DOI 10.22491/cmm.a003

Uma análise sobre o processo de securitização do ciberespaço*

An analysis of the cyberspace securitization process

Resumo: O ciberespaço manifesta-se como novo domínio para as relações de poder na medida que diferentes atores o utilizam para perseguir seus interesses. Por ser dotado de uma lógica desterritorializadora – na qual múltiplos entes podem atuar de forma anônima –, o ciberespaço desafia concepções tradicionais de segurança e defesa nacional, ao passo que fluxos digitais perpassam diferentes territórios. Considerada a inserção da infraestrutura básica de um Estado no domínio cibernético, englobando sistemas bancários, de telecomunicações, transportes e diversos agentes, como os militares, observa-se uma crescente dependência da sociedade para com o ciberespaço. Tal dependência pode ser explorada por uma miríade de atores internacionais. Nesse contexto, por intermédio da concepção da Escola de Copenhague a respeito do processo de reconhecimento de ameaças por agentes securitizadores, o presente artigo investiga o processo de securitização do ciberespaço mediante análise dos livros brancos de defesa do Brasil, Alemanha e França.

Palavras-chave: Ciberespaço. Segurança. Defesa. Território. Ameaças.

Abstract: Cyberspace manifests itself as a new domain for power relations as different actors use it to pursue their interests. Because it is endowed with a deterritorializing logic - in which multiple entities can act anonymously - cyberspace defies traditional conceptions of national security and defense, as digital flows cross different territories. Considering the insertion of the basic state infrastructure in the cyber domain, encompassing banking, telecommunications, transport and military systems, there is a growing dependence of society on cyberspace. Such dependency can be exploited by a myriad of international actors. In this context, through the conception of the Copenhagen School regarding the process of recognition of threats by securitizing agents, this article investigates the process of securitization of cyberspace by analyzing the white defense books of Brazil, Germany and France.

Keywords: Cyberspace. Safety. Defense. Territory. Threats.

Breno Pauli Medeiros
Exército Brasileiro, Escola de Comando e Estado-Maior do Exército, Instituto Meira Mattos.
Rio de Janeiro, RJ, Brasil.
breno.pauli@gmail.com

Alessandra Cordeiro Carvalho
Exército Brasileiro, Escola de Comando e Estado-Maior do Exército, Instituto Meira Mattos.
Rio de Janeiro, RJ, Brasil.
alessandraccarvalho27@hotmail.com

Luiz Rogério Franco Goldoni
Exército Brasileiro, Escola de Comando e Estado-Maior do Exército, Instituto Meira Mattos.
Rio de Janeiro, RJ, Brasil.
luizrfgoldoni@gmail.com

Recebido em: 13 dez. 2018
Aprovado em: 24 jan. 2019

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-489 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

* Esse artigo faz parte dos esforços de pesquisa do projeto 'Ciência, Tecnologia e Inovação em Defesa: Cibernética e Defesa Nacional', aprovado pelo Edital 27/2018, Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Defesa Nacional – PRÓ-DEFESA IV.

1 Introdução

O espaço cibernético representa um novo domínio das relações de poder. Dada a natureza desassociada, em parte, do espaço físico, o ciberespaço apresenta-se com lógica própria, na qual a concepção tradicional de fronteiras dificilmente impede o fluxo de informações no domínio cibernético. Como novo ambiente operacional, o ciberespaço integra ações privadas, militares, civis e estatais ao meio técnico-científico-informacional. Ao passo que o espaço cibernético se consagra como um domínio alternativo para o exercício das relações de poder, suas lógicas e peculiaridades engendram desafios aos domínios tradicionais.

Em decorrência do encolhimento de distâncias físicas, instantaneidade das comunicações e maior interdependência da sociedade para com o ciberespaço, surgem questionamentos sobre como pensar a defesa e a estratégia nesse novo domínio. Dentre esses, destacam-se indagações sobre securitização e quais seriam as "novas" ameaças.

Nesse novo ambiente – marcado pela flexibilização de fronteiras e territórios, multiplicidade e anonimato de atores – novas e velhas ameaças desafiam as concepções tradicionais de segurança e defesa nacional. É notória a frequência de ocorrências cibernéticas no cenário internacional. Ataques por *malwares*[1], *ransomwares*[2], DDoS[3], entre outros, além de expandir o número de possíveis agressores para atores não necessariamente estatais, tem se tornado ainda mais sofisticados, dificultando a identificação da autoria ou motivações para os ataques. Diante desse cenário de insegurança, o ciberespaço pode ser interpretado como um domínio para o exercício de poder, em paralelo com os domínios terrestre, marítimo, aéreo e espacial.

A presente pesquisa tem como objetivo investigar o processo de securitização do ciberespaço no Brasil, Alemanha e França, a partir da análise de conteúdo comparada entre seus respectivos Livros Brancos de Defesa. Estudar os documentos de defesa dos países selecionados possibilita evidenciar as ameaças, estratégias e práticas que compõe o processo de securitização do ciberespaço em Estados que foram alvos de espionagem e monitoramento no espaço cibernético (BRIDI; GREENWALD, 2013; WIKILEAKS, 2015).

Dadas as limitações do presente trabalho, serão analisados o *White Paper on German Security Policy and The Future of the Bundeswehr*, o *French White Paper: Defense and National Security* e o Livro Branco de Defesa Nacional do Brasil, acompanhado de sua versão mais recente, a minuta de 2016. A análise foi limitada aos Livros Brancos de Defesa dos países, uma vez que esses representam os documentos de defesa de mais alto escalão, determinando o tom e a abordagem dos documentos que os seguem hierarquicamente.

A fim de direcionar a análise de conteúdo desses documentos, a pesquisa será constituída por quatro perguntas principais: i) Existe alguma definição clara de segurança cibernética nos do-

1 Os tipos mais comuns de *malwares ou "malicious software"* são os vírus ou *worms* (vermes), os quais possuem a capacidade de provocar danos e se auto-replicar em redes de computadores e sistemas (GOLDANI, 2005).

2 Tipo de malware lucrativo que permite a inacessibilidade de dados armazenados em computadores, uma vez que os transforma em dados criptografados, exigindo do usuário pagamentos de resgate (SYMANTEC, 2016).

3 Técnica de ataque que envolve uma grande quantidade de computadores – podendo ser de conhecimento do proprietário ou não –, que sobrecarrega sites ou servidores por meio da saturação de solicitações de serviços, gerando a indisponibilidade do sistema (CARREIRO, 2012).

cumentos?; ii) O que os documentos exprimem sobre o setor cibernético?; iii) Quais são as ameaças consideradas? e iv) Qual é o posicionamento em relação ao envolvimento de outros setores da sociedade? Em paralelo, será realizada uma análise comparativa dos livros brancos de defesa nos aspectos que abordam as novas e tradicionais ameaças correlacionadas a questão cibernética, além de termos chave que contribuem para a compreensão a respeito da relevância dos assuntos propostos, mediante a elaboração de tabela comparativas e aglomerações de palavras que exprimem o tom e os termos mais proeminentes em cada documento.

Conforme a sociedade atual se insere no ciberespaço, atores o utilizam para a projeção de força e interesses. O caráter desterritorializador inerente ao domínio cibernético permite, por exemplo, que grupos terroristas recrutem dissidentes; agências de inteligência monitorem comunicações, e ativistas de movimentos sociais coordenem suas manifestações.

Essencialmente, o espaço cibernético surge como um espaço alternativo e paralelo aos domínios tradicionais de terra, ar e mar; porém, o ciberespaço não possui fronteiras, espaço aéreo e nem águas nacionais (HILDEBRANDT, 2013). Para que um ator opere no ciberespaço, não é necessária uma unidade de blindados, caças ou navios, basta uma conexão com a Internet. Dessa forma, a difusão de poder inerente ao ciberespaço proporciona um domínio operacional para atores particulares em paralelo com forças estatais (NYE, 2012). Fator que simultaneamente dota o ciberespaço de valor estratégico para os Estados, e pode representar um novo ambiente do qual emanam ameaças não necessariamente estatais.

