DOI: 10.5769/C2015011 or http://dx.doi.org/10.5769/C2015011

Brasil e Ciberterrorismo: desafios para o Rio 2016

Bruna Toso de Alcântara

***Resumo*— Sendo o país que sediará os jogos olímpicos de 2016 o Brasil possui a responsabilidade de se preparar para que os mesmos se deem de forma segura em território nacional. Assim, questões como o Ciberterrorismo, ainda que pareçam longe da realidade brasileira, devem ser levadas em consideração. Desta forma o presente artigo apresenta os desafios para as quais o Brasil deve atentar em prol de proteger o país durante o grande evento em 2016.**

Palavras-Chave—Ciberterrorismo, Brasil, Rio 2016.

***Abstract*— Being the country that will host the Olympic Games in 2016, Brazil has the responsibility to prepare itself to guarantee the safety of the games within national territory. Thus, issues such as Cyberterrorism, even though appearing to be far from the Brazilian reality, should be taken into consideration. Therefore, this paper presents the challenges for which Brazil should pay attention for the sake of protecting the country while hosting the big event in 2016.**

Keywords—*Cyberterrorism, Brazil, Rio 2016.*

I. INTRODUÇÃO

Com as organizações terroristas utilizando-se cada vez mais do ciberespaço para espalhar sua narrativa e com o crescente entrelaçamento das Infraestruturas Críticas dos Estados aos meios tecnológicos, o temor do Ciberterrorismo ronda diversos países ao redor do mundo.

Contudo, sem uma acordada definição internacional sobre os efeitos e características do que venha a ser esse tipo de terrorismo, proteger-se do mesmo se torna uma tarefa difícil e trabalhosa, que envolve não somente preparação, mas estudos acerca de suas possíveis consequências.

Nesse sentido, em que pese o Brasil não tenha atos de terrorismo como uma realidade próxima, enquanto anfitrião dos jogos olímpicos em 2016, ele deve se preparar para possíveis ataques cibernéticos nesse formato. Afinal, se tratando do ciberespaço, não podemos assumir padrões e muito menos que certos países não serão atingidos direta ou indiretamente por ações de terceiros.

Assim, o presente artigo se divide em duas partes. A primeira visa elucidar como o país pode entender o termo "Ciberterrorismo" e como esse fenômeno preocupa os países a nível internacional.

Já a segunda parte pretende mostrar os desafios para os quais o Brasil, em específico, deve atentar nessa seara e quais as possíveis medidas que podem ajudar a contorná-los.

II. CIBERTERRORISMO: ENTENDIMENTO, FORMAS DE ATUAÇÃO E COMBATE.

Em que pese o termo Ciberterrorismo tenha aparecido pela primeira vez em um artigo de Barry Collin [1], nos anos 1980, significando o perigo de ataques conduzidos à longa distância (como consequência da interseção entre mundo físico e virtual) e tendo como alvos Infraestruturas Críticas de um país (fazendo com que a população de um país não conseguisse "comer, beber, se locomover, ou viver") ainda não existe uma definição internacional padrão para esse fenômeno. Assim, o debate acerca das ameaças que o Ciberterrorismo apresenta continua vivo e ganhando cada vez mais relevância.

De fato, em estudo conduzido há pouco tempo pela Swansea University [2] 36% dos entrevistados admitiram ser muito importante que tomadores de decisão *(policymakers*) tivessem uma resolução das questões de definição em torno de terrorismo, e 35% marcaram como **quase** essencial a necessidade de uma definição específica de Ciberterrorismo para os mesmos. Ademais, 87% dos entrevistados considerou como elemento característico do Ciberterrorismo a motivação política e ideológica.

Sob esse prisma, talvez, o que possa ser mantido para as análises do Ciberterrorismo seja os quatro motivos clássicos que impulsionam atividades terroristas: 1) terrorista com só um foco (ou seja, a motivação deles vem de um assunto em particular, como os direitos dos animais), 2) terroristas ideológicos (que usam da violência para promover sua ideologia politica, a qual se pauta nos extremos da direita ou da esquerda) 3) terroristas nacionalistas (os quais buscam independência de um dado Estado ou entrar de um Estado para outro por razões étnicas ou geográficas) e 4) terroristas politico religiosos (que podem se tornar letais dado que entendem suas ações como atos sob ordens divinas)[3]

