DA CIBERSEGURANÇA À CIBERDEFESA AMERICANA: A *DIPLOMACIA DA INTERNET* COMO INSTRUMENTO DE PROTEÇÃO E DE INTEGRAÇÃO DOS ESTADOS DA OEA

GILLS LOPES MACÊDO SOUZA¹
MARCELO DE ALMEIDA MEDEIROS²

O governo deve estar ciente dos riscos de segurança cibernética e medidas pertinentes de prevenção, e deve assumir a responsabilidade e tomar medidas para aumentar a segurança das tecnologias de informação. (ONU, 2003).³

A Internet se converteu em instrumento indispensável aos Estados da OEA. Lamentavelmente, ela também gerou novas ameaças que colocam em perigo toda a comunidade mundial que a utiliza. (OEA, 2003).⁴

Resumo: O século XXI acentua ainda mais os conflitos de quarta geração, em que, de um lado, o ente estatal perde o monopólio weberiano do uso exclusivo da força e, do outro, as novas tecnologias da informação e comunicação se aliam a práticas delituosas e transfronteiriças. Uma forma de enfrentar tais ameaças – e que, por diversas vezes, fogem dos limites técnicos dos Estados – é a união em redes. A OEA, através do *Grupo de Peritos Governamentais em Matéria de Delito Cibernético* e da *Estratégia de Segurança Cibernética*, demonstra que a cooperação internacional de combate aos cibercrimes no continente americano está dentro dos padrões. Todavia, analisando a cibersegurança, percebe-se um *vacuum legis*, no que tange à ciberdefesa para este continente. Assim, este trabalho não se propõe a versar uma nova Doutrina Monroe para a proteção do ciberespaço americano; busca, porém, demonstrar a importância do tema *cyberwar* para as políticas de defesa dos países-membros da OEA e, por conseguinte, a negligência desta para com aquele, no sentido de evidenciar que, assim como as políticas de cibersegurança, as de ciberdefesa também são fulcrais para uma integração regional. Para tanto, este trabalho se aporta teoricamente em Peter Haas, Manuel Castells e Robert Putnam.

Palavras-chave: OEA. Ciberdefesa. Diplomacia da Internet.

Abstract: *The 21st century accentuates the fourth generation conflicts, where the state loses the Weberian monopoly on the legitimate use of physical force, and the new information and communication technologies ally themselves to criminal and cross-border practices. One way to tackle such threats – that many times scape the technical limits of states – is networks union. OAS, through its Working Group on Cyber-Crime and Cybersecurity Strategy, demonstrates that the international cooperation to combat cyber-crime at American continent is within acceptable standards. Nonetheless, when considering such cyber security subjects, perceives a gap regarding a cyber defense for this continent, mainly the cyber war theme. So, this work does not intend to relate to a new Monroe Doctrine concerned with protecting of the American cyberspace; indeed, it seeks to demonstrate the importance of cyber war theme to the defense policy of the members of OAS and,*

thus, its negligence with the aforesaid theme in order to show that, like cyber security policies, the cyber defense ones are also vital to a regional integration. Therefore, this paper is theoretically based on works of Peter Hass, Manuel Castells and Robert Putnam.

Keywords: OAS. Cyber defense. Diplomacy of the Internet.

INTRODUÇÃO

Integração regional pressupõe mais que a conexão de pessoas, espaços físicos e moedas. Nela, são levados também em consideração elementos outros, não tão visíveis – porém igualmente vitais –, como a cooperação técnica e os aspectos de segurança e defesa ciberespacial e das infraestruturas críticas informacionais. Pois, são estas últimas que fornecem o grau de tranquilidade e os recursos necessários para o tráfego e as transações interpessoais e interestatais.

No gozo pleno da *Era da Informação*, lidar com temas como cibersegurança (ou segurança cibernética ou, ainda, *cyber security*) e ciberdefesa (ou defesa cibernética ou, ainda, *cyber defense*) constitui um desafio e, ao mesmo tempo, uma necessidade imprescindível à sobrevivência do Estado. Com a Organização dos Estados Americanos (OEA) não é diferente, pois no cerne de sua essência estão os governos que lhe dão a razão de ser. Assim como os temas sensíveis e em voga, hoje, nos *fora* mundiais – e.g.: direitos humanos, meio ambiente, desenvolvimento integral⁵ etc. –, as diversas abordagens sobre as *novas* tecnologias de informação e comunicação (NTIC), sobretudo no que toca à Internet, começam a dominar as agendas internacionais e, conseqüentemente, tocar as da OEA.

