DOI:10.21544/1809-3191/regn.v22n2p381-410

A QUESTÃO DA SEGURANÇA E DEFESA DO ESPAÇO CIBERNÉTICO BRASILEIRO, E O ESFORÇO POLÍTICO-ADMINISTRATIVO DO ESTADO

Eduardo André Araujo de Souza[1]
Nival Nunes de Almeida[2]

RESUMO

O presente trabalho tem por objetivo estudar a Questão de Segurança e Defesa do Espaço Cibernético, seu meio regulatório, político e administrativo no que tange ao Estado Brasileiro. Abordam-se os esforços: a elaboração de políticas públicas, a reestruturação de órgãos governamentais e suas atualizações, e, são apontados desafios para o país como destacado pela Estratégia Nacional de Defesa.

Adota-se como base teórica a linha de pensamento construtivista das Relações Internacionais sob a ótica dos ensaios da Escola de Copenhagen e sua Teoria da Securitização. Considera-se ainda ao final, a corroboração da ideia de grande agilidade na politização e crescente securitização do Espaço Cibernético por parte do Estado Brasileiro suplantando o desafio histórico da baixa percepção do conceito de defesa.

Palavras-chave: Ciberespaço. defesa, segurança, políticas públicas.

[1] Mestre pelo Programa de Pós-Graduação em Estudos Marítimos (PPGEM) da Escola de Guerra Naval (EGN), Rio de Janeiro, RJ, Brasil. E-mail: eduardoandre@yahoo.com.br
[2] Doutor em Engenharia Elétrica. Professor do PPGEM-EGN, Rio de Janeiro, RJ, Brasil. E-mail: nivalnunes@yahoo.com.br

INTRODUÇÃO

Notadamente a primeira década dos anos 2000 no Brasil revelou a busca de uma maior representatividade do Estado Brasileiro junto à comunidade internacional, a estabilidade político-financeira do período permitiu que esforços nesse sentido fomentassem a pretensão incansável de um assento permanente no Conselho de Segurança da Organização das Nações Unidas por meio de ações militares de paz, como a MINUSTHA[3] e UNIFIL[4].

Os objetivos estratégicos e geopolíticos possibilitaram a retomada do investimento na segurança e na defesa sob a forma de projetos como o PROSUB[5] e PROGRAMA FX2[6], impulsionados pelas relações bilaterais das Indústrias de Defesa entre Brasil-França e Brasil-Suécia. Além disso, a questão da segurança cibernética,

[3] MINUSTAH - A Missão das Nações Unidas para Estabilização do Haiti foi criada pela Resolução Nº 1576/2004 do Conselho de Segurança da ONU em seu 5090º encontro (em 29 de Novembro de 2004) para restabelecer a segurança e normalidade institucional do país após sucessivos episódios de turbulência política e violência, que culminaram com a partida do então presidente, Jean Bertrand Aristide, para o exílio. A participação do Brasil foi autorizada pelo Decreto Legislativo Nº 207/2004 publicado no Diário Oficial da União - Seção 1 de 20/05/2004.

[4] UNIFIL - A Força Interina das Nações Unidas no Líbano criada em 1978 pelas Resoluções: Nº 475/1978 do Conselho de Segurança da ONU em seu 2074º encontro e 476/1978 do Conselho de Segurança da ONU em seu 2075º encontro para estabilizar a região meridional libanesa durante a retirada de tropas israelenses da área; reativada em 2006 pela Resolução Nº 1701/2006 do Conselho de Segurança da ONU em seu 5511º encontro (11 de Agosto de 2006). A participação brasileira dá-se desde 2011 com o comando da missão de paz da Força-Tarefa Marítima (FTM) autorizada pelo Decreto Legislativo Nº 741, de 2010.

[5] (PROSUB) - Programa de Desenvolvimento de Submarinos: firmado um acordo de transferência de tecnologia entre Brasil e França. O programa viabilizará a produção de quatro submarinos convencionais, que se somarão à frota de cinco submarinos já existentes. E culminará na fabricação do primeiro submarino brasileiro com propulsão nuclear. O PROSUB vai dotar a indústria brasileira da defesa com tecnologia nuclear de ponta – ponto destacado na Estratégia Nacional de Defesa. A concretização do programa fortalece, ainda, setores da indústria nacional de importância estratégica para o desenvolvimento econômico do país. Priorizando a aquisição de componentes fabricados no Brasil para os submarinos, o PROSUB é um forte incentivo ao nosso parque industrial. Além dos cinco submarinos, o PROSUB contempla a construção de um complexo de infraestrutura industrial e de apoio à operação dos submarinos, que engloba os Estaleiros, a Base Naval e a Unidade de Fabricação de Estruturas Metálicas (UFEM), no Município de Itaguaí. Disponível em: < https://www1.mar.mil.br/prosub/institucional >, acessado em 20 de novembro de 2016.

[6] PROGRAMA FX2 - Projeto FX-2 ou Programa FX-2 é um programa de reequipamento e modernização da frota de aeronaves militares supersônicas da FAB - Força Aérea Brasileira, criado em 2006 no governo do então presidente Luiz Inácio Lula da Silva, em substituição ao programa anterior, denominado Projeto FX, após acréscimos de vários requisitos e uma mudança nos requisitos estabelecidos no então Projeto FX. Disponível em: <http://www1.folha.uol.com.br/fsp/brasil/fc0310200913.htm>. Acesso em: 20 nov. 2016.

percebida em razão de incidentes desta natureza, promovidos ora por entes estatais, ora por organizações autônomas, revelou a vulnerabilidade dos sistemas no âmbito governamental e motivou uma gama de medidas, traduzidas em políticas públicas e leis que regulamentaram ainda mais o Espaço Cibernético[7] Brasileiro.

Houve ainda os eventos de repercussão mundial, nesta segunda década dos anos 2000, como a Jornada Mundial da Juventude (2013), a Copa do Mundo (2014), as Olimpíadas e Paraolimpíadas (2016), que fomentaram a criação de órgãos e políticas públicas, concernentes ao tema, em resposta à crescente sensação de medo presente na sociedade, quanto à potencialidade de uma gama diversa de ameaças, aumentando a preocupação com a proteção de dados confidenciais e *infraestruturas críitcas*[8] em nosso país.

Assim, com base no conceito de segurança numa vertente de pensamento das Relações Internacionais que lida com a ótica do Construtivismo e sua Teoria da Securitização, fundamentadas na Escola de Copenhagen, investiga-se a evolução do tema Segurança e Defesa cibernética na Administração Pública Federal e suas implicações no esforço do Estado Brasileiro em adaptar-se ao novo cenário de ameaças desta nova fronteira tecnológica.

FUNDAMENTOS DE SECURITIZAÇÃO

Não se intenciona aqui revisar os fundamentos teóricos das Relações Internacionais, mas demarcar algumas premissas, para que, em momento oportuno, se possa relacioná-las com o tema central do trabalho. Na visão dos teóricos das Relações Internacionais, o *realismo* define o sistema internacional como anárquico, condicionado pela incessante

[7] Espaço Cibernético ou ciberespaço - Um domínio global dentro do ambiente de informação que consiste de redes interdependente em infraestruturas de tecnologia da informação e dados incluindo a Internet, redes de telecomunicações, sistemas de computador, e processadores e controladores embarcados. (JP 12/03). ESTADOS UNIDOS DA AMÉRICA. Joint Chiefs of Staff. JP 3-13: Information Operations. 2006.
Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>. Acesso em: 18 ago. 2016. (tradução dos autores).

[8] Infraestruturas Críticas (IC) - instalações, serviços, bens e sistemas exercem significativa influência na vida de qualquer pessoa e na operação de setores importantes para o desenvolvimento e manutenção do país, como é o caso do setor industrial. Elas são importantes pelas facilidades e utilidades que fornecem à sociedade e, principalmente, por subsidiarem, na forma de recurso ou serviço, outras Infraestruturas Críticas, mais complexas ou não. Ao passar dos anos, a interdependências verticais das Infraestruturas Críticas, caracterizadas por um baixo acoplamento entre elas, deu lugar às interdependências horizontais altamente acopladas, com muitos pontos de interação em suas dimensões (BAGHERY, 2007).

busca de poder pelos Estados, priorizando a segurança militar na política internacional. Nesse sentido, os realistas enxergam a segurança como um segmento do poder, em que um ator alcança sua segurança quando ocupa uma posição dominante. Dessa forma, a anarquia caracteriza-se pela inexistência de um formulador de política internacional que seja independente e soberano acima do nível estatal. Portanto, a visão predominante do conceito de segurança realista está ligada ao poder de cada Estado para assegurar a sua sobrevivência, sendo este poder obtido em linhas gerais pelo emprego da força militar.

