SIMPÓSIO MERCADOS DE PROTEÇÃO E GOVERNANÇA DA SEGURANÇA

UNIVERSIDADE ESTADUAL DE LONDRINA

12 a 14 de junho de 2019

GT1: GOVERNANÇA MULTICÊNTRICA DA SEGURANÇA

Compondo ideais de risco: os mercados de cibersegurança e a produção da (in)segurança cibernética

Luísa Cruz Lobato
Pontifícia Universidade Católica do Rio de Janeiro
Doutoranda

Compondo ideais de risco: os mercados de cibersegurança e a produção da (in)segurança cibernética

Luisa Cruz Lobato[1]

Resumo: Esse artigo explora o papel de companhias privadas na produção da cibersegurança. Parte significativa destes atores está baseada em países ocidentais e seus aliados, a exemplo dos Estados Unidos, União Europeia e Israel, ao passo que mercados pujantes tem se consolidado nos principais países emergentes da Ásia e América Latina. Nesse sentido, atores privados são centrais para o desenvolvimento das tecnologias da informação e da Internet. Partindo desse pressuposto, argumenta-se que os mercados de TICs participam na produção do que se entende como segurança e insegurança na Internet mediante o modo como representam ameaças e riscos em seus anúncios e na comercialização de seus produtos e serviços. Busca-se compreender como essas práticas produzem e reforçam abordagens e entendimentos específicos sobre cibersegurança, bem como quais as implicações da participação do mercado na definição do que é segurança e insegurança online.

Palavras-chave: Cibersegurança. Relações Internacionais. Pierre Bourdieu.

1. Introdução

Esse artigo explora o papel de companhias privadas na produção da cibersegurança. Parte significativa destes atores está baseada em países ocidentais e seus aliados, a exemplo dos Estados Unidos, União Europeia e Israel, ao passo que mercados pujantes tem se consolidado nos principais países emergentes da Ásia e América Latina (NEWSWIRE, 2018). Nesse sentido, atores privados são centrais para o desenvolvimento das tecnologias da informação e da Internet (CASTELLS, 2010). Partindo desse pressuposto, argumenta-se que os mercados de TICs participam na produção do que se entende como segurança e insegurança na Internet mediante o modo como representam ameaças e riscos em seus anúncios e na comercialização de seus produtos e serviços. Busca-se compreender como essas práticas produzem e reforçam abordagens e entendimentos específicos sobre cibersegurança, e suas implicações para a definição do que é (in)segurança online.

Essa discussão permite situar, no campo das Relações Internacionais (R.I) e Estudos de Segurança, as disputas e alianças entre esses atores, atentando para o papel que dinâmicas de mercado desempenham na definição de elementos centrais da agenda de segurança. Isto ocorre, por exemplo, mediante a definição de prioridades e mecanismos de resposta a essas prioridades. Além disso, situar esses

[1] PUC-Rio; Doutoranda; l.cruzlobato@gmail.com.

atores no contexto de disputas com governos, especialistas em segurança, computação, engenheiros, a comunidade hacker e outros, aponta para a maneira complexa com a qual entendimentos e práticas de segurança e governança se constituem e se sobrepõem mediante diversas interações, bem como para o papel concreto desempenhado por companhias que têm na cibersegurança seu principal ativo. Tal análise possibilita, ainda, entender como dinâmicas de insegurança se constituem e se difundem nos campos da política de segurança e das R.I em contextos nos quais, por vezes, torna-se difícil distinguir onde começam e terminam práticas públicas e privadas, o que tem implicações importantes para o desenho de diversas formas de responsabilização.

Este trabalho é estruturado em três partes. Em um primeiro momento, revisita o tratamento dado pelos estudos de segurança nas R.I. aos atores privados e utiliza o conceito de "campo" (BOURDIEU, 2004) para fundamentar o argumento sobre o papel dos mercados na produção da (in)segurança cibernética. Tal participação pode ocorrer mediante o desenvolvimento e (não) uso de parâmetros de segurança, como a criptografia, em softwares, ou mediante a comercialização de produtos e serviços voltados para a proteção e combate a ameaças cibernéticas, o que ocorre no contexto de um campo dinâmico de disputas por recursos e por influenciar nas "regras do jogo". Sugerir a existência de um campo de disputas sobre a cibersegurança fornece uma base analítica consistente para discutir de que forma a competição de mercado molda práticas e entendimentos sobre cibersegurança, bem como quais são os resultados políticos das relações de poder e disputas em torno da definição do que é segurança na sociedade digital.

Em seguida, analisa-se os produtos e serviços anunciados publicamente por empresas do setor de defesa, companhias antivírus e "fornecedores" de vulnerabilidades. Argumenta-se que essas práticas concorrem para diferentes articulações de risco que influenciam o modo como as políticas de segurança são desenvolvidas e aplicadas. Tais articulações sugerem que essas companhias participam ativamente na definição dos riscos a serem priorizados, de como esses riscos são articulados e do tipo de resposta que se dá a eles. Conclui-se com uma reflexão a sobre o papel de arranjos híbridos entre público e privado na constituição de ideais de riscos à segurança.