Por outro lado, como Awan [4] explica, "dado que tipos de comportamento podem ser ligados a problemas e movimentos sociais, isso nos permite olhar para o Ciberterrorismo através das lentes da mudança social". Nesse sentido, pensar em motivos nos leva a tentar entender o Ciberterrorismo a nível social, enquanto parte das mudanças que vem ocorrendo desde a Revolução Informacional. Igualmente, se nos basearmos em uma concepção construtivista de mundo - para a qual 1) o mundo é constituído parcialmente por nossas crenças e ideias sobre ele 2) nosso conhecimento de mundo é socialmente construído e mantido, e 3) há uma importante dinâmica de interações entre o mundo das ideias e o das coisas de tal maneira que nossas ideias e realidades sociais são moldadas, reforçadas e impactadas uma na outra- o debate passa a se focar mais em como o conceito é construído e produzido

socialmente do que em sua definição com características *per se* [5]

De qualquer forma, parece que a nível prático, Weimann [6] é um autor que consegue elucidar de forma precisa o que vem ocorrendo atualmente [7]. Em outras palavras, ele explica que o uso de computadores feito por terroristas serve principalmente como um "facilitador de suas atividades, seja para propaganda, recrutamento, difamação de comunicações ou outros propósitos que não simplesmente o Ciberterrorismo". Ademais, Weimann [8] coloca em pauta que há uma confusão entre atividades de hacktivismo e Ciberterrorismo, fazendo com que atos menores tomem proporções maiores através da mídia. Todavia, Weimann ressalta que [...] mesmo assim o hacktivismo realça a ameaça do Ciberterrorismo [...]" uma vez que os terroristas podem se utilizar dos caminhos já trilhados pelos hacktivistas, mas daí para alcançar seus próprios propósitos de atingir governos. Ademais, segundo o autor, zonas cinzentas podem existir entre essas duas modalidades no ciberespaço, se os terroristas forem capazes de recrutar ou contratar hacktivistas ou se hacktivistas decidirem ir mais além e operar a nível de Infraestruturas Críticas.

Nesse sentido, o uso da internet por grupos terroristas deve ser levado em consideração e analisado de forma profunda, abrangendo principalmente análises sobre a Darknet ou Deep Web, uma vez que 99.8% das atividades terroristas ocorrem nesse (sub) mundo do ciberespaço [9].

Em realidade, se faz necessário entender primeiramente porque os terroristas estão se interessando pelo uso de computadores. Assim em linhas gerais podemos elencar: 1)oferece abrangência para espalhar sua narrativa de forma rápida e barata, atingindo o maior número possível de recrutas, 2) forma fácil de manter o anonimato dos participantes e a troca de informações, 3) facilidade de acesso a dados abertos que podem ser úteis aos planos terroristas 4) facilidade para obter financiamento, principalmente através do uso de entidades de caridade como fachada [10].

Em segundo lugar, dentro desses pontos elencados, o que tange o recrutamento e abrangência para a narrativa se torna potencialmente mais perigosos, tendo em vista que, segundo uma pesquisa feita pela RAND Corporation em 2013, a internet pode aumentar as oportunidades para a radicalização. Contudo não necessariamente acelerando o processo e não substituindo o contato físico necessário para a própria radicalização (*self-radicalisation*)[11].Como exemplo recente dessa atividade podemos citar o caso do grupo ISIS (Estado Islâmico), o qual com sua campanha nas redes sociais atraiu para sua causa mais de 18.000 combatentes estrangeiros de mais de 90 países[12] entre eles o Brasil [13].

Tomando o exemplo do ISIS percebe-se que o uso da internet por terroristas aumenta o fenômeno, já discutido mundialmente, do recrutamento de combatentes estrangeiros (FTF, em inglês), ou seja, pessoas que viajam para um estado diferente do seu com o objetivo de se juntarem ou receberem treinamento em apoio a atividades terroristas [14]. De fato de acordo com o Fórum Global Contra o Terrorismo (GCTF, em inglês), órgão criado em 2011 por 29 países e a União Europeia (incluindo a Colômbia como membro fundador e a Organização dos Estados Americanos como um *stakeholder*), um grupo de trabalho especifico nesse fenômeno já tem lugar e usa como base o documento chamado "Memorando de Marrakesh em Boas Práticas para uma Resposta mais Efetiva ao fenômeno do FTF".

