida por Libicki (2009, 117, tradução nossa) como "uma campanha de ataques cibernéticos lançada por uma entidade contra um estado e sua sociedade, principalmente, mas não exclusivamente, com o objetivo de afetar o comportamento do estado-alvo"[11]. A ciberguerra também pode ser definida como "uma ação ou conjunto associado de ações com uso de computadores ou rede de computadores para levar a cabo uma guerra no ciberespaço, retirar de operação serviços de internet e/ou de uso normal da população (energia, água, etc.) ou propagar códigos maliciosos pela rede" (Wendt 2011, 16, 21) e, para além de ataques às infraestruturas críticas, também visa afetar a soberania da nação atacada.

Já Dipert (2010, 398, tradução nossa) pontua que "se os ataques entre entidades políticas forem suficientemente 'generalizados', poderemos então falar de uma guerra cibernética"[12]. Levando essas conceitualizações em consideração, é importante ressaltar que nem todo ataque cibernético tem origem militar ou faz parte de uma guerra cibernética (Cavelty 2010).

Nessa perspectiva, Cavelty (2010) distingue níveis de ataques cibernéticos, o que ele chama de *cyberladder* (escada cibernética), sendo que quanto mais acima da escada estiver maior será seu dano potencial (Figura 1).

No primeiro degrau da escada de Cavelty (2010, 1, tradução nossa) está o cibervandalismo, ou ciber-hacktivismo. Este se caracteriza pela ação de modificar ou destruir conteúdos, invadindo sites ou desativando servidores, por exemplo. No segundo degrau está o crime de internet e, no terceiro, a ciberespionagem, os quais já ocorrem de forma rotineira, indepen-

dentemente de conflitos, tendo como vítima principal o setor corporativo, embora as redes governamentais também sejam alvos dessas atividades (Cavelty 2010).

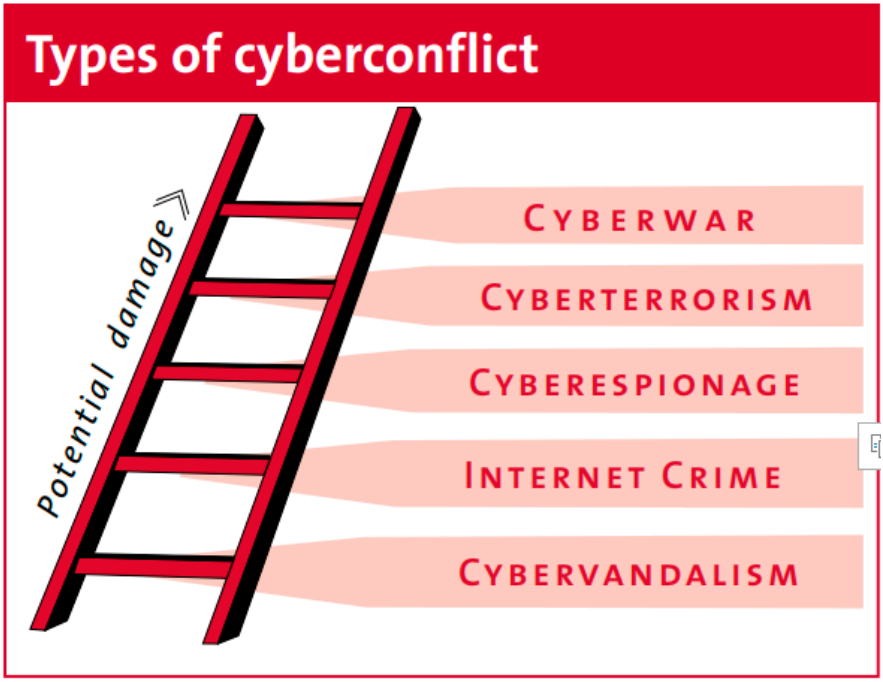


Figura 1 — Tipos de conflitos — escada cibernética *(Cyberladder)*.
Fonte: Cavelty (2010).

No quarto degrau está o ciberterrorismo que pode ser compreendido como "ataques ilegais de atores não estatais contra computadores, redes e as informações armazenadas nele, realizadas com o intuito de intimidar um governo (ou população) ou para obrigar determinado comportamento" (Cavelty 2010, 1, tradução nossa). Por fim, no último degrau da escada cibernética está a guerra cibernética. O termo, conforme Cavelty (2010, 2, tradução nossa), refere-se a uma guerra que ocorre no espaço virtual, envolvendo principalmente meios de tecnologia da informação, apesar de ponderar também que "cenários para uma guerra cibernética estratégica, ou seja, um conflito conduzido exclusivamente no mundo virtual, permanecem irrealistas neste momento".

Nas definições apresentadas podemos perceber um importante determinante da ideia de ciberguerra que é a falta de relação direta com o conceito tradicional de guerra, principalmente com o conceito clausewitziano. Essa não ligação nos faz constatar que a utilização do termo ciberguerra é feita com pouco cuidado conceitual e atende muito mais a interesses específicos dos atores do sistema, do que efetivamente a um complexo de características que definem uma guerra. Assim, a ciberguerra parece ser algo novo e que ainda está em construção, sendo possível até argumentar que tal fenômeno não existiu ainda, mas nem por isso deve-se desconsiderar as ameaças reais que os recursos cibernéticos produzem hodiernamente.

Apesar disso, deve-se considerar que um objetivo primordial na guerra cibernética deve ser possibilitar que as informações obtidas pelo meio cibernético possam trazer as possibilidades de ultrapassar esse domínio. Assim, para Silva (2014), nos domínios físicos e cognitivo da guerra pretende-se atacar as infraestruturas críticas de um país levando a paralisação ou a destruição de seus sistemas. A partir disso, o autor ressalta que, estrategicamente, a guerra cibernética teria como propósito atacar sistemas relacionados às infraestruturas nacionais de energia, ao sistema financeiro e à infraestrutura social, dificultando aos Estados manter sua capacidade de defesa e reação (Silva 2014).