Neste sentido, busca-se aqui realizar uma breve análise acerca de como a segurança e defesa cibernéticas são tratadas, no âmbito da OEA. Em seguida, demonstra-se que a *diplomacia da internet* – se bem empregada – constitui uma ferramenta assaz importante tanto à proteção quanto à integração dos países membros da organização inter-regional *supra*.

OS DESAFIOS AMERICANOS VIS-À-VIS ÀS NOVAS AMEAÇAS ASSIMÉTRICAS E CIBERNÉTICAS

Alguns fenômenos relacionados à interdependência complexa – como os processos de integração regional e de segurança coletiva baseada em arenas multilaterais –, são engendrados a partir de um movimento que, embora antigo, se adapta perfeitamente à junção entre capitalismo e facilidades/possibilidades oriundas da Revolução da Informação. Esse movimento é o da globalização⁶. Mas, conforme Held e McGrew (2001, p. 11-14), não há uma definição precisa e universal para globalização, e sim várias roupagens que diversos estudiosos lhe atribuem, sejam eles da corrente globalista ou adeptos de um viés mais cético, no que se refere às maravilhas de um mundo global. Para fins de escolha, adota-se, aqui, uma dessas roupagens: a de que a globalização é uma *compressão espaço-temporal*, ou seja, um fenômeno cuja ênfase é dada “ao modo como a comunicação eletrônica instantânea vem desgastando as limitações da distância e do tempo na organização e na interação sociais” (2001, p. 11).

Embora a serviço do desenvolvimento humano frente às suas necessidades e limitações, as ferramentas oriundas das NTIC também servem para propósitos outros, como os de (i) cunhos terrorista e criminoso transnacionais e (ii) manutenção do *status quo* estatal na política internacional.

Quanto ao primeiro propósito supracitado, percebe-se que as NTIC têm permitido ao terrorismo ascender suas ações da escala regional para a global, promovendo suas mensagens e causas através de ataques cada vez mais sofisticados e bem coordenados (KIRAS, 2001, *passim*). De acordo com Kiras (2001, p. 489-493), as tecnologias avançadas associadas à globalização têm impulsionado a ação terrorista – grupos ou células – principalmente nas áreas que envolvem:

- a) proselitismo: captação de novos seguidores e patrocinadores, utilizando poucos recursos, mas em grande escala, como folhetos de propaganda, material multimídia (o que inclui, *per se*, a internet como canal de difusão) etc.;
- b) coordenação: as NTIC têm permitido aos terroristas elaborar e coordenar ataques, a partir de diferentes países (ou regiões afastadas, dentro de um mesmo país), não importando suas distâncias;
- c) segurança: as questões de vigilância e contra-vigilância se encaixam nesta área, fazendo com que, sobretudo, as comunicações clandestinas

e/ou criptografadas dos terroristas se tornem, em última instância, difíceis de localizar;

- d) mobilidade: seja por intermédio de dispositivos eletrônicos móveis, seja pela globalização do comércio, o fato é que as tecnologias associadas à globalização dão aos terroristas a possibilidade de enfrentar o Estado, no que tange à comparação de recursos disponíveis a ambos os lados; e
- e) letalidade: embora os terroristas não obtenham nem utilizem largamente armas (químicas, biológicas, teleguiadas etc.) de destruição em massa, a era da globalização permite um acesso mais facilitado – e obtenção mais rápida – a esses tipos de armas cada vez menores em tamanho e maiores em poder destrutivo.

Todavia, em resposta a tais transgressões, cabe à comunidade global utilizar “de forma colaborativa, os recursos à sua disposição para diminuir o apoio ao terrorismo e demonstrar a ilegitimidade” (KIRAS, 2001, p. 480)⁷ dessas causas e mensagens. Nessa linha de raciocínio, Castells (2007, p. 205) argumenta que uma forma eficaz de os países combaterem tais ameaças transnacionais é se utilizarem da mesma ferramenta que permitiu a aliança entre criminosos e/ou terroristas: a articulação em rede.

Essa articulação, por parte dos governos, para combater os crimes e atos terroristas que utilizam recursos baseados em NTIC, é cada vez mais frequente. As polícias de praticamente todo o mundo mantêm constante contato entre si, graças a canais como a INTERPOL ou, mesmo, ao intercâmbio jurídico direto entre países, como as cartas rogatórias. A título de exemplo, até mesmo as polícias estaduais brasileiras investigam crimes baseados no acesso e uso da Internet.