Considerada a crescente pertinência da cibernética no contexto de segurança e defesa, o presente trabalho se justifica a partir do momento que representa um esforço analítico a respeito do processo de securitização do ciberespaço como domínio estratégico por potências regionais. No entanto, antes de se analisar tal processo no Brasil, Alemanha e França, se faz necessário apresentar alguns conceitos e definições para uma melhor contextualização sobre o tema.

2 **O ciberespaço: contextualização, conceitos e definições**

O espaço cibernético possui diversas definições – algumas mais abrangentes do que outras –, que contribuem para a existência de um amplo espectro de abordagens e compreensões (KUEHL, 2009). Algumas o consideram no aspecto mais teórico, como uma nova área de interação que permeia e interconecta as telecomunicações numa grande rede global, outras consideram os aspectos físicos e maleáveis das diferentes conexões e dispositivos interligados.

Lobato e Kenkel (2015, p. 24-25, tradução nossa) compreendem o ciberespaço de maneira ampla, como "a rede de informações mundial interconectada e a infraestrutura de comunicações que engloba a Internet, redes de telecomunicações, sistemas de computadores e as informações contidas neles". A definição proposta pelos autores, propõe uma abordagem ampla do conceito de espaço cibernético como sendo uma grande rede de comunicações interconectadas que engloba diversos atores ligados a ela.

Libicki (2009) oferece uma definição mais específica, pois interpreta o espaço cibernético como um meio menos tangível que os tradicionais domínios de terra, ar e mar. Para o autor, o espaço cibernético é composto por três camadas interconectadas: a primeira é representada pelo *hardware*, componentes eletrônicos físicos, na forma de fios, antenas, e toda sorte de dispositivos interconecta-

dos, incluindo desde computadores e celulares aos sistemas de armamentos, veículos aéreos não tripulados (VANTs), e assim por diante. A segunda camada – ou sintática –, consiste no *software*. Nessa se encontram as instruções e comandos que os desenvolvedores e engenheiros dão aos elementos da primeira camada para que os mesmos cumpram seu objetivo e se comuniquem uns com os outros. Por último, existe a camada semântica, na qual as informações são contidas na forma de dados binários a serem organizados em linhas de código ou qualquer outro tipo de informação.

Nesse contexto, o ciberespaço pode ser entendido como um domínio existente mediante a interconectividade de fluxos informacionais, no qual se inserem toda sorte de redes e infraestruturas críticas para a sociedade hodierna. Logo, a partir do momento que há conexão entre um ou mais dispositivos, o espaço cibernético se torna realidade, servindo como uma plataforma para variadas relações humanas. Por abranger atores distintos, o ciberespaço é palco para inéditas relações de poder. Estas engendram diferentes ameaças que interagem, modificam e exploram os fluxos informacionais do domínio cibernético.

A análise do ciberespaço demanda especial atenção a três elementos essenciais. Estes representam peculiaridades inerentes ao ciberespaço e impõem desafios teóricos e práticos às relações sociais. O primeiro elemento é a desterritorialidade do espaço cibernético. Considerando os elementos físicos da camada de *hardware* como dispositivos que atuam de forma análoga a nós numa grande rede de comunicações globais, composta por fluxos de informações, compreende-se que esses fluxos informacionais correspondem à uma lógica reticular inerente exclusivamente ao espaço cibernético que interliga os diferentes dispositivos físicos interconectados pelo ciberespaço. Sublinha-se que as tradicionais definições e interpretações de território o compreendem como a área geográfica delimitada por fronteiras, correspondendo à uma lógica zonal mediante o recorte espacial, na qual o Estado realiza o controle soberano do território[4].

A desterritorialidade do ciberespaço se faz presente a partir do momento que sua lógica reticular, na forma de fluxos interconectados, permeia o território de diferentes Estados; ou quando os dispositivos que servem de nós na rede do ciberespaço são controlados e/ou explorados por outros Estados. Ou seja, a interconectividade de diferentes pontos numa rede global acaba por permear[5] as fronteiras, tidas como fundamentais para a lógica zonal na qual o conceito de território é fundamentado.

O segundo elemento corresponde à difusão de poder no espaço cibernético. Conforme o domínio cibernético surge como espaço alternativo para o exercício do poder, a multiplicidade de atores na rede, em conjunto com a facilidade do acesso e aquisição de equipamentos e capacidades permitem a relativa redução do distanciamento de capacidades entre Estados militarmente mais fortes, Estados fragilizados, organizações e/ou indivíduos não estatais. Nesse contexto, o número de ameaças em potencial cresce exponencialmente, uma vez que novos atores utilizam o espaço cibernético tanto para o exercício de *soft* quanto de *hard power* (NYE, 2012). De fato, Marcos Guedes de Oliveira (2014), ao tratar do potencial inexplorado da guerra cibernética, alerta para

4 A concepção de lógica reticular e zonal parte da análise de território-rede, idealizada por Haesbaert (2007), na qual as diferentes territorialidades de grupos e indivíduos se mesclam com a hegemonia territorial de Estados. A abordagem aqui utilizada, no entanto, usa o termo no sentido mais específico ao ciberespaço, considerado a lógica reticular dos fluxos informacionais dentro da rede do ciberespaço que permeia as fronteiras da concepção zonal dos territórios estatais.

5 Trata-se de uma generalização. É sabido que países como China e Coréia do Norte possuem amplas restrições ao uso de suas telecomunicações e acesso à rede global de computadores.

as eventuais consequências decorrentes da atuação de indivíduos no ciberespaço que podem vir a afetar sistemas dos quais a sociedade depende. Segundo o autor:

> Um novíssimo campo de ação está relacionado com a facilitação de insurreições, manifestações e mesmo golpes via uso e manipulação de recursos compartilhados pelas redes de telefonia celular. O sucesso em operações com esse formato reduziria em muito os custos de intervenção aberta e militar em países menores e daria às nações dominantes dessa tecnologia um forte argumento em favor da não regulamentação internacional do meio cibernético (OLIVEIRA, 2014, p. 194-195).

A terceira peculiaridade decorre da incerteza que se desenvolve no domínio cibernético. Kallberg e Cook (2017), ao tratarem dos desafios do espaço cibernético para o pensamento militar tradicional, apontam que o anonimato e a dificuldade de se mensurar o impacto de um ataque cibernético são elementos que corroboram para o predomínio do princípio da incerteza inerente ao domínio cibernético. Dada sua natureza interconectada e altamente complexa, um eventual ataque é dificilmente quantificado ou mensurado, já que os efeitos não são necessariamente cinéticos e/ou imediatos, estando muitas vezes escondido debaixo de inúmeras camadas de rede semânticas e sintáticas.

O anonimato, por sua vez, pode ser utilizado como ferramenta tanto de proteção quanto de ataque. Tal característica pode ter como consequência a identificação errônea de um ataque cibernético, ocasionando um eventual contra-ataque a inocentes, levando à escalada descontrolada do conflito. O advento do novo domínio eleva o "derrotar o inimigo sem lutar" e o "fazer os outros lutarem suas batalhas" a outro patamar.

A combinação dos elementos de desterritorialidade, difusão de poder e incerteza permite que novas e velhas ameaças atuem no espaço cibernético, realizando um escopo de atos que vão desde a diplomacia à sabotagem, espionagem, monitoramento e mesmo a ataques com efeitos cinéticos. O espaço cibernético se consagra, dessa maneira, como palco para toda sorte de atores e ameaças.

Como exemplo, Edward Snowden – então analista da Agência de Segurança Nacional Norte Americana (NSA) –, no ano de 2013, em parceria com jornalistas de diferentes países revelou o programa de espionagem e monitoramento exercido pela NSA. Países como Brasil, Alemanha e França tiveram chefes de Estado, membros do governo e empresas monitoradas pela agência norte americana, com o auxílio de países aliados pertencentes ao chamado grupo "Cinco Olhos", composto por agências de segurança dos EUA, Canada, Austrália, Nova Zelândia e Reino Unido, que trabalhavam em conjunto, monitorando cidadãos ao redor do globo (BRIDI; GREENWALD, 2013; WIKILEAKS, 2015; PRIVACY INTERNATIONAL, 2015).