2. Atores privados e cibersegurança: reflexões a partir de Pierre Bourdieu e dos estudos de segurança nas R.I.

As R.I. proporcionam terreno fértil para o desenvolvimento de debates sobre cibersegurança, em particular no que toca o campo dos estudos de segurança e de defesa na disciplina (DUNN CAVELTY, 2008; HANSEN; NISSENBAUM, 2009). No entanto, um foco inicial na figura do Estado e nas disputas geopolíticas (MCCARTHY, 2015) dificulta a compreensão do papel dos atores privados na constituição da segurança e insegurança no Internet e negligencia a extensão e complexidade dos arranjos públicos-privados que são estabelecidos de modo a tornar possíveis os debates sobre retaliações e defesa ativa, bem como dificultando a distinção das fronteiras entre práticas privadas e públicas.

O estudo dos atores privados na segurança internacional expõe as disputas políticas e complicações advindas do entrelaçamento das práticas de uma gama de atores. Análises do tipo surgem no início dos anos 2000, favorecidas por contestações às bases teóricas da disciplina e por tentativas de expandir seu entendimento sobre poder, segurança e a realidade social (KRAUSE; WILLIAMS, 1997; BOOTH, 2007; BUZAN; HANSEN, 2009), abarcando uma variedade de temas relativos à privatização da segurança e uso da força (AVANT, 2005; ABRAHANSEN; WILLIAMS, 2009); o problema de como companhias privadas militares e de segurança produzem (in)segurança e a contestação da linha que divide público e privado na governança da segurança (BERNDTSSON; STERN, 2011; BIGO, 2013).

A “privatização” da segurança sugere tanto uma mudança de orientação da governança da segurança de atores governamentais para atores mercadológicos (LEANDER, 2010; DUNN CAVELTY, 2016) quanto uma expansão da atuação destes atores no campo da segurança internacional, mediante arranjos ainda mais complexos, que operam de modo relativamente independente, mas não prescindem da autorização do Estado para serem constituídos (BEVIR, 2009). Esse modo de governança se apoia no aprofundamento das políticas neoliberais iniciadas ainda na década de 1970 e que levaram a uma intensa terceirização de funções governamentais para o setor privado (ABRAHANSEM; WILLIAMS, 2009) e à integração de mecanismos de competição e precificação aos serviços públicos, de modo a conferir maior eficiência ao Estado (BEVIR, 2009). Uma atenção às mais

diversas formas de privatização expõe os distintos arranjos políticos entre Estados e atores privados (LEANDER, 2010).

Atores privados desempenham papel central no campo da cibersegurança. Empresas disputam o mercado, a definição da segurança/insegurança cibernética e as estratégias mais adequadas para lidar com inseguranças com agências do governo, especialistas independentes na área de tecnologia da informação e da área de segurança, e a comunidade hacker. Exemplos destas disputas incluem acordos e desacordos acerca de questões como: os tipos de fenômenos que constituem riscos de segurança e sua urgência; gravidade de um problema de segurança; a já legalidade de práticas retaliatórias; a constituição da segurança enquanto valor central à rede; etc.

O campo de cibersegurança é onde disputas simbólicas ocorrem. Bourdieu (2004) retrata o mundo social como um terreno dinâmico de disputas em campos que se entrecruzam, sobrepõem, mas são relativamente autônomos, constituindo-se por uma variedade de atores com interesses próprios. Cada ator em um campo tem sua própria trajetória e dispõe de uma quantidade de capital (econômico, cultural, político, intelectual, técnico, ou de outra natureza) relevante para determinar as condições de acesso ou a posição de um ator no mesmo (BOURDIEU; WACQUANT, 1992).

Nesse campo, os conceitos produzidos por especialistas em políticas públicas e de defesa podem ser influenciados por seu alinhamento político ou pela natureza de quem financia as pesquisas (MEDVETZ, 2012). Governos e atores privados competem para retratar atividades maliciosas de hackers como terrorista ou criminosa ao mesmo tempo em que consideram as atividades de caráter ‘benigno’ valorosas enquanto força de trabalho (LIBICKI et al., 2014). Em muitos casos, há disputa direta por recursos econômicos e recursos públicos se apresentam como particularmente desejáveis para companhias, governos e políticos. O problema da definição, por sua vez, se torna relevante à medida que concepções específicas de cibersegurança tendem a prevalecer sobre as outras, justificando, assim, a alocação de recursos para setores específicos, como agências de segurança nacional ou militares (BRITO; WATKINS, 2011). Notadamente, governos e empresas, ao combinarem conhecimento técnico em TICs e poder econômico, podem dispor de maior habilidade e recursos para desenvolver e reforçar parâmetros e protocolos de segurança, bem como desenvolver ou adquirir tecnologias, como criptografias mais fortes, sistemas e softwares seguros ou explorar vulnerabilidades.

Atores mercadológicos produzem caracterizações de ameaças cibernéticas por meio de anúncios, análises técnicas e estudos veiculados em mídia própria, como blogs, websites, relatórios e revistas. O setor de antivírus utilizou tais veículos para questionar o valor e utilidade desta tecnologia em relação ao desafio das coisas conectadas, sugerindo alternativas focadas na segurança do terminal e outros serviços (DUNN, 2014; MCAFEE, 2015). Ditas práticas possibilitam a expansão do poder relativo destes atores no campo, o que se traduz na busca pela expansão do mercado de cibersegurança, à medida que o "poder" no âmbito do mercado se vê fortemente associado ao número e natureza (governamental, comercial, usuários) de seus clientes e ao lucro gerado com seus produtos e serviços.

