DESAFIOS DA CIBERSEGURANÇA NO BRASIL ENTRE OS ANOS 2000 E 2017

Alexandre Ferreira da Silva Mendes[1]
Prof. Me. André Matsuno da Frota[2]

RESUMO

Para o presente documento foi realizada uma pesquisa sobre o posicionamento brasileiro frente aos desafios da cibersegurança entre os anos 2000 e 2017, com o objetivo de aumentar o entendimento sobre as ações tomadas pelo Brasil frente ao terrorismo, e sua vertente o ciberterrorismo. Para tanto, foi feito uma pesquisa bibliográfica que utilizou como referência os Estudos de securitização da Escola de Copenhagen e um levantamento bibliográfico dos documentos nacionais disponíveis relativos à temática do terrorismo e cibersegurança, tais como a Constituição Federal Brasileira de 1988 Estratégia Nacional de Defesa (2008), o Plano Nacional de Defesa Cibernética (2012), o Marco Civil da Internet (2011), e a Doutrina Militar de Defesa Cibernética (2014), para compreender em qual dos estágios de securitização se encontra o Estado brasileiro. O Brasil possui pouca documentação relativa ao tema, e nesta pouca bibliografia que possui, ainda não possui uma clara definição, e tampouco estratégias eficazes de combate quanto ao dado ao tema. Ao finalizar as leituras acima citadas, fica claro que o Estado brasileiro está aquém de restante do sistema internacional em relação às suas táticas de segurança, precisando encarar com mais seriedade e atenção suas questões relativas à segurança cibernética.

Palavras chave: Segurança. Terrorismo. Ciberespaço. Ciberterrorismo. Ciberdefesa.

[1] Alexandre Ferreira da Silva Mendes (aluno do Curso de Relações Internacionais da UNINTER).
[2] Prof. Me. André Matsuno da Frota (graduado em Geografia, especialista em Análise Ambiental e mestre em Ciência Política pela Universidade Federal do Paraná (UFPR).

1 INTRODUÇÃO

A questão da segurança sempre foi assunto em pauta nas discussões internacionais. Dentre essas discussões, está a Escola da Copenhagen e seus estudos quanto ao processo de securitização de um determinado Estado. De acordo com esta Escola, existem três estágios: “não politizado”; “politizado” e “securitizado”.

> Resumidamente, no primeiro estágio, o Estado não lida com o assunto e o mesmo não é alvo de debate público. No segundo estágio, o assunto é parte da agenda de políticas públicas do governo. No último estágio, o assunto torna-se questão de segurança através de um processo de securitização, onde o objeto pode ser uma ameaça ou alvo de uma ameaça (BUZAN et al., 1998 apud Frizzera, 2013, p. 61).

Para os estudos da Escola, qualquer assunto público pode ser alocado no espectro de não politizado, politizado ou securitizado, podendo variar entre eles (Silva, 2013, p.232). E nos anos mais recentes, precisamente a partir do início dos anos 2000, o assunto terrorismo, tornou-se de suma importância para a discussão no cenário internacional.

Desde o início dos anos 2000, no que tange o terrorismo e suas consequências, o mundo vem passando por grandes mudanças no cenário da segurança internacional. Com os ataques ocorridos em 11 de setembro de 2001, iniciou-se o terrorismo pós-moderno, modificando a imagem de paz e segurança que há tanto tentava-se estabelecer entre as nações. O terrorismo como até então se conhecia havia evoluído mais do que a comunidade internacional parecia esperar.

De acordo com Silva (2015, p. 184), “o terrorismo moderno manifesta-se através do sequestro de personalidades com vistas ao resgate ou libertação de companheiros presos; desvios de aviões de suas rotas; atentados à população civil; sabotagem e destruição de instalações”. Consequência disso é o clima recorrente de medo instaurado na população que procura reforçar suas medidas de segurança das melhores formas possíveis.

Vivemos, atualmente, em uma sociedade de informação, e, portanto, existem novos desafios no que se tocam às questões de segurança (LEITE, 2016, p. 3). Na vida contemporânea é praticamente impossível separar a vida social e a tecnologia, já que o ser social atual possui parte da sua vida entre o mundo físico e o mundo virtual.