Por outro lado, taticamente, teria como alvo os sistemas de comunicação, de controle e os de apoio à decisão, o que diminuiria a capacidade operacional e logística das Forças Armadas do país. Já operacionalmente, a ciberguerra teria como objetivo os sistemas de controle e a comunicação operacional, uma vez que, afetando ou destruindo estes, levaria ao comprometimento da capacidade de coordenação e manobra de um grupo das Forças Armadas. (Silva 2014).

Portanto, as guerras cibernéticas poderiam comprometer ou destruir infraestruturas críticas dos países, ameaçando os sistemas de segurança e colocando em risco a soberania, além de se caracterizar por avançar também em alvos civis. Todavia, é possível entender que mais do que um fim em si mesma a guerra cibernética poderia ser mais uma etapa da guerra tradicional, ou talvez mais um recurso de poder ao invés de um sistema de conflitualidade específico. Essa dinâmica é que, ainda hoje, provoca divergências sobre a existência ou não da possibilidade de uma ciberguerra.

Sobre as Infraestruturas Críticas Nacionais, o Artigo 2º da Portaria nº 2, de 8 de fevereiro de 2008, do Gabinete de Segurança Institucional da Presidência da República do Brasil, define Infraestruturas Críticas (IEC) como "as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional". Na referida portaria, em seu Artigo

3º, expõe-se que são consideradas áreas prioritárias de IEC: "I - Energia; II - Transporte; III - Água; IV - Telecomunicações; e V — Finanças." (Gabinete De Segurança Institucional 2008, s. p.).

Portanto, os alvos preferenciais dos ataques em uma ciberguerra seriam os programas de computador que controlam ou gerem os setores econômico-empresarial e/ou de serviços públicos (Fernandes 2012a), ou seja, as infraestruturas críticas, sendo estas:

> i) comando das redes de distribuição de energia elétrica; ii) comando das redes de distribuição de água potável; iii) comando das redes de gestão dos caminhos de ferro; iv) comando das redes de gestão do tráfego aéreo; v) comando das redes de informação de emergência; vi) comando das redes bancárias, possibilitando a inabilitação das contas, ou seja, apagando o dinheiro registado em nome dos cidadãos; vii) comando das redes de comunicações em geral e em particular (incluindo as redes de estações de rádio e de televisão); viii) comando dos links com sistemas de satélites artificiais (incluindo fornecedores de sistemas telefônicos, de sinais para tv, de previsões de tempo e de sistemas gps); ix) comando da rede do Ministério da Defesa (incluindo também outros ministérios-chave, como o do Interior e da Justiça, e o próprio Banco Central); x) comando dos sistemas de ordenamento e recuperação de dados nos sistemas judiciais, incluindo os de justiça eleitoral. (Fernandes 2012a, 58).

O *malware Stuxnet* é considerado um marco no que diz respeito ao nível alcançado pelos ataques cibernético, já que foi o primeiro que teve como alvo uma infraestrutura crítica de um Estado, no caso as instalações nucleares do Irã, também afetando outros países como Indonésia, Índia, Estados Unidos, Austrália, Inglaterra, Malásia e Paquistão. Dessa forma, este mudou a noção de vulnerabilidades no ciberespaço (Demchak and Dombrowski 2011; Silva 2014; Wendt 2011).

A utilização dessas ferramentas como armas cibernéticas para uso em infraestruturas críticas dos países, ou de modo a ameaçar a soberania dos Estados é uma preocupação no que diz respeito à evolução para uma guerra cibernética. O *Stuxnet* demonstrou que "armas cibernéticas" estão sendo desenvolvidas também para alvos civis, objetivando efeitos estratégicos (Olson 2012, 73). Porém, ainda não é possível entender o ataque feito com esse *malware* com uma guerra cibernética em si, talvez um ato de guerra, mas não como um novo modelo virtual e tecnológico da guerra. Ainda assim, não há informações suficientes para atestar que ataques cibernéticos tenham resultado em danos de grandes proporções contra infraestruturas estratégicas ou centros de comando e controle (Teixeira Júnior, Vilar-Lopes, and Freitas 2017). A partir do abordado, é importante compreen-

der as possibilidades e as dificuldades que ainda imperam na regulação de comportamentos no nível cibernético e nas sanções a serem aplicadas aos transgressores, pontos relevantes para se discutir acerca da evolução de ataques cibernéticos para uma ciberguerra.

Uma questão a ser discutida trata da legislação internacional no que diz respeito ao ciberespaço e a legalidade de atos repressivos. Diante das regras, normativas e regimes para a atuação internacional e para a qualificação da guerra há dificuldades para abranger a lógica da cibernética. Apesar de iniciativas individuais por parte dos Estados e institucionalmente, como no caso da OTAN, para tratar da problemática (Demchak and Dombrowski 2011; Lobato and Kenkel 2015), não existem resoluções ou acordos internacionais que regulamentem como lidar com as novas dinâmicas envolvidas no ciberespaço (Dipert 2010). Tal lacuna muitas vezes parece ser proposital, visto que essa nova seara de atuação bélica é bastante complexa e quanto mais aberta sua regulação for, mais os estados poderão utilizar-se desse meio para atingir seus objetivos no espaço interacional sem sofrer tal pressão em relação aos seus atos, e o *Stuxnet* é um bom exemplo dessa suposta liberdade.

Nesse sentido, a indefinição do conceito de guerra cibernética e a falta de bases legais para uma adequada atuação internacional na área também trazem dificuldades em termos de segurança jurídica, para os decisores políticos agirem adequadamente em caso de ciberataques ou em uma ciberguerra (Fernandes 2012a).