Decorrente da espionagem no Brasil, é pertinente a fala de Celso Amorim (2013, p. 289), a respeito do contínuo estreitamento da linha que separa a espionagem online e a guerra cibernética a partir de características como a incerteza no ciberespaço:

> O monitoramento de dados e a guerra cibernética têm em comum o emprego de instrumentos de altíssima tecnologia para atividades que importam em graves violações de soberania. Quando o objeto do monitoramento vai além da mera observação, e visa a tomada de conhecimentos tecnológicos, a fronteira entre a espionagem e a guerra fica

> ainda mais difícil de ser determinada. Conceitualmente, não haveria diferença, salvo talvez no que diz respeito a danos imediatos, entre um ato de espionagem, de busca de informações econômicas e tecnológicas, e um ataque tradicional para a obtenção de um recurso econômico.
>
> O monitoramento e a guerra cibernética podem alvejar tanto países tidos como hostis ou como ameaças imediatas quanto países amigos e aliados. Já sabemos que esse foi o caso na interceptação de dados. Não se pode excluir que o mesmo ocorra com ataques cibernéticos, provenientes de qualquer quadrante. Essas duas atividades ilustram em tons muito fortes alguns dos novos desafios da segurança internacional.

O monitoramento exposto por Snowden representa a exceção a regra, já que devido à multiplicidade de atores e anonimato no ciberespaço é improvável identificar com precisão a atuação de atores nacionais. Porém, é possível vislumbrar a atuação de atores estatais no espaço cibernético, sem que ocorra uma confirmação ou reconhecimento oficial.

Talvez um dos exemplos mais emblemáticos seja o caso Stuxnet. Trata-se de um *malware* que contaminou os computadores de centrífugas nucleares iranianas, sabotando o projeto nuclear do país. Todos os indícios apontam para um ataque cibernético realizado pelos Estados Unidos em conjunto com Israel para atrasar o programa nuclear daquele país. No entanto, estadunidenses e/ou israelenses nunca assumiram de fato a autoria do ataque (KENNEY, 2015).

O monitoramento ou a sabotagem cibernética realizada por outros Estados, constituem "velhas ameaças" no sentido de que sempre houve espionagem, sabotagem e guerras entre países. Porém, estas se tornam "velhas ameaças" no ciberespaço a partir do momento que a difusão de poder às obriga a atuar paralelamente com outros agentes.

No que tange as novas ameaças do espaço cibernético, tem-se aquelas não apenas provocadas por estados para os fins mencionados acima, mas também, as ameaças promovidas por atores não estatais. Ou seja, são transpassadas as ameaças do nível estatal para o nível dos indivíduos. Estes, por exemplo, passam a ser capazes de desestabilizar governos mediante a realização de ataques com as mais variadas motivações. Dentre as ameaças não estatais podem ser apontados o ativismo cibernético, o crime cibernético e o terrorismo cibernético.

O ativismo cibernético é caracterizado como a mistura entre as ações *hacker* e o ativismo político, de forma a inviabilizar servidores ou sítios eletrônicos (CEPIK; CANABARRO; BORNE, 2014). Pode-se dizer, ainda, que o ciberativismo envolve-se em questões voltadas a determinadas causas a partir da realização de ataques aos governos e empresas que apresentam-se em contradição com seus ideais, de forma a induzi-los a reavaliar suas decisões institucionais, a fim de chamar a atenção do público à causa defendida (ZUCCARO, 2012).

Definido como ato ou omissão cometida em violação a uma lei no espaço cibernético, o crime cibernético apresenta-se como uma atividade criminal relacionada à invasão ilegal à computadores, manipulação de informações, sabotagem de equipamentos e roubo de dados (SAINI; RAO; PANDA, 2012). De forma mais abrangente, pode-se dizer que o cibercrime é o desenvolvimento de ações ilícitas a serem aplicadas em sistemas e redes de computadores. Utilizando-se da espionagem cibernética para testar configurações e sistemas de defesa a fim de ter acesso a informações sigilosas, cibercriminosos podem realizar sabotagens cibernéticas ao gerar empecilhos por meios eletrônicos (CEPIK; CANABARRO; BORNE, 2014).

O ciberterrorismo, mesmo que não possuindo uma definição amplamente aceita – tendo em vista a variação do termo componente terrorismo – (CHEN, 2014), é interpretado, de forma geral, como ações realizadas por atores não estatais contra redes e sistemas de computadores, capazes de resultar em violência contra civis. No mais, os ataques devem conter motivação política e gerar danos físicos além de virtuais (POLLIT, 1998; WEIMANN, 2005; KENNEY, 2015). Segundo Dorothy Denning (2000), ameaças cibernéticas contra computadores, redes e sistemas indicam a busca por intimidação dos governos e das populações, almejando o alcance de objetivos sociais e políticos de grupos e indivíduos. Além disso, o ciberterrorismo visa uma ampla escala de exibição e publicidade, assim como no terrorismo tradicional (COLLIN, 1997).

Independente das motivações de determinadas ameaças, é percebido que o espaço cibernético se demonstra como ambiente no qual diferentes ações são realizadas com variáveis níveis de sucesso. A interconectividade ao passo que aproxima as pessoas e permite uma gama de atividades e facilidades antes inimagináveis, abre também portas para ameaças há pouco impensáveis. Logo, diversos Estados percebem a importância da segurança e defesa cibernética nacionais, uma vez que ataques dessa natureza podem gerar danos físicos, políticos, econômicos e sociais irremediáveis.

3 **A securitização do ciberespaço**

O cenário internacional pós-Guerra Fria ensejou a discussão de novos temas na agenda internacional que passaram a ganhar maior relevância nos anos 1990, tornando-se necessária a introdução de novos modelos de análise de segurança (FARRET, 2014). Pela insuficiência do debate teórico-epistemológico do período, a produção, antes concentrada em questões estadocêntricas, ampliou-se para análises de atores não estatais e individuais, demonstrando que o sistema internacional deveria ser analisado não apenas através das relações interestatais. Assim, conceitos até então considerados imutáveis passaram a ser redefinidos (BUZAN; HANSEN, 2012).

Baseada nas premissas da corrente construtivista, a Escola de Copenhague desenvolve o conceito teórico de securitização. Compreendendo o alargamento do campo da segurança internacional, a Escola amplia o conceito de segurança para além do domínio político-militar ao introduzir novos setores de análise: o econômico, o ambiental e o societal. Pra isso, utiliza-se da análise dos discursos e das unidades de segurança para verificar a securitização de determinado tema.

Por meio da teoria de securitização, novas formas de análise de segurança passaram a ser consideradas por intermédio dos discursos e do posicionamento de agentes não-estatais e individuais no sistema internacional. Assim, novas ameaças internacionais, anteriormente ligadas essencialmente ao Estado, passaram a ser melhor percebidas e entendidas (MOTTA, 2014). Esse aspecto possibilitou que os estudos fossem estendidos para a segurança dos indivíduos e demonstrou casos em que o Estado e a sociedade não se equilibram como, por exemplo, quando minorias nacionais são ameaçadas pelo próprio Estado ou, quando este mobiliza a sociedade para a confrontação de ameaças internas ou externas (BUZAN; HANSEN, 2012).

De acordo com Grace Tanno (2003), os processos de construção de segurança iniciam-se a partir de discursos realizados por atores interessados em estabelecer as agendas de segurança, podendo, dessa forma, sofrer o processo de securitização. Contudo, tal processo não depende apenas dos agentes securitizadores como, também, necessita que a proposta seja socialmente reconhecida como uma ameaça à segurança. Em outras palavras, para que seja criada uma situação de segurança a partir do discurso, é preciso que a audiência a qual ele se dirige e a qual requisita os meios necessários para o objeto que virá a ser securitizado concorde voluntariamente com o discurso, direcionando o ato de securitização (AMARAL, 2008).