O Memorando de Marrakesh não é compulsivo perante as leis internacionais e se apresenta dividido em quatro grandes grupos, que se subdividem em um total de 19 boas práticas. Esses grandes grupos foram intitulados: detecção e intervenção contra a violência extremista; detecção e intervenção no recrutamento facilitação; detecção e intervenção contra viagem e combate; e detecção e intervenção sobre retornos. [15] Tendo como intuito principal coletar e difundir boas práticas entre uma variedade de países para combater o FTF [16]

Além disso, a RES 2178 (2014) do Conselho de Segurança da ONU também aborda o assunto, "[...] expressando grave preocupação que os combatentes terroristas estrangeiros estão usando sua ideologia extrema para promover o terrorismo". [17]

Diante desse quadro, é interessante a proposta de Ginkel [18] em medidas repressivas em duas categorias: duras e suaves. As primeiras seriam

> [...] focadas na negação do acesso as narrativas extremistas dos grupos e apoiadores terroristas, através do bloqueio de mensagens ou a retirada do ar de websites, e da proibição de distribuição e comunicação de conteúdo radical, além de repressão criminal para as pessoas por trás de tais ações.

Contudo, como alerta Ginkel, e corroboramos com a autora, implementar tais medidas em países com uma democracia já estabelecida podem ser contraproducentes e mesmo que as páginas sejam "desligadas" de forma efetiva, outras , cada vez mais escondidas e de difícil acesso surgirão.

Já as medidas suaves seriam mais ao nível de contrapropagandas, podendo se dar na forma de campanhas publicas (a exemplo do Centro para Comunicações Estratégicas Contra o Terrorismo, nos Estados Unidos); narrativas alternativas (a exemplo do Radical Middle Way, do Reino Unido, como uma tentativa de diálogo com grupos mulçumanos sobre o papel da religião no século XXI); contra narrativas (a exemplo do programa "Say no to Terror" a qual se utiliza de vários mecanismos para criar uma contra narrativa sobre elementos selecionados da narrativa terrorista).

Por fim haveria ainda o papel da mídia convencional, que como Ginkel coloca, é um tema controverso, uma vez que depende dos meios convencionais de comunicação deixar-se ou não influenciar pela narrativa terrorista.

Como último ponto de medidas no combate ao uso terrorista da internet, e da prática do Ciberterrorismo (enquanto veículo de radicalização e recrutamento) vale a pena lembrar o compromisso, também não compulsório legalmente, da NETMundial, que ocorreu em Abril de 2014 no Brasil, cujo documento final menciona a questão da segurança da internet, de forma mais geral, baseada em uma "forte cooperação entre os diferentes *stakeholders*"[19]. Ainda, exemplos que podem inspirar o Brasil podem basear-se em países individualmente, como Estados Unidos e Reino Unido, que possuem estratégias contra o Ciberterrorismo, uma vez

que ambos sofreram consequências físicas da distribuição livre da narrativa terrorista[1].

Diante disso, o que se torna claro é que independente do que for realmente o Ciberterrorismo, e de como evoluirá o debate conceitual sobre ele, um país hoje deve atentar para 1) atividades hacktivistas em suas redes, uma vez que elas podem ser o "caminho das pedras" para ataques mais perigosos 2)abrangência da narrativa terrorista, a qual incita a radicalização e pode proporcionar a participação de estrangeiros em causas terroristas e 3) medidas contra a narrativa terrorista que não causem pânico à população nem prejudiquem o abertura democrática da internet.

Tendo isso em mente, na próxima seção adentramos para as especificidades de um país que não vê o terrorismo como uma realidade próxima e assim, consequentemente, tem que superar alguns desafios se quiser proporcionar um nível de segurança excelente durante o Rio 2016.

III. Desafios para o Brasil

O Brasil já sediou de forma exitosa os Jogos Mundiais Militares em 2011; a Rio+20 em 2012; a Jornada Mundial da Juventude, com a presença de Sua Santidade o Papa Francisco, a Copa das Confederações em 2013 e, mais recentemente, a Copa do Mundo em 2014. Contudo, em que pese à experiência que o país adquiriu quanto à segurança em grandes eventos, algumas questões ainda merecem atenção para o Rio16, sendo uma delas o terrorismo, e mais especificamente o Ciberterrorismo.

Uma vez que o país está em evidência internacional, como anfitrião de grandes eventos, e dada sua extensão assegurar a segurança das Infraestruturas Críticas e das conexões cibernéticas que envolvem o território nacional se torna primordial. Afinal, mesmo que o Brasil não tenha um histórico de atos terroristas, sempre se deve lembrar que grandes eventos se tornam por si mesmos uma "grande vitrine"[20] para atuações terroristas, sejam elas oriundas de organizações específicas ou de lobos solitários.