Para ilustrar a problemática da falta de uma legislação que regule o âmbito da guerra cibernética, Fernandes (2012a, 54) aponta alguns questionamentos, entre eles, como "saber se um determinado ciberataque poderá ser considerado um ato de guerra?", ou "se os seus protagonistas poderão, ou deverão, ser tratados de forma similar aos combatentes ou se as ciberarmas poderão ser legalmente equiparadas a armas físicas?". Portanto, é fundamental haver certas disposições em tratados internacionais que os Estados possam seguir, o estabelecimento de parâmetros de atuação no ciberespaço, definindo quais ações configuram ataques a soberania estatal e, assim, sustentar suas ações diante de um ato de ciberguerra (Fernandes 2012a). Sem tais regulações o uso indiscriminado e deturpado desse recurso tende a crescer a favorecer os Estados mais tecnológicos e desenvolvidos.

Contudo, uma questão essencial diz respeito à necessidade da identificação precisa do agressor, para poder fazer inferências seguras e, assim, efetuar a represália ao ator transgressor. No entanto, diante da estrutura do ciberespaço, é muito difícil identificar as fontes dos ataques cibernéticos. Isso é chamado de "problema de atribuição" e leva a negação de credibilidade aos ciberataques, especialmente porque os países podem alegar que,

apesar de originados em seus territórios, os ataques não foram perpetrados por seus governos (Dipert 2010, 385).

Ao abordar o tema, Olson (2012) avalia o fato de que grupos independentes podem ser controlados por uma grande potência, dificultando a atribuição de responsabilidade diante de ataques cibernéticos. Nesse sentido, o autor, alertando os Estados Unidos para esse cenário, propõe:

> O valor da utilização de "fantoches" na guerra cibernética é que eles complicam ainda mais a possibilidade de atribuir responsabilidade. Uma potência pode identificar e mapear vulnerabilidades e, em seguida, coordenar ataques usando intermediários. Mapeamentos passados de vulnerabilidades de rede e infraestrutura não foram tratados como um ato de guerra. Assim, contanto que a potência hostil utilize "fantoches", haverá poucas medidas diretas que os EUA poderão tomar, ainda que se conheça a fonte de informações que possibilita os ataques. (Olson 2012, 77).

Logo, o que no começo poderia ser um problema para o Estado — a dificuldade em identificar os perpetradores dos ataques — passa, após uma percepção estratégica de interesses, a ser talvez uma benesse para conquistar o que se deseja no sistema internacional sem ser punido por eventuais ilegalidades cometidas ao longo desse ato.

Outro ponto importante relacionado a questão da ciberguerra diz respeito à soberania dos países no ciberespaço. Como definir o espaço soberano de cada país de modo que este possa agir diante de um ataque cibernético justificando este ameaçar sua soberania? Diante das incertezas postas no espaço cibernético, as ameaças invisíveis, a facilidade do anonimato e a falta de regulação tem se justificado a necessidade de impor limites soberanos no mundo virtual (Demchak and Dombrowski 2011).

O estabelecimento de fronteiras cibernéticas possibilitaria aos Estados desenvolverem capacidades de controle soberano desse território de modo a melhorarem suas capacidades de cibersegurança e ciberdefesa. Desta forma, criaria condições dos Estados identificarem e, se fosse o caso, retaliarem agressores externos (Demchak and Dombrowski 2011). A interconectividade dos sistemas e a ausência de regulamentação no ciberespaço facilitam ataques que possam promover rupturas políticas e militares, principalmente devido ao potencial desse cenário de controlar objetos físicos e a dificuldade de rastreamento do agressor (Lobato and Kenkel 2015).

No entanto, essas questões de limites, controles e fronteiras geram uma série de críticas sobre as implicações destas como ferramentas de controle dos fluxos internos dos países e as possibilidades de uso autoritário por parte dos governos, estabelecendo limites mais rígidos na esfera ciberné-

tica, podendo levar a violações dos direitos e da liberdade dos cidadãos e demais agentes internos, ou mesmo modificar a noção do que é compreendido como um direito. Ademais, geram receios sobre as possibilidades de intervenção em territórios apontados como fontes de ataques cibernéticos, além das críticas acerca da utilização de uma lógica Westfaliana para tratar de questões de uma complexidade que talvez demandassem análises e soluções diferentes do que se está acostumado no sistema internacional atual (Ayres Pinto, Freitas, and Pagliari 2018).

Entretanto, segundo Demchak e Dombrowski (2011), há um consenso sobre a necessidade de regulamentação do ciberespaço, seja pelos Estados individualmente, seja por meio de regimes internacionais. Essas iniciativas estão tomando forma nas estratégicas norte-americana e chinesa e nas ações institucionais observadas, por exemplo, nas iniciativas no âmbito da OTAN (Demchak and Dombrowski 2011; Lobato and Kenkel 2015).

Tendo em vista todas as questões levantadas nesta seção, com as preocupações crescentes com relação a ataques às infraestruturas críticas e as possibilidades do desencadear de uma ciberguerra, Olson (2012) propõe que as vulnerabilidades persistentes e as ameaças de um ataque contínuo e coordenado levam a impossibilidade de defender completamente uma rede vasta - como as redes de abastecimentos de petróleo, as quais dependem de sistemas computacionais - contra um inimigo invisível. Desse modo, alerta que "o potencial prejuízo econômico de uma campanha cibernética coordenada por uma grande potência contra gargalos nos sistemas mundiais (ou nacionais) seria incalculável" (Olson 2012, 80). Mas a pergunta é: isso seria guerra? A reposta pode ser: diretamente não, mas poderia ser parte de um contexto maior de conflitualidade que chegaria ao tradicional enfretamento bélico.