Portanto, entende-se por securitização o processo no qual o Estado é ameaçado existencialmente, sendo necessárias ações emergenciais que podem, inclusive, ultrapassar leis e procedimentos políticos (BUZAN; WEAVER; WILDE, 1998). Logo, securitização cibernética pode ser interpretada como o processo de ação emergencial contra uma ameaça em potencial no espaço cibernético. São considerados atores do ambiente cibernético os estados, as instituições, as corporações industriais e empresariais, os setores financeiros e de serviços, grupos de ativistas políticos e religiosos, criminosos digitais, entre outros. A variedade e quantidade de atores multiplicam-se na medida em que avança a tecnologia e o acesso à informação. Dentre esses atores, podem ser observados tanto aqueles que irão promover o discurso securitizador, como os atores que podem ser considerados ameaças à segurança estatal.

O processo de securitização é melhor vislumbrado no setor militar, uma vez que o monopólio da força do estado moderno torna-o legítimo para a proteção nacional diante de ameaças à segurança nacional. Dessa forma, o Estado é considerado o objeto de referência, enquanto que as elites militares são os atores securitizadores responsáveis pela determinação das ações às ameaças mediante os atos de fala (TANNO, 2003). O processo de securitização se torna evidente no momento em que o ciberespaço é reconhecido pelos documentos de defesa como um domínio estratégico no qual emanam diferentes ameaças.

A extensão das ameaças e das vulnerabilidades irá variar de acordo com as capacidades relativas e absolutas dos envolvidos (BUZAN; WEAVER; WILDE, 1998). Entretanto, quando levado ao âmbito cibernético, a assimetria de capacidades e a crescente vulnerabilidade das infraestruturas críticas transformam a natureza da ameaça, uma vez que as peculiaridades inerentes ao ciberespaço dificultam a prevenção contra os ataques cibernéticos.

O ciberespaço amplia as formas com as quais se pode abalar a estabilidade organizacional do Estado; a organização da primavera árabe dispensa maiores comentários. Ações cibernéticas com motivações políticas[6] que visam desestabilizar o governo de forma a divulgar determinado ideal podem provocar danos a outros setores da sociedade, tornando a securitização mais complexa e sensível. Ainda, podem provocar a perda de legitimidade interna e externa de um Estado caso não se proponha a securitizar o setor político contra as ameaças cibernéticas.

6 As ameaças políticas podem ser classificadas como ameaças intencionais – quando um Estado não reconhece a legitimidade de um Estado/governo estrangeiro ou o governo é rejeitado por um grupo no âmbito doméstico por conflitos de princípios distintos – e ameaças estruturais – quando há contradições nos princípios organizacionais do Estado (TANNO, 2003). Consoante Buzan, Weaver e Wilde (1998), as ameaças existentes no setor político a um Estado são aquelas que desafiam a soberania nacional, uma vez que uma ameaça no âmbito político pode ser transferida para os outros setores (BUZAN; WEAVER; WILDE, 1998).

As ameaças econômicas podem ser consideradas como aquelas "dirigidas aos setores econômicos que garantem a sobrevivência do Estado e que são fundamentais no esforço de guerra" (TANNO, 2003). Em vista da interdependência, ameaças a estabilidade econômica de um Estado podem ser entendidas como globais (BUZAN, WEAVER, WILDE, 1998). Dessa forma, as ameaças cibernéticas que visam ganhos econômicos mediante roubo de informações bancárias – tanto na escala do indivíduo como empresarial ou estatal, por exemplo – podem provocar danos econômicos e financeiros ao Estado, além de transferir esses danos para outros setores interligados.

Por fim, mesmo não tratando especificadamente da revolução da informação no estudo de segurança, a Escola de Copenhague apresenta, por intermédio da teoria de securitização, como, quando e quais consequências os atores políticos percebem como ameaça existencial à segurança a partir dos atos de fala – ou discursos políticos –, criando uma agenda de segurança emergencial. O universo cibernético amplia a gama de ameaças que passam a ser, inclusive, menos perceptíveis, por conta das questões de anonimato e incerteza anteriormente mencionadas. Essas peculiaridades do novo domínio ensejam novas abordagens no processo de securitização.

4 O ciberespaço nos livros brancos de defesa

Tendo em vista a eventual defasagem entre as medidas de segurança e de defesa nacional em relação ao acelerado avanço da tecnologia, os Estados passam a preocupar-se em proteger e reduzir suas vulnerabilidades por meio de medidas capazes de promover algum tipo de desenvolvimento estatal no âmbito da segurança, especificamente em relação à cibernética. Diante da nova arena de poder que o espaço cibernético representa, é analisado o processo de securitização nos livros brancos de defesa da Alemanha, França e Brasil mediante o reconhecimento do ciberespaço como domínio estratégico.

Alemanha

No Livro Branco da Política de Segurança Alemã e o Futuro das Forças Armadas (*White Paper on German Security Policy and the Future of the Bundeswehr*), editado em 2016, são apresentados os desafios para a política de segurança do país. Na esfera das ameaças encontram-se a questão do terrorismo, das armas de destruição em massa, do descontrole de migração, conflitos interestatais, controle climático, entre outros. Tratando especificamente do domínio cibernético, há uma clara preocupação com as vulnerabilidades do Estado frente a possíveis ataques cibernéticos. Sobre o tema, o documento afirma serem necessárias "medidas urgentes para a proteção contra ameaças" (GERMANY, 2016, p. 36, tradução nossa).

O documento alemão não oferece uma definição clara sobre segurança cibernética. Entretanto, apresenta o conceito de domínio da informação como o espaço no qual as informações são geradas, processadas, disseminadas, discutidas e armazenadas. Conforme o Livro Branco da Política de Segurança Alemã, o espaço cibernético é tido como espaço virtual de todos os sistemas da Tecnologia da Informação vinculados ou vinculáveis em escala global.

É apontado, no documento, a gravidade dos ataques cibernéticos à infraestruturas críticas que podem gerar consequências à população civil, expondo que os efeitos dos ataques não podem ser resolvidos em um futuro previsível, uma vez que a tendência é que essa questão continue a se agravar. Ainda, é apresentado que a cibernética e o domínio da informação são áreas de importância estratégica e internacional, sendo necessária a melhora do tempo de resposta como prevenção aos ataques cibernéticos e operações de informação, colocando como prioridade a proteção e a defesa cibernética.

> Devemos tomar medidas preventivas para reduzir esse risco por meio de mecanismos de construção de confiança e resolução de conflitos. Existem poucas áreas em que a segurança interna e externa estão tão estreitamente entrelaçadas quanto no espaço cibernético. A situação de ameaça no espaço cibernético exige uma abordagem holística no âmbito da política de segurança cibernética (GERMANY, 2016, p. 38, tradução nossa).

Em relação ao setor cibernético, o Livro Branco da Política de Segurança Alemã prioriza a necessidade de reduzir as vulnerabilidades das infraestruturas críticas nacionais, como sistemas de comunicação, energia e logística. No tocante às ameaças consideradas no documento, é apresentada preocupação em relação a ataques de atores não estatais, como grupos terroristas, crime organizado, além de indivíduos especializados que poderiam provocar sérios danos com mínimos esforços. Tais ameaças confirmam a preocupação com atos que podem ser provocados por agentes não-estatais. Assim, indivíduos são percebidos como atores internacionais, conforme análise do documento alemão. Tal fato, por si só, ensejaria densa discussão teórica relativa às relações internacionais, o que extravasa, em muito, os propósitos e limites do presente artigo.

O documento não apresenta especificamente a relação do espaço cibernético com a esfera civil, mas deixa claro a importância da transparência entre os setores público e privado e a necessidade de cooperação com outros estados. Conforme o Livro Branco da Política de Segurança Alemã, apenas por meio de uma política de segurança cibernética e uma política externa cibernética seria alcançada uma efetiva proteção contra cibercriminosos e ataques cibernéticos. As informações obtidas no documento são sumarizadas na tabela a seguir.

Tabela 1 - Sumário das informações obtidas no Livro Branco da Política de Segurança Alemã

Ano de edição	2016
Existe alguma definição clara de segurança cibernética nos documentos?	Não
O que esses documentos exprimem sobre o setor cibernético?	Área de importância estratégica e internacional. É priorizada a proteção e defesa cibernética.
Quais são as ameaças consideradas?	Atores não estatais. Grupos terroristas, crime organizados, indivíduos especializados em danos infraestruturais.
Qual é o posicionamento em relação ao envolvimento de outros setores civis?	Não especifica, mas afirma a necessidade de transparência entre os setores para o combate das ameaças cibernéticas.