Parcerias público-privadas (PPPs) e a terceirização de serviços de segurança são dois arranjos resultantes das dinâmicas do campo da cibersegurança. Justifica-se o recurso às PPPs com base nas especificidades das TICs, ao serem tecnologias predominantemente desenvolvidas e operadas pelo setor privado, e nas demandas que surgem dadas as novas dinâmicas de segurança, quando ciberataques e programas maliciosos entendidos como ameaças à paz e segurança internacionais. As principais alianças resultantes dessas dinâmicas são híbridas, isto é, marcadas por uma dificuldade em se distinguir onde finda o público e inicia o privado (BIGO, 2013; BERNDTSSON; STERN, 2011; CARR, 2016). A segurança de sistemas de computador civis e militares, bem como o desenvolvimento de novas soluções de cibersegurança por parte e para os governos envolvem, por exemplo, serviços delegados ou compartilhados com o setor privado – o que prontamente aponta para o forte viés privatista do campo (DUNN CAVELTY, 2016).

Uma dinâmica que ainda merece destaque é a constituição de um complexo industrial[2] de cibersegurança, que gera padrões de cooperação entre o setor privado e o governo às custas de uma competição aumentada entre empresas por uma parcela do mercado governamental (DEIBERT, 2013; HARRIS, 2014). A cristalização deste tipo de arranjo no campo da cibersegurança se segue à introdução de novos temas de segurança à agenda política de contratantes de defesa e companhias em busca de contratos de pesquisa e desenvolvimento (DEIBERT, 2013; HARRIS, 2014). Tais dinâmicas levam as companhias a adotar estratégias de mercado orientadas a proporcionar maior espaço para a comercialização de seus produtos e serviços.

[2] Complexos industriais são alianças público-privadas de natureza híbrida mediante os quais governos incentivam acordos institucionais com o setor privado.

3. Companhias privadas: os novos-velhos provedores de cibersegurança

O termo “companhias privadas” compreende uma vasta categoria de atores participando do mercado da cibersegurança, o que inclui desde companhias não especializadas em TICs, como bancos, até provedores de Internet e redes sociais. De maneiras distintas, esses atores concorrem para a construção daquilo que se vivencia como segurança e insegurança na rede. Por vezes, isso pode ocorrer de modo direto, a exemplo da participação ativa de empresas e bancos em operações de derrubada de botnets e no desenvolvimento de sistemas seguros para suas operações (SILVA, 2017; BANCO CENTRAL DO BRASIL, 2018), ou mais indireto, como, por exemplo, o modo como mídias sociais são utilizadas em operações de contra-informação (HERRICK, 2016) ou servem de proxy para o roubo de dados pessoais e para a condução de ciberataques, graças vulnerabilidades existentes nessas plataformas (JABEE; ALAM, 2016). Há, ainda, uma categoria distinta de empresas que anunciam e comercializam produtos e serviços voltados para a proteção e análise de risco contra softwares maliciosos, intrusões de terceiros e ciberataques. A fim de prover uma análise mais consistente, categoriza-se essas companhias em três grupos:

(1) Empresas de antivírus ou proteção de terminais, cujo foco é no desenvolvimento de softwares para detectar, bloquear e eliminar malwares, também se engajando em pesquisa e análise de ameaças. Seu público alvo inclui usuários, empresas de diversos tamanhos e governos;
(2) Fornecedores de vulnerabilidades, compreendendo companhias que lucram com a comercialização de vulnerabilidades não corrigidas para softwares e sistemas ou mecanismos para explorá-las;
(3) Contratantes de defesa, um grupo caracterizado pela parceria tradicional com agências de segurança e inteligência para fins de segurança nacional. Esse grupo passou a se envolver no mercado para a guerra cibernética e tecnologias de vigilância.

Apesar de não ser exaustiva, a divisão acima sugere que as soluções e estratégias desenvolvidas para lidar com problemas de cibersegurança variam no mercado, assim como seus efeitos. Por vezes, a relação entre governos ou mercados pode conduzir a práticas que violam direitos e contribuem para a crescente insegurança na Internet.

O desenvolvimento de mercados de cibersegurança é profundamente influenciado pelas atividades de grupo restrito de países e companhias privadas baseadas nos Estados Unidos, Israel e Reino Unido, hoje os países que mais investem em cibersegurança no mundo (CYBER SECURITY VENTURES, 2019). No caso dos EUA, isto se deve, dentre outros fatores, à sua centralidade no desenvolvimento das TICs e à sua vanguarda nos esforços de securitização do espaço cibernético (DUNN CAVELTY, 2008). Além disso, o país ainda concentra grande parte das companhias de tecnologia mais poderosas do mundo e serve de *hub* para inúmeras outras companhias estrangeiras.