Ainda hoje existe a preocupação de que um "filho do *Stuxnet*" possa estar sendo desenvolvido para atingir alguma infraestrutura crítica, ou estar flutuando por algum tempo, aparentemente inofensivo e despercebido até ser desencadeado em uma data específica ou em um tipo programa. Esse *malware* poderia parar milhões de computadores ao mesmo tempo, enviar comandos de destruição a outros, substituir dados, afetar redes de energia, água, transportes ou sistemas financeiros (Demchak and Dombrowski 2011), mas nada de real e concreto ainda foi vivenciado

Por fim, devido ao potencial destrutivo de uma possível guerra cibernética nos campos econômico, social e físico, Olson (2012) alerta para a necessidade de lhe conferir o grau de importância e preocupação, assim como incentivar estudos na área, do mesmo modo que é dado às armas nucleares. Porém, para isso, é essencial que novas conceituações de guerra,

baseadas na sociabilidade efetiva do século XXI trazida especialmente pela globalização, sejam elementos centrais desses novos conceitos.

Assim, tendo em vista a imprecisão do conceito de guerra cibernética, o aumento dos ataques no âmbito cibernético, as possibilidades de ataques escalarem para uma guerra cibernética, o potencial destrutivo de armas cibernéticas, bem como o aumento da dependência dos recursos de tecnologia da informação pelos Estados e pelas empresas, tem-se, por consequência, um aumento das vulnerabilidades dos Estados frente as ameaças cibernéticas.

Para entender essa dinâmica conceitual no contexto nacional, o tópico seguinte investigará brevemente como o Brasil vem inserindo e trabalhando com a temática do setor cibernético em suas políticas e estratégias de defesa.

## PREOCUPAÇÃO COM AS NOVAS AMEAÇAS: A DEFESA CIBERNÉTICA DO BRASIL E A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS

Como mencionado, os avanços tecnológicos, os novos meios e ameaças nos conflitos contemporâneos, fazem com que o ciberespaço se torne elemento essencial ao se pensar a política de defesa dos Estados. No contexto da América Latina, o Brasil é o país que mais sofreu ataques cibernéticos nos últimos anos e, por outro lado, é o terceiro país que mais faz ataques cibernéticos no mundo (Oliveira *et al.* 2017). Os ataques sofridos demonstram "tanto a fragilidade brasileira em defesa cibernética como sua força, pois em uma guerra a possibilidade de neutralizar o oponente é primordial" (Oliveira *et al.* 2017, 67).

Nessa perspectiva, com o aumento do número de ataques ao Brasil renova-se constantemente a preocupação acerca das medidas a serem tomadas no âmbito da ciberdefesa e da cibersegurança. Partindo disso, essa seção enfatizará as medidas que estão sendo adotadas pelo país, trabalhando principalmente com seus documentos de defesa e como esses entendem a ideia de ciberguerra.

O Livro Branco de Defesa do Brasil (LBDB) salienta que "a ameaça cibernética se tornou uma preocupação por colocar em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional" (Ministério da Defesa 2012b, 69).

Assim, o país inseriu o setor cibernético no tripé estratégico para a defesa nacional, juntamente com o aeroespacial e o nuclear, e, a partir disso, estaria estimulando o desenvolvimento de pesquisas e novas tecnologias, assim como a capacitação de recursos humanos, de modo a elevar seus mecanismos de defesa nacional e buscar a maximização da segurança de

infraestruturas e informações. Nesse sentido, para o projeto de defesa cibernética, o LBDB prevê a destinação de valor estimado de R$ 839,90 milhões até 2031 (Ministério da Defesa 2012b).

> A implantação do Setor Cibernético tem como propósito conferir: confidencialidade, disponibilidade, integridade e autenticidade dos dados que trafegam em suas redes, os quais são processados e armazenados. Esse projeto representa um esforço de longo prazo, que influenciará positivamente as áreas de ciência e tecnologia e operacional. Sob a coordenação do Exército, significativos avanços têm se concretizado na capacitação de pessoal especializado e no desenvolvimento de soluções de elevado nível tecnológico. (Ministério da Defesa 2012b, 69).

Desse modo, no que diz respeito ao setor cibernético, a Estratégia Nacional de Defesa (END) dispõe da necessidade de capacitação no amplo espectro de usos industriais, educativos e militares, incluindo como prioritária as tecnologias de comunicação entre todos os contingentes das Forças Armadas. Nesse sentido, aponta a necessidade de desenvolver o aparato tecnológico do país assim como a formação de recursos humanos, frisando sobre a importância de se estabelecer uma política de formação de cientistas para atuar na área cibernética - do mesmo modo na espacial e na nuclear - com a aproximação entre a produção científica e as atividades relativas ao desenvolvimento tecnológico da Base Industrial de Defesa (Ministério da Defesa 2012a).

Ressalta-se entre prioridades apontadas na END: fomentar a pesquisa científica e estruturar a produção de conhecimento na área, além de incrementar medidas de apoio tecnológico por meio de laboratórios específicos; desenvolver sistemas computacionais de alto desempenho e tecnologias que permitam o planejamento e a execução da Defesa Cibernética; fortalecer o Centro de Defesa Cibernética, para que possa evoluir para o Comando de Defesa Cibernética das Forças Armadas; aprimorar a Segurança da Informação e Comunicações (SIC), principalmente no que diz respeito à Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa); e desenvolver a capacitação para a proteção das infraestruturas estratégicas. Ademais, prevê a criação da Escola Nacional de Defesa Cibernética (Ministério da Defesa 2012a).