Quanto maior for a dependência tecnológica de uma nação, maior é a possibilidade que grupos de crime organizado e ciberterroristas causem danos na economia e segurança desta nação (CHAGAS, 2012, p. 11). A partir dessa afirmação,

percebe-se que os perigos que podem atingir a população não estão mais restritos exclusivamente ao meio físico, mas também podem ser praticados no meio virtual por grupos que possuam o conhecimento necessário para tal.

Assim, o terrorismo clássico ganha uma nova vertente com o ciberterrorismo, que possui como característica sua realização através do ciberespaço para a prática de ações terroristas (Leite, 2016, p.7). A interconectividade dos Estados virou um atrativo para grupos que não mais precisam estar presentes para poder realizar seus ataques.

As consequências mais prováveis de um ataque ciberterrorista são em maior parte econômicas ou psicológicas, não podendo ser resumidas apenas à estas. Os terroristas podem se infiltrar no controle de metrôs, de navios e até mesmo no sistema de controle aéreo, provocando o caos (LIMA, 2006 *apud* Chagas, 2012, p. 36). E dessa maneira, serviços que dependem de conexões com a rede, alguns, mesmo possuindo conexões fechadas, tornaram-se convidativos a grupos terroristas que os veem como uma maneira eficaz de propagar suas ideias de terror.

Dessa foram, surge o debate sobre as temáticas de cibersegurança e ciberdefesa. A primeira, de acordo com Leite (2016, p.7), "que envolve a ação das forças policiais e dos serviços informáticos, e a segunda, que decorre exclusivamente das forças armadas". Sendo que uma não está exclusiva apenas ao território de dada força, e vice-versa.

Embora o Brasil não possua um histórico de ataques terroristas (ALCÂNTARA, 2015, p. 86), é importante pensar que porque não há atos de ciberterrorismo ocorrendo, não implica necessariamente que a potencial ameaça ciberterrorista não deva ser tratada como um risco, pelo contrário, nenhum país está livre da ameaça terrorista (KOLLER, 2000 *apud* LIMA, 2006, p.43 *apud* CHAGAS, 2012, pág. 47). Não se pode pensar que o país está seguro demais, e, portanto, deixar questões como essa de lado.

Embora o Brasil possua políticas públicas de defesa cibernética, tais como a Estratégia Nacional de Defesa (2008), o Plano Nacional de Defesa Cibernética (2012), o Marco Civil da Internet (2011) e a Doutrina Militar de Defesa Cibernética (2014), a ameaça cibernética no Brasil tornou-se assunto em pauta apenas após o escândalo envolvendo Edward Snowden (O'NEILL, 2013 *apud* SILVA E PRINS, 2013, p.231), que mostrou ao país as suas fraquezas e deficiências em cibersegurança.

Sabendo da importância que é tratar de maneira apropriada as questões relacionadas à segurança nacional, e internacional, este artigo procura abordar através de uma análise bibliográfica da Constituição Federal Brasileira de 1988 Estratégia Nacional de Defesa (2008), o Plano Nacional de Defesa Cibernética (2012), o Marco Civil da Internet (2011) e a Doutrina Militar de Defesa Cibernética (2014), afim de preparar o terreno para uma discussão mais profunda sobre as questões relativas à temática do ciberterrorismo diferenciando-o de outras formas de ativismo tecnológicos, e por fim analisar os documentos supracitados nas suas partes referentes ao assunto da cibersegurança e ciberterrorismo demonstrando a importância de um estudo adequado sobre tal tema.

2 CIBERTERRORISMO E CIBERDEFESA

2.1 DA SECURITIZAÇÃO AO TERRORISMO GLOBAL

Entre a comunidade global, assuntos relativos à segurança internacional são bastante recorrentes nos dias atuais, sendo tratados por todas as esferas relacionadas ao tema. Entretanto, por muito tempo as questões relativas à segurança foram temas, quase que exclusivamente, militares. Apenas com a chegada da Escola de Copenhagen, após a Guerra Fria, que surge a visão mais global sobre segurança, e se percebe que outras esferas, tais como: política, econômica, ambiental e societal são afetadas. (DUQUE, 2009, p. 50).