Fonte: Baseado em Germany (2016)

A Alemanha atribui o surgimento de novas ameaças como um dos fatores que levou à necessidade de reformulação do seu livro branco, argumentando que "novas ameaças e perigos surgiram além daqueles que já existiam" (GERMANY, 2016, p. 15). No que tange as ameaças oriundas do domínio cibernético, há uma sessão dedicada exclusivamente ao combate a "Ameaças aos sistemas de informação e comunicação, linhas de suprimento, rotas de transporte e comércio, bem como ao fornecimento seguro de matérias-primas e energia" (GERMANY, 2016, p. 41). Nessa sessão, a prosperidade da sociedade alemã é tida como dependente do uso de comunicações e informações globais, e qualquer "interrupção do acesso a esses bens públicos globais em terra, no ar, no mar, no domínio cibernético e da informação e no espaço envolve riscos consideráveis para a capacidade de nosso estado funcionar e para a prosperidade de nossos cidadãos" (GERMANY, 2016, p. 41).

O texto sustenta a necessidade de aprimoramento de pessoal e tecnologia para melhor atuação estatal no ciberespaço. Talvez, como consequência, em abril de 2017, foi criado o Cyber and Information Space Command (CIR), que corresponde ao braço cibernético das forças armadas alemãs (WERKHÄUSER, 2017).

França

Na análise do Livro Branco da Defesa e Segurança Nacional Francesa (French White Paper on Defence and National Security), elaborado, em 2013, pelo governo francês, é constatada a preocupação com ataques cibernéticos – juntamente com ameaças de proliferação nuclear, pandemias e terrorismo –, logo nas primeiras linhas do prefácio escrito pelo então presidente François Hollande.

O documento considera a crescente inserção da sociedade francesa nos meios de comunicação como uma forma de vulnerabilidade. Nesse sentido, ressalta que o acesso universal ao ciberespaço e a não identificação de responsáveis (logo, a questão da incerteza, anteriormente discutida) são seus principais agravantes. No contexto, são aludidas as ameaças no ciberespaço, desde cibercriminosos à ataques cibernéticos liderados por outras nações. Por essas colocações, visualiza-se no Livro Branco francês que o ciberespaço é entendido como ambiente essencial ao Estado, palco de desafios e conflitos em potencial. "A possibilidade de um grande ciberataque em sistemas nacionais de informação num cenário de guerra cibernética constitui uma ameaça extremamente grave para a França e os seus parceiros europeus" (FRANCE, 2013, p. 43).

Em relação às perguntas que compõem a análise comparativa proposta neste artigo, o Livro Branco da Defesa e Segurança Nacional Francesa não oferece uma definição clara de segurança cibernética. Porém, interpreta o ciberespaço como área de conflitos e o considera uma prioridade estratégica em relação à proteção contra ameaças e ataques. Em relação às ameaças, são considerados tanto agentes não estatais quanto Estados que podem desenvolver espionagem e ataques cibernéticos. A respeito da introdução do setor civil como auxílio para a proteção nacional, o documento, apesar de envolver outros setores do governo – além das Forças Armadas –, não aborda a questão do envolvimento civil. A tabela 2 apresenta uma síntese das informações obtidas.

Tabela 2 - Sumário das informações obtidas no Livro Branco da Defesa e Segurança Nacional Francesa

Ano de edição	2013
Existe alguma definição clara de segurança cibernética nos documentos?	Não
O que esses documentos exprimem sobre o setor cibernético?	O ciberespaço é considerado área de confronto e de ameaças. É percebido como prioridade estratégica a partir da proteção contra ciberataques.
Quais são as ameaças consideradas?	Não estatais, como cibercrime e terrorismo à empresas estatais. Considera a possibilidade de ataques cibernéticos em um cenário de ciberguerra.
Qual é o posicionamento em relação ao envolvimento de outros setores civis?	Apesar de envolver outros setores do governo, além das Forças Armadas, não aborda a questão do envolvimento civil.

Fonte: Baseado em France (2013)

No caso da França, não são consideradas novas ameaças especificamente. Isso se deve, de acordo com o Livro Branco francês, ao fato de que as ameaças aludidas no documento já terem sido abordadas na versão anterior, publicada em 2008. No entanto, o documento trata, em sua introdução, da disseminação de riscos e ameaças. Entre elas, o terrorismo, ciberameaças, crime organizado, a proliferação de armas convencionais e nucleares. Riscos pandêmicos, tecnológicos e naturais são tidos como questões estratégicas que podem ter consequências danosas para a França (FRANCE, 2013, p.10).

O Livro Branco da França apresenta uma sessão específica ao combate a ciberameaças, que, conforme o texto, se tornam proeminentes conforme a sociedade francesa passa a depender mais de sistemas informacionais interconectados. A capacidade de se proteger contra ataques cibernéticos é tratada como uma questão de soberania nacional. Assim, como o documento alemão, o Livro Branco francês enaltece a necessidade de desenvolvimento de pessoal e capacidades para operação no ciberespaço. Tal como no caso alemão, não há qualquer menção a ideia de criação do COMCYBER, unidade de guerra cibernética que se tornou operacional três anos após a publicação do Livro Branco francês (REEVE, 2016).

Brasil

A transversalidade entre as novas e as tradicionais ameaças indicaram a necessidade de adequação dos novos temas à realidade brasileira. Com interesse em promover transparência e diálogos entre as instituições nacionais, a sociedade e a comunidade internacional no âmbito da defesa, o Livro Branco de Defesa Nacional (LBDN) brasileiro propõe ser um mecanismo de cooperação entre os países da América do Sul.

Nesse sentido, o setor cibernético foi incluído ao documento no status de prioridade estratégica nacional, juntamente com os setores nuclear e espacial. A incorporação do setor ao LBDN relaciona-se com a criação do Livro Verde: Segurança Cibernética no Brasil, publicado em 2010. Preliminarmente elaborado na intenção de ser referência para a criação de um "Livro Branco: Política Nacional de Segurança Cibernética", o documento apresenta diretrizes estratégicas nacionais de cibersegurança, assim como aponta esforços de cooperação e diálogo internacional, principalmente no âmbito da *Organization for Economic Co-operation and Development* (OCDE).

O Livro Verde designa e elucida os principais setores estratégicos brasileiros em níveis de oportunidades e desafios que envolvem a segurança cibernética, sendo eles: político-estratégico, econômico, social e ambiental, CT&I, educação, legal, cooperação internacional e segurança das infraestruturas críticas. Por meio destes, propõe uma macro-coordenação entre setores e interagências que atuam na esfera da cibersegurança, com a finalidade de fortalecer o espaço cibernético brasileiro. O referido documento deixa claro também que o desenvolvimento de estratégias e normas asseguram o crescimento de incentivos a pesquisa e inovação, gerando a capacitação de recursos humanos, maior proteção das infraestruturas críticas e cooperação nacional e internacional.

Vislumbrando a estruturação da segurança cibernética no Brasil, o Livro Verde apresenta como proposta de agenda inciativas para

> [...] apoiar e fortalecer suas atividades, de forma a viabilizar e agilizar tanto a formulação de políticas, normas e regulação, a pesquisa e o desenvolvimento de metodologias e tecnologias, quanto à cooperação internacional e a implantação e promoção de uma macro-coordenação que propicie a integração de processos, visando assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações de interesse do Estado brasileiro e da sociedade, bem como a resiliência de suas infraestruturas críticas (BRASIL, 2010, p. 25).

Por mais que o Livro Verde não tenha concretizado o objetivo de lançar a política nacional de cibersegurança, possibilitou a abertura do planejamento estratégico nacional de segurança cibernética para a Estratégia Nacional de Defesa (END), para a Política Nacional de Defesa (PND) e, logo, para o LBDN. Os apontamentos propostos alcançaram o escopo de fomentar a proteção e o desenvolvimento do ciberespaço brasileiro, principalmente ao evidenciar a relevância que as demais nações conferem ao tema. Dessa forma, o interesse em atribuir importância ao setor cibernético traduziu-se em determinar premissas para um projeto de ciberdefesa e apresentar esforços de atuações interagências, conforme indicado no LBDN de 2012. Para isso, o Livro Branco designa como responsabilidade do Exército Brasileiro a defesa do espaço cibernético[7].