Logo, no âmbito das ameaças criminosas oriundas do (ou que ocorrem no) ciberespaço, os Estados, há quase uma década, se articulam para combatê-las, nas suas diversas formas: pornografia infantil, *defacement* – mudança do conteúdo de um sítio virtual por outro –, roubo de dados, desvio de valores etc. Outrossim, no que toca às ameaças terroristas, amiúde os departamentos de investigação se municiam de armas *high-tech* para encontrar, perseguir e capturar mentores e partícipes delituosos, como visto na captura e morte de Osama Bin Laden pelas forças especiais americanas (aportadas em investigações da CIA e do FBI), no primeiro semestre de 2011. Portanto, o combate eficaz às ameaças cibernéticas não estatais

– ou paraestatais – (cibersegurança) se mostra assaz recorrente, tanto por parte do Estado enquanto ator unilateral, quanto no que tange à cooperação internacional.

Já o segundo propósito oriundo da utilização desvirtuada das NTIC cogita aspectos analíticos mais complexos, que envolvem projeção de cenários (tipos ideais) e um fator inexistente (se comparado à cibersegurança): o *vacuum legis* quanto à matéria. Tem-se que a manutenção do *status quo* estatal na política internacional engendra, *per se*, um desafio hercúleo aos estudiosos, bem como aos próprios Estados, a saber: e quando não é o indivíduo ou um grupo de indivíduos, e sim um ator estatal, o responsável por criar e/ou proferir ataques cibernéticos a outro ator estatal? Baseado em qual dispositivo legal se legitimaria uma investigação contra ele ou, mesmo, como ele seria punido?

A Estônia, por exemplo, em 2007, culpa a Rússia por ataques cibernéticos à sua infraestrutura informacional – à época, uma das mais sofisticadas do mundo –, colocando em risco negócios de empresas multinacionais e serviços governamentais internos e oferecidos aos cidadãos. Desde então, (i) a Organização do Tratado do Atlântico Norte (OTAN) mantém um centro especializado em ciberdefesa, o *Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE), na capital estoniana, Tallinn, e (ii) o acesso à rede mundial de computadores se tornou um direito fundamental na Estônia⁸ (SOUZA, 2010, p. 48). É a globalização demonstrando pragmaticamente todas as suas “implicações também para a governança e para a participação democrática” (FERGUSON, 2002, p. 107).

Não obstante, diversos Estados, nos últimos quatro anos, acompanharam a OTAN e criaram seus próprios órgãos voltados à ciberdefesa, com destaques para os Estados Unidos da América (EUA), Brasil e, mais recentemente, China e Inglaterra. A título de exemplificação de como o assunto vem sendo tratado no Reino Unido, Nick Harvey (*apud* Hopkins, 2011)⁹, ministro das forças armadas britânicas, disse que a “ação no ciberespaço fará parte do futuro campo de batalha”. O assunto é levado seriamente também pelo Exército Brasileiro¹⁰, com a criação do primeiro Centro de Defesa Cibernética (CDCiber), em Brasília.

No âmbito do combate aos delitos informacionais praticados por criminosos e/ou terroristas, a OEA possui um organismo de consulta específico, que é o *Grupo de Trabalho sobre Delito Cibernético*. Porém, no que toca às questões de defesa cibernética, a OEA é omissa.

Aqui, faz-se mister a introdução da acepção de Clarke e Knake (2010, p. 6)¹¹ para o termo *cyberwar*, como sendo as “ações de um Estado-nação para penetrar em computadores ou redes de uma outra nação, para efeitos de causar-lhe danos ou interrupção”.

O tema *cyberwar* (ciberguerra ou guerra cibernética, eletrônica ou informacional) é inserido nesta discussão, no sentido de demonstrar uma diferenciação necessária entre cibersegurança e ciberdefesa. Aquela com uma conotação mais civil; e esta, pautada por um viés mais militar; cabendo às Forças Armadas a salvaguarda da soberania nacional frente a uma ameaça externa.

Como visto, os desafios frente às novas ameaças assimétricas e cibernéticas são muitos e abrangem todas as esferas em que seja necessária a intervenção do Estado: desde a local, passando pela nacional; e da inter-regional, tocando o global. Cabe, agora, analisar como a OEA desenvolve suas políticas de segurança e defesa cibernéticas, no intuito de vislumbrar, assim, a manifestação da *diplomacia da internet* no seio desta organização.

A DIPLOMACIA DA INTERNET NO ÂMBITO DA OEA

Negociações internacionais, por vezes, permitem aos líderes de governo fazer o que deseja fazer em privado, mas são incapazes de fazer domesticamente. (PUTNAM, 1988, p. 457).¹²

Negociações envolvendo questões que tocam à tutela do Estado, tanto no âmbito nacional quanto no internacional, são analisadas/explicadas por diferentes ângulos. Como metodologia de análise política, parte-se, aqui, de um pressuposto em que as questões inerentes ao ciberespaço – governança da internet e direitos fundamentais de acesso à informação e ao sigilo eletrônico, por exemplo –, são arroladas num jogo de dois níveis (*two-level game*).