A securitização em si, é sobre questões, muitas vezes hipotéticas e futuras que argumentam duas predições basicamente: o que irá acontecer se não for tomada nenhuma ação securitizante e o que ocorrerá se a mesma for tomada. (SILVA e PRINS, 2013, p. 231)

Nesse contexto, estudar sobre os possíveis perigos à sociedade global mais e mais integrada, em especial à evolução terrorista, é de interesse da securitização internacional. Em *Security: A New Framework For Analisys* (Wæver et alii, 1998), após análise sobre ameaças societais, concluiu-se que os processos de globalização acentuam problemas relacionados, tais como migração e intolerância religiosa. (DUQUE, 2009, p. 66).

2.2 TERRORISMO CLÁSSICO

Não é o objetivo deste artigo esgotar todas as fontes sobre o terrorismo e suas vertentes, mas, contribuir modestamente para uma elucidação maior sobre o tema através de uma discussão bibliográfica sobre os assuntos propostos, relacionando-os com a segurança internacional.

Pode-se afirmar que o terrorismo é, uma estratégia, tendo por escopo o estabelecimento de um clima de permanente insegurança na sociedade. (SILVA, 2015, p. 183). De acordo com o *Federal Bureau of Investigation (FBI*):

> Terrorismo é o uso ilícito de violência contra pessoas ou bens para intimidar ou coagir um governo, a população civil ou parte dela, para alcançar objectivos políticos ou sociais […]. Contudo, nem todo o acto ilícito de violência é considerado de terrorismo (ANDRADE, 1999 *apud* DIAS, 2011, p. 2).

O terrorismo é um fenômeno que tem as suas raízes na aurora da civilização. Sua prática esteve presente na história da humanidade como expressão de pura violência. (MESQUITA, 2012, p. 13) E, desde então, ao longo da história o termo sofreu várias modificações ao longo até chegar ao cunho religioso mais conhecido atualmente.

A palavra terrorismo nasceu com a Revolução Francesa, no período que ficou conhecido como Reino do Terror (1793-1794) comandado por *Maximilien de Roberspierre*, líder dos jacobinos, quando milhares de pessoas foram mortas na guilhotina. (RODRIGUES, 2013).

Por volta da década de 80 do século passado, influenciados pela Revolução Teológica Mulçumana no Irã, grupos tais como o *Hezbollah* (Partido de Deus) e o *Hamas* fizeram forte uso de ataques contra os cidadãos israelenses, militares ou não, incorporando um novo elemento nesse conflito: o terrorista suicida. (MESQUITA, 2012, p. 14). Essa incorporação, criou um nível de perigo nunca visto anteriormente ao tornar qualquer pessoa em um explosivo em potencial.

Os ataques ocorridos contra as torres gêmeas em Nova York, e o Pentágono, em Washington, iniciaram indagações da imprensa mundial sobre o futuro dos Estados frente a esse inimigo invisível: o terrorismo moderno, travestido de radicalismo religioso. (SILVA, 2015, p. 182)

2.3 TERRORISMO MODERNO

Diversos conflitos ocorrendo ao redor do globo são irrigados pelas três principais religiões monoteístas do mundo: Judaísmo, Cristianismo e Islamismo. Eventos estes, que insistem em sangrar inúmeras sociedades, tendo o radicalismo religioso como um dos principais geradores do terrorismo moderno. (SILVA, 2015, p. 182).

É certo que o dia 11 de setembro mudou a figura do terrorismo, vestindo-o com uma capa religiosa afim de combater as civilizações ocidentais. O terrorismo moderno, tornou-se uma ameaça endêmica em todas as esferas das sociedades do Oriente e do Ocidente após esses eventos, nascendo, por conseguinte, uma nova era a era do medo, da insegurança. (SILVA, 2015, p. 187).

Foi a partir desta data que o terrorismo fundamentalista islâmico passou a receber tamanha, senão, quase que total atenção. E desde então, a palavra “terrorismo” passou a ser relacionada (pelos ocidentais) aos acontecimentos desta

data e à fé islâmica em sua forma fundamentalista. (CHAGAS, 2012, p. 16). Agora, o terror possuía um nome.