No âmbito da coordenação do Exército, são indicados os avanços na capacitação de recursos humanos, assim como a competência de agir e proteger o ciberespaço. De forma a estimular o avanço e as inovações tecnológicas para a base industrial de defesa, o LBDN aponta para a construção de sistemas e de componentes críticos nacionais. Além disso, o documento apresenta o Centro de Defesa Cibernética do Exército (CDCiber) como o agente responsável por fortalecer a segurança, possuir a liberdade de ação de resposta a incidentes cibernéticos, capacitar recursos humanos e proteger o ciberespaço brasileiro. Para tais fins, o CDCiber atua em conjunto com outros órgãos governamentais que abrangem o setor.

A inserção do setor cibernético ao âmbito de setores estratégicos de defesa é apresentada no LBDN na forma de "conferir confidencialidade, disponibilidade, integridade e autenticidade aos dados que trafegam em suas redes, os quais são processados e armazenados" (BRASIL, 2012, p. 71). Além de

7 Conforme os mais altos documentos de Defesa do Brasil (LBDN, PND e END) existem três setores estratégicos para a Defesa nacional: cibernético – sob responsabilidade do Exército –; nuclear – sob responsabilidade da Marinha – e espacial, sob responsabilidade da Força Aérea.

demonstrar ser um objetivo a longo prazo, o documento também aponta para ações a serem executadas no curto prazo, tendo em vista a dinamicidade que o setor possui. São elas: i) construção da sede do CDciber; ii) aquisição de infraestrutura, equipamentos de apoio e soluções de *hardware* e *software* de defesa; iii) capacitação de recursos humanos e; iv) projetos que estruturem o setor cibernético.

Tem-se, portanto, que o LBDN expõe de forma abrangente os indicativos e as competências que se atribuem ao setor cibernético. Em questões de conceitos e definições, não foram especificados os temas que compreendem o escopo do espaço cibernético, dificultando a congruência de informações e formulações dos termos para a atuação dos órgãos responsáveis. Não apenas, não foram identificadas as ameaças que são oferecidas ao ciberespaço brasileiro. Em relação a atuação de outros atores na defesa cibernética, o LBDN menciona apenas a participação de órgãos governamentais que já possuíam alguma ligação com o setor.

É importante salientar, ainda, que a primeira edição do Livro Branco de Defesa Nacional brasileiro foi publicada em 2012; a segunda edição, de 2016, somente seria aprovada em dezembro de 2018 pelo Congresso Nacional[8]. O presente artigo utilizou como fonte a versão de 2012 e a minuta do documento de 2016, aprovada na íntegra pelo Congresso[9]. Diante da capilaridade das tecnologias de informação e comunicação na sociedade brasileira, a minuta do LBDN de 2016 alerta para os desafios que são postos ao país pela natureza híbrida ou irregular dos "conflitos do futuro", que aglutinam ações de combate regular com elementos informacionais e cibernéticos, podendo ser realizado por atores estatais e não estatais. O surgimento de guerras cibernéticas, de maneira geral, também é tido como um desafio para a defesa brasileira.

Na minuta do LBDN, tem-se que a "ameaça cibernética tornou-se 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" (BRASIL, 2016. p. 57). Ainda assim, o LBDN não caracteriza especificamente o que seria ameaça cibernética. No entanto, o setor cibernético, em conjunto com o nuclear e espacial, mantém-se considerados estratégicos e prioritários para a defesa nacional.

O documento de 2016 ainda não oferece uma definição clara sobre o que seria segurança cibernética. O ciberespaço é tido como prioridade a partir do momento que, por intermédio dele, se pode causar danos a infraestrutura e a sociedade que está cada vez mais inserida nas tecnologias de informação e comunicação. Em relação às ameaças, o documento comenta brevemente sobre a possibilidade de ataques cometidos por agentes estatais e não estatais, porém não se aprofunda na identificação ou caracterização destes. Por fim, a respeito do envolvimento com o setor civil, o LBDN além de tornar o Exército Brasileiro responsável pela defesa do espaço cibernético, envolve outros setores do governo e militares, considera a participação em fóruns internacionais, e aborda a questão do envolvimento civil, mediante a aproximação das Forças Armadas com o setor privado e a academia.

Dessa forma, é possível visualizar nos documentos de defesa apresentados que os esforços em promover regulações e objetivos claros para a atuação no setor cibernético encontram-se em

8 O decreto legislativo PDS 137/2018 que aprovou as novas diretrizes para a Política Nacional de Defesa (PND), para a Estratégia Nacional de Defesa (END) e a atualização do Livro Branco da Defesa Nacional (LBDN) foi publicado no Diário Oficial da União em 17 de dezembro de 2018.

9 Para uma análise aprofundada dos documentos de defesa do Brasil e de outros países da América do Sul, consultar a obra "Guia de Defesa Cibernética na América do Sul" de Oliveira et al (2017).

fase inicial. Por mais que, no intervalo entre os dias atuais e o LBDN de 2012, tenha sido apresentada a minuta do LBDN em 2016, é demonstrada pouca evolução em questões de objetivos, metas e aspirações entre eles. Tendo em vista a dinamicidade que o espaço cibernético oferece e a velocidade que as ameaças se transformam no mundo contemporâneo, chama-se atenção para a necessidade de tornar os mecanismos efetivos no combate aos ataques cibernéticos, assim como os documentos influírem com clareza as especificidades de atuação para o órgão responsável.

Tabela 3 - Sumário das informações obtidas no Livro Branco de Defesa Nacional (LBDN)[10]

Ano de edição	2016 (minuta)
Existe alguma definição clara de segurança cibernética nos documentos?	Não
O que esses documentos exprimem sobre o setor cibernético?	O setor cibernético é visto como prioritário, pois por intermédio do ciberespaço se pode causar danos a infraestrutura
Quais são as ameaças consideradas?	Estatais e não estatais. Não há uma maior profundidade sobre quais seriam essas ameaças.
Qual é o posicionamento em relação ao envolvimento de outros setores civis?	Envolve outros setores do governo e militares, considera a participação em fóruns internacionais, mas não aborda o envolvimento civil.

Fonte: Baseado em Brasil (2016)

A versão mais recente do LBDN brasileiro determina o estabelecimento do Comando de Defesa Cibernética (ComDCiber) como organização militar conjunta, na qual estão subordinados o CDCiber e a Escola Nacional de Defesa Cibernética (ENaDCiber). A criação do ComDCiber "tem como principais atribuições, dentre outras, planejar, orientar, supervisionar e controlar as atividades operacional, de inteligência, doutrinaria, de ciência e tecnologia, bem como de capacitação no Setor Cibernético de Defesa" (BRASIL, 2016, p. 58). Nesse ponto, é identificada uma progressão institucional da questão cibernética nos documentos brasileiros, em decorrência da criação de um comando mais abrangente e portanto, mais capacitado hierarquicamente em termos de pessoal, recursos e infraestrutura que o CDCiber, como estabelecido pela versão do LBDN de 2012.

A criação do ComDCiber evidencia, portanto, uma evolução na percepção do valor estratégico atribuído ao setor cibernético pelo governo brasileiro como agente securitizador. Contudo, é importante ressaltar que não se trata de uma ramificação das Forças Armadas como ocorre com o CIR alemão e o COMCYBER francês.