Dessa maneira, para contribuir com a Segurança Nacional no que se refere ao setor cibernético, a END prevê o desenvolvimento de medidas para a segurança das infraestruturas estratégicas (energia, transporte, água, finanças e comunicações), assim como o aperfeiçoamento dos dispositivos e procedimentos de segurança que possam reduzir a vulnerabilidade dos sistemas de Defesa Nacional. Também é previsto a intensificação de par-

cerias estratégicas com o entorno geográfico de modo a contribuir com a estabilidade regional (Ministério da Defesa 2012a).

Salientando sobre a proteção das infraestruturas estratégicas nacionais, o documento incentiva as seguintes ações para o desenvolvimento de soluções nacionais inovadoras:

> [...] sistema integrado de proteção de ambientes computacionais; simulador de defesa cibernética; ferramentas de conteúdo web; ferramentas de inteligência artificial; algoritmos criptográficos e autenticação próprios; sistema de chaves-públicas da Defesa; sistema de análise de artefatos maliciosos; ferramentas de análise de interesse para o setor cibernético (voz, vídeo, idioma e protocolos); sistema de certificação de Tecnologias da Informação; sistema de apoio à tomada de decisão; sistema de restabelecimento do negócio; sistemas de gestão de riscos; sistema de consciência situacional; computação de alto desempenho; rádio definido por software; e pesquisa científica por meio da Escola Nacional de Defesa Cibernética, de instituições acadêmicas no âmbito do Ministério da Defesa e demais instituições de ensino superior nacionais e internacionais. (Ministério da Defesa 2012a, 39).

Todavia, a END traz também em seu corpo, quando trabalha a ideia de flexibilidade, a compreensão que os meios digitais não irão substituir os meios tradicionais da guerra. Vejamos o texto: "[A END] [...] rejeita a tentação de ver na alta tecnologia, alternativa ao combate, assumindo-a como um reforço da capacidade operacional" (Ministério da Defesa 2012a, 75). Ou seja, apesar de reconhecer a importância de tais tecnologias, a coloca como um patamar abaixo dos meios tradicionais.

A Política de Defesa Cibernética (PDC), aprovada no final de 2012, visa coordenar e integrar as ações de defesa cibernética no âmbito do Ministério da Defesa nas áreas de inteligência, ciência e tecnologia, operacional, doutrina e recursos humanos. Assim, esta dispõe da criação do Sistema Militar de Defesa Cibernética (SMDC), na qual participam civis e militares da Marinha, do Exército e da Aeronáutica (Ministério da Defesa 2012c).

Já a Doutrina Militar de Defesa Cibernética (DMDC) aborda aspectos mais técnicos e operacionais de modo a coordenar as ações militares no âmbito da defesa cibernética (Oliveira *et al.* 2017). No que se refere à guerra cibernética, a DMDC define alguns processos gerais de coordenação, planejamento e conduções de operações de ciberguerra (Ministério da Defesa 2014).

No âmbito da segurança cibernética, ressalta-se a elaboração do Livro Verde de Segurança Cibernética (LVSC), o qual objetiva reunir propostas e

diretrizes básicas sobre a temática (Oliveira *et al.* 2017). Este livro destaca os desafios presentes no âmbito da segurança das infraestruturas críticas nacionais:

> Falta de clareza e de identificação das interdependências nas infraestruturas críticas e entre infraestruturas críticas, e seus respectivos graus de criticidade e impactos; Ausência de integração das várias políticas setoriais, iniciativas e investimentos de segurança das infraestruturas críticas; Movimentos tardios de definição de prioridades estratégicas da Nação e harmonização das estratégias, com foco na prevenção; Limitado leque das infraestruturas críticas nacionais já priorizadas; Crescentes riscos de ataques cibernéticos a Sistemas SCADA; Insuficiente número de equipes de resposta e tratamento de incidentes em rede computacionais nos vários segmentos da sociedade, bem como insuficiente número de especialistas com competência para desempenhar tais atividades. (Mandarino Júnior and Canongia 2010, 40–1).

Além disso, o LVSC aponta as diretrizes a serem contempladas na Política Nacional de Segurança Cibernética no que se refere às infraestruturas críticas nacionais. Entre as diretrizes, pode-se mencionar a iniciativa para a formulação da Política Nacional de Segurança das Infraestruturas Críticas e o mapeamento do grau de vulnerabilidade dos sistemas de informação e das infraestruturas críticas do país, de modo a definir os requisitos de segurança e desenvolver um sistema de monitoramento de ameaças cibernéticas (Mandarino Júnior and Canongia 2010).

Também abrange, entre suas diretrizes, a elaboração de uma metodologia para avaliações de risco, identificando o grau de interdependência dos serviços das infraestruturas críticas do país, de modo a desenvolver ou adaptar uma metodologia comum para avaliar as vulnerabilidades das infraestruturas críticas, dos seus sistemas e serviços e, assim, criar um sistema dinâmico que contemple medidas preventivas, proativas e reativas contra as ameaças e ataques cibernéticos. Por fim, prevê o desenvolvimento de um programa de capacitação dos gestores atuantes nas infraestruturas críticas, o qual contemplaria tópicos como "análise e gestão de riscos, segurança das infraestruturas críticas da informação, resiliência operacional e organizacional, monitoramento e resposta a ataques cibernéticos." (Mandarino Júnior and Canongia 2010, 47).

Em suma, apesar da necessidade de maior aporte financeiro para investimentos em pessoal, material e pesquisa, sendo que as vulnerabilidades ainda são marcantes no setor, devem-se destacar os avanços obtidos nos últimos anos (Lobato and Kenkel 2015; Silva 2014). Nesse sentido, obser-

va-se, antes de tudo, a prioridade dada ao setor cibernético considerado um dos três setores estratégicos nos documentos de defesa do país.