Clausewitz lembra ainda que os litígios entre Estados no modelo realista culminam através da violência extremada dos conflitos bélicos, sendo estes a expressão da política por outros meios:

> "A guerra, então, é apenas um verdadeiro camaleão, que modifica um pouco a sua natureza em cada caso concreto, mas é também, como fenômeno de conjunto e relativamente às tendências que nela predominam, uma surpreendente trindade em que se encontra, antes de mais nada, a violência original de seu elemento, o ódio e a animosidade, que é preciso considerar como um cego impulso natural, depois, o jogo das probabilidades e do acaso, que fazem dela uma livre atividade da alma, e, finalmente, a sua natureza subordinada de instrumento da política por via da qual ela pertence à razão pura." (CLAUSEWITZ, 2010, p.30).

A partir deste entendimento, optou-se pela busca de um segmento teórico das Relações Internacionais que ampliasse seus fundamentos não só na inter-relação de estruturas Estatais visto que o conceito de novas guerras[9], e a assimetria destas, acaba por envolver uma significativa ordem de atores não estatais, desde Organizações Não Governamentais (ONGs) a grupos paramilitares e terroristas, que não são privilegiados nos estudos do Realismo tão pouco do *Neorrealismo*[10].

[9] Ver Kaldor, Mary (2013) In defence of new wars. Stability: International Journal of Security and Development.

[10] O Neorrealismo ou realismo estrutural é uma teoria das Relações Internacionais, apresentado inicialmente por Kenneth Waltz em seu livro de 1979, Theory of International Politics. O neorrealismo surgiu a partir da doutrina estadunidense de ciência política, e reformula a tradição realista de Edward Hallett Carr, Hans Morgenthau e Reinhold Niebuhr. Os realistas em geral argumentam que o poder é o fator mais importante nas relações internacionais. O neorrealismo ainda se subdivide em ofensivo e defensivo (tradução nossa). Jakobsen, Jo. Neorealism in International Relations – Kenneth Waltz. Disponível em: <http://www.popularsocialscience.com/2013/11/06/neorealism-in-international-relations-kenneth-waltz>. Acesso em: 26 Jul. 2016.

Na visão construtivista, linha dominante de pensamento da Escola de Copenhagen[11], considera-se a anarquia como um constructo social, , sendo esta o que os Estados fazem dela, portanto diferenciando-se da visão realista nesse ponto.

No que tange à segurança internacional, construtivismo e realismo aproximam-se, na medida em que têm o Estado como unidade privilegiada na estrutura política internacional. Assim, cria-se a ideia de que a realidade é socialmente construída, em que suas estruturas são formadas por ideias compartilhadas (WENDT, 1992).

Logo, não há limitação do conceito de segurança, já que o mesmo sofre continuamente processos de construção e reconstrução, abrindo espaço para a permanente possibilidade de transformação. No que diz respeito ao campo da segurança, as possíveis mudanças sistêmicas acontecem sempre relacionadas ao Estado. Assim sendo, o construtivismo possui uma maior abertura empírica que possibilita maior moldagem para tratar também de questões relacionadas às percepções de ameaça à segurança. Essas percepções, então, são construídas a partir de estímulos externos.

Diante dos questionamentos sobre segurança, ameaças e paz na agenda de segurança internacional, e por estes relacionarem-se estritamente às temáticas militares, fez-se necessário a criação de conceitos e categorizações específicas para acompanhar a demanda de diferentes tópicos que foram incluídos nas agendas estratégicas dos Estados. Assim, Buzan et al (1998, p.23) desenvolveram a teoria da securitização, a qual se refere ao processo metodológico de apresentação de uma questão em termos de segurança.

Dessa forma, a dinâmica de cada uma das categorias/setores de segurança pode ser classificada como Militar, Ambiental, Social, Econômica e Política, e determinada por Objetos de referência, como Atores funcionais, Atores de securitização e Dinâmica de funcionamentos particulares (BUZAN et al, 1998, p. 27).

[11] A Escola de Copenhagen de Estudos de Segurança é uma escola de pensamento acadêmico com suas origens nas teorias de Relações Internacionais publicadas na obra de Barry Buzan: Povos, Estados e o Medo: O Problema de Segurança Nacional em Relações Internacionais. A Escola de Copenhagen coloca particular ênfase nos aspectos sociais da segurança. Seus principais teóricos associados com a escola são: Barry Buzan, Ole Wæver e Jaap de Wilde. Muitos dos membros da escola trabalharam no Instituto de Pesquisa da Paz de Copenhagen. A principal contribuição da Escola de Copenhagen e a obra: Segurança: Um Novo Enquadramento para Análise, escrito por Buzan, Wæver e de Wilde.A teoria centra-se em três conceitos-chave: Setores; Complexos de Segurança Regionais; Securitização. (Eriksson, Johan 'Revisiting Copenhagen Observers or Advocates?: On the Political Role of Security Analysts', Cooperation and Conflict 34, n. 3, 1999, p. 311-3.

Os setores para securitização seriam espécies de lentes pelas quais as questões são observadas. O analista, por exemplo, deve ter consciência de que, em cada setor, encontram-se valores e características próprios, e de que a natureza das ameaças modifica-se de setor para setor, tornando a securitização institucional ou *ad hoc* (BUZAN et al, 1998, p.27, tradução nossa). Nas palavras dos autores da Escola de Copenhagen, "a definição exata e os critérios de securitização são constituídos pelo estabelecimento intersubjetivo de uma ameaça existencial com um indicativo suficiente para ter efeitos políticos substanciais" (BUZAN et al, 1998, p.25, tradução nossa).

No que se refere aos objetos, Buzan et al (1998, p.25) afirmam também que qualquer grupo ou indivíduo pode tornar-se um objeto de referência, caso tenha sua segurança/existência ameaçada. Porém, para que uma ameaça se torne um problema de segurança na agenda política, é preciso que "um representante estatal declare uma condição de emergência, reivindicando o direito de utilizar quaisquer meios necessários para barrar um desenvolvimento ameaçador" (BUZAN et al, 1998, p.21, tradução nossa).

No construtivismo, trabalha-se ainda a ideia de segurança como "um discurso por meio do qual as identidades e as ameaças são constituídas em vez de ser uma condição objetiva" (BUZAN; HANSEN, 2012, p.366).

Sendo assim, o ator de securitização é aquele que securitiza uma questão, declarando que o objeto de referência encontra-se ameaçado. Logo, o ator funcional é aquele que afeta a dinâmica do setor do qual faz parte.

Dessa forma, enquadra-se a segurança como um tipo especial de política, definindo a abrangência de questões públicas em três categorias, a saber: não politizado, politizado e securitizado. Buzan et al (1998, p.23) afirmam que a primeira acontece quando o Estado não lida e não faz da questão um assunto de debate público e de decisão e, portanto, não requer atenção ao nível político; a segunda ocorre quando o assunto torna-se parte de políticas públicas, exigindo decisão governamental e alocação de recursos; até chegar à condição de securitizado, significando que a questão é vista como uma ameaça existente, que requer medidas de emergência aceleradas, podendo violar regras legais e sociais, sendo, assim, uma versão mais extremada da politização.

Nesse sentido, é importante ressaltar que se deve entender o conceito de ameaça como "qualquer acontecimento ou ação (em curso ou previsível) que contraria a consecução de um objetivo e que pode ser causador de danos, materiais ou morais [para algum objeto], podendo ser de

variada natureza" (COUTO, 1988, p.329). Desse modo, os teóricos da Escola de Copenhagen veem a segurança como uma questão de sobrevivência e, portanto, quando existir qualquer preocupação, esta será definida como sendo uma ameaça existencial, não necessariamente pela existência em si, mas pela justaposição a algum objeto referente, podendo ser, tradicionalmente, mas não obrigatoriamente, o Estado, incorporando o governo, o território e a sociedade.

Nesse contexto, apresenta-se uma narrativa de um processo de securitização ocorrido durante os protestos populares no Brasil em 2013, quando fica claro que, em decorrência de todas as suas etapas, culminou-se com as ações "*não discursivas*" de monitoração das redes sociais pelo Centro de Defesa Cibernética (CDCiber) e pela Agência Brasileira de Inteligência (ABIN). Nesse caso, os Órgãos de Inteligência, como Agente Securitizador, identificam uma Ameaça (à paz social) e convencem as autoridades (Poder Executivo) a adotar medidas securitizadoras, atuando assim na monitoração das redes sociais.

