

Resenha de: Oliveira, Marcos Aurélio Guedes de; Gama Neto, Ricardo Borges; Lopes, Gills Vilar. 2016. *Relações internacionais cibernéticas (CiberRI): oportunidades e desafios para os estudos estratégicos e de segurança internacional*. Recife: Ed. da UFPE. (Coleção Defesa e Fronteiras Virtuais; 3).

Rev. Bras. Est. Def. v. 5, n° 1, jan./jun. 2018, p. 219-223
 DOI: 10.26792/RBED.v5n1.2018.75027
 ISSN 2358-3932

 ALUYSIO ATHAYDE

Aos chamados três tradicionais espaços comuns globais – o marítimo, o aéreo e o espacial – soma-se, nas últimas décadas, o ciberespacial. Num esforço exemplar, este terceiro volume da Coleção “Defesa e Fronteiras Virtuais”, por meio de seus autores e organizadores sul-americanos, traz reflexões que buscam entrelaçar o cabedal teórico das Relações Internacionais com os estudos de Segurança e Defesa Cibernética.

Para tanto, os autores demonstram que as CiberRI não são de análise exclusiva dos especialistas de Segurança da Informação. Numa época em que “*only an expert can deal with the problem*”,¹ o especialista que permeia o imaginário geral, quando o assunto é cibernética, é aquele que domina técnicas relacionadas à encriptação, controles de acesso, protocolos digitais de segurança e barreiras contra ataques virtuais. Não retirando em absoluto a importância desse profissional da Segurança da Informação, podemos dizer, juntamente com os autores, que restringir a discussão das CiberRI a esse âmbito é *despolitizá-la*, pois retira-se as implicações quanto ao papel da Defesa das relações interestatais, do *soft* e do *hard power*, que são geradas por esse novo ambiente que é o espaço cibernético.

Olhar para as principais teorizações das Relações Internacionais para pensar o ciberespaço é fundamental para a compreensão do fenômeno. É o que se propõe a primeira parte do livro intitulada “Oportunidades e Desafios Teóricos”. O que falar do ciberespaço, algo que ainda não se sabe se é um *ambiente* ou um *universo paralelo*, em que a noção de fronteira é praticamente inexistente e para o qual os organismos internacionais ainda não conseguiram traçar parâmetros básicos dentro do Direito Internacional Público? Ambiente altamente anárquico, poderíamos dizer juntamente com os teóricos clássicos das RI.²

Aluysio Athayde – Doutorando em Ciências Sociais pela PUC-Rio. Mestre em Ciências Sociais com ênfase em Antropologia pela Pontifícia Universidade Católica do Rio de Janeiro.

Importantes autores da área, como o livro demonstra, já sentenciaram que a guerra cibernética é real, acontece na velocidade da luz, é global e prescinde do campo de batalha. O *Macfee Virtual Criminology Report*, citado ao longo da obra, é prova incontestada das cinco características citadas acima e, principalmente, a ideia de que a guerra cibernética já está em pleno andamento. O *report* aponta uma competição entre vários Estados, no que ele chamou de “Guerra Fria Cibernética”. Exemplo interessante dessa guerra é o *worm* Stuxnet. Considerado a primeira “arma cibernética da história”, o Stuxnet foi desenvolvido para controlar as centrífugas de enriquecimento de urânio iranianas e é considerado o primeiro *worm* que espiona e reprograma sistemas industriais. Realistas, integrantes da Escola Inglesa ou Neoliberais das RI poderiam dar conta de um fato desses? A anarquia do sistema é referência importante dentro dessas teorias e, como já citado, pode dar conta de parte do contexto atual. Mas, como falar em fronteiras e territórios nessa *topologia* do espaço virtual?

Se as RI sempre se centraram na questão da territorialidade e da função do Estado em manter as tradicionais fronteiras de mar, terra e ar, o ciberespaço traz um novo desafio a uma geopolítica clássica. Enquanto para alguns pensadores há a necessidade de uma demarcação de fronteiras para um mundo virtual que pode transbordar suas potências para o mundo real, gerando fatos políticos e até militares, para outros é preciso atentar-se para o fato do aspecto público do ciberespaço, não sendo um local que possa ser dominado pelo Estado sem o risco desse infringir direitos como o de privacidade e o de sigilo das correspondências. A possibilidade de uma *geocibernética* ainda é questão importante e indefinida.