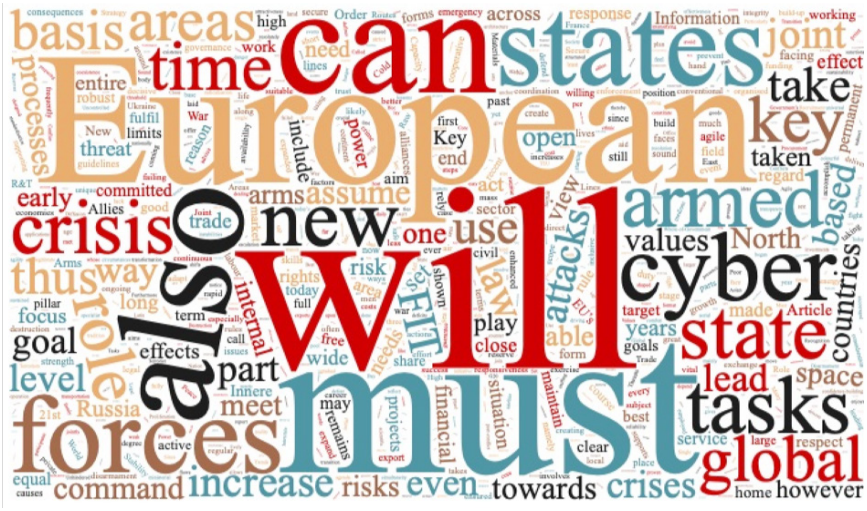
5 **Análise comparativa dos documentos**

No que tange a análise comparada dos conteúdos dos documentos, buscou-se evidenciar os variados níveis de proeminência atribuídos pelos Estados em questão a temas específicos.

10 Apesar de no presente artigo serem abordadas tanto as edições de 2012 quanto de 2016, por questões metodológicas, a análise sumária restringe-se ao último documento, ou seja, a versão mais recente do LBDN publicado pelo Brasil, tal como ocorreu nas análises da Alemanha e França.

Com o intuito de evidenciar a proeminência de determinados temas nos documentos, foi feita a análise de contagem automatizada do número de ocorrências de palavras em cada livro branco, resultando na agregação de palavras a seguir:

Figura 1 - Agregação de palavras do Livro Branco de Defesa da Alemanha



Fonte: Baseado em Germany (2016)

É notória a proeminência do contexto europeu em relação ao nacional. Observa-se, ainda, que a temática cibernética aparece com significada frequência no texto. Isso ocorre devido à utilização ampla do prefixo "cyber" ao longo do livro, empregado para se referir a "ciberameaças", "ciberataques", "ciberespaço", entre outros.

A figura 2 apresenta graficamente as palavras e temas mais presentes no documento francês.

Figura 2 - Agregação de palavras do Livro Branco de Defesa da França

Fonte: Baseado em France (2013)

Sem maiores aprofundamentos, nota-se, rapidamente, a substituição do termo "european", destaque na análise do documento alemão, pela palavra "world", no texto francês. O termo "cyber" não possui no documento francês a mesma proeminência verificada no documento alemão. A agregação de palavras oriunda do Livro Branco francês evidencia um discurso mais imperativo, quando comparado ao documento alemão, enquanto a temática de ameaças aparece de forma mais proeminente ao longo do texto.

Figura 3 - Agregação de palavras do Livro Branco de Defesa do Brasil[11]

Fonte: Baseado em Brasil (2016)

A aglomeração de palavras na minuta de 2016 evidencia a proeminência da participação militar na defesa, quando comparado aos outros países. Enquanto os demais livros brancos não chegam a distribuir atribuições para diferentes forças ou setores civis, a minuta do LBDN é objetivo e categórico, mantendo as áreas de responsabilidade para cada ramo das Forças Armadas e determinando a criação do ComDCiber.

Dando continuidade à análise comparativa, foi desenvolvida a tabela 4 que trata sobre a quantidade de páginas totais dos documentos, o número de páginas que abordam a questão das ameaças, novas ameaças e especificamente a questão cibernética.

Tabela 4 - Comparativo de páginas entre os livros brancos

	Total de Páginas	Páginas dedicadas a ameaças	Páginas dedicadas a novas ameaças	Páginas dedicadas à questão cibernética
Alemanha	143	24	1	28
França	135	52	0	23
Brasil	185	12	1	15

Fonte: Baseado em France (2013), Brasil (2016) e Germany (2016)

11 A incidência de preposições se deve a dois fatores: as peculiaridades da língua portuguesa e a impossibilidade de exclusão de termos na ferramenta de análise empregada.

Como observado na análise específica de cada país, a categorização de "novas ameaças" é quase inexistente, de forma que ocorre a disparidade do número de páginas que abordam a temática das "novas ameaças" e das "ameaças". Isso se dá em decorrência do tratamento dado as ameaças não estatais, que apesar de seu ineditismo no domínio cibernético, são categorizadas como ameaças pelos documentos de defesa. Fato que indica um amadurecimento do discurso securitizador dos países e destoa da concepção de ameaças única e exclusivamente estatais.

Outro ponto relevante corresponde ao número maior de páginas para a questão cibernética em relação às ameaças, elemento que condiz com a interpretação vigente nos documentos de que o ciberespaço não é apenas o espaço para ameaças, mas também um domínio estratégico para o desenvolvimento dos países em questão.

A abordagem comparativa também considerou as palavras chave presentes nos documentos, sobre as quais foram elencados os seguintes termos: Defesa, Segurança, Militar, Exército, Aeronáutica, Marinha, Terrorismo, Drogas e Ciber (com suas variações em inglês para análise dos documentos da Alemanha e França). Foram identificados, em seguida, a frequência na qual os termos aparecem nos documentos, a fim de evidenciar a proeminência de determinados assuntos em relação aos outros.

Tabela 5 - Comparação dos termos-chave

Termos chave	Defesa (Defence)	Segurança (Security)	Militar (Military)	Exército (Army)	Aeronáutica (Air Force)	Marinha (Navy)	Terrorismo (Terrorism)	Drogas (Drugs)	Ciber (Cyber)
Alemanha	53	99	49	2	0	0	13	0	28
França	136	136	83	2	2	4	18	2	24
Brasil	132	73	118	58	39	68	2	4	16

Fonte: Baseado em France (2013), Brasil (2016) e Germany (2016)

Nota-se uma maior proeminência da temática cibernética em relação aos temas terrorismo e drogas, temáticas tradicionais nos documentos de defesa. Essa ocorrência se explica pela atuação do tráfico de drogas e terrorismo através do ciberespaço, em paralelo com as ameaças que surgem no domínio cibernético. Ainda, o ciberespaço não é categorizado somente como uma temática de ameaça, como ocorre com os temas de terrorismo e drogas, mas como um domínio estratégico a ser securitizado e, concomitantemente, desenvolvido do ponto de vista econômico, social, governamental e civil.

É notório também o envolvimento do setor militar no discurso brasileiro, citando os militares e os diferentes braços das Forças Armadas em uma frequência muito maior que os demais países.

A partir da análise comparada dos documentos, é possível identificar congruências e divergências políticas no que tange a valorização estratégica do ciberespaço por nações que estão desenvolvendo suas políticas de defesa cibernética.

Nesse sentido, é importante salientar que dentre os países analisados, o Brasil é o único que não possui documentos voltados especificamente para a cibersegurança no nível estratégico. Por mais que o Livro Verde de Segurança Cibernética de 2010 seja um documento peculiar que tenha servido de base para os documentos de defesa posteriores, não foram criados novos docu-

mentos que condizem com a realidade que o setor cibernético se encontra atualmente. Enquanto Alemanha e França já são possuidoras de documentos específicos vigentes para o setor, sendo eles o *National Cybersecurity Strategy* (GERMANY, 2016) e o *National Cybersecurity Strategy* (FRANCE, 2015), respectivamente; no caso brasileiro, o documento que aborda a questão cibernética é a Doutrina Militar de Defesa Cibernética (BRASIL, 2014).

6 **Conclusões**

A recorrente preocupação com as ameaças oriundas de agentes estatais e não estatais, assim como o reconhecimento de vulnerabilidades infraestruturas e sociais decorrente da maior inserção da sociedade e consequente dependência do espaço cibernético, legitima-o como palco para as relações de poder na atualidade. Dessa forma, a análise da securitização do ciberespaço nos Livros Brancos de Defesa Nacional do Brasil, Alemanha e França auxiliam na determinação e na comparação de estratégias de segurança e defesa nacional.