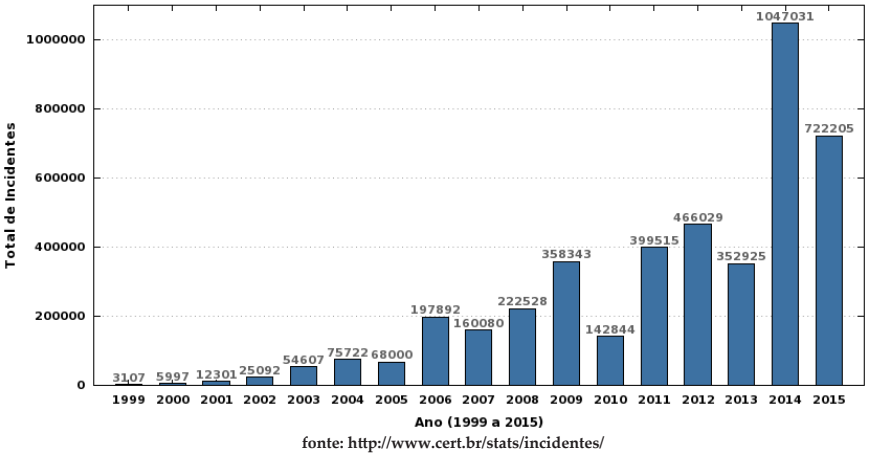
A QUESTÃO DA CIBERNÉTICA NO BRASIL: POLITIZAÇÃO VERSUS SECURITIZAÇÃO?

> "a preocupação tanto com os conteúdos quanto com o tipo de uso, e a respectiva segurança da Internet, crescem em igual medida aos desenvolvimentos tecnológicos e ao número de usuários, observados, especialmente, ao longo dos últimos anos." (Livro Verde – Segurança Cibernética no Brasil, Brasil, 2010, p.31).

De acordo com o Centro de Estudos de Resposta e Tratamento de Incidentes de Segurança para a Internet Brasileira (CERT.br), o Brasil possui o maior número de internautas da América Latina, cerca de 50 milhões[12]. Em 2013, o CERT.br recebeu notificações de 352.925 tipos de ataques no país, número que chegou a alcançar 466.029 em 2012. Comparando-se com o relatório de 2002, quando se reportou pouco mais de 25.000 ataques, os incidentes cibernéticos apresentaram um aumento superior a 1.800% em uma década. Isso demonstra o crescimento vertiginoso não só de usuários de internet no país como também na quantidade e diversificação dos ataques virtuais, conforme constatado no *Gráfico I* abaixo. Ainda de acordo com as estatísticas de 2015, advindas do *Gráfico II*, os incidentes reportados partiram majoritariamente de dentro do território nacional (54,02%), seguido por EUA (11,16%) e, depois, China (10,59%).

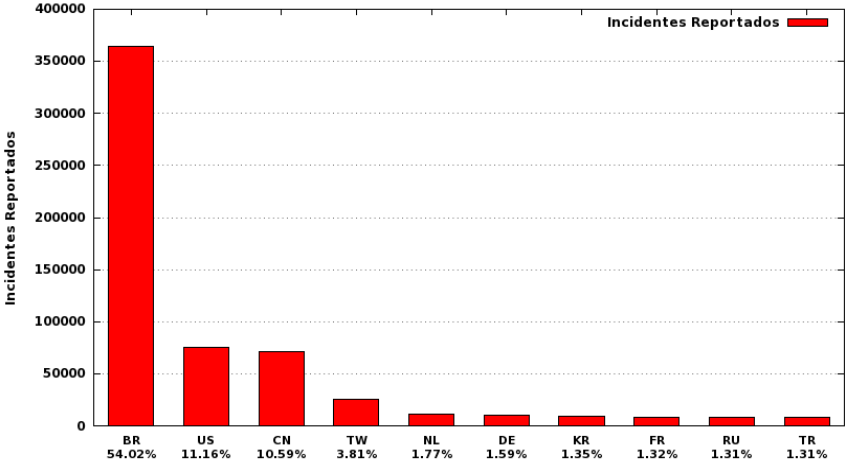
[12] Ver <http://cetic.br/noticia/nic-br-divulga-segunda-parte-da-pesquisa-tic-domicilios-sobre-o-uso-da-internet-no-brasil/>. Acesso em 10 out 2016.

Gráfico I: Total de incidentes reportados ao CERT.br por ano



fonte: http://www.cert.br/stats/incidentes/

Gráfico II: CERT.br Incidentes reportados (Top 10 CCs origem de ataques)



fonte: http://www.cert.br/stats/incidentes/2015-jan-dec/top-atacantescc.png

Em 2011, os incidentes reportados pelo Centro tinham como alvo, preferencialmente, empresas privadas e bancos. Já nos anos seguintes, os ataques estenderam-se para *sites* e sistemas governamentais, entre eles, os *sites* da Presidência da República e da Receita Federal. Essa situação revela uma potencial preocupação com a fragilidade do sistema de segurança cibernética do governo brasileiro [13].

[13] Ver http://www.cert.br/stats/incidentes/. Acesso em: 10 Out. 2016.

Por exemplo, um ataque que paralisasse o *site* da Receita Federal, às vésperas do prazo de entrega das declarações de imposto de renda do cidadão brasileiro, poderia trazer grandes prejuízos não só de ordem financeira para a União, mas à imagem da Secretaria da Receita Federal.

Portanto, faz-se necessário uma categorização e tipificação das várias formas de conflito no ciberespaço, das possíveis vulnerabilidades, das ameaças e das suas fontes, "para que sejam alocadas responsabilidades aos cidadãos, ao Estado; sejam estabelecidas contramedidas e investigações criminais" (DUNN, 2010, p.1, tradução nossa). De acordo com Buzan et al (1998, p.25), dependendo de como se enquadra uma questão, as respostas a ela irão variar. Assim, quanto mais securitizado for um evento social, mais excepcional e extremo podem ser as respostas governamentais a ele. Tratar da mesma forma o ativismo, os crimes, o terrorismo e os atos de guerra cibernéticos seria um erro. Por isso mesmo, o Guia de Referência para a Segurança das Infraestruturas críticas da Informação (CANONGIA; GONÇALVES JÚNIOR; MANDARINO JUNIOR, 2010, p.129-139) conceitua e determina tais elementos.

Ainda que se possa afirmar que o Espaço Cibernético não tenha sido plenamente securitizado no Brasil, pode-se dizer que a cibernética é objeto de preocupação no âmbito da segurança e da defesa. Assim, a cibernética tem sido uma área priorizada recentemente pelo governo brasileiro, notando-se isso especialmente pelo que afirma Celso Amorim, ex-ministro da Defesa:

> "Ao contrário de cem anos atrás, tempo do Barão do Rio Branco, quando o Brasil comprava do exterior praticamente todos seus principais equipamentos de defesa sem a capacidade de nacionalizar sua produção, hoje o desenvolvimento de capacidades autônomas na indústria de defesa é um objetivo fundamental de nossa política. A Estratégia Nacional de Defesa, cuja segunda edição foi lançada no ano passado e agora acaba de ser apreciada pelo Congresso Nacional, define três áreas prioritárias desse esforço: a nuclear, a cibernética e a espacial". (AMORIM, 2013, p.308-309).