Assim, com base nas recentes discussões acadêmicas, políticas e militares foram identificadas quatro grandes áreas as quais o Brasil precisa atentar no que tange ao terrorismo, e consequentemente a sua vertente cibernética, para encerrar com o devido prestígio esse ciclo de grandes eventos. Estes seriam: 1) Necessidade de uma legislação interna, a qual tipifique o que é terrorismo para o Brasil; 2) a construção de uma cultura de segurança nessa seara, a nível real e virtual; 3) o fato de conseguir assegurar a capilaridade das comunicações eletrônicas dentro e fora do território nacional; e 4) a necessidade do fortalecimento das instituições responsáveis pela tomada de ações antiterroristas.

A. Legislação interna

O Brasil não conseguiu até o presente momento chegar a um consenso sobre o que seria um ato terrorista, e por isso não possui tipificação a nível penal sobre o assunto. Assim, como aponta André Luís Woloszyn, especialista em segurança, defesa e inteligência e analista de assuntos estratégicos [21] há a existência de um paradoxo frente à atitude brasileira, ou seja, ao mesmo tempo em que o país repudia internacionalmente e considera o terrorismo um crime a nível interno não há uma tipificação frente ao mesmo.

De fato a nível internacional

> Brasil tem apoiado as decisões da AGNU e do CSNU contra o terrorismo, sendo parte das doze principais convenções no âmbito das Nações Unidas, das quais **nove já foram internalizadas e ratificadas**. No âmbito regional, o Brasil é signatário das três convenções da Organização dos Estados Americanos (OEA) relacionadas ao terrorismo. [22]

Já internamente, a Constituição da República Federativa do Brasil de 1988 traz como preceito fundamental o repúdio ao terrorismo (artigo 4º, inciso VIII), complementado pelo artigo 5° (inciso XLIII) o qual declara o terrorismo como crime inafiançável e insuscetível de graça ou anistia**.** [23]Também possuímos algumas leis que tratam do assunto (Lei de Crimes Hediondos-Lei nº 8.072, de 1990- e Lei de Segurança Nacional-Lei nº 7.170, de 1983).Contudo, como explica Woloszyn [24] elas se tornam "inócuas" uma vez que ferem tanto o principio da objetividade jurídica (a qual exige a definição clara e precisa das ações constituidoras dos tipos penais [25]) quanto o princípio constitucional da reserva legal (o qual atesta que não há crime sem que haja lei anterior que o defina)[26].

Lasmar [27] aponta alguns argumentos, que podem explicar a formação do paradoxo explicitado por Woloszyn. Estes seriam: 1) qualquer tratamento da questão do terrorismo poderia estigmatizar a população muçulmana brasileira, 2) o reconhecimento da existência de atividades terroristas em território brasileiro poderia afetar o turismo internacional no Brasil 3) existência de um corpo normativo de combate ao terrorismo ou o reconhecimento de sua existência levariam a uma construção de uma imagem de alinhamento brasileiro com a política externa estadunidense da "Guerra Global Contra o Terror" e isso poderia ser visto como uma política externa e interna provocativa, que poderia atrair problemas políticos e de segurança para o Brasil 4) existência do temor de que grupos de movimentos sociais legítimos venham a ser taxados de grupos terroristas e 5) envolvimento de vários políticos da alta cúpula governamental em atividades ou grupos que se utilizaram da violência política durante a ditadura militar brasileira a fim de combatê-la.

Quanto ao primeiro e quarto argumento, uma possibilidade seria tentar fazer uma processo mais aberto e democrático quanto ao texto jurídico da dita tipificação. Talvez através de uma plataforma online, de modo que tanto a sociedade mulçumana quanto grupos de movimento social legítimos sejam abarcados.

O terceiro argumento parece um pouco deslocado. Afinal como Embaixador Samuel Pinheiro Guimarães colocou, em um Seminário recente sobre o terrorismo:

> Enquanto o Brasil mantiver internamente um convívio pacífico, harmonioso entre as

[1] Quando se fala em consequências físicas de Ciberterrorismo me refiro ao caso dos Irmãos Tsarnaev, que plantaram bombas na maratona de Boston em Abril de 2013 e ao estudante universitário Roshnara Choudry que esfaqueou um membro do Parlamento britânico com uma faca em 2010. Em ambos os casos a inspiração para instauração do terror (radicalização) teve origem em conteúdo online. [12]

> diferentes comunidades, de um lado; e, no sistema internacional, ter posições que façam com que ele continue na linha de defesa da paz, de defesa do desarmamento, de repúdio ao terrorismo, de solução pacífica das controvérsias, nós estaremos criando as principais condições para evitar que o Brasil seja incluído no rol das nações que são objeto de eventuais atentados terroristas. [28]

Por fim, quanto ao quinto argumento, infelizmente essa é uma realidade na história brasileira e deve ser superada socialmente, através de mecanismos como a Comissão da Verdade.

