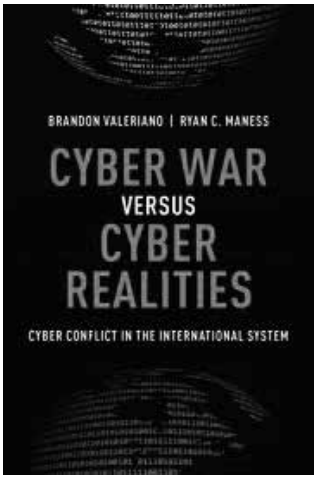
E depois do hype?
Uma abordagem sobre as reais implicações do ciberespaço para as questões de segurança

Tiago Pedro Vales

RYAN C. MANESS
E BRANDON VALERIANO
Cyber War versus Cyber Realities

Oxford,
Oxford University Press,
2015, 288 páginas



O advento da internet, do ciberespaço e da popularização das tecnologias da informação tem suscitado importantes discussões sobre a emergência de ameaças a diversos objetos de referência, ou seja, a elementos caros à existência ou ao bom funcionamento das atividades sociais e estilos de vida. O conjunto dos argumentos e estudos sobre os potenciais e as limitações dos atores no ciberespaço não contribuem, necessariamente, a uma melhor definição desses agentes. O que se tem, a partir de então, é uma espécie de *cyberhype*, que tende a exagerar certas visões, principalmente quanto à gravidade e implicações das chamadas novas ameaças que o ciberespaço seria capaz de impor ao sistema internacional. É neste sentido que vem o contributo de Brandon Valeriano e Ryan Maness ao propor uma investigação rigorosa sobre as ameaças do ciberespaço, ou, como chamam, *cyberthreats*. Ancorados em uma visão construtivista da segurança e olhando exemplos atuais de conflitos envolvendo o ciberespaço, os autores buscam delimitar qual o alcance das ameaças, bem como agentes e as respostas que a eles têm sido sugeridas. O argumento central evoca um constrangimento do impacto que o ciberespaço significaria para as relações internacionais. Ao contrário do que vem sido veiculado por meios de comunicação, por estudos acadêmicos, por integrantes de setores ligados à segurança e até mesmo pelas sugestões levantadas por chefes de Estado e organizações internacionais, as *cyberthreats* têm sido relativamente moderadas, com alcance restrito e episódico.

Os autores apresentam os temas de maneira suficientemente clara e simples. Enquanto tratam das implicações políticas do ciberespaço e das ameaças, abordam

 https://doi.org/10.23906/ri2017.54r02

de forma bastante didática alguns termos técnicos próprios das ciências tecnológicas. O resultado é um trabalho bastante completo em termos de análises políticas e inclusivo o suficiente para que os leitores leigos na área tecnológica possam compreender. Essa facilidade na abordagem dos temas venha, talvez, da familiaridade dos autores com temas envolvendo a segurança cibernética. Valeriano e Maness, professores doutores ligados à universidade de Cardiff e Illinois, respetivamente, possuem uma vasta bibliografia voltada para as questões de conflitos, guerra e políticas para o ciberespaço e suas implicações para as relações internacionais.

DELIMITANDO OS CONCEITOS E DEFININDO OS AGENTES

A discussão inicial do livro passa pelo processo de construção das ameaças à segurança em torno do ciberespaço. Adotando uma postura crítica sob as lentes do construtivismo, Valeriano e Maness discutem a ascensão do ciberespaço como uma nova arena de conflito no sistema internacional. Considerando que as atuações no ciberespaço ou mesmo as políticas voltadas para este ambiente podem tornar-se instrumentalizáveis, portanto, sendo transformadas em uma ferramenta de política externa, governos mundo afora podem tratar agressões no ciberespaço como passíveis de respostas no mundo físico. Neste sentido, conflitos virtuais podem escalar para ações reais. Contudo, como os autores objetivam mostrar, embora exista esse entendimento, inclusive amparado por atos jurídicos, as observações empíricas demonstram o contrário. Países podem até sofrer ações cibernéticas, mas não parecem estar dispostos a retaliar, ao menos abertamente, tanto nas formas físicas quanto cibernéticas[1].