Da mesma forma, o general do Exército Brasileiro e então comandante do Centro de Defesa Cibernética (2011) no Brasil, José Carlos dos Santos, em entrevista para a revista Época, ao ser perguntado se a cibernética será um novo campo das Forças Armadas, afirmou:

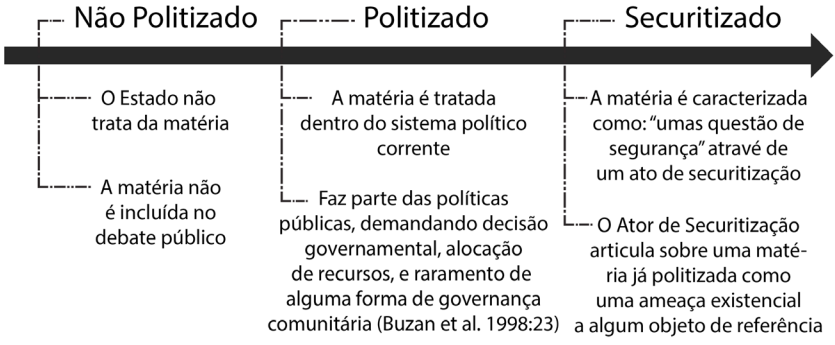
> "É uma nova governança. Eu diria que diversos países estão na mesma situação. Os Estados criaram seu comando cibernético em 2009. A Alemanha ativou seu centro de defesa cibernética neste ano, a Inglaterra no ano passado. O Brasil criou o Centro de Defesa Cibernética em agosto do ano passado. Essa era digital é um contexto novo. [...] Podemos, sim, contratar civis. Está dentro de nossas previsões a contratação de especialistas em regime de prestação de serviços. Basicamente estamos cuidando da formação do nosso pessoal. A partir de 2012, a matéria tecnologia para informação e comunicação se tornará obrigatória para todos os nossos futuros oficiais. Nas escolas de formação dos nossos sargentos, o assunto também será introduzido. É uma possibilidade contratar [hackers]. A imprensa diz que os Estados Unidos já fazem isso. Eles teriam até um grupo de hackers que trabalharia em prol do governo americano. Eles não se identificam como tal, mas trabalham. [No Brasil] São registrados milhares de incidentes de rede por dia. Logicamente um porcentual desses incidentes é de tentativas de intrusão em serviços internos do Exército. Recentemente, tivemos no Recife uma intrusão num serviço social, de distribuição de água. Um grupo, o FatalErrorCrew, conseguiu acessar um banco de dados dessa operação. Foi dado crítico? Bom, crítico, não. Mas mostrou uma vulnerabilidade. Eram dados de militares vinculados àquela operação". (SANTOS, 2011).

Sendo assim, encontra-se no âmbito militar brasileiro uma preocupação com a defesa e a segurança cibernética dos sistemas virtuais e da infraestrutura do país. A política adotada pelas Forças Armadas brasileiras é a de defesa-ativa[14], não buscando atacar outras nações, seguindo a linha pacifista histórica de posicionamento e obediência direta ao texto constitucional em seu Artigo 4º incisos I a VII, visando primordialmente proteger os próprios sistemas e neutralizar possíveis ataques e intrusões.

Levando-se em consideração a elaboração de Buzan et al (1998), referente à categorização do tratamento de questões públicas, podemos dividir o tratamento da segurança cibernética pelo Brasil em três etapas: até o ano 2000, não politizado; a partir de então, politizado; e em 2008, se inicia um processo de securitização, conforme se ilustra na Figura 1.

[14] Defesa-ativa: Capacidade de identificar o ataque cibernético e sua origem e na mesma medida, se oportuno for, retaliar o atacante e seus sistemas. Disponível em <https://gestao.consegi.serpro.gov.br/cobertura/noticias/a-favor-de-uma-defesa-ativa-contra-ataques-ciberneticos>, acesso em: 16 ago. 2016.

Figura 1: Spectro de Securitização



fonte: Contemporary Security Studies, pag. 170 [15]

Cronologicamente, até o final dos anos 1990, não foram criados documentos relevantes concernentes ao tema, nem debates ou preocupações quanto aos riscos e às vulnerabilidades foram observados. Certamente, pelo fato da cibernética e seus elementos se encontrarem em processo de formação e evolução, juntamente com as Tecnologias de Informação e Comunicação (TICs). A partir de então, conforme o Estado Brasileiro percebe a necessidade e a importância de tal tecnologia, há uma institucionalização da questão, designação de capacidades e demarcação de conceitos.

A partir do ano 2000, tem-se o marco inicial do processo de politização da questão de Segurança e Defesa Cibernética com o Livro Verde Sociedade da Informação no Brasil (TAKAHASHI, 2000), do Ministério da Ciência e Tecnologia. O livro representa uma visão mais ampla para estabelecer contornos e diretrizes de um programa de ações rumo à Sociedade da Informação no Brasil.

O referido programa versa sobre as oportunidades e os riscos de uma sociedade em rede e informatizada; sobre economia, trabalho e comércio eletrônico; sobre universalização dos serviços de internet como forma de

[15] Collins Alan. Contemporary Security Studies. Oxford University Press, 12 de jan de 2016.

cidadania; sobre como a informatização auxilia a educação; sobre transparência governamental para colocar o "governo ao alcance de todos", além de abordar questões mais específicas de Pesquisa e Desenvolvimento (P&D) e infraestrutura avançada. Basicamente, são definidos conceitos ligados à informática e são propostos projetos de disseminação da internet pelo território nacional.

Em termos de segurança cibernética (até então denominado segurança da informação), no mesmo ano, o governo publicou o Decreto No. 3.505 de 13 de junho de 2000, instituindo a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, aplicando a definição de pressupostos básicos, conceituações, objetivos, diretrizes, alocação de recursos e de responsabilidades. A legislação federal ainda instituiu o Comitê Gestor da Segurança da Informação (CGSI), o qual tinha a função de assessoria e era subordinado à Secretaria-Executiva do Conselho de Defesa Nacional; portanto, nota-se uma preocupação inicial com a segurança da informação do Estado.

Em seguida, por meio da Lei Federal No 10.683, de 28 de maio de 2003, foi criado o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o qual tinha como uma de suas competências a de coordenar as atividades de inteligência federal e de segurança da informação. O GSI/PR passou por diversas revisões de funções e atividades, tendo sido atualizado com o Decreto No. 8.100 de 04 de setembro de 2013.

Ainda, na estrutura do GSI/PR, destacam-se dois órgãos "cujas atividades por eles desenvolvidas inserem-se no esforço de construção de estratégia da segurança cibernética" (BARROS, 2011). Não obstante, o Decreto Presidencial No. 5.772 de 08 de maio de 2006 criou o Departamento de Segurança da Informação e Comunicações (DSIC), com o objetivo de exercer exatamente as atividades de segurança da informação. O segundo órgão é a Agência Brasileira de Inteligência (ABIN), o qual atua nas vertentes de inteligência e contra inteligência em prol do Estado, tendo como função, entre outras, "avaliar as ameaças internas e externas à ordem constitucional".

Outros órgãos criados serviram para potencializar o surgimento da segurança cibernética, quais sejam o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC), o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Publica Federal (CTIR.gov), o Comitê Gestor da Internet (CGI), o Núcleo de Informação e Coordenação do Ponto BR (Nic.br) – este último mantendo também o já citado CERT.br –, o Centro de Estudos sobre as Tecnologias

da Informação e da Comunicação (CETIC.br) e o Centro de Estudos e Pesquisas em Tecnologias de Rede e Operações (CEPTRO.br), entre outros.

Assim sendo, até 2005, houve um processo de politização do tema da segurança cibernética – inicialmente entendido como segurança da informação –, com a criação de órgãos, documentos oficiais, discussões, centros de estudos, determinação de recursos, etc. O tema ainda não havia alcançado um grau de preocupação concernente a uma ameaça existencial propriamente dita, mas apenas um objeto de preocupação inicial e de debate político. Observa-se, assim, que há um processo de entendimento da área cibernética como uma questão de segurança, senão plenamente, ao menos potencialmente existente, iniciando, portanto, a construção de uma ideia de securitização.

Nesse sentido, a Política Nacional de Defesa (Decreto No. 5484, de 30 de Junho de 2005) menciona brevemente o tema em duas seções. Dessa forma, temos as primeiras citações diretas referentes ao tema "ataque cibernético":

> "6.19 **Para minimizar os danos de possível ataque cibernético**, é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento. [...] XII - **aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos** e, se for o caso permita seu pronto restabelecimento". (BRASIL, 2005, grifo nosso).