Tal dominância não impede que a cibersegurança seja um campo dinâmico, no qual práticas e disputas entre atores relevantes frequentemente extrapolam fronteiras nacionais e substancialmente afetam as dinâmicas e termos do debate sobre cibersegurança em outros países. Exemplo disso é o caso brasileiro, onde movimentos legislativos e políticos se seguiram às revelações feitas por Edward Snowden acerca do programa de espionagem dos EUA, no ano de 2013, culminando na aprovação do Marco Civil da Internet, que tramitava no Congresso Nacional desde 2009, e no encontro NETMundial, além da instauração de uma Comissão Parlamentar de Inquérito para investigar denúncias de espionagem pelos EUA, e da apresentação junto à ONU, de uma proposta de resolução sobre privacidade na era digital. O debate nacional sobre defesa cibernética também acompanha de perto preocupações do ocidente, com a ciberguerra (DUNN CAVELTY, 2012) e o ciberterrorismo (Dziundziuk, 2018).

A seguir, analisa-se os produtos e serviços anunciados publicamente por algumas das principais empresas do setor de defesa, companhias antivírus e “fornecedores” de vulnerabilidades atuando no campo da cibersegurança. O rol de empresas selecionadas não exaure a variedade de empresas atuando no setor, tampouco pretende dar conta da miríade de práticas e modos de compor o que hoje se tem por cibersegurança. O objetivo é mostrar que as práticas analisadas concorrem para diferentes articulações de risco que, por sua vez, influenciam substancialmente o modo como as políticas de segurança são desenvolvidas e aplicadas - algumas vezes, extrapolando as fronteiras do "setor cibernético". Tais articulações sugerem que essas companhias participam ativamente na definição dos riscos a serem priorizados, de como esses riscos são articulados e da resposta que se dá a eles.

Empresas de antivírus / proteção de terminais

A indústria de antivírus surge em paralelo às redes de computadores. O foco do setor é no desenvolvimento de softwares para prevenir, detectar e remover programas malignos de computadores, com o suporte de pesquisas voltadas para a descoberta e análise de ameaças cibernéticas e tendências de segurança. A crescente sofisticação dessas ameaças tem levado a indústria a se "reinventar" a partir de uma maior atenção aos riscos de se estar conectado, que envolvem ameaças que vão desde o roubo de identidades até a exploração de vulnerabilidades e a difusão de *ransomware* em redes. (YADRON, 2014; MCAFEE, 2015).

As plataformas de proteção terminais compreendem uma variedade de modelos de proteção: detecção baseada em assinaturas; direcionada a usuários corporativos, domésticos ou governamentais (KASPERSKY, s.d; MCAFEE, s.d; SYMANTEC, s.d) e oferta de serviços de gestão de risco (AVIRA, s.d; BITDEFENDER, s.d). A maioria desses modelos utiliza uma abordagem defensiva para proteger dispositivos, redes e atividades online, como análises heurísticas e comportamentais, proteção contra vulnerabilidades e plataformas de gestão de risco básicas, que incluem conceitos como defesa fortificada, cujo objetivo é reduzir as chances de acesso não autorizado, e defesa resiliente, buscando assegurar o funcionamento ininterrupto de infraestruturas e serviços críticos, além de aumentar a capacidade de um sistema de se recuperar de ataques. O foco principal é reforçar o sistema e a infraestrutura do terminal de modo a reduzir os riscos de intrusões. Devido à ação ser condicionada à descoberta da ameaça, a segurança defensiva é, por natureza, responsiva (ROSENQUIST, 2013).

A indústria de antivírus tem abraçado as estratégias discursivas utilizadas por círculos da segurança e defesa, que enfatizam o risco de exploração de vulnerabilidades e a possibilidade de perda, roubo ou interrupção de informações (SYMANTEC, s.d; KASPERSKY, s.d). Para responder a estes riscos, uma parcela da indústria tem, lentamente, voltado a atenção para serviços voltados à identificação, compreensão e/ou mitigação de riscos, não apenas para parar ataques em curso, mas também para evitar que aconteçam. Mas à medida que essa abordagem "preventiva" se populariza no campo, ela alimenta a expansão do mercado para além da indústria de antivírus, com novas companhias sendo criadas e com contratantes de defesa se voltando cada vez mais para esse mercado (DEIBERT, 2013; HARRIS, 2014).

Fornecedores de vulnerabilidades

Esta categoria se aplica às companhias envolvidas no controverso mercado para vulnerabilidades "zero-dia".[3] Devido ao uso dessas vulnerabilidades para fins ofensivos e de vigilância, este é um mercado que, a princípio, apresenta-se como restrito a governos e a programas de recompensas financiados por empresas do setor de tecnologia. Fornecedores de vulnerabilidades se distinguem de pesquisadores que as reportam para esses programas por buscarem lucro com o desenvolvimento de ferramentas para explorar as vulnerabilidades (um tipo de programa malicioso denominado "*exploit*"). O sigilo é valioso para esta parte do mercado, à medida que um exploit somente poderá ser desenvolvido se a vulnerabilidade em questão não houver sido corrigida ou já explorada por terceiros.