Portanto de maneira geral, constata-se a necessidade de uma tipificação do terrorismo na legislação interna, lembrando a igual necessidade, de um debate no corpo jurídico que se desenvolverá para a vertente cibernética. Fazendo a ressalva de que ao se analisar a vertente cibernética o melhor caminho seria a não direção aos extremos. Em outras palavras, não se pode tipificar o Ciberterrorismo enquanto proporções de uma guerra cibernética, tendo em vista que ainda não se sabe ao certo o que o mesmo significa ou como se desenvolverá. A única certeza que temos é que podemos tipifica-lo enquanto uma forte ferramenta de influência para atos terroristas, mesmo assim, o debate deve ser levado para a sociedade, atingindo principalmente os grupos mais vulneráveis a essa influência online.

B. Construção de uma cultura de segurança real e no ciberespaço

Tendo em vista que o Brasil, não possui um histórico contendo atos terroristas, esse é um aspecto que não está na cultura brasileira. Como explicado por Salaberry [29]

> A nossa cultura é de os homens colocarem a carteira no bolso da frente e as mulheres a bolsa para frente quando andam em um lugar que não conhecem. Mas alguém tem medo de passar ao lado de um cesto de lixo?

Assim, existe a necessidade de trabalhar a percepção da população acerca do terrorismo, desmistifica-lo como distante, e improvável de ocorrer no país – principalmente quando se trata de sua vertente no ciberespaço. Afinal, se 2016 será o fim do ciclo de grandes eventos ele pode ser também o início de uma cultura de segurança, com o cuidado de que ela não se "torne paranoia, ao ponto de desrespeitar os direitos individuais, os direitos civis, os direitos humanos" [30].

Em especifico ao Ciberterrorismo, aspectos como higiene cibernética, e conscientização via palestra e *workshops* aparecem como possibilidades. Aumentar sensibilização da população se torna uma ferramenta essencial.

Contudo a divulgação dessas iniciativas deve ser mais massificada e atingir principalmente a população mais vulnerável (adolescentes, imigrantes de zonas de conflito e a comunidade israelita e mulçumana) A referência à população mais vulnerável se dá uma vez que já estamos vivenciando um problema de valores, que perseguirá muito a próxima geração.

Esse problema de valores se reflete na sociedade desde os ataques de 11 de Setembro de 2001 e se consolida no aumento de partidos de extrema – tanto direita quanto esquerda – ao redor do mundo. Por isso, a necessidade de abordar adolescentes, imigrantes de zonas de conflito e a comunidade israelita e mulçumana brasileiras.

Ademais, o uso da contra narrativa frente às informações terroristas disponíveis se torna uma alternativa. Mas como todo assunto sensível, essa narrativa deve ser ponderada em sua forma de abrangência, e nesse ponto a cooperação internacional pode vir a ajudar. Experiências de países que já lidam com o assunto podem ajudar o Brasil a traçar um perfil do que fazer e, principalmente, do que não fazer.

C. Assegurar a capilaridade das comunicações eletrônicas dentro e fora do território nacional

O fato de o Brasil ser um país "gigante pela própria natureza" não só apresenta uma dificuldade quanto a possíveis atos de terrorismo físico como também no âmbito cibernético. Afinal, mesmo que durante os grandes eventos recentes se tenha utilizado da tecnologia para manter a capilaridade da atuação militar [31], esse mesmo uso traz vulnerabilidades para a manutenção de comunicações efetivas e seguras.

Nesse ponto, ainda que haja um engajamento integrado de órgãos de inteligência, segurança e defesa [32] existe a necessidade de reforçar linhas de comunicação. Em outras palavras, se a comunicação entre as unidades de defesa, segurança ou inteligência forem cortadas (total ou parcialmente) e supondo hipoteticamente um fim terrorista por trás dessa ação, criar estratégias alternativas de comunicação ou mesmo um sistema de *backup* que restaure rapidamente as conexões, se torna imperativo.