Para Putnam (1988, *passim*), criador de tal concepção, tal jogo assume, necessariamente, que política doméstica e relações internacionais estão de alguma forma entrelaçadas. Ou seja, segundo o autor estadunidense, o sucesso (ou não) das negociações internacionais levadas a cabo pelo Estado é função de sua capacidade de negociação interna. É mister, então, entender as transações não como a vontade estática e monolítica dos Estados, mas como duas mesas postas

em dois níveis interativos entre si. Nesse prisma, as explicações se voltam não para “o” Estado unitário, mas para “os” tomadores de decisão, onde, segundo Putnam (1988, p. 434, 436):

1. no Nível I (internacional), negociadores representam seus Estados e sentam-se numa mesa, com o objetivo de tentar acordos; e
2. no Nível II (nacional), grupos domésticos – agências burocráticas, grupos de interesse, classes sociais [sob a pressão da opinião pública (ou não)] – se sentam noutra mesa para discutir a ratificação de tais acordos.

Putnam ainda introduz um componente relevante para tal jogo: o “*win-set*”. Tal componente pode ser definido como “o conjunto de todos os acordos possíveis de Nível I que ‘ganhariam’ – isto é, que obteriam a maioria necessária entre os votantes – quando fossem simplesmente aprovados ou rejeitados” (PUTNAM, 1988, p. 437)¹³. Assim, quando o negociador se senta à mesa internacional (Nível I), sua única certeza é o fato de que todos os acordos acertados dentro do *win-set* serão ratificados no Nível II. O que se traduz numa espécie de silogismo político, uma vez que: (i) “*win-sets* mais largos tornam acordos no Nível I mais prováveis, *ceteris paribus*” (PUTNAM, 1988, p. 437)¹⁴; e (ii) “o tamanho relativo¹⁵ dos respectivos *win-sets* do Nível II afetará a distribuição de ganhos conjuntos da barganha internacional” (PUTNAM, 1988, p. 440)¹⁶. Assim, a necessidade de que os acordos sejam ratificados no Nível II pode afetar as negociações no Nível I, de modo que “nenhum dos dois jogos possa ser ignorado pelos principais tomadores de decisão” (PUTNAM, 1988, p. 434)¹⁷.

É essa lógica na relação entre doméstico e internacional que envolve os principais *fora* de discussão hodiernos, no que tange aos aspectos cibernéticos, quer sejam eles no âmbito das negociações internacionais do Fórum de Governança da Internet das Nações Unidas (Nível I), quer nas manifestações civis brasileiras contra o Projeto de Lei encabeçado pelo Senador Eduardo Azeredo sobre cibercrimes (Nível I). Sendo este último caso a materialização de uma máxima de Putnam (1988, p. 445)¹⁸, quando afirma que, no Nível II, “a politização [de um dado tema] geralmente ativa grupos que estão menos preocupados com os custos de um não acordo, reduzindo, por conseguinte, o efetivo *win-set*”.

Assim, analisando as questões pertinentes à defesa e à segurança do ciberespaço, identifica-se a realização de um jogo de dois níveis. No Nível II desse jogo, sentam-se à mesa os grupos de interesse nacionais no assunto, como: corpo

diplomático, Forças Armadas, segurança pública e sociedade civil organizada (sobretudo, ativistas de direitos humanos, *lobbies* da mídia e grupos ligados às ciências da computação e informação); lembrando que, neste Nível, os limites das ações do representante nacional – negociador – na mesa internacional são estipulado pelo *win-set*, gerando, assim, os *inputs* para o Nível I. Já no primeiro nível, os chefes negociadores¹⁹ praticam o que se chama aqui de *Política da Internet*, *i.e.*, um conjunto de ações diplomáticas que visam à proteção do *win-set* nacional acerca do ciberespaço. Essa proteção é necessária, uma vez que os outros governos, sentados à mesa internacional, buscam expandir seus interesses a custas dos *win-sets* dos outros (PUTNAM, 1988, p. 454).

Logo, a *Diplomacia da Internet* é um conjunto de pressupostos que orienta as relações internacionais digitais, englobando, necessariamente, quatro partes fulcrais do Estado: (i) o governo nacional; (ii) a sociedade civil organizada; (iii) o corpo diplomático; e (iv) as Forças Armadas.