A partir disso avanços foram observados, como a implantação do Simulador Nacional de Operações Cibernéticas (Simoc), voltado ao treinamento de militares em combate cibernético, que oferece também simulações para a academia, buscando despertar o interesse de profissionais para a pesquisa e capacitação na área. Outro avanço foi a criação do Centro de Defesa Cibernética (CDCiber), em 2010, dentro do Exército, que atualmente compreende uma das estruturas do Comando de Defesa Cibernética das Forças Armadas (ComDCiber), que coordena o SMDC (Lobato and Kenkel 2015; Silva 2014).

Ademais, foi criada a Escola Nacional de Defesa Cibernética (ENaDCiber), inaugurada em fevereiro de 2019, a qual já funcionava como núcleo desde janeiro de 2015. A escola tem estrutura de ensino dual, civil e militar, e tem como missão "fomentar e disseminar as capacitações necessárias à Defesa Cibernética [...] bem como contribuir com as áreas de pesquisa, desenvolvimento, operação e gestão do assunto e para a melhoria da qualificação da mão de obra nacional para o setor" (Ministério da Defesa 2019, s. p.).

Por fim, quando olhamos para os documentos brasileiros que versam sobre sua defesa, em especial dos que tratam da área cibernética, é possível perceber que há um valioso esforço em construir elementos sólidos para o desenvolvimento das atividades das forças armadas nessa seara. Porém, os documentos não trazem efetivamente um entendimento específico e direto sobre guerra cibernética, dando ao Estado brasileiro maior flexibilidade de ação quando entenda necessário no mundo virtual.

## CONSIDERAÇÕES FINAIS

Este artigo pretendeu discutir alguns aspectos referentes aos ataques cibernético e à ciberguerra, bem como compreender as ações que estão sendo tomadas pelo Brasil nesse setor. Assim, distinguiu-se alguns dos principais conceitos discutidos ao abordar a cibernética nas relações internacionais, explorou-se fatores que poderiam levar um ataque cibernético desencadear uma ciberguerra e as dificuldades enfrentadas na regulamentação de ações e comportamentos no âmbito cibernético, bem como identificou-se os avanços obtidos pelo Brasil diante das novas ameaças e ataques advindos do ciberespaço.

Nesse sentido, ao debruçar-se em discutir as conceitualizações de guerra cibernética, buscou-se deixar claro como essa deve ser compreendida e diferenciada dos demais ataques cibernéticos. A partir disso, alguns pontos

devem ser observados. Uma guerra cibernética pode vir a ocorrer com a constatação de ataques cibernéticos coordenados, efetuados com propósitos políticos e militares, que venham a afetar as infraestruturas críticas, a população ou os organismos de defesa de uma nação, ou que visem atacar diretamente a soberania de um Estado. Esses ataques, para serem considerados atos de guerra cibernética, deveriam equivaler a um ato de violência contra o Estado atacado.

A ciberguerra deve ser compreendida no contexto da revolução dos assuntos militares, e especula-se como a guerra do futuro. Uma ameaça que se tornou uma das grandes preocupações das defesas nacionais devido as vulnerabilidades inerentes de todas as infraestruturas que dependem dos sistemas computacionais. Além disso, salienta-se a consideração do potencial de se efetuar ataques imprevisíveis, anônimos, até mesmo, invisíveis e, talvez, destrutíveis às infraestruturas críticas dos Estados por meio do ciberespaço, principalmente se usado como arma combinada, destacando-se a facilidade em coordenar ataques a longa distâncias com o domínio do poder cibernético.

Outro ponto discutido diz respeito a falta de regulamentação internacional quanto às ações, comportamentos e a legalidade de atos repressivos no ciberespaço. Essas dificuldades se estabelecem pelo fato de não haver previsão jurídica e normativa nos regimes e instituições internacionais acerca das ações no ciberespaço. Nesse sentido, alguns Estados têm buscado encontrar soluções individualmente com tentativas de estabelecer limites soberanos ou fronteiras no espaço cibernético de modo a facilitar a identificação de agressores e garantir a punibilidade das ações que julgam transgredir sua soberania.

A dificuldade de rastreamento do agressor, a questão da atribuição de responsabilidade, a dificuldade em delimitar espaços soberanos e a falta de regulamentação internacional são considerados importantes entraves para sanções ou represálias em casos de ataques cibernéticos. No entanto, vários questionamentos se acercam e novas críticas surgem - como os mencionados na segunda seção do artigo - a partir das possibilidades apresentadas. Além disso, observa-se a falta de alternativas novas que fujam da lógica utilizada para a resolução dos problemas tradicionais nas relações internacionais. Isso tudo dificulta tanto a tomada de ações adequadas diante de ataques ou diante da possibilidade de uma guerra cibernética quanto em termos de segurança jurídica.

Um conflito do nível apontado para uma ciberguerra ainda não ocorreu, apesar de poder tornar-se uma realidade diante do constante e rápido aperfeiçoamento tecnológico, que levam a interconexão dos sistemas, e do alcance exponencial do poder cibernético entre os atores, estatais e não-es-

tatais, sendo que os Estados estão cada vez mais investindo tanto em meios defensivos como ofensivos no âmbito ciberespaço.

Assim, ao se explorar a atuação brasileira na área, salientam-se as vulnerabilidades presentes e a necessidade de maior atenção e aporte financeiro de modo a desenvolver pesquisas e ferramentas avançadas para a área. O treinamento e a capacitação de profissionais, as pesquisas na área e o desenvolvimento de programas e mecanismos que visem melhorar as capacidades de defesa e segurança cibernética do Brasil devem ser constantemente aperfeiçoados. Ademais, torna-se importante, diante da acelerada digitalização dos dados da população e do Estado, repensar estratégias de proteção destes, tanto no nível governamental quanto no que diz respeito ao setor privado.