Devemos lembrar que priorizar a capilaridade em meio a um território tão extenso é um assunto importante e sério, ainda mais dado o fluxo de pessoas que grandes eventos como os jogos olímpicos podem proporcionar. Lugares de difícil comunicação e acesso também devem ser levados em consideração, e adequados com infraestrutura ou pessoal qualificado.

Não só os canais de comunicação eletrônica internos devem ser protegidos, como também as vias de tráfego de informações com a INTERPOL[2], AMERIPOL[3] e MERCOSUL [33] devem ser asseguradas, para que não haja falseamento de informações tampouco para que haja a falta delas em uma situação de emergência.

Por fim, mapear caminhos deixados pelos hackers e a partir daí perceber até onde a narrativa terrorista está chegando se torna também imprescindível. Afinal com cinco dos dez grupos de hackers mais ativos do mundo [34], o Brasil pode, sem perceber, ter mais vias cibernéticas de acesso a seu território do que se imagina.

D. Fortalecer instituições responsáveis

Juntamente com a construção de uma cultura de segurança é necessário que recursos materiais, tecnológicos e principalmente humanos atinjam os órgãos responsáveis pela proteção da esfera cibernética do país.

O engajamento com outros setores da sociedade [35] e a instrução oriunda de países estrangeiros [36] são partes da

[2] INTERPOL, em português significa "Organização Internacional de Polícia Criminal".

[3] AMERIPOL em português significa: "Comunidade de Polícia da América"

solução, mas a necessidade de aumentar proporcionalmente esses esforços é existente.

A cultura de segurança a ser construída deve levar em consideração o trabalho já desempenhado para a proteção do país pelas instituições responsáveis. Não me refiro a explicitar métodos, mas uma boa divulgação de casos exitosos poderia contribuir para o entendimento da necessidade de investimentos na área de segurança, em especial na cibernética.

Outro ponto é que o Ciberterrorismo em específico ganhe um lugar no debate com a sociedade, talvez através da grade curricular da Escola Nacional de Defesa Cibernética [37]. Nesse sentido, elaborar um plano de carreira para manter o pessoal especializado dentro do setor público é fundamental, assim podemos criar um banco de profissionais brasileiros trabalhando efetivamente dentro do território nacional.

Por fim, vale a ressalva de que no âmbito do ciberespaço a máxima de "quanto mais nacional melhor" é a que vale atualmente. Assim, investimentos são necessários, a percepção desses investimentos é imprescindível e a conduta ética dos profissionais em um ambiente tão aberto é fundamental.

IV. CONCLUSÕES

O Brasil não é nenhum país inexperiente no que tange a organização e segurança de grandes eventos. Todavia isso não pode se tornar sinônimo de uma conduta leviana com a segurança nacional.

Tendo isso em mente e partindo especificamente para a questão do terrorismo cibernético, existem áreas de preocupação nacional que devem merecer atenção se quisermos que o país encerre seu ciclo de evidência - enquanto país-sede de grandes eventos- com "chave-de- ouro".

Assim, o Brasil deve atentar para quatro grandes áreas antes que os jogos olímpicos aconteçam em 2016. Essas áreas seriam: 1) Necessidade de uma legislação interna, a qual tipifique o que é terrorismo para o Brasil; 2) a construção de uma cultura de segurança voltada para a cibernética, ao nível de implicações reais e virtuais; 3) o fato de conseguir assegurar a capilaridade das comunicações eletrônicas dentro e fora do território nacional; e 4) a necessidade do fortalecimento das instituições responsáveis pela tomada de ações antiterroristas.

Cada uma dessas áreas possui especificidades e compõem, em parte, preocupações de ordem internacionais (como por exemplo, o manejo de contra narrativas e uma tipificação do terrorismo, e de sua vertente cibernética). Se formos capazes de supri-las, isso não só garantirá uma boa administração dos jogos Rio2016, como também poderia nos ajudar na construção de uma doutrina de segurança que equilibre os anseios de um estado de direito democrático com medidas securitárias apropriadas.