Detalhes acerca das atividades de companhias neste mercado se tornaram públicos com o vazamento de dados da companhia italiana Hacking Team. A empresa publicamente anuncia um modelo ofensivo de cibersegurança, o que compreende o uso de programas maliciosos e vulnerabilidades zero-dia para organizações encarregados da aplicação da lei e responsáveis pela segurança nacional (HERN, 2015; HACKING TEAM, s.d), e fornece ferramentas para governos combaterem atividades criminosas e terroristas. Muito embora a companhia alegue não comercializar com atores não-governamentais e governos na "lista negra" de diversas organizações internacionais, pesquisas de segurança, além de documentos sigilosos vazados, sugerem o contrário (HERN, 2015). Um "backdoor"[4] foi utilizado para vigiar um jornalista marroquino (CITIZEN LAB, 2012) enquanto bases de dados dos EUA foram utilizadas como partes de atividades de espionagem, ancoradas na ferramenta de controle remoto da companhia (MARCZAK et al., 2014).

Outras companhias proeminentes no mercado são a Endgame e a Zerodium. O envolvimento da Endgame no mercado de zero-dias lhe rendeu o título de "Blackwater do hackeamento", em referência à companhia militar privada Blackwater e seu controverso envolvimento na guerra do Iraque. A companhia passou por uma reformulação de seu modelo de negócios e atualmente atende ambos os mercados comercial e governamental, oferecendo soluções de big data e um programa de

[3] Uma falha em um software, geralmente desconhecida pelo programador ou companhia responsável por seu desenvolvimento.
[4] Falhas ou brechas mediante as quais um sistema pode ser explorado por terceiros.

inteligência que analisa a informação do sistema do cliente, comparando-a com a pesquisa da companhia sobre programas maliciosos (GREENBERG, 2014).

O CEO e pesquisador-chefe da Zerodium, por sua vez, chegou a afirmar que a parceria entre agências de inteligência e fornecedores de vulnerabilidades seria senso comum (BEKRAR *apud* SCHWARTZ, 2013). Atualmente, o modelo de negócios da companhia consiste na aquisição e revenda de vulnerabilidades zero-dia para clientes do governo e do mercado. A mesma chegou a oferecer cerca de um milhão de dólares por um exploit para iOS (NEWMAN, 2016).

Mais recentemente, a israelense NSO Group, conhecida por fornecer softwares espiões para governos, ganhou notoriedade com a publicação de uma série de relatórios, pelo Citizen Lab, indicando o uso de "exploits" e de sua ferramenta "Pegasus", por governos, para espionar ativistas e dissidentes políticos (MARCZAK et al., 2018). O spyware comercializado pela empresa possibilita a escuta de chamadas, o registro das teclas digitadas, a leitura de mensagens e o rastreamento do histórico da Internet em um telefone-alvo, além do uso remoto do microfone e a câmera de um aparelho celular. Em diferentes ocasiões, serviços e produtos da companhia foram utilizados para perseguição direcionada de dissidência política em pelo menos quarenta e cinco países (MARCZAK et al., 2018). A empresa afirma possuir autorização de agências do governo para comercializar soluções para o combate ao crime e ao terrorismo, sustentando que não opera o sistema que fornece (BBC BRASIL, 2019; NSO GROUP, s.d).

Pressões para tornar o ciberespaço mais seguro contribuíram criaram mercado com opções defensivas e ofensivas para a cibersegurança, guerra cibernética e tecnologias de vigilância (BRITO; WATKINS, 2011). Reformulações como as da Endgame e Zerodium, indicam que parte dos fornecedores de vulnerabilidades têm buscado expandir suas atividades para além do setor governamental. O envolvimento nesse mercado vem acompanhado de uma maior abertura a medidas ofensivas para lidar com ameaças cibernéticas. Ancorado na estratégia militar, esse modelo se caracteriza pela adoção de medidas como a condução de reconhecimento e vigilância, a interceptação de comunicações, a negativa de acesso e recursos, o comprometimento de sistemas e o comprometimento de sua integridade (ROSENQUIST, 2013).

Contratantes de defesa

Contratantes tradicionais do setor de defesa se voltaram para o mercado de cibersegurança em atenção ao seu crescimento exponencial[5] e motivados por restrições no orçamento de defesa do governo dos EUA (MORGAN, 2016). Companhias já estabelecidas no mercado e novas companhias passaram a se envolver no mercado para guerra cibernética e tecnologias de vigilância, o que faz de agências de segurança e inteligência do governo seus principais clientes. Há também evidências de seu envolvimento no mercado de vulnerabilidades, muito embora os detalhes de tal envolvimento sejam pouco claros[6] (BRITO; WATKINS, 2011; DEIBERT, 2013; HARRIS, 2014). Essas companhias reconhecem publicamente a aliança com setores da segurança nacional (LOCKHEED MARTIN, s.d; BOEING, s.d; NORTHROP GRUMMAN, s.d; RAYTHEON, s.d; BOOZ ALLEN HAMILTON, s.d; PALANTIR, s.d) e é bastante comum sua presença em feiras do setor de defesa em diversos países: na edição de 2019 da LAAD Defense and Security era possível encontrar representações de companhias como a Boeing, a Lockheed Martin e a Bae Systems (LOBATO, 2019).