O crescimento das novas organizações terroristas, denominadas de “novo terrorismo” ou terrorismo contemporâneo, na região do Oriente Médio, caracteriza-se por elevado grau de fanatismo e extremismo religioso, com objetivos difusos. Inexiste uma causa definida e suas ações são de extrema violência e radicalismo, fruto de uma interpretação parcial e distorcida do livro sagrado do Islã. (MESQUITA, 2012, p. 15)

No mundo constantemente mutável surge a *Al-Qaeda* (A Base), que mudaria por completo a face de terrorismo internacional. Diferente de outros grupos anteriores, esta organização deflagra sua guerra particular contra a civilização ocidental, focada, principalmente, nos Estados Unidos. Vide os atentados realizados em setembro de 2001.

Esta organização não possui um território específico, tampouco população a defender, o que a torna mais apta a escapar de medidas de combate por parte da Comunidade Internacional. (MARTINS, 2010, p. 29). Por este motivo, atacar a destruir alvos extraterritoriais, altamente evasivos e móveis, é infrutífero com as armas modernas, concebidas e desenvolvidas numa era de invasão e conquista territorial.

Em entrevista à Folha, Gabriel Weimann (MORAES, 2011), afirma que os ataques de 11 de setembro, só foram possíveis graças à internet. O uso de redes sociais torna mais fácil para que organizações como a *Al-Qaeda* atraiam simpatizantes, divulguem suas ideias, e captem informações sobre seus alvos de maneira legal.

A cada dia, existem novas informações sobre organizações terroristas que chamam a atenção para as formas como estas usam o espaço cibernético para a sua atuação; seja como forma de disseminar suas ideias, recrutar novos membros em redes sociais, ameaçar e executar ataques aos seus inimigos ou expor em vídeos as execuções feitas em nome de sua causa. (GARDINI, 2014, p.9).

O recrutamento para atividades deste tipo ocorre por meio da rede, de acordo advogado especializado em Direito Autoral, Nehemias Gueiros Jr.

> O modo de funcionamento é bastante fácil: os terroristas abrem contas gratuitas em provedores como ‘Hotmail’ e ‘Yahoo’, escrevem uma mensagem, mas não a enviam, arquivando-a somente na pasta de “Rascunho”. Utilizando-se do mesmo login e da mesma senha colectivamente, outros membros acedam o ‘*’Web Mail’*, leem a mensagem e apagam-na, ou seja, a mensagem jamais foi enviada, nunca saiu do provedor e não há qualquer registro ou rastro dela na Internet (DIAS, 2011, p. 11).

Com a evolução tecnológica, os meios pelos quais é possível propagar o terror também evoluem. Quanto mais uma sociedade se torna tecnologicamente sofisticada, maior será a possibilidade dela se tornar alvo vulnerável de possíveis ataques. (GORI; PAPARELA, 2006, p. 5 *apud* CHAGAS, 2012, p. 11). Por consequência disso, nasce uma nova faceta para o terrorismo moderno: o ciberterrorismo.

2.4 CIBERESPAÇO

O espaço cibernético constitui um novo e promissor cenário para a prática de toda a sorte de atos ilícitos, incluindo o crime, o terrorismo e o contencioso bélico entre nações, caracterizado pela assimetria, pela dificuldade de atribuição de responsabilidades e pelo paradoxo da maior vulnerabilidade do mais forte. (CARVALHO, 2016, p. 1). Este espaço não possui dimensões, e, portanto, é possível utilizá-lo de quase qualquer lugar do mundo com pouco risco de detecção. O ciberespaço constitui-se em um novo espaço de sociabilidade que não é presencial e que possui impactos importantes na produção de valor, nos conceitos éticos e morais nas relações humanas. (Leite, 2016, p. 4). É neste sociedade da informação, que surgem os novos desafios para as questões relacionadas à segurança.

Antes de discutir sobre o ciberterrorismo, é preciso abordar alguns conceitos que estão relacionados ao mesmo, e podem ampliar seu entendimento, deixando claro que nem todos os ataques informáticos são considerados ataques terroristas.