É o governo que reconhece os interesses estatais, em meio às transformações da globalização, e implementa políticas para se adaptar a elas – o que inclui as matérias de segurança e cibersegurança para manter a ordem interna no ciberespaço.

A sociedade civil organizada é encarregada da dupla função de legitimar as ações governamentais e, quando necessário, assessorar/aconselhar os tomadores de decisão; constitui, portanto, uma fonte inesgotável de conhecimento.

O corpo diplomático, para defender os interesses do Estado na arena internacional, tendo o ciberespaço ora como ferramenta de trabalho (espécie de embaixada e repartição interna digitais), ora como objeto de discussão (governança da internet, crimes de *cyberwar*, vazamento de informações ultrassecetas, objeto de direitos humanos etc.).

E as Forças Armadas, para salvaguardar digitalmente as informações e dados do corpo diplomático, a integridade do governo nacional, monitorar, defender e contra-atacar potenciais ameaças à soberania nacional (infraestrutura crítica informacional, monitoramento por radar, telecomunicações e outros sistemas digitais).

Conforme apregoa Ferguson (2002, p. 103), “a difusão da nova tecnologia no cotidiano do cidadão” forçou “os governos a utilizá-la em todos os aspectos possíveis de atendimento e administração pública”. Manter toda essa base

informacional, assim como as infraestruturas críticas necessárias ao seu funcionamento é papel do Estado. Porém, quando a ameaça possui recursos técnicos e/ou tecnológicos mais avançados que os de um determinado Estado, o mesmo deve buscar outras ferramentas para se proteger. Portanto, pensar novas soluções de segurança e defesa internacionais deve estar sempre na pauta tanto do corpo diplomático quanto do militar. No âmbito da OEA, não deve ser diferente, pois, dentre seus *propósitos essenciais*, estabelecidos em sua *Carta*, está o de garantir a paz e a segurança continentais (OEA, 2003).

Deste ponto, parte-se do pressuposto haasiano de que os tomadores de decisão, que não detêm conhecimentos técnicos necessários às “[...] crescentes incertezas e complexidades técnicas dos problemas de interesse global” (HAAS, 1992, p. 1)²⁰, devem buscar apoio em comunidades epistêmicas, a fim de que eles possam (re)definir os interesses estatais e desenvolver soluções viáveis a problemas específicos. Ainda, segundo Haas (1992, p. 2-3), essas comunidades são redes de influentes estudiosos baseados no conhecimento (*knowledge-based experts*) de determinada área ou tema, que dão conselhos/assessoramento aos tomadores de decisão, ajudando-os a identificar seus interesses. Apesar de voltar seu estudo para entender e explicar como a coordenação política internacional se desenrola, a visão de Haas acerca do papel da informação e do conhecimento – em suas palavras, “controle do conhecimento e da informação é uma importante dimensão do poder” (HAAS, 1992, p. 2)²¹ – serve de aporte para vislumbrar, aqui, uma outra possibilidade à defesa dos interesses e da soberania estatais (mais especificamente, à ciberdefesa): as comunidades epistêmicas transnacionais. Pode-se dizer que a OEA se encaixa nesta última, pois seus *experts* – como aqueles que compõem o *Grupo de Trabalho sobre Delito Cibernético* –, por exemplo,

podem influenciar os interesses do Estado, quer por identificá-los diretamente para os tomadores de decisão ou, iluminando as dimensões salientes de um problema a partir do qual os tomadores de decisão podem, então, deduzir os seus interesses. (HAAS, 1992, p. 4)²².

No mesmo ano dos ataques do 11 de setembro, foi criada, na Hungria, a *Convenção de Budapeste sobre Cibercrimes*. Este documento, além de tipificar e buscar maneiras de punir os delitos cibernéticos, demonstra toda a preocupação que o ciberespaço gera para os entes estatais, sobretudo no que tange às transações econômico-financeiras. Além de possuir um capítulo específico para as *medidas a tomar a nível nacional*, a Convenção tem também um capítulo que trata apenas da

Cooperação Internacional, encorajada “[...]para efeitos de investigações ou de procedimentos relativos a infrações penais relacionadas com sistemas e dados informáticos, ou para recolher provas sob a forma eletrônica de uma infração penal” (CONVENÇÃO..., 2001, p. 15)²³.

Portanto, desde 2001, se tem um documento que busca – ainda que debaixo de fortes contestações por grande parte de ativistas de direitos humanos e da sociedade civil organizada brasileira – padronizar uma articulação punitiva para os cibercrimes e, sobretudo, o *modus operandi* de combatê-lo, com ênfase na cooperação internacional, na articulação em redes.