Mesmo que a regulação desse novo espaço tenha se mostrado ainda tímida, o espaço cibernético encontra-se em crescente protagonismo. Vem se fortalecendo, então, o conceito de Guerra Centrada em Redes – *Network-Centric Warfare* –, que compreende o uso extensivo das redes de informação, elevando o ciberespaço como um novo teatro de operações.

Na segunda parte, intitulada “Oportunidades e Desafios Empíricos”, encontramos discussões centradas em acontecimentos atuais e muito importantes.

A Revolução nos Assuntos Militares (RAM), desde os anos de 1980, trouxeram transformações nas operações militares e na simbologia que permeia os conflitos atuais. Tidas como “limpas”, “precisas”, “cirúrgicas”, as ações militares atuais ganharam um *status* asséptico, contrapondo-se às ações de guerras tradicionais. Nessa transformação, as imagens introjetadas, por gerações passadas, da guerra como longas campanhas militares e com muitas baixas – imagem típica da “Síndrome do Vietnã” – tende a se dissolver em um símbolo novo de uma guerra enxuta em que passa a ser

tolerável o uso cirúrgico da violência: a banalização da violência em conflitos vistos como *tragedy-free*. Essa busca por maior eficiência dos ataques requer uma gestão precisa de informações, bem como um domínio do espaço cibernético. A eliminação da *fricção* consequente dessa eficiência, com a justificativa da crescente racionalização da guerra, não deixa o conflito mais humano. Ela desvincula os combatentes das ações diretas, enfraquecendo os conflitos morais, banalizando o ato de matar e naturalizando a condição da guerra ante a sociedade.

Outro fato atual importante é a insegurança cibernética. Ela pode ser mitigada por cooperações entre os países. Uma cultura de Segurança Cibernética, por exemplo, poderia ser alcançada através de constantes trocas de informação entre os membros da esfera cibernética das Américas. Como poderá ser visto nas argumentações dos autores, a OEA pode liderar uma cooperação entre os seus membros, bem como estimular trocas entre o setor público, a sociedade civil e os governos americanos. A Argentina vem investindo no reforço da sua Segurança da Informação e na Defesa Cibernética do país. O Brasil ainda precisa dar passos mais ousados nesse sentido, como também outros países da região. A força das potências cibernéticas, como é o caso da China, é mais que um aviso para que os países busquem traçar estratégias acertadas sobre a sua Segurança e Defesa Cibernética.

A terceira e última parte do livro, “Oportunidades e Desafios Metodológicos”, conta com um interessante glossário de termos das CiberRI e uma importante lista bibliográfica de artigos e livros acerca do tema.

“Relações Internacionais Cibernéticas” trata da temática de forma precisa e vasta, e deixa ecoar uma questão: um Estado, necessitando fortalecer sua Defesa e Estratégia no mundo atual, pode acessar informações sigilosas de seus cidadãos (assim como manipular dados públicos no ciberespaço)? Ou essa *ética da convicção* (*sensu* Weber) deve render-se a uma *ética da responsabilidade* (*idem*) para que Estados e órgãos intergovernamentais não se tornem *ciberleviatãs*?

REFERÊNCIAS

Bull, Hedley. 1977. *The anarchical society: a study of order in world politics*. New York: Columbia University Press.

Oliveira, Marcos Aurélio Guedes de; GAMA NETO, Ricardo Borges; LOPES, Gills Vilar. 2016. *Relações internacionais cibernéticas (CiberRI): oportunidades e desafios para os estudos estratégicos e de segurança internacional*. Recife: Ed. da UFPE. (Coleção Defesa e Fronteiras Virtuais; 3).

Weber, Max. 2002. *Ensaio de Sociologia*. Rio de Janeiro: LTC.

Wendt, Alexander. 1999. *Social theory of international politics*. Cambridge, UK: Cambridge University Press.

NOTAS

1. Como diz a famosa artista Laurie Anderson em sua canção “Only an expert”.
2. Cf. Bull 1977; Wendt 1999.