No momento em que o espaço cibernético é reconhecido como palco de relações econômicas, políticas, militares e socais, entende-se que o discurso securitizador dos Estados toma forma em seus documentos de defesa. Nos documentos consultados e analisados, o setor cibernético é considerado um domínio prioritário e estratégico, no qual são definidas (mesmo que de maneira abrangente) as ameaças e vulnerabilidades que um Estado está sujeito. Os responsáveis pela proteção do Estado no ciberespaço também são determinados. No mais, a prática de identificação de ameaças e objetivos por agentes securitizadores – que neste caso é o Estado – condiz com o processo securitizador capitaneado pela Escola de Copenhague.

Portanto, a recorrente presença da questão do ciberespaço e seu reconhecimento como domínio estratégico e prioritário de um ponto de vista de defesa nacional, legitima e justifica o presente trabalho. Ainda que impostos os desafios teóricos ao serem consideradas as peculiaridades do ciberespaço, buscou-se alinhar uma abordagem prática de análise comparativa do setor cibernético nos Livros Brancos de defesa da Alemanha, França e Brasil. Com isso, compreende-se que as perspectivas do setor cibernético brasileiro ainda devem ser exploradas de forma a direcionar as diretrizes entre os agentes atuantes, assim como oferecer atribuições e possibilidades de crescimento à segurança cibernética no Brasil.

Referências

AMARAL, Arthur Bernardes do. **A Guerra ao Terror e a tríplice fronteira na agenda se segurança dos Estados Unidos**. 2008. Dissertação (Mestrado em Relações Internacionais) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2008.

AMORIM, Celso. Segurança Internacional/ novos desafios para o Brasil. Contexto Internacional, Rio de Janeiro, v. 35, n. 1, p. 287-311, 2013.

BRASIL. Ministério da Defesa. **Livro Verde: Segurança Cibernética no Brasil**. Brasília, 2010.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília, 2012.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. Brasília, 2014.

BRASIL. Ministério da Defesa. **Minuta do Livro Branco de Defesa Nacional**. Brasília, 2016.

BRIDI, Sônia; GREENWALD, Glenn. Documentos revelam esquema de agência dos EUA para espionar Dilma. **Fantástico,** [S.l.], 1 set. 2013. Disponível em: http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html. Acesso em: 26/11/2018.

BUZAN, Barry; WEAVER, Ole; WILDE, Jaap De. **Security:** a new framework for analysis. Boulder: Lynne Rienner Publishers, 1998.

BUZAN, Barry; HANSEN, Lene. **A evolução dos estudos de segurança internacional.** UNESP: São Paulo, 2012.

CARREIRO, Marcelo. A Guerra cibernética: cyberwarfare e a securitização da Internet. **Revista Cantareira**, Niterói, RJ, n. 17, p. 123-137, jul./dez. 2012.

CEPIK, M.; CANABARRO, D. R.; BORNE, T. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: CEPIK, M. (Org.). Do 11 de setembro de 2001 à "Guerra Contra o Terror": reflexões sobre o terrorismo no século XXI. Brasília: Instituto de Pesquisa Econômica Aplicada, 2014. p. 161-186.

CHEN, T. **Cyberterrorism after Stuxnet**. Carlisle: United States Army War College Press, 2014.

COLLIN, B. Future of cyberterrorism: the physical and virtual worlds converge. **Crime and Justice International**, Chicago, v. 13, n. 2, p. 15-18, 1997.

DENNING, D. E. **Cyberterrorism**: testimony before the special oversight panel on terrorism. [S.l.]: Terrorism Research Center, 2000.

FARRET, Nerissa Krebs. A securitização do narcotráfico nos Estados Unidos e a influência no Brasil. **Conjuntura Global**, Curitiba, v. 3, n.2, p. 117-123, abr./jun. 2014.

FRANCE. **French White Paper on defence and national security**. Paris, 2013.

FRANCE. **National Cybersecurity Strategy. Paris**, 2015.

GERMANY. **White Paper on German Security Policy and the future of the Bundeswehr**. Berlin, 2016.

GERMANY. **National Cybersecurity Strategy.** Berlin, 2016.

GOLDANI, Carlos Alberto. **Malwares**. [S.l.]: Unicert Brasil Certificadora, abr. 2005.

HAESBAERT, Rogério. Território e multiterritorialidade: um debate. **Geographia**, Niterói, RJ, v. 9, n. 17, p. 19,46, 2007. Disponível em: http://periodicos.uff.br/geographia/article/view/13531/8731. Acesso em: 12 fev. 2018.

HILDEBRANDT, Mireille. Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace. **University of Toronto Law Journal**, [S.l.], v. 63, n. 2, p. 196-224, 2013.

KALLBERG, Jan; COOK, Thomas. **The unfitness of traditional military thinking in cyber**. **IEEE Access**, Piscataway, v. 5, 2017.

KENNEY, Michael. Cyber-terrorism in a post- Stuxnet world. **Orbis**, Amsterdam, v. 59, n. 1, p. 111-128, 2015.

KUEHL, Daniel T. **From cyberspace to cyberpower**: defining the problem. Washington, DC: National Defense University, 2009.

LIBICKI, Martin C. **Cyberdeterrence and cyberwar**. Santa Monica, CA: Rand Corporation, 2009.

LOBATO, Luisa Cruz; KENKEL, Kai Michael. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, Brasília, v. 58, n. 2, p. 23-43, 2015.

MOTTA, B. V. C. **Securitização e política de exceção**: o excepcionalismo internacionalista norte-americano na segunda Guerra do Iraque. 2014. Dissertação (Mestrado em Relações Internacionais) – Universidade Estadual Paulista Júlio de Mesquita Filho; Universidade Estadual de Campinas; Pontifícia Universidade Católica de São Paulo, São Paulo, 2014.

NYE, Joseph S. **O futuro do poder**. São Paulo: Benvirá, 2012.

OLIVEIRA, Marcos Aurélio Guedes de. (In)Conclusão: Sobre a Necessidade de se Pensar a Defesa a Partir do Poder Cibernético. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo Bento; GONZALES, Selma Lúcia de Moura (Org.). **Segurança e Defesa Cibernética:** da fronteira física aos muros virtuais. Recife: UFPE, 2014. p. 193-196.

OLIVEIRA, Marcos Guedes de et al. **Guia de defesa cibernética na América do Sul**. Recife: UFPE, 2017.

POLLITT, M. Cyberterrorism: fact or fancy? Computer Fraud and Security, Amsterdam, v. 1998, n. 2, p. 8-10, 1998.

PRIVACY INTERNATIONAL. London, 1 Feb. 2011. Disponível em: https://bit.ly/2WdGYIU. Acesso em: 26 out. 2018.

REEVE, Tom. France unveils cyber command in response to 'new era in warfare'. **SC Media UK**, London, Dec. 2016. Disponível em: https://scmagazineuk.com/france-unveils-cyber-command-response-new-era-warfare/article/1475678. Acesso em: 21 dez. 2018.

SAINI, Hemraj; RAO, Yerra Shankar; PANDA, Tarini Charan. Cyber-crimes and theis impacts: A review. **International Journal of Engineering Research and Applications**, Ghaziabad, v. 2, n. 2, p. 202-209, mar-abr, 2012.

SYMANTEC. **Internet security threat report**. Mountain View, CA, abr. 2016. v. 21.

TANNO, Grace. A contribuição da escola de Copenhague aos estudos de segurança internacional. **Contexto internacional**, Rio de Janeiro, v. 25, n. 1, p. 47-80, jun. 2003. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292003000100002&lng=en&nrm=iso. Acesso em: 13 fev. 2019.

WEIMANN, Gabriel. Cyberterrorism: the sum of all fears? **Studies in Conflict and Terrorism**, Abingdon, v. 28, n. 2, p. 129-149, 2005.

WERKHÄUSER, Nina. German army launches new cyber command. DW, Bonn, 01 April 2017. Disponível em: https://p.dw.com/p/2aTfJ. Acesso em: 21 dez. 2018.

WIKILEAKS. **Espionnage Élysée**. [S.l.], 2015. Disponível em: https://wikileaks.org/nsa-france/. Acesso em: 27/10/2017

ZUCCARO, Paulo Martino.Tendência global em segurança e defesa cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. *In*: BARROS, O. S. R.; GOMES, U. M.; FREITAS, W. L. (org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 49-77.