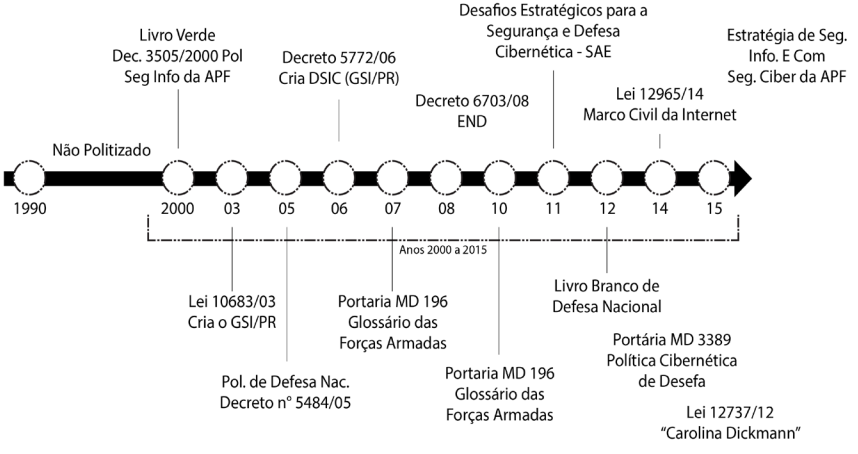
A partir dessa Política Nacional de Defesa, ampliam-se as produções de documentos legais brasileiros os quais fomentam o debate público de Defesa Nacional, incluindo então a segurança cibernética; sendo eles o Glossário Militar das Forças Armadas (2015), a Estratégia Nacional de Defesa[16] (2008; 2012), o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (CANONGIA; GONÇALVES JÚNIOR; MANDARINO JUNIOR, 2010), o Livro Verde: Segurança Cibernética no Brasil (CANONGIA; MANDARINO, 2010), o relatório

[16] A Estratégia Nacional de Defesa (END) foi aprovada pelo Decreto Nº 6.703, de 18 de Dezembro de 2008; revisada em 2012 de acordo com o Decreto Legislativo Nº 373, de 25 de Setembro de 2013 implicando em alterações na Política Nacional de Defesa e no Livro Branco da Defesa

Desafios Estratégicos para a Segurança e Defesa Cibernética (BARROS; GOMES, 2011), o Livro Branco de Defesa Nacional (BRASIL, 2012a), a Política Cibernética de Defesa (BRASIL, 2012b) e a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (BRASIL, 2015). A consequência é a percepção pelo Estado brasileiro da potencialidade e dos riscos de ataques cibernéticos às infraestruturas críticas e da segurança da informação no país, alocando publicamente espaços em documentos legais que promovem a discussão e o crescimento da importância do tema, tendo o Gabinete de Segurança Institucional da Presidência da República e o Exército Brasileiro como órgãos principais de atuação no setor cibernético.

Em síntese, pode-se apresentar a evolução da tratativa da segurança cibernética pelo Estado Brasileiro com um direcionamento da questão para uma possível securitização. Temática esta que, nos anos 1990, ainda se encontrava não politizada e que, em consequência da maior integração da sociedade brasileira com o Espaço Cibernético, somada a eventos de ordem internacional (*Malware* Stuxnet – Irã/2011, e ciberataque DDos – Estônia/2007), adquiriu maior relevância, principalmente nas forças armadas brasileiras, que responderam, por meio de documentos oficiais, conforme ilustrado na Figura 2, os quais serão tratados na próxima seção.

Figura 2: Arcabouço Politico-Administrativo do Espaço Cibernético Brasileiro



fonte: Elaborado pelos autores

RESPONSABILIDADES, POLÍTICAS E ESTRATÉGIAS NO ESPAÇO CIBERNÉTICO DO BRASIL

Em um primeiro momento, cabe relembrar uma diferenciação semântica, descrita no Glossário das Forças Armadas (BRASIL, 2015) , entre defesa e segurança e, então, estudar sua aplicação e estruturação no ambiente cibernético brasileiro. O termo defesa é entendido como "o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança" (BRASIL, 2015, p.76), ou ainda, como uma "reação contra qualquer ataque ou agressão real ou iminente". (BRASIL, 2015, p.76).

Por sua vez, segurança é colocada como uma "Condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais. Sentimento de garantia necessária e indispensável a uma sociedade e a cada um dos seus integrantes, contra ameaças de qualquer natureza. Condição que resulta do estabelecimento e conservação de medidas de proteção que assegurem um estado de inviolabilidade contra atos ou influências hostis" (BRASIL, 2015, p.252).

A segurança no âmbito cibernético contempla ações que compreendem aspectos e atitudes tanto preventivas quanto repressivas, enquanto defesa cibernética refere-se a ações operacionais, de caráter ofensivo, caracterizadas por ataques cibernéticos (neste sentido composto pela participação de elementos estatais). Sendo assim, apesar de algumas diferenças conceituais, não se pode isolar completamente um conceito do outro.

Existe uma interligação de atribuições em relação ao setor cibernético que demanda atuação tanto em defesa quanto de segurança, haja vista que, no meio cibernético, a origem é de difícil determinação, os meios utilizados e os danos prováveis de um ataque podem atingir tanto sistemas militares como também serviços públicos da sociedade (CANONGIA, 2009, p.98). Nessa linha, o então Ministro da Defesa à época, Celso Amorim, em discurso de abertura no terceiro Seminário de Defesa Cibernética em outubro de 2012 pronunciou-se da seguinte maneira:

> "Não tenho dúvidas, por exemplo, de que a proteção de estruturas críticas do país – usinas hidroelétricas, linhas de transmissão, bases de dados do sistema financeiro, para não falar dos próprios meios das Forças Armadas

> – pertencem à Defesa. A identificação e perseguição de *hackers* ou *crackers* é tarefa da Segurança [pública]. Mas há áreas cinzentas entre uma e outra". (AMORIM, 2012).

Dessa forma, no Brasil, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e o Ministério da Defesa (MD) – acompanhado ainda pela Secretaria de Assuntos Estratégicos (SAE), pela Marinha do Brasil, pela Força Aérea Brasileira e pelo Exército Brasileiro (catalizador do assunto conforme indicado no Tópico CT&I, Item2, pag. 37 da Estratégia Nacional de Defesa) –, atuam na condução das políticas, debates públicos e projetos do setor cibernético para o país. No tocante à segurança pública, a identificação de *hackers* em território nacional, por exemplo, fica sob a responsabilidade da Polícia Federal (PF) – subordinada ao Ministério da Justiça, como atributos de crime comum, ou seja, a PF estaria encarregada por ações de prevenção de incidentes e de repressão também no âmbito cibernético. No entanto, ao se levar em consideração a participação das Forças Armadas (Exército) nas ações de segurança cibernética em grandes eventos que ocorreram no país, tais quais: a Conferência Rio+20 em 2012, a Copa das Confederações em 2013 e a Copa do Mundo em 2014, notamos uma situação nebulosa, isto é, uma sobreposição de atribuição de funções em operações.

Dessa forma, o GSI/PR e o MD destacam-se na construção de um ambiente politizado que caminha para a securitização da cibernética, tornando-se os líderes na elaboração das diretrizes desse setor. Nesse sentido, o GSI/PR tem como uma de suas funções de coordenar: a inteligência e a segurança da informação, transformando-a na engrenagem principal para a organização da estratégia da segurança cibernética no país (MANDARINO JR., 2009). Da estrutura do GSI/PR, destacam-se ainda o DSIC e a ABIN.

O DSIC tem como atribuições, entre outras, regulamentar a segurança da informação e comunicações para toda a Administração Pública Federal (APF), realizar acordos internacionais de troca de informações sigilosas, ser o ponto de contato com a Organização dos Estados Americanos (OEA) para assuntos de terrorismo cibernético e manter o centro de tratamento e resposta (CERT.br) a incidentes nas redes de computadores da APF.

A ABIN atua nas tarefas de inteligência, por meio da produção de conhecimentos sobre fatos e situações de imediata ou potencial influência no processo decisório; na ação governamental, sobre a salvaguarda e sobre a segurança da sociedade e do Estado; e nas atividades de contra inteligência pela adoção de medidas que protejam os assuntos sigilosos relevantes para o Estado e a sociedade e que neutralizem ações de inteligência executadas em benefício de interesses estrangeiros.

A construção da securitização cibernética não ocorre tão somente por documentos legais e criação de órgãos da APF, mas também por meio de discursos públicos. Primeiramente, durante a 68ª Assembleia Geral das Nações Unidas, em discurso de abertura, a então presidente do Brasil Dilma Rousseff proferiu as seguintes palavras:

> "As tecnologias de telecomunicação e informação não podem ser o novo campo de batalha entre os Estados. Este é o momento de criarmos as condições para evitar que o espaço cibernético seja instrumentalizado como arma de guerra, por meio da espionagem, da sabotagem, dos ataques contra sistemas e infraestrutura de outros países" (ROUSSEFF, 2013).

Percebe-se, nesse caso, a conclamação internacional para a construção de uma governança[17] global da internet e uma real preocupação com os riscos de um ataque cibernético, especialmente quando coloca os sistemas e infraestruturas como objetos de referência e, portanto, como algo existencialmente ameaçado. O discurso da presidente ainda demonstrou preocupação com a privacidade e com os dados pessoais dos cidadãos brasileiros, alvo de espionagem pela agência americana *National Security Agency* (NSA) em 2013, colocando, assim, a sociedade brasileira como um objeto referencial. Ademais, o fato gerador provocado pelo incidente de violação de segurança cibernética foi estopim e motivador para que, em 2014, fosse aprovado o Marco Civil da Internet, projeto que estava com pauta de votação trancada desde sua proposição em 2009. Ainda que não tenha propriamente fins de defesa ou segurança nacional, a Lei Ordinária de Nº 12.965, de 23 de Abril de 2014 regula a utilização da internet no país, prevendo princípios, garantias, direitos, responsabilidades e deveres para usuários e empresas, tratando de neutralidade, privacidade, retenção de informações e dados, entre outros. Portanto, esse Marco Civil representa uma importante regulamentação interna e, igualmente, uma abertura ainda maior da discussão do tema para a sociedade.