REFERÊNCIAS

[1] Collin B. C (1997) The future of cyberterrorism. *Crime & Justice International* 13 (2). Disponível em: http://www.cjimagazine.com/archives/cji4c18.html?id=415 Acesso em 19 de Abril de 2015. (tradução nossa)

[2] Macdonald, S., Jarvis, L., Chen, T. & Lavis, S. (2013). *Cyberterrorism: A Survey of Researchers*. Cyberterrorism Project Research Report (No. 1), Swansea University. Disponível em: www.cyberterrorism-project.org Acesso em 17 de Abril de 2015. (tradução nossa)

[3] Awan, I.(2014) Debating the term cyber-terrorism: Issues and problems, *Internet Journal of Criminology.ISSN 2045-6743 [online]* . Disponível em: http://www.internetjournalofcriminology.com/ Acesso em 19 de Abril de 2015 p.02 (tradução nossa)

[4] Charvat, J P I A G. *Cyber Terrorism: A New Dimension in Battlespace*. Disponível em: https://ccdcoe.org/publications/virtualbattlefield/05_CHARVAT_Cyber%20Terrorism.pdf.Acesso em 19 de Abril de 2015. P.02 (tradução nossa)

[5] Jarvis, L., Nouri, L. & Whiting, A. (2014) 'Understanding, Locating and Constructing Cyberterrorism'. In: Chen, T., Jarvis, L. & Macdonald, S. (eds) (2014) *Cyberterrorism: Understanding, Assessment and Response* (New York: Springer) Disponível em: http://www.springer.com/computer/information+systems+and+applications/book/978-1-4939-0961-2 Acesso em: 19 de Abril de 2015. p.34-35 (tradução nossa)

[6] Weimann, G. (2005) The sum of all fears? *Studies in Conflict & Terrorism,* 28 (2). p.133

[7] Weimann, G (2004) *Us Institute of Peace December*. Special Report 119 [online] Disponível em: http://webcache.googleusercontent.com/search?q=cache:W8chjRrx0AMJ:www.usip.org/sites/default/files/sr119.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br Acesso em 19 de abril de 2015.p.05 (tradução nossa)

[8] Para entendimento maior sobre a preferencia do uso do autor ver: Awan, I.(2014) Debating the term cyber-terrorism: Issues and problems, *Internet Journal of Criminology.ISSN 2045-6743 [online]*

[9] Algemene Inlichtingen en Veiligheidsdienst (AIVD), (2012) *Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age*. Disponível em: https://www.aivd.nl/english/publications-press/@2873/jihadism-web/ Acesso em 19 de Abril de 2015. p.05 (tradução nossa)

[10] Weimann, G. (2005) The sum of all fears? *Studies in Conflict & Terrorism,* 28 (2); Ginkel, B. van. *Responding to Cyber Jihad: Towards an Effective Counter Narrative*. International Center Counter Terrorism (ICCT) Research Paper March 2015. Disponível em: http://www.clingendael.nl/publication/responding-cyber-jihad-towards-effective-counter-narrative Acesso em 19 de Abril de 2015. (tradução nossa)

[11] Behr, I. von; Reding, A; Edwards, C. Luke G. (2013) *Radicalization in the Digital Era*. Research reports RAND Corporation. Disponível em: http://www.rand.org/pubs/research_reports/RR453.html Acesso em 19 de Abril de 2015 (tradução nossa)

[12] Liang, C.S. (2015) *Cyber Jihad: Understanding and Countering Islamic State Propaganda*. Geneva Center of security Policy (GCSP) Policy Paper 2015/2. Disponível em: http://www.gcsp.ch/Emerging-Security-Challenges/Publications/GCSP-Publications/Policy-Papers/Cyber-Jihad-Understanding-and-Countering-Islamic-State-Propaganda Acesso em 19 de Abril de 2015. P.02 (tradução nossa)

[13] Canthanéde, E; Matais A.(2015) Governo detecta recrutamento de jovens pelo Estado Islâmico. *Estadão [online]* Disponível em: http://internacional.estadao.com.br/noticias/geral,governo-detecta-recrutamento-de-jovens-pelo-estado-islamico,1655354 Acesso em 19 de Abril de 2015.

[14] Global CounterTerrorism Forum. The Hague-*Marrakech Memorandum on Good Practices for a More Effective Response to the FTF Phenomenon*. Disponível em: https://www.thegctf.org/web/guest/foreign-terrorist-fighters;jsessionid=2C659E5ECACBD47050353F462BA883CF.w142 Acesso em 19 de Abril de 2015.p.01(tradução nossa)

[15] Ibid.