> Adicionalmente, para se qualificar como ciberterrorismo, um ataque deve resultar em violência contra pessoas ou propriedades, ou ao menos, causa estragos suficientes para gerar medo. Ataques que levam à morte ou ferimentos corporais, explosões, quedas de avião, contaminação da água, ou uma perda econômica severa, seriam exemplos. Ataques sérios contra infraestruturas poderiam ser atos de terrorismo, dependendo do seu impacto. Ataques que interrompem serviços não-essenciais ou que seriam apenas uma chateação custosa, não seriam. (Tradução minha, DENNING, 2000 apud DIAS, 2011, p 9.)

Segurança cibernética ou cibersegurança, é o termo referente à proteção e garantia de utilização de informações estratégicas, principalmente aquelas ligadas às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. (CARVALHO, 2016, p. 8). Em concordância, Militão (2014) afirma que este conceito que se referente às forças de segurança de uma sociedade, e refere-se ao combate do cibercrime e ao hacktivismo através da utilização das forças policiais.

Hacktivismo é o termo utilizado para caracterizar a união do hacking com o ativismo político. Este difere-se do ciberterrorismo, pois, não tem intenções de ferir fisicamente ou criar terror. Esta forma de ativismo utiliza-se de métodos de hacking normalmente declarados ilegais, mas, que possuem como ideia principal difundir uma mensagem ao maior número de pessoas. (LEITE, 2012, p. 6)

Cibercrime é a prática de atos criminosos através do uso de computadores e internet. Estes podem ser relativos aos conteúdos; violação de confidencialidade e dados pessoais; burla informática e telecomunicações; falsidade informática; dano e sabotagem; acesso ilegítimo; ou de autodeterminação, chamados de *cyberbulling* e *cyberstalking* (LEITE, 2012, p. 6)

Ciberespionagem é uma variante do original, mas que é realizada por Estados afim de recolher informações para obter vantagens estratégicas. (LEITE, 2012, p. 6)

Defesa cibernética é o conjunto de ações defensivas, exploratórias e ofensivas, no contexto militar, realizadas no espaço cibernético, que visam proteger os sistemas de informação, obter dados de inteligência e causar danos aos sistemas do oponente. (CARVALHO, 2016, p. 8)

Ciberterrorismo, como se pode perceber através do nome, é a união prática do terrorismo e o do ciberespaço. (MILITÃO, 2014, p. 27).

Um ato de terrorismo cibernético ocorre quando um indivíduo ou uma organização usa uma rede de computadores para sobrecarregar e destruir um sistema de gerenciamento de energia nacional. O ciberterrorismo não ocorre quando um suicida (homem-bomba) destrói uma rede elétrica ou usa a internet para adquirir informações sobre como construir uma arma química (CHE, 2007, p. 8 *apud* CHAGAS, 2012, p. 31)

As raízes do ciberterrorismo foram percebidas no início dos anos 1990, quando o rápido crescimento do uso da internet e o debate sobre a “sociedade da informação” provocaram vários estados sobre os riscos potenciais enfrentados pela alta conectividade em rede e pela alta “tecnodependência” dos Estados, especialmente os Estados Unidos (WEIMAN, 2004, p. 2 *apud* CHAGAS, 2012, p. 28).

As questões relativas à segurança cibernética são cada vez mais como uma função estratégica dos governos de economias desenvolvidas. É preciso criar estratégias para proteção das infraestruturas críticas, segurança da informação e comunicação, entre outras.

2.5 SOBRE O BRASIL

Com base na importância do tratamento adequado ao tema do terrorismo, e sua nova vertente, o ciberterrorismo, é preciso perguntar se o Brasil está dando atenção ao devido tema e qual sua posição no chamado processo de securitização.

De acordo com o postulado pela Escola de Copenhagen, o discurso de securitização per se não garante um processo de securitização. O que precisa ser verificado é se há um consenso com relação à ameaça que legitime ações extraordinárias para lidar com o assunto (Silva, 2013, p. 234). Ou seja, mesmo que o Brasil possua a iniciativa e documentação que toquem no referido tema de segurança e cibersegurança, apenas isso não é o suficiente para considerar que o mesmo esteja dando o tratamento adequado ao tema.

