DOI: 10.5433/2176-6665.2019v24n1p380

SEGAL, A. M. **The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age**. New York: PublicAffairs, 2016, ISBN: 9781610394161, 322f.

Friedrich Maier[1]

O livro em tela fornece ao leitor interessado na conexão entre as temáticas de relações internacionais e os impactos gerados pelas tecnologias de informação e comunicação (TICs) – principalmente, pelo ambiente por elas criado, o ciberespaço – uma grande revisão por meio de uma narrativa agradável, pautada em ampla base factual. O argumento central de Segal ao longo dos nove capítulos é apontar como o ciberespaço é utilizado, crescentemente, enquanto elemento de estadismo (*statecraft*), associando-se, dessa forma, às visões corriqueiras das relações internacionais em termos de poder – agora, em termos de ciberpoder.

O capítulo inicial apresenta a hipótese central do autor: os acontecimentos concentrados no período que vai de junho de 2012 até junho de 2013 marcaram um "Ano Zero" para a cibersegurança, isto é, marcaram a ampliação das discussões midiáticas e governamentais sobre o tema. Em junho de 2012, uma extensa reportagem de David Sanger ao jornal *The New York Times* revelaria as origens do Stuxnet, o vírus de computador que danificou centrífugas nucleares na usina de Natanz, no Irã. Exatamente um ano depois, em junho de 2013, as revelações do caso Snowden, o maior vazamento de informações da comunidade de Inteligência na história dos EUA, abalaram relações diplomáticas e trouxeram o ciberespaço e o controle da internet para o centro do debate.

Desses dois marcos, o primeiro por apresentar um ponto de inflexão nas "armas cibernéticas" (pela primeira vez um vírus de

1 Mestrando no Programa de Pós-Graduação da Faculdade de Filosofia e Ciências de Marília da Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP, Marília, SP, Brasil). ORCID: https://orcid.org/0000-0003-2695-905.

Submetido em 19/07/2018; aprovado em 25/01/2019.

computador causou danos físicos, materiais) e o segundo por explicitar o altíssimo nível da espionagem estatal, Segal extrai conclusões valiosas para compreender como o poder pode ser exercido no novíssimo ambiente. Tais conclusões compõem o segundo capítulo, focado em discernir as características básicas de uma "potência cibernética": "economias grandes ou tecnologicamente avançadas; instituições públicas que canalizam a energia e a inovação do setor privado; agências militares e de inteligência aventureiras e um tanto vorazes; e uma história atraente para contar sobre o ciberespaço."[2] (p. 34).

Observamos, nesse momento, uma reposição da argumentação de cariz realista. A definição de uma "potência cibernética" rememora a longa tradição de debate estadocêntrico da disciplina de Relações Internacionais. Se em 1948, em *A política entre as nações*, Morgenthau apontava fatores como população, extensão territorial e nível industrial, na definição dos atores com maior possibilidade de intervenção na arena internacional, Segal reformula essas características, adequando-as ao ciberespaço. Com isso, o autor perfaz uma ponderação dos principais pontos de destaque nas estratégias para o ciberespaço de Estados Unidos da América e China – as duas "potências cibernéticas" atuais. Há também um panorama sobre a Rússia, um concorrente a cada dia mais "ameaçador".

Definidas em linhas gerais as formas de atuação dos três Estados dentro do ciberespaço, o próximo capítulo (terceiro) assume um caráter informativo. Aqui compilam-se uma série de ataques cibernéticos, como o *hacking* da empresa de entretenimento *Sony* (2014) e os ataques de negação de serviço lançados contra a Estônia, em 2007, e Geórgia, em 2008, desde origens (endereços de IP) russas, para demonstrar suas especificidades. Dos casos elencados, depreende-se que a atribuição, elemento chave nas teorias de dissuasão, não é tão simples no ciberespaço, uma vez que tanto mecanismos de triangulação de navegação, quanto o uso de "hackers terceirizados" (os *proxies*) dificultam a localização precisa de um ataque, bem como a extensão de seus interesses.

Nesse sentido, o capítulo também discute como, muitas vezes, não se sabe se o ataque vem de um grupo de hackers com fins meramente

2 No original: "large or technologically advanced economies; public institutions that channel the energy and innovation of the private sector; adventurous and somewhat rapacious military and intelligence agencies; and an attractive story to tell about cyberspace."

financeiros, ou se é um ataque cibernético coordenado centralmente por uma autoridade estatal. O panorama é dificultado pelos fatores técnicos por detrás da atribuição. Muitas vezes, a origem de um ataque é descoberta a partir de complexas estruturas de inteligência que não podem ser explicitadas ao público em geral e, principalmente, aos outros competidores.

É justamente sobre a dissuasão e a atual movimentação das potências para garanti-la também no mundo cibernético que o quarto capítulo fornece um panorama das principais ações estatais sobre o assunto. Estados Unidos e China teriam um "embate de excepcionalismos" (Internet livre X Internet soberana) na arena global da Internet, dado o pioneirismo e capacidade inovadora deste e a pujança econômica dessa. Irã, Coreia do Norte e Israel são outros três atores importantes, o primeiro, aliás, talvez seja o país que melhor conhece as redes cibernéticas dentro dos EUA (p. 87).