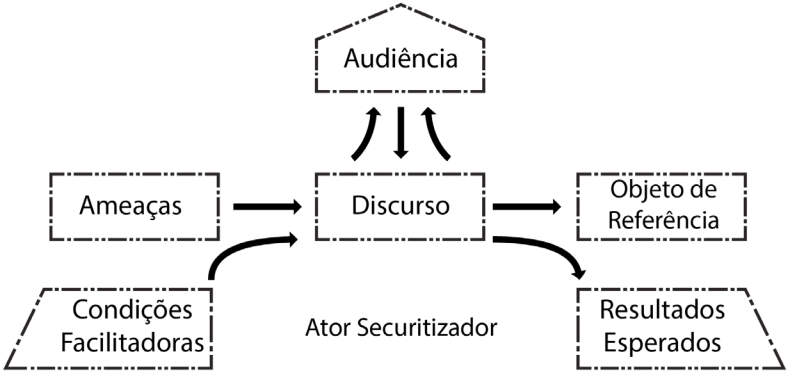
[17] "Governança é um conjunto de práticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, otimizar a aplicação de recursos, reduzir os custos, suportar as melhores decisões e consequentemente alinhar TI aos negócios." PERES, João Roberto. A vez da governança corporativa. Revista Abinee. Numero 43, pagina 25, Outubro 2007. Disponível em: http://www.abinee.org.br/informac/revista/43j.pdf. Acesso em: 16 ago. 2016.

Anteriormente, na apresentação do Livro Verde: Segurança Cibernética no Brasil (BRASIL, 2010b), o então Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República, Jorge Armando Felix, não só apregoou a necessidade de garantir a segurança nacional, como também proclama a formulação de uma Política Nacional de Segurança Cibernética, expressando o tema como uma ameaça à segurança estatal:

> "Assim, motivado por esta missão e considerando a necessidade de assegurar dentro do espaço cibernético ações de segurança da informação e comunicações como fundamentais para a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação; a possibilidade real e crescente de uso dos meios computacionais para ações ofensivas por meio da penetração nas redes de computadores de setores estratégicos para a nação; e o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade; foi instituído Grupo Técnico para estudo e análise de matérias relacionadas à Segurança Cibernética. [...] Recomendo, portanto, a leitura desta obra, cuja publicação considero significativo incremento no arcabouço de documentos que objetivam garantir a Segurança Nacional, e convido-os a contribuir com propostas e sugestões para a evolução da mesma, visando formular, colaborativamente, à Política Nacional de Segurança Cibernética" (CANONGIA; MANDARINO, 2010, p.5-6).

Ao final de suas palavras, percebe-se um chamamento à audiência pública, para que haja participação e contribuições com propostas e sugestões, levando o tema mais uma vez para a esfera da sociedade, expondo assim de maneira clara o modelo teórico da Teoria da Securitização proposto por Buzan et al (1998, p. 25) e todos os seus componentes, conforme a Figura 3.

Figura 6: Modelo teórico da Teoria da Securitização



Fonte: Security: A New Framework for Analysis

Em relação ao papel do MD, num primeiro momento, o Exército Brasileiro foi designado para conduzir o setor cibernético no país; havendo previsibilidade para a criação de um Comando de Defesa Cibernética das Forças Armadas – como acontece nos EUA com a USCYBERCOM[18] – no qual a Marinha, o Exército e a Força Aérea trabalhariam integradamente.

Importante analisar a END de 2008, na qual os primeiros esforços com viés político-estratégico foram feitos com relação ao setor cibernético. Segundo a respectiva estratégia, "o Ministério da Defesa e as Forças Armadas intensificarão as parcerias estratégicas nas áreas cibernética, espacial e nuclear" (BRASIL, 2008), colocando particular ênfase no "aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos" (BRASIL, 2008). Nota-se pelo documento, portanto, que a cibernética é colocada pela primeira vez como um setor decisivo para a conservação do país ao alegar que os "três setores estratégicos – o espacial, o cibernético e o nuclear – são essenciais para a defesa nacional" (BRASIL, 2008).

Mesmo assim, como consequência da END de 2008, em 09 de novembro de 2009, o MD, por meio da Diretriz Ministerial 14 (Doutrina Militar de Defesa Cibernética), determinou as responsabilidades de coordenação e integração do setor cibernético ao Exército Brasileiro, no âmbito das Forças Armadas.

Em seguida, em 2010, foi lançado o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (CANONGIA; GONÇALVES JÚNIOR; MANDARINO JUNIOR, 2010), elaborado e organizado por especialistas de 13 órgãos da APF, propondo como objetivos gerais: (i) levantar e avaliar as potenciais vulnerabilidades e riscos que possam vir a afetar a segurança das infraestruturas críticas, identificando e monitorando suas interdependências; (ii) propor, articular e acompanhar medidas necessárias das infraestruturas; (iii) - estudar, propor e acompanhar a implementação de um sistema de informações com dados atualizados das infraestruturas; (iv) pesquisar e propor um método de identificação de alertas e ameaças da segurança de infraestruturas críticas da informação.

[18] United States Cyber Command (USCYBERCOM) é um comando conjunto das forças armadas norte-americanas subordinado ao Comando Estratégico dos Estados Unidos da América. O comando está localizado em Fort Meade, Maryland, e centraliza as operações no ciberespaço, organiza os recursos cibernéticos existentes e sincroniza defesa de redes militares dos EUA.

Nesse caso, percebe-se novamente uma preocupação de alta relevância com as infraestruturas críticas do país, colocando-as como potenciais vítimas à ameaça cibernética. Ainda em 2010, foi lançado o Livro Verde: Segurança Cibernética no Brasil (CANONGIA; MANDARINO, 2010), o qual apresenta uma breve visão do país no que se refere às oportunidades e aos desafios em termos político-estratégicos, econômicos, sociais e ambientais, ciência, tecnologia e inovação, educação, legalidade, cooperação internacional, e segurança das infraestruturas críticas, tendo como foco central a segurança cibernética. Além do mais, contém diretrizes estratégicas para formulação de uma possível futura Política Nacional de Segurança Cibernética para o país (BRASIL, 2010b, p. 17, 33).

Mais tarde, em 2012, é elaborado o documento que, pela primeira vez, aloca publicamente recursos para o setor cibernético. O Livro Branco de Defesa Nacional (BRASIL, 2012a) – que, apesar de aprovado na Câmara dos Deputados e no Senado, e ainda não sancionado, é documento disponível no site do governo brasileiro – trata a cibernética como um desafio, denominando-a com um tipo de "conflito do futuro" (BRASIL, 2012a, p.28), e coloca a defesa cibernética propriamente como um novo tema no plano internacional. O livro também observa as infraestruturas do país como ameaça existencial ao afirmar que a "ameaça cibernética tornou-se uma preocupação por colocar em risco a integridade de infraestruturas [...] essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional" (BRASIL, 2012a, p.69). O documento supracitado ainda defende que a proteção do espaço cibernético abrange variadas áreas, desde capacitação, inteligência, pesquisa científica, preparo e emprego operacional e gestão de pessoal até a proteção dos próprios ativos e capacidade de atuação em rede.

Outra publicação importante concernente ao tema em âmbito brasileiro foi a Política Cibernética de Defesa de 2012. A finalidade da Política é nortear "as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos" (BRASIL, 2012b). Esse documento solidifica o entendimento acerca das possibilidades e dos limites da atuação cibernética brasileira, tendo em vista a sensibilidade que esse espaço e ferramenta de poder possui. Mais uma vez, para além da atuação do MD, uma audiência pública é convocada para colaborar com processo de construção do setor cibernético:

> "a) a eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa;" (BRASIL, 2012b).

O documento cita o Sistema Militar de Defesa Cibernética (SMDC), órgão militar com o intuito de prevenir ataques aos sistemas de informática de todo o Brasil, o qual é coordenado pelo Estado-Maior Conjunto das Forças Armadas. Dessa forma, o país insere-se no modelo de gestão cibernética das grandes potências, ainda que apenas inicialmente.