A questão do peso dos atores estatais e a ascensão de atores não estatais tem sido uma discussão constante nos estudos das interações no ciberespaço. Valeriano e Maness apontam para uma direção que não faz coro com o entendimento comum. A ideia de que o ambiente do ciberespaço, anárquico, aberto a inovações permite que atores não estatais concorram com atores estatais de maneira mais equilibrada é contestada. Segundo os autores, as capacidades de ataque e defesa no ciberespaço refletem as capacidades de articulação de recursos e conhecimento técnico, o que é muito mais provável dentro da esfera estatal do que em organizações com limitados recursos ou indivíduos, por mais habilidosos que sejam. Ainda considerando a capacidade dos estados em desenvolverem armas ou defesas cibernéticas, os resultados das investigações empíricas em casos emblemáticos como os ciberataques à Estônia em 2007, ou o vírus *Stuxnet* em 2011, apontam para o Estado como grande articulador desses empreendimentos, embora contem com o apoio de indivíduos e grupos especializados no cumprimento de determinadas tarefas.

DINÂMICAS DE PODER E A INFLUÊNCIA DO CONTEXTO REGIONAL

O grande e exagerado destaque que se tem dado às questões do ciberespaço pelos *media* entre outros agentes tem resultado em uma quase banalização dos termos ou do prefixo «*cyber*». Apesar do fácil entendimento que

o prefixo remete, ou seja, simplificadamente a interações em ambiente virtual, um trabalho de investigação requer uma definição mais pormenorizada. Neste sentido, Valeriano e Maness partem não só para a definição mais precisa do objeto de estudo, mas também, ao fazê-lo, oferecem uma completa revisão de literatura acerca do ciberespaço e especificidades, ataques, conflitos, guerra, espionagem, armas (pp. 28-33). O que chama a atenção é a reflexão sobre o poder no ciberespaço. O contributo dos autores nesta questão é uma discussão que vai para além da difusão do poder e parte para como se configura o poder do Estado no ciberespaço. Essas abordagens são completadas por uma interessante discussão sobre o papel da teoria na abordagem dos conflitos no ciberespaço que se estende a aspetos como a dissuasão e contenção, conceitos fundamentais para o desenvolvimento do argumento central (p. 54).

O regionalismo não só está presente como explica várias motivações para os conflitos e ataques no ciberespaço. Analisando uma série de incidentes cibernéticos, os autores percebem que as dinâmicas regionais onde há certa animosidade nas relações diplomáticas entre países são traduzidas em hostilidades virtuais, ainda que não levem a consequências mais graves. Este é o caso, por exemplo, da Rússia e ex-repúblicas soviéticas, sendo os casos mais significativos os da Estônia e o da Georgia, Índia e Paquistão, China e Taiwan, China e Japão, entre outros (p. 120). Para além das demonstrações de força e poder, o contexto histórico das relações políticas entre os países é um elemento relevante para as análises sobre os conflitos no ciberespaço. Por fim, novamente, os autores atentam para uma reação e atenção exagerada dos *media*, mesmo porque os resultados esperados pelos autores dos ataques não são necessariamente atingidos (p. 163).

Por fim, Valeriano e Maness abordam o grande desafio da regulamentação das atividades no ciberespaço. Baseados em suas observações, os autores ousam propor algumas diretrizes a serem consideradas para a aplicação de um futuro sistema internacional de normas para o ciberespaço.

O mais interessante, talvez, seja uma conclusão que soa como uma provocação teórica. Os autores entendem que o ciberespaço está situado entre dois marcos teóricos, ou seja, é algo mais do que um mero poder suave, mas por hora, não representa um domínio do poder duro. Definitivamente, o livro é um trabalho de investigação relevante para o campo das relações internacionais e estudos de segurança. R:I

NOTA

[1] De fato, há várias diretivas ou recomendações com o objetivo de endereçar ou servir de base para futuras regulamentações sobre o comportamento dos estados perante as hostilidades provenientes do ciberespaço. Entre vários documentos estão as estratégias de ciber-segurança dos países, tendo vários já formulado suas diretivas. Num âmbito internacional, o *Tallinn Manual on the International Law Applicable to Cyberwarfare*, parece ser o documento mais relevante. Embora não seja adotado como norma jurídica, tem sido uma iniciativa para tratar as questões de ciberguerra como campo do direito internacional.