Esse raciocínio aponta, novamente, para a dificuldade de avançar medidas de retaliação críveis – ponto central para as referidas teorias de dissuasão. Essas, gestadas durante o período da Guerra Fria e principalmente voltadas para o caso das armas nucleares, reposicionavam a antiga percepção do "equilíbrio do poder" – também elemento perene de nossa disciplina – a partir de expressões como "destruição mútua assegurada" ou "guarda-chuva nuclear". O problema do novo ambiente, para além da atribuição, é definir tanto as "linhas vermelhas" para a retaliação, quanto a proporcionalidade dos ataques.

Entretanto, não devemos pensar o ciberespaço como apenas um elemento ofensivo. Aliás, esse não é nem de longe o panorama mais adequado ao novo ambiente. A espionagem, foco do capítulo cinco, é a atividade que de elemento sempre presente na história das relações internacionais eleva-se a ponto crucial para o desenrolar da diplomacia, economia e política no século XXI. A explicação do panorama em que "todos espionam a todos" é claramente um dos pontos altos do livro de Segal, por demonstrar a ubiquidade das tecnologias de espionagem e seu alto valor para o estadismo, *online* ou *off-line* (p. 111-28).

Com grande sagacidade o autor questiona o epíteto atribuído ao governo chinês de "maior espião comercial do mundo" ao contrastá-lo à gigantesca rede de espionagem montada pelos EUA – e em parte revelada por Snowden. Na China os interesses econômicos mobilizam um

mercado de informações comerciais roubadas, obtidas principalmente por grupos de hackers independentes, cujas relações com as empresas estatais e os agentes governamentais são fluídas e nebulosas. Enquanto isso, a comunidade de inteligência dos EUA aproveita-se da liderança no desenvolvimento das novas tecnologias digitais para coletar massivamente bilhões de dados e metadados e, ao mesmo tempo, sabotar equipamentos infraestruturais implantando "portas de entrada" secretas em roteadores, servidores e outros – equipamentos que são enviados para diversos clientes ao redor do globo.

Nesse sentido, dois capítulos complementam esse panorama anônimo, complexo e conflituoso do ciberespaço traçado pelo autor. O sexto capítulo tem por foco as discussões entorno da "soberania dos dados", levantadas pelas revelações Snowden. Comenta-se sobre as movimentações estatais que visam a exercer maior controle de partes das benesses – econômicas e de inteligência – que emergem do ciberespaço. A resposta alemã, de reserva de mercado em setores de informação considerados "cruciais" para a soberania do Estado, é um claro exemplo dessa compreensão (p. 154-7). Multas e restrições crescentes por parte das agências reguladoras europeias contra as empresas gigantes de tecnologia dos EUA também entram no mesmo panorama explicativo. Ao contrário dos discursos apologéticos sobre o ciberespaço, principalmente nos anos de 1980 e 1990, não observamos um desafio do novo ambiente à soberania estatal. Pelo contrário, a tendência é de um reforço do Estado, principalmente a partir de sua adaptação à dinâmica digital.

Em mesmo diapasão, o oitavo capítulo fornece uma compilação interessante das principais respostas de alguns governos às revelações Snowden. Nesse quadro o papel do Brasil é exaltado por Segal. O autor apresenta como o governo brasileiro de então adotou posturas fortes no nível internacional em busca de uma organização da Internet diversa daquela proposta e dominada pelos estadunidenses. Tanto as discussões no âmbito da União Internacional de Telecomunicações (ITU) quanto o Marco Civil da Internet representam pontos interessantes nesse argumento. Todavia, pontua-se a debacle da proposta brasileira justamente no seu ponto de ápice: o encontro do NETmundial (2014) e sua declaração final, que apresentava uma concepção da Internet muito mais próxima da visão e dos interesses estadunidenses do que nas primeiras asserções brasileiras, em 2013. Novamente, Segal dá a entender que apesar

das inovadoras características do ciberespaço, a arena internacional permanece pautada nas asserções da *Realpolitik*.

O capítulo final é um exercício de prognóstico. O autor tenta apontar alguns padrões que poderão emergir a partir do fim do que ele chamade "Pax Digital Americana". A crescente dependência e acomodação das empresas privadas às cada vez mais restritivas regulações estatais, o impacto da computação quântica para a criptografia e a espionagem e o futuro das alianças internacionais que procuram avançar agendas normativas são alguns dos pontos de reflexão do autor nesse momento. As próximas duas décadas serão determinantes nos procedimentos de regulação do ciberespaço que pode pender, tanto para um reforço do unilateralismo, com a fragmentação – ainda maior – da Internet em seções territoriais "soberanas", quanto ao multilateralismo, com a organização de novas formas de "governança da Internet". Sobre o último ponto, as divergências sobre o "tipo de multilateralismo" também afloram: enquanto os EUA defendem-no a partir de "organizações privadas", outros atores, como China e Rússia, apostam numa coordenação governamental.

Enfim, o livro de Segal tem muito a adicionar ao debate de cibersegurança e relações internacionais. Mesmo com a reposição das principais categorias analíticas da tradição de pensamento realista – notadamente, as reflexões sobre "potências cibernéticas" e "poder cibernético" – o livro fornece um amplo conjunto de informações sobre o desenvolvimento dos problemas do ciberespaço e da cibersegurança. A argumentação central, o avanço do estadismo no ciberespaço, principalmente a partir do "Ano Zero" é uma forma interessante de compreender os desdobramentos dessas tecnologias para as relações internacionais. Entretanto, cabe pontuar, essa visão deixa de lado outras nuances do "mundo cyber", como seu padrão compósito e sua intrínseca relação com o Estado – desde o início da Grande Rede e não somente a partir do Ano Zero.