Por fim, tem-se na Estratégia Nacional de Defesa de 2012, que é uma atualização da END de 2008, um documento legal, possuindo alguns pontos atualizados importantes que merecem ser citados. Primeiramente, nessa nova estratégia o setor cibernético adquire uma seção exclusiva para apontamento de prioridades. Uma delas é expansão do CDCiber para uma atuação integrada das Forças Armadas, ao afirmar que se deve "fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas" (BRASIL, 2012c).

Outra prioridade é conduzir o tema para o debate acadêmico ao propor a necessidade de "fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional" (BRASIL, 2012c). Inclusive, neste ponto, propõe-se um estudo conjunto entre Ministros, Secretários e GSI/PR com vistas à "criação da Escola Nacional de Defesa Cibernética" (BRASIL, 2012c).

Portanto, no campo da segurança cibernética, as ações ganharam maior investida a partir da criação do DSIC no GSI/PR[19] , em 2006, e no campo da Defesa Cibernética, destaque maior passou a ser dado através da elaboração da END. O conjunto regulatório até aqui apresentados, acompanhados pela criação e atuação de órgãos estatais possuem papel imprescindível pela atribuição de competências no que tange a segurança e defesa cibernéticas, podendo ser encarados como uma sistematização do processo de enfrentamento às ameaças existentes no setor cibernético.

Ponderando-se na mesma medida, os breves discursos apresentados podem ser vistos como uma forma de alcançar a legitimação junto à opinião pública em busca da securitização, haja vista que seu discurso torna-se mais aceitável em virtude da associação entre possíveis ataques cibernéticos em âmbito nacional com incidentes ocorridos diariamente. Sendo assim, conforme apontou Buzan e Hansen (2012, p.366), a segurança Defesa Cibernética a uma securitização ainda em desenvolvimento no país.

[19] O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) deu lugar a Casa Militar sob o Ministério da Casa Civil conforme a Medida Provisória Nº 696 de 2 de Outubro de 2015.

CONSIDERAÇÕES FINAIS

Na abordagem inicial deste trabalho, foram apontadas as aspirações do Estado brasileiro a uma participação mais ativa junto à comunidade internacional, cujos esforços, nesse sentido, foram materializados com a presença crescente de nossas forças armadas junto às ações de caráter humanitário da Organização das Nações Unidas, em razão do favorável cenário econômico mundial nos anos 2000, que colocaram o Brasil em destaque. Todavia, neste contexto, o Governo brasileiro foi vitimado como objeto de espionagem cibernética de origem estatal norte-americana. Ainda nesse sentido, foi possível perceber que existe no Estado brasileiro uma estrutura basilar pronta para atuar nas áreas de segurança e defesa cibernética, ainda que em desenvolvimento, perante os desafios internacionais que se apresentam.

Num segundo momento, o estudo buscou uma referência teórica para analisar o processo evolutivo do arcabouço político-administrativo na questão de Segurança e Defesa do Espaço Cibernético Brasileiro. Dentre as linhas de pensamento sobre o conceito de Segurança das Relações Internacionais declinou-se da linha de pensamento realista, por esta última, em sua essência, trabalhar precipuamente com entes estatais na arena internacional e sua busca pelo poder, afastando de sua essência a atuação dos demais atores não estatais e sua ordem de influência na cena geopolítica.

Encontrou-se amparo na Teoria da Securitização, advinda da "Escola de Copenhagen", segundo a qual o conceito de Segurança dá-se por um constructo social numa postura construtivista, em razão do posicionamento pós Guerra-fria, em que, diante da possibilidade de um holocausto nuclear, afastou-se a visão exclusivamente militarista para resolução dos conflitos e deu-se sustentação ao posicionamento das relações do Estado com demais atores de ordem diversa (Estatais ou não), abrindo a possibilidade de uma assimetria nessas interações tão comuns no enfrentamento de ameaças cibernéticas.

Avaliou-se o tema Segurança Cibernética, provocado derradeiramente por casos de forte clamor social, como a "espionagem da National Security Agency", que tornou oportuno acelerar medidas e projetos, que impulsionaram investimentos e capacitação, visando à formação e à organização de um Sistema Nacional de Segurança e Defesa Cibernética, principalmente no âmbito da Defesa por força da END, em

detrimento de históricos e significativos obstáculos afeitos à cultura de Defesa.de históricos e significativos óbices afeitos a cultura de Defesa.

Grandes eventos internacionais transcorridos no País nos últimos anos representaram a oportunidade de trazer a baila o apoio e o envolvimento da opinião pública para a matéria de Segurança e Defesa, materializando-se através da ação direta do Ministério da Defesa no âmbito da segurança orgânica dos locais onde se realizaram os eventos e junto ao Ministério da Justiça, Polícia Federal, na manutenção da ordem e da paz no Espaço Cibernético.

A instabilidade da Ordem Mundial do pós Guerra ao Terror - campanha militar desencadeada pelos Estados Unidos em resposta aos ataques de 11 de setembro de 2001 -, devido à assimetria das ações terroristas, está presente também em uma arena tecnologicamente superior e de ordem quase que "etérea" como o Espaço Cibernético. Essa instabilidade trouxe uma oportunidade para os atores governamentais de materializar discursos, políticas e ações nos setores de Segurança e Defesa cibernética, mesmo que estes não repercutam em investimentos proporcionais às reais necessidades do Estado Brasileiro. No entanto, conseguiu-se estruturar uma ordem de políticas públicas e instituições com intuito de trabalhar nesta nova fronteira de atuação, desde questões públicas não politizadas até politizadas.

Por fim, destacou-se, neste artigo, apoiado na Escola de Copenhague, que a segurança não é uma condição objetiva, mas sim um discurso que constitui identidades e ameaças. Assim sendo, pode-se depreender que o Estado Brasileiro busca por identidades e ameaças cibernéticas, conduzindo a questão da Segurança e Defesa Cibernética a uma securitização, que está em desenvolvimento no país.

BRAZILIAN CYBERSPACE'S ISSUE ON SECURITY AND DEFENSE, AND THE POLITICAL-ADMINISTRATIVE EFFORT OF THE STATE

ABSTRACT

The present work mains to study Cyberspace´ Security and Defense issues, its regulatory aspects, political and administrative sets to the Brazilian State. Focusing the efforts made as: public policies development; government agencies restructuring and updating, and the challenges for the country are pointed out on the National Defense Strategy. International Relations´ foundation on constructivism is adopted as an academic basis from Copenhagen School perspective essays and its Theory of Securitization as a support for analysis and research. It is also considered at the end, corroborating the idea of great agility in the politicization and growing securitization of the Cybernetic Space by the Brazilian State supplanting the historical challenge of the low perception of Defense´s concept.
Key-words: Cyberspace, defense, Security, public policies.

REFERÊNCIAS

AMORIM, Celso. Discurso de abertura. In: SEMINÁRIO DE DEFESA CIBERNÉTICA, 3., 2012, Brasília: MD. Disponível em: <https://www.youtube.com/watch?v=dkUcymtvcUk>. Acesso em: 20 set. 2015.

_____. Segurança Internacional: novos desafios para o Brasil. *Contexto Internacional*, Rio de Janeiro, v. 35, n.1, p.287-311, 2013. Disponível em: <http://www.scielo.br/pdf/cint/v35n1/a10v35n1.pdf>. Acesso em: 26 set. 2015.

JORGE, Bernardo Wahl Gonçalves Araújo. Estados Unidos, poder cibernético e a "guerra cibernética: do Worn Stuxnet ao Malware Flame/ Skywiper-e além. *Boletim Meridiano 47*, v.13, n. 131, 2012. Disponível em: <http://seer.bce.unb.br/index.php/MED/article/view/7051/5623>. Acesso em: 25 set. 2015.

AZAMBUJA, Darcy. *Teoria geral do estado.* São Paulo: Globo, 1957. p. 17-53. Disponível em: <http://www.faroldoconhecimento.com.br/livros/Pol%C3%ADtica/AZAMBUJA,%20Darcy.%20Teoria%20geral%20do%20Estado.pdf>. Acesso em: 20 set. 2015.

BARROS, Otávio Santana de Rêgo; GOMES, Ulisses de Mesquita (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Secretaria de Assuntos Estratégicos, 2011. Disponível em: <http://www.sae.gov.br/site/wpcontent/uploads/Seguranca_Cibernetica_web.pdf>. Acesso em: 16 dez. 2014.

BRASIL. Decreto nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 30 jun. 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm>. Acesso em: 10 jun. 2015.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 18 dez. 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 12 dez. 2015.