Já com as questões de defesa, o que se visualiza é um imenso *gap*. A história comprova que o fato de haver legislação, não impede que guerras ocorram. Porém, esse vazio se estende não apenas a quem faz as leis, mas também a quem as propõe, através de estudos e debates, *i.e.*, à sociedade civil organizada.

Apesar de não contemplar por completo a *diplomacia da internet*, a OEA dá os primeiros sinais em busca dessa consolidação: em julho de 2011, na cidade de Santiago, Chile, ocorrerá a Conferência Sub-regional da OEA, com o tema “Novo ambiente de segurança, novas alternativas para a defesa”, onde, dentre outros assuntos, a questão das ameaças assimétricas estão presentes²⁴. Como se vê, o tema está começando a sair da marginalização ou dos encontros de tecnologias da informação e comunicação, e passando a tomar voz política.

CONSIDERAÇÕES FINAIS

Para manter a ordem interna, o Estado utiliza-se dos órgãos responsáveis, vinculados à segurança pública (corporações policiais); e para garantir a sua soberania internacional, ele conta com suas três Armas: exército, marinha e aeronáutica. Todavia, a relação entre defesa nacional e segurança pública tem estreitado bastante, nos últimos anos, sobretudo graças ao advento dos chamados conflitos de quarta geração, em que o campo de batalha pode ser qualquer lugar do globo e cuja ameaça ao Estado pode vir tanto do indivíduo ou de um grupo de indivíduos, quanto de outro ente estatal.

No Brasil, por exemplo, o papel das Forças Armadas está positivado no Art. 142 da sua Carta Magna; já o da Segurança Pública, no Art. 144. Embora tenha sido

de fundamental importância para o êxito contra o tráfico de drogas e de armas em alguns morros do Rio de Janeiro, a introdução das Forças Armadas foi assaz contestada, pois sua utilização – ao lado das forças policiais especiais – é vista, por alguns especialistas²⁵, como um completo desvio de sua imaculada função de resguardar a soberania nacional de uma ameaça externa, e não interna.

O caso brasileiro exemplifica também, de forma análoga, o que ocorre no âmbito da defesa e da segurança do ciberespaço. Em outras palavras, os dois conceitos, dificultando – ainda mais – a proteção do espaço cibernético.

Assim, a execução da *diplomacia da internet* implica dizer que:

1. os assuntos de cibersegurança sejam tratados por órgãos ligados à segurança pública e que os assuntos de ciberdefesa sejam tratados por órgãos ligados à defesa nacional.
2. o governo nacional acolha as demandas da sociedade civil, no que tange aos assuntos pertinentes às TIC, pois as universidades detêm um bem que órgão nenhum pode possuir por completo: conhecimento em constante expansão.
3. o corpo diplomático seja instruído, desde sua formação, sobre os principais riscos e potencialidades advindos do ciberespaço.

Porém, como analisado, mesmo se a OEA possui um grupo de trabalho para tratar dos crimes cibernéticos e da cibersegurança, vale frisar que este é uma espécie de conselho consultivo das “Reuniões de Ministros da Justiça ou de outros Ministros ou Procuradores-Gerais das Américas”, na esfera do seu Departamento de Cooperação Jurídica²⁶. Falta-lhe, portanto, um órgão específico para lidar com assuntos concernentes à ciberdefesa e que possa se envolver nas mais diversas áreas correlatas, como direito internacional, redes de computadores / telemática e estudos de defesa.

A OTAN (através do NATO CCD COE) e, em certa medida, a União Europeia (no âmbito do European Conference on Information Warfare and Security – ECIW) já possuem órgãos ou *fora* voltados à defesa cibernética. Além de Brasil (CDCiber) e EUA (U.S. Cyber Command), Reino Unido (Cyber Security Operations Centre on Government Communication Headquarters), China (Cyber Blue Team) e Coreia do Norte (Cyber Warfare Unit 121)²⁷ também possuem os seus respectivos órgãos. Em pleno limiar do século XXI, se a OEA não preencher esse vácuo, ela tende a ficar defasada quanto aos assuntos que envolvem a realidade da *Era da Informação*.

Uma possível alternativa para isto seria a criação de um órgão, ainda que embrionário, que pudesse aglutinar representantes militares dos países que possuem esse tipo de órgão, para promover um intercâmbio sobre seus projetos e expectativas para o continente americano. Brasil e EUA, com seus órgãos precitados, são exemplos plausíveis para esse primeiro e necessário passo.