Os serviços oferecidos por essa categoria incluem: proteção à infraestrutura crítica, vigilância, análise de dados, segurança da informação, capacidades operacionais, segurança na nuvem, análise de big data, entre outros. A maior parte delas desenvolveu unidades “ciber”, especializadas em serviços de análise de risco e ameaças, beneficiando-se do intercâmbio de especialistas entre governo e setor privado (HARRIS, 2014; BOOZ ALLEN HAMILTON, s.d), e oferecendo um rico portfólio de soluções ofensivas e defensivas a seus clientes governamentais. O foco dessas soluções tende a ser a coleta de informações para fins de inteligência e para a proteção de máquinas e redes, bem como a investigação de ataques e a adoção de mecanismos punitivos. As companhias também oferecem centros de operações que incluem serviços de treinamento de pessoal, investigação de ameaças, rastreamento e resposta a incidentes. A defesa, no caso destas soluções, não necessariamente se restringe ao ambiente do terminal.

[5] Dados de 2016 apontam que o governo dos EUA investiu cerca de 100 bilhões de dólares no mercado de cibersegurança na última década (Morgan, 2016).

[6] As atividades de empresas contratantes de defesa tendem a ser sigilosas e seu envolvimento no mercado de vulnerabilidades é ainda mais obscuro. Anúncios de empregos, combinados com as descrições das soluções anunciadas, oferecem pistas sobre esse envolvimento. A Raytheon, por exemplo, oferta vagas em sua subsidiária “Blackbird” para analistas de ameaças, especialistas em engenharia reversa e pesquisadores de vulnerabilidades. A companhia é especializada em serviços de vigilância das comunicações para agências de espionagem.

Com soluções que buscam detectar e analisar para prever, o foco é na defesa ativa, um conjunto de medidas para conter intrusões, podendo servir a fins investigativos, defensivos e punitivos. A implementação destas medidas ocorre sem o consentimento de ao menos uma das partes afetadas pela intrusão e podem impactar sistemas de terceiros. Essas táticas incluem desde medidas “benignas” de coleta de informações até medidas mais agressivas que visam inibir/impedir o funcionamento de sistemas remotos (DITTRICH; HIMA, 2015). O conceito foi importado da doutrina militar norte-americana por meio de políticas de compartilhamento de informações e práticas de coordenação de respostas previstas em PPPs e cláusulas de contratos de defesa, processo este também favorecido pela mobilidade de mão-de-obra e ideias entre governos e empresas, o que contribuiu para alinhar suas estratégias de segurança (DEWAR, 2014; HARRIS, 2014).

Assim, além de investirem no campo da cibersegurança, essas companhias também contribuem para promover uma abordagem de segurança que pode adquirir contornos ofensivos. De um modo geral, companhias de cibersegurança já não mais adotam a estratégia de reforçar sistemas e aguardar para bloquear uma ameaça. Grande parte das soluções atualmente disponíveis no mercado incluem pelo menos uma ferramenta básica de gestão de risco. O recente apelo à defesa ativa ilustra o modo como essas companhias produzem noções de segurança por meio de suas práticas.

4. Compondo ideais de risco: defesa ativa como exemplo da contribuição das companhias para a criação de paradigmas na cibersegurança.

A competição e expansão do mercado para a cibersegurança trouxe consigo uma maior variedade de companhias atuando neste mercado e também de soluções para lidar com uma diversidade de problemas de segurança que perpassam e, muitas vezes, extrapolam as fronteiras da vida online. Não somente isso: esse processo também vem acompanhado de uma expansão na fronteira daquilo que é praticado como cibersegurança: para além de assegurar a integridade de um terminal ou um ambiente de sistema específico contra ataques e invasões de terceiros, cibersegurança também passa a significar a antecipação desses e de uma série de outros riscos que têm nos malwares, softwares espiões e vulnerabilidades em sistemas seu meio e principal razão de ser. Em outras palavras, isso significa que falhas no código e métodos desenvolvidos especificamente para explorá-las se

tornam justificativa para a adoção de medidas mais proativas de segurança como, por exemplo, a atuação de equipes de respostas a incidentes ou a automatização de determinadas respostas a incidentes de segurança, e, ao mesmo tempo, produtos atraentes para governos e companhias de cibersegurança. Resultado disto é a crescente confusão e o dinâmico rearranjo da fronteira entre "ameaças cibernéticas" e a vida cotidiana.

Esse processo ocorre devido a uma constante (re)articulação dos elementos que compõem práticas de antecipação, o que ocorre tanto em virtude de disputas entre grupos de atores no campo da cibersegurança quanto motivado por novas percepções e modos de retratar riscos e ameaças, e a uma sobreposição de um conjunto de concepções de risco baseadas em medidas defensivas, ofensivas e de defesa ativa (ver tabela 1).

Tabela 1: Abordagens predominantes entre as companhias de cibersegurança.