[16] Ibid

[17] S/RES/2178 (2014) p.02 (tradução nossa)

[18] Ginkel. Op. cit. p.04 (tradução nossa)

[19] *NETMundial.Multistakeholder Statement* (2014) Disponível em http://netmundial.br/netmundial-multistakeholder-statement/ Acesso em 19 de Abril de 2015. P.05

[20] Campos, A. J. de *Terrorismo e Grandes Eventos*. In: Seminário Internacional Terrorismo e Grandes Eventos (2013: Brasília, DF).Terrorismo e grandes eventos [recurso eletrônico].Câmara dos Deputados, Comissão de Relações Exteriores e de Defesa Nacional. Brasília: Câmara dos Deputados, Edições Câmara, 2014. P.58

[21] Woloszyn, A. L *O Terrorismo do Século 21 e a Democracia*. In: Seminário Internacional Terrorismo e Grandes Eventos (2013: Brasília, DF).Terrorismo e grandes eventos [recurso eletrônico].Câmara dos Deputados, Comissão de Relações Exteriores e de Defesa Nacional. Brasília: Câmara dos Deputados, Edições Câmara, 2014. P.34 (grifo nosso)

[22] Mariani, C.B. *Como o Brasil está inserido no combate internacional ao terrorismo?* Disponível em: http://relacoesinternacionais.com.br/politica-externa/como-o-brasil-esta-inserido-no-combate-internacional-ao-terrorismo/ Acesso em 22 de Abril de 2015 (grifo nosso)

[23] BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil:* texto constitucional promulgado em 5 de outubro de 1988, com as alterações adotadas pelas Emendas Constitucionais nº 1/92 a 67/2010 e pelas Emendas Constitucionais de Revisão nº 1 a 6/94. Brasília, DF: Senado Federal, Subsecretaria de Edições Técnicas, 2011

[24] Woloszyn Op. cit.

[25] Mesquita, L.E.G. *O Terrorismo e a sua probabilidade de ocorrência no Brasil.*(2012) Trabalho de Conclusão de Curso. Escola Superior de Guerra. Rio de Janeiro 2012. P.37

[26] Woloszyn Op. cit.

[27] Lasmar, J.M. A legislação brasileira de combate e prevenção do terrorismo quatorze anos após 11 de Setembro: limites, falhas e reflexões para o futuro. *Revista de Sociologia Política*, v. 23, n. 53, p. 47-70, mar. 2015.

[28] Guimarães, S.P. *Terrorismo e Grandes Eventos*. In: Seminário Internacional Terrorismo e Grandes Eventos (2013: Brasília, DF).Terrorismo e grandes eventos [recurso eletrônico].Câmara dos Deputados, Comissão de Relações Exteriores e de Defesa Nacional. Brasília: Câmara dos Deputados, Edições Câmara, 2014. p.71

[29] Salaberry, L.A.S. *Terrorismo e Grandes Eventos*. In: Seminário Internacional Terrorismo e Grandes Eventos (2013: Brasília, DF).Terrorismo e grandes eventos [recurso eletrônico].Câmara dos Deputados, Comissão de Relações Exteriores e de Defesa Nacional. Brasília: Câmara dos Deputados, Edições Câmara, 2014. p.64

[30] Daher, D. *Terrorismo e Grandes Eventos* In: Seminário Internacional Terrorismo e Grandes Eventos (2013: Brasília, DF).Terrorismo e grandes eventos [recurso eletrônico].Câmara dos Deputados, Comissão de Relações Exteriores e de Defesa Nacional. Brasília: Câmara dos Deputados, Edições Câmara, 2014. P.78

[31] Arruda, J.C. *Terrorismo e Grandes Eventos* In: Seminário Internacional Terrorismo e Grandes Eventos (2013: Brasília, DF).Terrorismo e grandes eventos [recurso eletrônico].Câmara dos Deputados, Comissão de Relações Exteriores e de Defesa Nacional. Brasília: Câmara dos Deputados, Edições Câmara, 2014. P. 70

[32] Daher Op. cit. p.76

[33] Ibid. p.77

[34] Raposo, A. C. Terrorismo e Contraterrorismo: desafio do século XXI**.** *Revista Brasileira de Inteligência*. Brasília: Abin, v. 3, n. 4, set. 2007. p. 46

[35] Salaberry, Op. cit. p.65

[36] Arruda, Op. cit. p.72

[37] Matsuura, S. Brasil terá Escola Nacional de Defesa Cibernética. *O Globo [online*] disponível em http://oglobo.globo.com/sociedade/tecnologia/brasil-tera-escola-nacional-de-defesa-cibernetica-15914957 Acesso em 22 de Abril de 2015.

:

Bruna Toso de Alcântara, graduanda de Relações Internacionais da Universidade Federal de Santa Maria, Santa Maria-RS, Brasil, E-mail: brunatoso@hotmail.com