Aponta-se, contudo, que desde que o setor cibernético foi considerado prioritário para a defesa do país, este vem se destacando e recebendo consideráveis recursos financeiros, principalmente no contexto das Forças Armadas, bem como tem-se buscado, até certo ponto, incentivar as pesquisas e a capacitação de pessoal no âmbito militar e no meio acadêmico. Do mesmo modo, os documentos de segurança e defesa enfatizam a preocupação acerca das infraestruturas críticas, buscando identificar os principais desafios, potencialidades e meios para a redução das vulnerabilidades nos sistemas de segurança e defesa. Desde então, alguns projetos tomaram forma como o SMDC, o Simoc, o CDCiber e o ComDCiber e a ENaDCiber, os quais devem ser estudados mais profundamente em trabalhos futuros.

## REFERÊNCIAS

Araújo Jorge, Bernardo Wahl G. de. 2012. "Das guerras cibernéticas". *XI Ciclo de Estudos Estratégicos da Escola de Comando e Estado-Maior do Exército (ECEME)*: 1–26 (Maio). Rio de Janeiro.

Ayres Pinto, Danielle Jacon, Riva Sobrado Freitas, and Graciela de Conti Pagliari. 2018. "Fronteiras virtuais: um debate sobre segurança e soberania do estado". In *Fronteiras contemporâneas comparadas: desenvolvimento, segurança e cidadania*, edited by Danielle Jacon Ayres Pinto, Maria Raquel Freire, and Daniel Chaves: 40–53. Macapá: Editora da UNIFAP.

Cavelty, Myriam Dunn. 2010. "Cyberwar: concept, status quo, and limitations". *Center for Security Studies (CSS)* 71: 1–3 (Abril).

Charap, Samuel. 2015. "The ghost of hybrid war". *Survival* 57, no. 6: 51–8.

Clausewitz, Carl Von. 2010. *Da guerra*. São Paulo: Ed. Martins Fontes.

Curran, Kevin, Kevin Concannon, and Sean Mckeever. 2008. "Cyber terrorism attacks". In *Cyber warfare and cyber terrorism*, edited by Lech J.Janczewski, and Andrew M. Colarik. New York: Information Science Reference: 1–6.

Demchak, Chris, and Peter Dombrowski. 2011. "Rise of cybered westephalian wge". *Strategic Studies Quarterly 5*, no. 1: 32–61.

Dipert, Randall. 2010. "The ethics of cyberwarfare". *Journal of Military Ethics* 9, no. 4: 384–410.

Fernandes, Hugo Miguel Moutinho. 2016. "As novas guerras: o desafio da guerra híbrida". *Revista de Ciências Militares* 4, no. 2 (Nov.): 13–40. Lisboa.

Fernandes, José Pedro Teixeira. 2012a. "A ciberguerra como nova dimensão dos conflitos do século XXI". *Relações Internacionais*: 53–69 (Março).

_____. 2012b. "Utopia, Liberdade e Soberania no Ciberespaço". *Revista Nação e Defesa* 133: 11–31. Portugal: Instituto de Defesa Nacional.

Gabinete de Segurança Institucional. 2008. *Portaria GSIPR Nº 2, de 8 de Fevereiro de 2008*. Institui Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC) e dá outras providências. https://contadores.cnt.br/legislacoes/portaria-gsipr-no-2-de-8-de-fevereiro-de-2008.html.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu, and Phillip Laplante. 2011. "Dimensions of cyber-attacks: social, political, economic and cultural**".** *IEEE Technology and Society Magazine*: 28–38 (Spring).

Hoffman, Frank G. 2007. *Conflict in the 21st century: the rise of hybrid wars*. Virginia: Potomac Institute for Policy Studies Arlington.

Libicki, Martin. 2009. *Cyberdeterrence and cyberwar*. Pittsburgh: RAND Corporation.

Lobato, Luísa Cruz, and Kai Michel Kenkel. 2015. "Discourses of cyberspace securitization in Brazil and in the United States". *Revista Brasileira de Política Internacional* 58, no. 2: 23–43. http://dx.doi.org/10.1590/0034-7329201500202.

Mandarino Júnior, Raphael, and Claudia Canongia (Org.). 2010. *Livro Verde: Segurança Cibernética do Brasil*. Departamento de Segurança da Informação e Comunicações. Brasília: GSIPR/SE/DSIC.

Ministério da Defesa. 2012a. *Estratégia Nacional de Defesa - END*. Brasília. https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf.

_____. 2012b. *Livro Branco de Defesa Nacional*. Brasília. https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf.

_____. 2012c. *Política de Defesa Cibernética — PDC*. Brasília. https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf.

_____. 2014. *Doutrina Militar de Defesa Cibernética — DMDC*. Brasília. https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

_____. 2015. *Glossário das Forças Armadas*. 5. ed. Brasília. http://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf.

_____. 2019. *Escola Nacional de Defesa Cibernética é inaugurada em Brasília*. Notícia. Brasília, 11 de fevereiro de 2019. https://www.defesa.gov.br/noticias/52690-escola-nacional-de-defesa-cibernetica-e-inaugurada-em-brasilia.

Nye, Joseph. 2012. "Guerra e paz no ciberespaço". *O Estado de S. Paulo* (Abril). Internacional. http://www.estadao.com.br/noticias/impresso,guerra-e-paz--no--ciberespaco-,861242,0.htm.

Nye Jr., Joseph S. 2011. *The future of power*. New York: Public Affairs.

Oliveira, Marcos Aurelio Guedes, Graciela De Conti Pagliari, Adriana A. Marques, Lucas Soares Portela, and Walfredo Bento Ferreira Neto. 2017. *Guia de defesa cibernética da América do Sul*. Recife: Ed. UFPE.

Olson, Soren. 2012. "'Treino de Sombra': a guerra cibernética e o ataque econômico estratégico". *Military Review*: 73–83 (Set./Out.).

Rid, Thomas. 2013. *Cyberwar will not take place*. New York: Oxford University.