Não se propõe, com este trabalho, uma nova versão da Doutrina Monroe, para fechar ciberespaço americano aos assuntos estrangeiros, mas um fortalecimento das fronteiras do ciberespaço para não deixar que potenciais ameaças não adentrem aqui. Isso evita muitos inconvenientes reais que se originam no mundo virtual, o que inclui responder a um ciberataque com o uso de força militar, conforme já se prega o Pentágono²⁸.

Tendo em vista que “o uso do ciberespaço por Estados-nação com objetivos políticos, diplomáticos e militares não têm de ser, no entanto, acompanhado por bombardeios e batalhas físicas” (CLARKE e KNAKE, 2010, p. 11)²⁹, torna-se imprescindível a união entre aqueles que fazem a *diplomacia da internet*, no continente americano. Assim sendo, a OEA continua efetivando – e, concomitantemente, atualiza – uma de suas razões de ser: defender e assegurar a integridade do continente, em suas mais diversas topologias.

REFERÊNCIAS

CASTELLS, Manuel. **Fim do Milênio**. 4. ed. Tradução: Klauss B. Gerhardt e Roneide V. Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3).

CHANDA, Nayan. **Sem Fronteira**. Rio de Janeiro: Record, 2011.

CLARKE, Richard; KNAKE, Robert K. **Cyber war: the next threat to national security and what to do about it**. Nova Iorque: HarperCollins Publishers, 2010.

CONVENÇÃO de Budapeste sobre cibercrimes. 2001. Disponível em: <<https://www.safernet.org.br/site/sites/default/files/Convencao-sobre-o-Cibercrime.pdf>>. Acesso em: 3 jun. 2011.

FERGUSON, Martin. Estratégias de governo eletrônico: o cenário internacional em desenvolvimento. *In*: EISENBERG, José; CEPIK, Marco (Org.). **Internet e política: teoria e prática da democracia eletrônica**. Belo Horizonte: Editora UFMG, 2002. p. 103-140.

HELD, David; MCGREW, Anthony. **Prós e contras da globalização**. Tradução: Vera Ribeiro. Rio de Janeiro: Jorge Zahar, 2001.

HOPKINS, Nick. UK developing cyber-weapons programme to counter cyber war threat. 30 maio 2011. Disponível em: <<http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive>>. Acesso em: 2 jun. 2011.

KIRAS, James D. Terrorism and globalization. *In*: BAYLIS, John; SMITH, Steve (Org.). **The globalization of world politics: an introduction to international relations**. Oxford: Oxford University Press, 2001. cap. 21, p. 479-497.

(OEA) ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Conselho Permanente. OEA/Ser.G CP/INF.3964/96 rev. 1, de 6 de outubro 1997. **Carta da Organização dos Estados Americanos**. Disponível em: <<http://www.oas.org/juridico/portuguese/carta.htm>>. Acesso em: 20 maio 2011.

(ONU) ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembleia Geral. A/RES/57/239 (2003). **Creation of a global culture of cybersecurity**. Disponível em: <<http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N02/555/22/PDF/N0255522.pdf>>. Acesso em: 21 maio 2011.

PUTNAM, Robert D. Diplomacy and domestic politics: the logic of two-level games. **International Organization**, Massachusetts, v. 42, n. 3, p. 427-460, 1988.

SOUZA, Gills Lopes M. **A cibersociedade anárquica: análise do uso das Tecnologias de Informação e Comunicação nos conflitos internacionais do século XXI à luz da Escola Inglesa de Relações Internacionais**. 2010. 61 f. Trabalho de Conclusão de Curso (Monografia) – Curso de Relações Internacionais, Universidade Estadual da Paraíba, João Pessoa, 2010.

NOTAS

¹ Gills Lopes Macêdo Souza, bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) junto ao Mestrado em Ciência Política da Universidade Federal de Pernambuco

(UFPE), bacharel em Relações Internacionais pela Universidade Estadual da Paraíba (UEPB) e membro do Núcleo de Estudos de Política Comparada e Relações Internacionais (NEPI/CNPq/UFPE).

² Marcelo de Almeida Medeiros, Doutor em Ciência Política pelo *Institut d'Études Politiques de Grenoble* (1997) e Livre-docente em Ciência Política pelo *Institut d'Études Politiques de Paris* (2010), é Professor Associado de Ciência Política do Departamento de Ciência Política da Universidade Federal de Pernambuco (UFPE) e Pesquisador do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

³ Tradução livre do autor. Texto original: “[...] *government [...] must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of [...] information technologies*”.

⁴ Tradução livre do autor. Texto original: “*La Internet [...] se han convertido en instrumentos indispensables para los Estados Miembros de la OEA. [...] Lamentablemente, la Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de Internet*”.

