CONJUNTURA INTERNACIONAL
76 ▪ Conjuntura Internacional ▪ Belo Horizonte,
ISSN 1809-6182, v.15 n.2, p.76 - 78, ago. 2018

Resenha

Cybersecurity: geopolitics, law and policy

Friedrich Maier[34]

DOI: 10.5752/P.1809-6182.2018v15.n2.p76

Recebido em: 21 de maio de 2018
Aprovado em: 08 de junho de 2018

A cibersegurança desponta como um novo tema de pesquisa dentro da disciplina de Relações Internacionais (RRII). Questões como o impacto das tecnologias de informação e comunicação (TICs) na agenda diplomática, a soberania digital, ataques cibernéticos e sua possibilidade como arma estratégica, a espionagem industrial e outras, reverberam em artigos e textos que pretendem mirá-las desde uma perspectiva internacional. Todavia, nota-se a falta de um substrato teórico adequado para lidar com os problemas cibernéticos, que a despeito das recentes tentativas de securitização desse novíssimo ambiente, parecem desafiar o padrão estadocêntrico da disciplina, cujo peso da tradição anglo-saxã – e suas análises *problem solving* – ainda se faz sentir.

Nesse contexto, o livro *Cybersecurity: geopolitics, law and policy*, de Amos N. Guiora, pode ser considerado um bom representante dessa linha de pensamento, pois lida com os problemas cibernéticos focando quase que exclusivamente na perspectiva estatal; seus dez capítulos podem ser divididos em duas partes. A primeira, compreendendo os cinco primeiros, fornece a definição, histórico e desenvolvimento do ciberespaço. Aqui o foco recai em apresentar os principais problemas que emergem desse contexto, a partir do conceito de *ciberterrorismo*, procurando evidenciar a urgência do debate de cibersegurança. Assim, Guiora procura aproximar o leitor dos perigos do ciberespaço uma vez que "o impacto de longo prazo de um ataque cibernético é mais poderoso do que um único ato de terrorismo." (p. 20, tradução nossa).

Já a segunda parte (capítulos de 6 a 10) propõe uma série de questionamentos sobre as medidas necessárias para conter o ciberterrorismo e, além disso, atuar de modo mais eficiente em relação aos ataques cibernéticos, seja na melhoria de defesas, seja na ampliação de capacidade de retaliação. Nesse sentido, a centralidade de cooperação entre Estados, Organizações Internacionais, setor empresarial e população em geral, as dificuldades de atribuição e retaliação contra ataques cibernéticos, e a crescente vulnerabilidade ocasionada pelos recentes desenvolvimentos no campo da tecnologia (a "Internet das Coisas", principalmente) são pontos desenvolvidos pelo autor. Sobre os temas, mesmo quando reconhece que uma efetiva segurança do ciberespaço demanda altos níveis de cooperação, Guiora preconiza o melhoramento nas legislações regulatórias, o aperfeiçoamento nos padrões de aplicação da lei e a dissuasão como peças-chave – mecanismos

3. Graduado em Relações Internacionais pela UNESP-FFC- Marília. Mestrando em Ciências Sociais pela mesma instituição. ORCID: https://orcid.org/0000-0003-2695-4905

4. "the long-term impact of a cyber attack is more powerful than a single act of terrorism."

estadocêntricos. A argumentação nesse momento tem por base o entendimento de que o combate ao terrorismo tem muito a ensinar sobre o combate ao ciberterrorismo.

Mais especificamente sobre a questão da cooperação, apontamos a relevância dos vários relatos de conversas que o autor teve com representantes do setor empresarial. Guiora aponta uma grande desconsideração da cibersegurança por parte do setor privado, uma vez que medidas como o treinamento de pessoal, a implementação de *firewalls* mais sofisticados e padrões de resposta a ataques de vazamento de dados são medidas custosas que desafiam a visão orientada ao lucro dos executivos. Para dificultar o problema, ainda há grande receio na comunicação de vazamentos e invasões cibernéticas por parte das corporações, principalmente pelos impactos negativos na imagem e na carteira de clientes que podem gerar.