BRASIL. Ministério da Defesa. Portaria nº 3.389/MD, de 21 de dezembro de 2012. Política Cibernética de Defesa. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 21 dez.2012b. Disponível em: <http://www.jusbrasil.com.br/diarios/44578940/dou-secao-1-27-12-2012-pg-11>. Acesso em: 10 mai. 2015.

BRASIL. Ministério da Defesa. Portaria normativa nº 9/GAP/MD, de 13 de Janeiro de 2016, MD35-G-01. Aprova o Glossário das Forças Armadas. 5 ed. 2015. Disponível em: <http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35_g_01_glossario_ffaa_5_ed_2015.pdf>. Acesso em: 16 ago. 2016.

BRASIL. Ministério da Defesa. Portaria normativa nº 196/GAP/MD, de 22 de fevereiro de 2007, MD-MD35-G-01. Aprova o Glossário das Forças Armadas.

BRASIL. Ministério da Defesa. *Livro Branco de Defesa Nacional*. Brasília: MD, 2012a. Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 20 jan. 2015.

BRASIL. Ministério da Defesa. *Estratégia Nacional de Defesa*. Brasília: MD, 2012c. Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/end.pdf>. Acesso em: 11 jan. 2015.

BAGHERY, E. et al. *The State of the Art in Critical Infraestructure Protection:* a framework for convergence. Faculty of Computer Science, University of New Brunswick, Fredericton, N.B. Canada, 2007. Disponível em: <http://glass.cs.unb.ca/~ebrahim/papers/CIPFramework.pdf>. Acesso em: 11 jan. 2016.

BUZAN, Barry. *People, States and Fear:* an Agenda for the International Security Studies in the Post-Cold War Era. Boulder, Colorado: Lynne Rienner, 1991.

BUZAN, Barry; HANSEN, Lene. *A evolução dos estudos de segurança internacional.* São Paulo: Editora Unesp, 2012. 576p.

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. *Security:* a new framework for analysis. Londres: Lynne Rienner Publishers, 1998.

CANONGIA, Claudia; MANDARINO, Raphael (Org.). *Livro Verde:* segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC. 2010. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 02 dez. 2014.

CANONGIA, Claudia; GONÇALVES JÚNIOR, Admilson; MANDARINO JUNIOR, Raphael. (Org.). *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*. Brasília: Gabinete de Segurança Institucional da Presidência da República, nov. 2010. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em: 13 jan. 2015.

CANONGIA, Claudia; MANDARINO, Raphael. Segurança Cibernética: o desafio da nova sociedade da informação. *Revista Parcerias Estratégicas do Centro de Gestão e Estudos Estratégicos*; v.14; n.29; p. 21-46, 2009. Disponível em: <http://dsic.planalto.gov.br/artigos/101-artigo-sobre-seguranca-cibernetica-revista-parceriasestrategicas-cgee>. Acesso em: 16 abr. 2015.

CARREIRO, Marcelo. A guerra cibernética: ciberwarfare e a securitização da internet. *Revista Cantareira*, ed. 17, 2012. Dossiê guerras, conflitos e tensões, p. 123-137. Disponível em: <http://www.historia.uff.br/cantareira/v3/wp-content/uploads/2013/05/e17a9.pdf>. Acesso em: 15 nov. 2014.

CARVALHO, Paulo Sérgio Melo de. Conferência de Abertura: o Setor Cibernético nas Forças Armadas Brasileiras. In: BRASIL. *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília, Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

CAVALCANTI, Elmano Pontes. Revolução da informação: algumas reflexões. *Caderno de Pesquisa em Administração*, São Paulo, v.1, n.1, 1995. Disponível em: <http://www.ancibe.com.br/artigos%20de%20si/artigo%20-%20Revolu%C3%A7%C3%A3o%20da%20informa%C3%A7%C3%A3o%20-%20algumas%20reflex%C3%B5es.pdf>. Acesso em: 28 mar. 2015.

CLARKE, Richard; KNAKE, Robert. *Cyber War:* the next threat to National Security and what to do about it. New York: Harper Collins, 2010.

CLAUSEWITZ, Carl Von. *Da Guerra*. São Paulo: Editora WMF Martins Fontes, 2010, p.30.

CRUVINEL, Tereza; CAVALCANTI, Leonardo. Celso Amorim diz que Brasil é vulnerável contra ataques cibernético: as ações de espionagem da agência americana de segurança revelaram a fragilidade do Brasil na proteção a dados e informações. *Correio Braziliense*, Brasília, 22 set. 2013 Disponível em: <http://www.correiobraziliense.com.br/app/noticia/politica/2013/09/22/internas_polbraeco,389429/celso-amorim-diz-que-brasil-e-vulneravel-contra-ataques-cibernetico.shtml>. Acesso em: 11 jun. 2015.

DUNN, Myriam. Cyberwar: concepts, status quo, and limitations. *CSS Analysis in Security Police,* ETH Zurich, n. 71, p. 1-3, April 2010. Disponivel em: <http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-71.pdf>. Acesso em: 11 jan. 2015.

FERREIRA NETO, Walfredo Bento. *Por uma geopolítica cibernética:* apontamentos da grande estratégia brasileira para uma nova dimensão da guerra. 2013. 178 f. Dissertação (Mestrado em Estudos Estratégicos da Defesa e da Segurança) - Programa de Pós-Graduação em Estudos Estratégicos. Universidade Federal Fluminense, Rio de Janeiro, 2013.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security and the Copenhagen School. *International Studies Quarterly*, n.53, p. 1155-1175, 2009. Disponível em: <http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf>. Acesso em: 15 jan. 2015.

KALDOR, Mary. *New and Old Wars:* organized violence in a Global Era. Polity Press, 1998. p.1-216.

_____. *Old Wars, Cold Wars, New Wars, and the War on Terror.* Cold War Studies Center, School of Economics, London. p.1-10. Feb. 2005. Disponível em: <http://dspace.cigilibrary.org/jspui/bitstream/123456789/8613/1/Old%20Wars%20Cold%20Wars%20New%20Wars%20and%20the%20War%20on%20Terror.pdf?1>. Acesso em: 11 fev. 2015.

MANDARINO JR, Raphael. *Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético.* 2009. Monografia (Especialização em Ciência da Computação: gestão da segurança da informação e comunicações) - Universidade de Brasília, Brasília, 2009. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf>. Acesso em: 03 mai. 2015.

_____. Reflexões sobre Segurança e Defesa Cibernética. In: BARROS, Otávio Santana de Rêgo; GOMES, Ulisses de Mesquita (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética. Secretaria de Assuntos Estratégicos.* 2011. Disponível em: <http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf>. Acesso em: 16 jun. 2015.

MUGGAH, Robert; GLENN, Misha; DINIZ, Gustavo. S*ecuritização da Cibersegurança no Brasil*. Instituto Igarapé. Disponível em: <http://igarape.org.br/desconstruindo-a-seguranca-cibernetica-no-brasilameacas-e-respostas>. Acesso em: 12 jul. 2016.

PERES, João Roberto. A vez da governança corporativa. *Revista Abinee*. Numero 43, pagina 25, Outubro 2007. Disponível em: http://www.abinee.org.br/informac/revista/43j.pdf. Acessado em: 16 ago. 2016.

ROUSSEFF, Dilma. Discurso da Presidente. In: *Debate Geral da 68ª AGNU*. Nova Iorque/EUA. 2013. Disponível em: <http://www2.planalto.gov.br/acompanhe-oplanalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-naabertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua>. Acesso em: 15 jan. 2015.

SANTOS, José Carlos dos. Podemos recrutar "hackers". *Revista Época.* 2011. Disponível em: <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.<html>. Acesso em: 03 mai. 2015.

SENIWATI. The Securitization Theory and Counter Terrorism in Indonesia. *Academic Research International,* Hasanuddin University, v. 5, n.3, p.231 - 238, 2014. Disponível em: <www.savap.org.pk/journals/ARInt./Vol.5(3)/2014(5.3-26).pdf>. Acesso em: 14 jul. 2016.

TAKAHASHI, Tadao (Org.). *Sociedade da Informação no Brasil:* Livro Verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: <http://livroaberto.ibict.br/bitstream/1/434/1/Livro%20Verde.pdf>. Acesso em: 03 mai. 2015.

WENDT, Alexander. Anarchy is what States Make of it: the social construction of power politics. *International Organization*, v.46, n.2, p.391-425. 1992. Disponível em: <http://ic.ucsc.edu/~rlipsch/Pol272/Wendt.Anarch.pdf>. Acesso em: 20 out. 2016.

Recebido em: 22/04/2016
Aceito em: 09/12/2016