⁵ O desenvolvimento integral “abrange os campos econômico, social, educacional, cultural, científico e tecnológico, nos quais devem ser atingidas as metas que cada país definir para alcançá-lo” (OEA, 1997).

⁶ Globalização entendida em sua dimensão moderna, marcada pela celeridade dos fluxos proporcionada pelas tecnologias da informação. E não em sua dimensão histórica como analisada por Chanda (2011).

⁷ Tradução livre do autor. Texto original: “*The resources at their disposal collaboratively to diminish support for terrorism and demonstrate the illegitimacy*”.

⁸ Apenas em 2011, impactada pela *onda por democracia nos países árabes*, a ONU, através de um relatório, reconheceu o acesso à Internet como um direito fundamental. Cf. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Conselho de Direitos Humanos. **A/HRC/17/27**, de 16 de maio de 2011. Disponível em: <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>. Acesso em: 12 jun. 2011.

⁹ Tradução livre do autor. Texto original: “*Action in cyberspace will form part of the future battlefield*”.

¹⁰ Segundo a Estratégia Nacional de Defesa do Brasil, cabe ao Exército Brasileiro a guarda pelo setor estratégico do ciberespaço. Além deste, os outros dois setores estratégicos são: o nuclear (sob a guarda da Marinha do Brasil) e o espacial (a cabo da Força Aérea Brasileira). Cf. MINISTÉRIO DA DEFESA DO BRASIL. Estratégia Nacional de Defesa. Disponível em: <https://www.defesa.gov.br/eventos_temporarios/2009/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>. Acesso em: 26 jun. 2011.

¹¹ Tradução livre do autor. Texto original: “[...] *actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption*”.

¹² Tradução livre do autor. Texto original: “*International negotiations sometimes enable government leader to do what they privately wish to do, but are powerless to do domestically*”.

¹³ Tradução livre do autor. Texto original: “[...] *the set of all possible Level I agreements that would “win” – that is, gain the necessary majority among the constituents – when simply voted up or down*”.

¹⁴ Tradução livre do autor. Texto original: “[...] *larger win-sets make Level I agreement more likely, ceteris paribus*”.

¹⁵ Ainda segundo Putnam (1988, p. 442-443), o tamanho do *win-set* depende do tamanho relativo das forças “isolacionistas” (que se opõem à cooperação internacional) e “internacionalistas” (que oferecem todo o suporte possível para que haja tal cooperação).

¹⁶ Tradução livre do autor. Texto original: “[...] *the relative size of the respective Level I1 win-sets will affect the distribution of the joint gains from the international bargain*”.

¹⁷ Tradução livre do autor. Texto original: “*Neither of the two games can be ignored by central decision-makers[...]*”.

¹⁸ Tradução livre do autor. Texto original: “*Politicization often activates groups who are less worried about the costs of no-agreement, thus reducing the effective win-set*”.

¹⁹ Cf. Putnam, 1988, p. 456-459.

²⁰ Tradução livre do autor. Texto original: “[...] *growing technical uncertainties and complexities of problems of global concern*”.

²¹ Tradução livre do autor. Texto original: “[...] *control over knowledge and information is an important dimension of power*”.

²² Tradução livre do autor. Texto original: “*can influence state interests either by directly identifying them for decision makers or by illuminating the salient dimensions of an issue from which the decision makers may then deduce their interests*”.

²³ Tradução livre do autor. Texto original: “[...] *para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para recolher provas sob a forma electrónica de uma infracção penal*”.

²⁴ Os autores deste artigo, através do trabalho intitulado *Uma Convenção sobre Cyberwars para as Américas?*, também foram agraciados com uma bolsa da Embaixada Americana no Brasil para participar do referido evento.

²⁵ Vide, por exemplo, nota da Associação de Estudos de Defesa do Brasil (ABED): http://www.abed-defesa.org/files/forcas_armadas_e_seguranca_publica.pdf.

²⁶ Cujo endereço eletrônico é <http://www.oas.org/juridico/spanish>.

²⁷ Para mais detalhes acerca dos órgãos responsáveis pela defesa – e ataque – cibernética norte coreanos, cf. CLARKE e KNAKE, 2010, cap. 1, *passim*.

²⁸ Cf. GORMAN, Siobhan; BARNES, Julian E. *Cyber combat: act of war: pentagon sets stage for u.s. to respond to computer sabotage with military force*. 31 maio 2011. Disponível em: <<http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>>. Acesso em: 4 jun. 2011.

²⁹ Tradução livre do autor. Texto original: “*The use of cyberspace by nation-states for political, diplomatic, and militar goals does not, however, have to be accompanied by bombing raids or tank battles*”.