Mas são nas relações internacionais – ou geopolíticas, como afirma o autor – que vemos propostas e afirmações mais contundentes. Em realidade, podemos ler o texto aproximando-o muito de um "receituário oficial" do governo dos Estados Unidos da América sobre o ciberespaço. Um exemplo é o esforço intelectual do autor para corroborar o "alargamento" do artigo 51 da Carta das Nações Unidas no caso da cibersegurança. Guiora afirma explicitamente que sob "informações de inteligência viáveis, relevantes, corroboradas e confiáveis" (p. 58, tradução nossa[3]) uma nação tem o *direito* de um *ataque preventivo* para evitar a concretização de um ataque cibernético.

A lógica por detrás do argumento retoma os avisos da primeira parte: ataques cibernéticos podem causar tanto ou mais danos que ataques terroristas e, sendo assim, o ataque preventivo, implicitamente reconhecido como direito neste último, aplica-se também ao primeiro ponto. Não há discussão sobre as controvérsias e entendimentos divergentes gerados pela "ampliação" do direito de autodefesa.

Compreendo que Guiora tem por objetivo central em seu livro avançar, retoricamente, um entendimento que vem se expandindo dentro dessa problemática: os papeis da dissuasão e da regulação como elementos de securitização do ciberespaço. As rápidas menções às especificidades desse ambiente, aos diversos mecanismos de triangulação de navegação e à dificuldade de especificar as origens dos ataques não dirimem o mantra: o ciberespaço é um ambiente *crescentemente perigoso* e precisa ser securitizado.

Fica como questionamento se todo o construto teórico não tem como um dos objetivos fornecer substrato para uma conclusão que incomodaria o analista internacional um pouco mais crítico:

> A combinação de capacidades ofensivas-defensivas, no contexto do princípio da proporcionalidade do direito internacional, sugere que **atacar o sistema de computadores de um Estado-nação é uma forma legítima de autodefesa**, se o alvo representar **uma ameaça vi**ável. [...] Em relação ao Irã, a introdução de um vírus de computador reflete a proporcionalidade se a medida de autodefesa estiver contida em uma indústria nuclear que pode ser usada para fins ofensivos e agressivos. (GUIORA, 2017, p. 50, negrito e tradução nossa[4])

Ou seja, diante de uma "ameaça viável" Guiora propõe a razoabilidade de ataque em infraestruturas computacionais de outro Estado-nação. O vírus *Stuxnet* que atacou a usina nuclear iraniana de Natanz fica, assim, justificado. Esse ataque cibernético – o primeiro a apresentar *impactos físicos, materiais* – pas-

3. "viable, time relevant, corroborated, and reliable intelligence information"

4. "The combination of offensive-defensive capabilities, in the context of the international law principle of proportionality, suggest that attacking a nation-state's computer system is a legitimate form of selfdefense, if the target poses a viable threat. [...] Regarding Iran, introducing a computer virus reflects proportionality if the self-defense measure is contained to a nuclear industry that can be used for offensive and aggressive purposes."

sa, dentro do livro, de "ato de guerra" (como muitos teóricos de RRII consideram) para "forma legítima de autodefesa". Claramente uma classificação muito mais propícia aos interesses estadunidenses.

Em síntese, as problemáticas levantadas por Guiora não são totalmente satisfeitas nas atuais configurações do direito internacional, nem na retórica dissuasória – como o autor propõe ao longo de seu trabalho. Enquanto novos entendimentos em organismos multilaterais podem levar o primeiro a dimensionar e regular melhor o ciberespaço, o segundo esbarra numa compreensão limitada da complexidade do mundo cibernético: um ambiente no qual a atribuição de um ataque, além de dificultada por recursos de triangulação, é também turvada pelo recente padrão de operação de *hackers financiados por Estados* (*proxies*). Sendo assim, preconizar um direito de autodefesa preventivo contra ou com ataques cibernéticos é o mesmo que abrir uma caixa de Pandora na política internacional.

Referências

GUIORA, A. N. **Cybersecurity: geopolitics, law and policy**. Boca Raton, FL: Routledge, ISBN: 978-1-315-37023-1, 2017, 170p.