Na Constituição da República Federativa do Brasil de 1988, está escrito em seu artigo art. 4º, inciso VIII, o repúdio ao terrorismo, completado pelo art. 5º (inciso XLIII) que o declara como crime inafiançável e insuscetível de graça ou anistia (BRASIL, 1988). Entretanto, não há uma tipificação para o mesmo, e dessa forma, não é possível classificar o que seria um ato terrorista praticado em terras nacionais.

O problema de uma aprovação antiterror no Brasil, está em atingir os movimentos sociais, quando estes realizassem ações como invasões de hidrelétricas e barragens, prédios públicos, terras da União e bloqueios de estradas. (MESQUITA, 2012, p. 36)

Embora o Brasil não possua lei específica que criminalize o terrorismo, o mesmo não pretende ser coadjuvante apenas quando se trata sobre o ciberespaço. Para Carvalho (2016, p. 6) é preciso ressaltar a clarividência do poder público brasileiro ao alçar o Setor Cibernético como um dos setores estratégicos da defesa, conforme estabelece a Estratégica Nacional.

> Segurança cibernética refere-se à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da administração pública federal (Brasil, 2011 *apud* CRUZ JUNIOR, 2013, p 9).

Em sua Política Nacional de Defesa (2012), o Brasil prevê a criação de dois campos distintos: a Segurança Cibernética, que fica a cargo da Presidência da

República e a Defesa Cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas. (DEFESA, 2014, p. 17).

Com a criação da Política Nacional de Defesa, o Estado brasileiro define o que é ameaça e ataque cibernético, bem como o conceito de defesa cibernética.

Ameaça cibernética é a causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse. (DEFESA, 2014, p. 18). Dentro da lógica da defesa dos seus interesses, é de esperar que atores mal- intencionados procurem manipular e controlar os fluxos de informação que circulam nas redes de comunicações dos diversos países, afetando a disponibilidade e a utilização segura do ciberespaço (Nunes, 2012, p. 118)

Ataque cibernético são ações que podem interromper, negar, degradar, corromper ou destruir informações ou sistema computacionais armazenados. (DEFESA, 2014, p. 21).

Defesa cibernética é o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (DEFESA, 2014, p. 18).

Em comparação aos Estudos realizados pela Escola de Copenhagen sobre os estágios de securitização, percebe-se que o Brasil já direciona a sua atenção à ciberdefesa e cibersegurança. Entretanto, da mesma forma, o mesmo ainda possui pouca clareza nas definições de atitudes que deve e pode tomar frente às ameaças reais e virtuais. Sendo assim, o Brasil ainda se encontra no estágio de “não-securitizado”, ou seja, reconhece a importância do devido tratamento às questões de segurança, mas ainda precisa criar programas para ampliação e divulgação das estratégias de segurança.

De acordo com Nunes (2012, p 119) os benefícios da livre utilização do ciberespaço serão atingidos apenas se formos capazes de proteger as infraestruturas de informação nacionais, ao fornecer um nível aceitável de segurança, fiabilidade e disponibilidade na sua exploração.

3 CONCLUSÃO

Com base no que foi argumentado até então sobre questões de segurança, e naquilo que foi discutido referente à Constituição Federal Brasileira de 1988, a Estratégia Nacional de Defesa (2008), o Plano Nacional de Defesa Cibernética (2012), o Marco Civil da Internet (2011) e a Doutrina Militar de Defesa Cibernética (2014), relativos ao tratamento brasileiro para o tema cerne deste trabalho, percebe-se que o Brasil ainda possui um longo caminho até atingir um estado de securitização, permanecendo apenas até o presente momento com sua defesa politizada. O Brasil precisa planejar um sistema de defesa adequado, para estar atualizado com os mecanismos e meios de ataques existentes. (CRUZ JÚNIOR, 2013, p.9)

Mesmo sendo o terrorismo um assunto antigo e há tanto debatido em reuniões internacionais ao longo do tempo, o Brasil ainda não possui uma definição clara do mesmo, e tampouco sua tipificação como crime, como é possível observar em sua Constituição Federal de 1988. Relativamente, ainda que possua documentos que tratem de questões da sua cibersegurança, o Estado brasileiro possui poucas fontes sobre este tema, o que torna suas fontes para discussão bastante pequenas.