Silva, Júlio Cezar Barreto Leite da. 2014. "Guerra cibernética: a guerra no quinto domínio, conceituação e princípios". *Revista da Escola de Guerra Naval* 20, no. 1: 193-211 (Jan./Jun.). Rio de Janeiro.

Singer, Peter Warren, and Allan Friedman. 2014. *Cybersecurity and cyberwar: what everyone needs to know*. 1. ed. New York: Oxford University Press.

Teixeira Júnior, Augusto W. M., Gills Villar Lopes, and Marco Túlio Delgobbo Freitas. 2017. "As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica". *Carta Internacional* 12, no. 3: 30–53. Belo Horizonte.

Vaczi, Nobert. 2016. *Hybrid warfare: how to shape special operations forces.* 103 p. Dissertação (Mestre em Ciência e Arte Militar) — Faculdade da Escola de Comando e Estado-Maior do Exército dos Estados Unidos, Fort Leavenworth, Kansas.

Vilar-Lopes, Gills. 2016. *Relações Internacionais Cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos da segurança internacional.* 171 p. Tese (Doutorado em Ciência Política) — Universidade Federal de Pernambuco, Recife.

Wendt, Emerson. 2011. "Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos". *Revista Brasileira de Inteligência* 6: 15–26 (Abril). Brasília.

NOTAS

1. "[...] the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers." (Singer and Friedman 2014, 13).
2. "[...] cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online." (Singer and Friedman 2014, 13).
3. "Cyberspace is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared. This means that it is not merely a physical place and thus defies measurement in any kind of physical dimension. But cyberspace isn't purely virtual. It comprises the computers that store data plus the systems and infrastructure that allow it to flow. This includes the Internet of networked computers, closed intranets, cellular technologies, fiber-optic cables, and space-based communications." (Singer and Friedman 2014, 13).
4. "[...] a set of resources that relate to the creation, control and communication of electronic and computer-based information — infrastructure, networks, software, human skills. This includes not only the internet of networked computers, but also intranets, cellular technologies, and space--based communications." (Nye Jr. 2011, 123).
5. "[...] as any act by an insider or an outsider that compromises the security expectations of an individual, organization, or nation." (Gandhi *et al.* 2011, 29).
6. "[...] is hence a human deed that explores the vulnerabilities of the virtual sphere, managing to harm informational systems or even, in light of modern life's online dependency, material daily life." (Lobato and Kenkel 2015, 27).
7. "0[...] involves virtual modification or destruction of content, e.g., hacking websites or disabling a server by data overload. [...] the effects of such incidents are limited in time and relatively harmless." (Cavelty 2010, 01).
8. "Cyber terrorism is the premeditated, polically motivaded attacks against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents." (Curran, Concannon, and McKeever 2008, 01).
9. "[...] an indispensable precondition for assessing the concrete danger and its importance, allocating responsibilities, implementing preventive and reactive countermeasures, and conducting criminal investigations." (Cavelty 2010, 01)
10. "So far there is no known act of cyber "war," when war is properly defined. This of course does not mean that there are no political cyber offenses. But all known political cyber offenses, criminal or not, are neither com-

mon crime nor common war. Their purpose is subverting, spying, or sabotaging." (Rid 2013, 10).

11. "A campaign of cyberattacks launched by one entity against a state and its society, primarily but not exclusively for the purpose of affecting the target state's behavior, would be strategic cyberwar." (Libicki 2009, 117).
12. If the attacks between political entities are sufficiently "widespread" we might then speak of a cyberwar." (Dipert 2010, 398).

GUERRA CIBERNÉTICA, AMEAÇAS ÀS INFRAESTRUTURAS CRÍTICAS E A DEFESA CIBERNÉTICA DO BRASIL

## RESUMO

Diante das dinâmicas emergidas com as novas tecnologias, esse estudo propõe debater sobre os novos moldes de ações ofensivas e defensivas no ciberespaço, buscando compreender algumas dinâmicas envolvidas diante das potencialidades de um cenário de ciberguerra. Nessa perspectiva, a pergunta central que este artigo procura responder é: de que forma esses novos moldes e dinâmicas ligadas aos recursos cibernéticos poderiam ser compreendidos diante de um potencial cenário de ciberguerra? Os atores estatais têm desenvolvido estratégias específicas para lidar com as novas dinâmicas impostas pelo ciberespaço, tanto numa dinâmica defensiva e resiliente, como ofensiva. Contudo uma série de fatores característico deste espaço precisam ser melhor compreendidos frente as vulnerabilidades enfrentadas pelos Estados. Assim, após o debate teórico-conceitual sobre ciberguerra, o artigo analisa o posicionamento do Brasil frente a tais dinâmicas tendo como base de análise os documentos estratégicos de defesa do país.

Palavras-chave: Ciberespaço; Ciberguerra; Infraestruturas Críticas; Segurança Internacional; Defesa.

## ABSTRACT

In view of the dynamics that emerged with the new technologies, this study will discuss about the new forms of offensive and defensive actions in cyberspace, seeking to understand its dynamics involved ahead of the potential occurrence of a cyberwar scenario. In this perspective, the central question that this article seeks to answer is: how could these new patterns and dynamics linked to cyber resources be understood in the face of a potential cyberwar scenario? State actors have developed specific strategies to deal with the new dynamics imposed by cyberspace, both in a defensive and resilient and offensive dynamic. However, a series of factors characteristic of this space need to be better understood in view of the vulnerabilities faced by States. So, after this theoretical-conceptual debate on cyberwar, the article aims to understand Brazil's position in face of such dynamics, based on the country's defense strategy documents.

Key-words: Cyberspace; Cyberwar; Critical Infrastructures; International Security; Defense.

**Recebido em 02/03/2020. Aceito para publicação em 22/02/2021.**