Categoria	**Empresa**	**Defensivo**	**Ofensivo**	**Defesa ativa**
Antivírus / proteção de terminal	Avira	Avira Antivirus for Small Business	-	-
	Avast	Avast Business Cybersecurity Solutions	-	-
	Bitdefender	Bitdefender Total Security 2019	-	-
	Kaspersky Labs	Kaspersky Total Security for Businesses	-	Anti-Targeted Attack
				Threat Management & Defense
	McAfee	McAfee Endpoint Security	-	-
	Symantec	Symantec Advanced Threat Protection	-	DeepSight Intelligence
Fornecedores de	Zerodium	-	-	Zero-Day Research Feed

vulnerabilidades	Hacking Team	-	Remote Control System	-
	Endgame	-	-	Endgame Platform
	NSO Group	-	Pegasus[7]	-
Contratantes do setor de defesa	Bae Systems	-	-	National Security and Law Enforcement Solutions
	Boeing	Advanced Malware Assessment	-	TAC - Advanced Analytics
	Booz Allen Hamilton	Attack Surface Reduction	Cyber Warfare solutions	Cyber Fusion Center
				Incident Response
	Lockheed Martin	-	Cyber Electronic Warfare	Intelligence-driven Defense
		-	Henosis	Cyber Crime Center
		-	-	LM Solution
	Northrop Grumman	Security Services (ex: antivírus)	Cyber Mission Platform	Security Services (ex: honeypots, resposta a incidentes)
	Raytheon	Cyber Hardening	-	Proactive and dynamic defense (ex: análise de redes sociais, análise de mídia)
		-	-	Vulnerability Research Ranges
		-	-	UK Cyber Innovation Centre
	Palantir	Palantir Foundry	-	Palantir Gotham

Abordagens defensivas se centram na fortificação contra uma ameaça "externa". Já abordagens predominantemente ofensivas partem de uma concepção

[7] A ferramenta não é anunciada abertamente no site da empresa.

de risco baseada na premissa: "a melhor defesa é um bom ataque" (MEDAIRY, s.d.). Não basta expurgar o vírus ou invasor do sistema; é necessário também "sair" do ambiente do sistema de modo a retaliar ou lançar um primeiro ataque ao sistema do adversário. Assim, abordagens ofensivas pressupõem o uso de ferramentas que visem invadir e mesmo causar danos a outros sistemas, sendo comuns nos setores militar e de defesa.

Mas é na defesa ativa que a antecipação se torna elemento central para a constituição do risco. Na defesa ativa, um número crescente e granular de informações serve de base para se conhecer e, assim, poder agir para se lidar com um problema de segurança. Na prática, ela pressupõe atividades de detecção, identificação, reação e prevenção de ataques por meio de uma série de movimentos sobrepostos e, algumas vezes, pouco coordenados, como medidas para aperfeiçoar técnicas de detecção, coleta de inteligência, o uso de honeypots e DNS falsos, identificação de IP, criação de websites falsos com programas maliciosos embutidos, acesso remoto ao sistema do agressor, entre outros. Inclui, também, métodos diversos de coleta de dados para o melhor conhecimento sobre a ameaça. Dados coletados mediante tais processos alimentam estratégias para prevenir ataques futuros.

A defesa ativa se torna atraente por compreender medidas que incluem, mas não se restringem à possibilidade de retaliar um ataque (DENNING, 2014; DEWAR, 2014). Seu crescimento enquanto opção atraente para lidar com riscos cibernéticos intensificou debates sobre o uso de medidas ofensivas por atores privados e os respectivos requerimentos legais para conduzi-las (STEPTOE, 2012; DENNING, 2014; LOBATO, 2018), um debate que coexiste com a adoção *ad hoc* destas medidas pelas companhias (DITTRICH; HIMA, 2005).

Enquanto paradigma de cibersegurança, a defesa ativa autoriza a adoção de medidas invasivas em nome da antecipação de riscos, servindo como resposta à crescente complexidade dos riscos cibernéticos. Ela também pressupõe o imperativo de se aumentar a superfície de coleta de dados que tornem possível conhecer melhor um problema ainda desconhecido. Mesmo que ciberataques sejam inevitáveis (RAYTHEON, 2017), há uma grande zona cinzenta separando a certeza de que irão ocorrer um dia da incerteza com relação a quando irão ocorrer, quem irá conduzi-los, com que fim e com que meios.

A previsibilidade de um risco depende de se conhecer mais, de modo a se antecipar uma ameaça. Esse modelo de segurança antecipatória invoca diversas formas de controle disponíveis. Exemplos incluem o uso de "segurança por obscuridade", isso é, a confiança de que o sigilo sobre o método de segurança utilizado é eficiente em dificultar, ou mesmo, impedir, um ataque bem-sucedido; o uso de estratégias para ludibriar um possível "agressor", de modo a poder obter dados a seu respeito e a respeito de seu método de ataque; e o aumento da superfície de coleta de dados, aqui consistindo ou em dados sobre um ataque ou ameaça específica ou expandindo-se para incluir mecanismos de coleta de dados sobre pessoas, e.g., práticas de vigilância.

A expertise exigida para a realização desse tipo de atividade também é importante na composição e validação dos panoramas de risco sobre os quais se ancora a defesa ativa. Uma análise das ofertas de emprego por empresas do setor aponta para a complexidade e variedade de competências necessárias para o conhecimento do problema. Essas companhias não somente oferecem oportunidades de carreiras nas áreas de engenharia de software, resposta a incidentes, engenharia reversa de malwares, análise de ameaças, análise de SIGINT (*signals intelligence*) e HUMINT (*human intelligence*), engenharia e análise de operações na nuvem, entre outras, como também uma variada gama de oportunidades de desenvolvimento profissional, como estágios, bolsas de estudo, estruturas acadêmica e de pesquisa, além de exigir/produzir certificados que contribuem para processos de autorização e descentralização da expertise em relação ao campo científico (LEANDER, 2018, LEANDER; WAEVER, 2019).