De acordo com (MORESI, 2012) a Segurança Cibernética vem sendo um dos grandes desafios enfrentados pelos Governos dos diversos países, principalmente na garantia do funcionamento de infraestruturas críticas tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, dentre outras. O Brasil não pode ficar aquém do Sistema Internacional, se quiser manter a sua segurança nivelada com o restante do mundo.

Na contemporaneidade, em uma sociedade tão interligada, deixar de debater os assuntos relativos à salvaguarda da população nacional, é praticamente o mesmo que baixar suas defesas para ataques.

> A Segurança e a Defesa cibernética vêm se caracterizando cada vez mais como uma função estratégica de Governo em Economias desenvolvidas, ou não, incluindo questões de: proteção das infraestruturas críticas; segurança da informação e comunicações; cooperação internacional; construção de marcos legais; e capacitação de recursos humanos. (MORESI, 2012, p. 1)

Em resposta do crescente perigo do ciberterrorismo e suas ameaças, sugere-se que sejam realizadas políticas de conscientização nacional sobre o uso da internet

e seus perigos, assim como campanhas de promoção da segurança de dados e fortalecimento de sistemas críticos.

REFERÊNCIAS

ALCÂNTARA, Bruna. **Brasil e Ciberterrorismo: Desafios para o Rio 2016**. Proceedings Of The The Ninth International Conference On Forensic Computer Science, [s.l.], p.84-89, 20 jun. 2015. ABEAT. http://dx.doi.org/10.5769/c2015011

BRASIL. **Constituição da República Federativa do Brasil (1988).** Promulgada em 05 de outubro de 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em 26 de março de 2018

CHAGAS, Morgana Santos das. **Ciberterrorismo: as possibilidades da expansão do terror nas relações internacionais**. 2012. 53 f. Monografia (Especialização) - Curso de Relações Internacionais, Universidade Estadual da Paraíba, João Pessoa, 2012. Disponível em: <http://dspace.bc.uepb.edu.br/jspui/handle/123456789/11089>. Acesso em: 10 out. 2017.

CORDEIRO, Caroline; PRINS, Ricardo. **Defesa Cibernética – Um Caminho para Securitização?** Conjuntura Global, [s.l.], v. 2, n. 4, p.230-236, 31 dez. 2013. Universidade Federal do Parana. http://dx.doi.org/10.5380/cg.v2i4.35600.

CRUZ JÚNIOR, Samuel César da. **A SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL E UMA REVISÃO DAS ESTRATÉGIAS DOS ESTADOS UNIDOS, RÚSSIA E ÍNDIA PARA O ESPAÇO VIRTUAL.** 2013. Disponível em: <http://repositorio.ipea.gov.br/handle/11058/1590>. Acesso em: 23 mar. 2018

DEFESA, Ministério da. **Doutrina Militar de Defesa Cibernética.** 2014. Disponível em: <http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em: 26 mar. 2018.

DIAS, Viriato Caetano. **De terrorismo convencional ao ciberterrorismo: um estudo de caso sobre o papel da Al-Qaeda**. 2011. 13 f. Dissertação (Mestrado) - Curso de Relações Internacionais e Estudos Europeus, Universidade de Évora, Évora, 2011. Disponível em: <http://macua.blogs.com/moambique_para_todos/2011/07/de-terrorismo-convencional-ao-ciberterrorismo-um-estudo-de-caso-sobre-o-papel-da-al-qaeda.html>. Acesso em: 10 out. 2017.

DUQUE, Marina Guedes. **O papel de síntese da escola de Copenhague nos estudos de segurança internacional**. Contexto int., Rio de Janeiro, v. 31, n. 3, p. 459-501, dez. 2009. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292009000300003&lng=en&nrm=iso>. Acesso em: 16 dez. 2017.

FRIZZERA, Guilherme. **Análise de discurso como ferramenta fundamental dos estudos de Segurança – Uma abordagem Construtivista**. Conjuntura Global**,** [s.l.], v. 2, n. 2, p.59-63, 30 jun. 2013. Universidade Federal do Parana. http://dx.doi.org/10.5380/cg.v2i2.35334.

GARDINI, Mayara Gabrielli. **Terrorismo no ciberespaço: o poder cibernético como ferramente de atuação de organizações terroristas**. Fronteira: Revista de iniciação científica em relações internacionais, Belo Horizonte, v. 13, n. 2526, p.7-33, 2014. Disponível em: <http://periodicos.pucminas.br/index.php/fronteira/article/view/10461/10543>. Acesso em: 23 mar. 2018.

LEITE, Ana Marta Xavier Ferreira. **A Problemática Da Cibersegurança E Os Seus Desafios**. 2016. Disponível em: <http://cedis.fd.unl.pt/wp-content/uploads/2017/10/CEDIS-working-paper_DSD_A-problemática-da-cibersegurança-e-os-seus-desafios.pdf>. Acesso em: 09 nov. 2017.

MESQUITA, Luiz Eduardo Garcia de. **O Terrorismo E A Sua Probabilidade De Ocorrência No Brasil**. 2012. 64 f. Monografia (Especialização) - Curso de Altos Estudos de Política e Estratégia, Escola Superior de Guerra, Rio de Janeiro, 2012.

MORAES, Márcia Soman. **Internet transformou a Al Qaeda em 'McDonalds do terror', diz especialista.** 2011. Disponível em: <http://www1.folha.uol.com.br/mundo/2011/09/972760-internet-transformou-a-al-qaeda-em-mcdonalds-do-terror-diz-especialista.shtml>. Acesso em: 23 mar. 2018.

MORESI, Eduardo Amadeu Dutra. **Defesa Cibernética: um estudo sobre a proteção da infraestrutura e o software seguro**. In: SEGUNDA CONFERENCIA IBEROAMERICANA DE COMPLEJIDAD, INFORMÁTICA Y CIBERNÉTICA, 2., 2012, Orlando. Memorias del Segunda Conferencia Iberoamericana de Complejidad, Informática y Cibernética. Orlando: International Institute Of Informatics And Systems, 2012. p. 1 - 6. Disponível em: <http://www.iiis.org/CDs2012/CD2012IMC/CICIC_2012/PapersPdf/CB869BT.pdf>. Acesso em: 23 mar. 2018.

SILVA, Leodefane Bispo da. **Terrorismo Moderno E Fundamentalismo Religioso: Uma Era De Incertezas No Âmbito Global**. Akrópolis: Revista de Ciências Humanas da UNIPAR, Paraná, v. 23, n. 2, p.181-189, jul. 2015. Semestral. Disponível em: <http://revistas.unipar.br/index.php/akropolis/article/view/5765/3268>. Acesso em: 26 mar. 2018.

SILVA, Caroline Cordeiro Viana e; PRINS, Ricardo. **Defesa Cibernética: Um Caminho para Securitização?**. Conjuntura Global, Curitiba, v. 2, n. 4, p.230-236, dez. 2013. Quadrimestral.

MARTINS, Raúl François Carneiro. **Acerca de "Terrorismo" e "Terrorismos"**. 2010. Disponível em: <https://www.idn.gov.pt/publicacoes/cadernos/idncaderno_1.pdf>. Acesso em: 23 mar. 2018.

MILITÃO, Octávio Pimenta. **Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional**. 2014. 97 f. Dissertação (Mestrado) - Curso de Ciência Política e Relações Internacionais, Departamento de Estudos Políticos, Faculdade de Ciências Sociais e Humanas (fcsh), Lisboa, 2014. Disponível em: <https://run.unl.pt/handle/10362/14300>. Acesso em: 23 mar. 2018.

NUNES, Paulo Fernando Viegas. **A definição de uma estratégia nacional de cibersegurança.** 2012. Disponível em: <https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf>. Acesso em: 23 maio 2018.

Comentado [AU1]: Não serve como referência acadêmica.