Enquanto o imperativo de antecipação sobre o qual se ancora a defesa ativa não é novo, as composições de risco que ajudam a constituí-lo são únicas. Elas compreendem o modo como ameaças cibernéticas são compreendidas, p.ex., em termos de sua inevitabilidade e potencial de alcance, da expertise exigida para realizar tarefas que vão desde a análise de ameaças até a capacidade de detectar vulnerabilidades em sistemas - e o modo como essa expertise é autorizada pelo setor privado; e da dificuldade em se estabelecer limites claros entre o que é defesa e o que é agressão online. Isso ocorre principalmente em um cenário onde se percebe a capacidade limitada dos Estados em prover segurança (HOFFMAN; LEVITE, 2017).

Além disso, ao se apoiarem no uso de segurança por obscuridade e envolverem ações de vigilância, muitas companhias passam a operar no limite da legalidade

(DEWAR, 2014; LOBATO, 2018). Essa legalidade possui dois componentes: um é a existência ou inexistência de legislação diretamente proibindo a adoção de medidas mais ofensivas dentro do universo da defesa ativa sem a autorização de governos (p.ex.: *Computer Fraud and Abuse Act*, nos EUA, e lei 12.737/2012, no Brasil). O outro é o modo como se torna difícil avaliar a legalidade das práticas das companhias quando a arquitetura da Internet entra na equação.

O fato de a defesa ativa compreender desde a simples instalação de patches de software para corrigir vulnerabilidades de segurança até tentativas de invadir sistemas para recuperar ativos digitais roubados ou esforços para danificar o sistema de um adversário, torna mais complicado distinguir práticas legais daquelas ilegais. Quando se trata da arquitetura da Internet, um fator complicador é o modo como uma ação direcionada, e.g., vigilância ou intrusão, pode repercutir para além do intuito inicial ou ser utilizada pelos Estados para perseguir seus próprios cidadãos (MARCZAK et al., 2014; 2018). A infraestrutura da Internet pode exacerbar os limites dessas práticas, expondo, para além de um possível alvo, toda uma cadeia de pessoas que com este se relaciona e comunica.

Notadamente, as composições de risco em torno da defesa ativa não podem ser pensadas isoladamente das práticas do setor privado, quer porque se constituem a partir destas, quer porque as práticas de setor privado e setor público frequentemente se confundem. O modelo de subcontratação de especialistas em análise de dados e cibersegurança expõe bem essa confusão: a terceirização de serviços relacionados à cibersegurança para o setor privado é vista como resposta ao problema de falta de mão de obra especializada e conhecimento no governo e imediato reconhecimento da competência de companhias privadas na condução desse tipo de assunto (BHATTACHARYA, 2018).

É por meio de como companhias desenham e concebem seus produtos, como articulam os discursos a seu respeito e como sua mão-de-obra e práticas vêm a se confundir com aquelas dos governos que a defesa ativa efetivamente se realiza. Isso ocorre mais claramente no contexto de um “comércio de armas digitais” (DEIBERT, 2013:348) para o qual a sobreposição e confusão entre abordagens defensiva, ofensiva e de defesa ativa são bastante favoráveis, à medida que expandem o espaço de atuação das companhias, como mediante a requisição de sua expertise para lidar com problemas de segurança complexos, ou mesmo proporcionando um espaço mais amplo para sua atuação no mercado e um espaço reduzido para a atuação de

mecanismos de responsabilização - alguns dos quais permanecem substancialmente anacrônicos diante das relações híbridas entre público e privado.

5. CONSIDERAÇÕES FINAIS

Atores privados têm servido como fornecedores de segurança, além de influentes produtores de (in)segurança em diferentes esferas. Há crescente disputa em torno da legitimidade para adoção de medidas retaliatórias e do incremento nas capacidades de companhias privadas em coletar inteligência para lidar com intrusões nas suas redes e de seus clientes. O papel do setor privado de moldar a cibersegurança mediante a definição de padrões para o comércio de soluções do gênero, se torna fundamental. Entretanto, empresas operam sob uma lógica distinta daquela de governos, particularmente ao atuarem movidas primordialmente por interesses econômicos próprios, alguns dos quais não se ajustam bem à dinâmica dos problemas de segurança. Empresas tendem a compreender e reproduzir segurança com base em uma avaliação permanente e quase nunca em termos de garantias legais.

O mercado que sustenta o comércio de soluções de cibersegurança se alimenta da competição em torno da definição do que ela é. A defesa ativa como resposta a ciberataques é sintomática de uma longa preocupação com a busca por possibilidades para lidar com ameaças futuras em um contexto de informação limitada e insuficiente. Seu apelo para a defesa para além do terminal tem por base uma forma antecipatória de gestão de risco, baseada no uso de incidentes passados como variáveis para predizer futuros incidentes, e se alimenta do discurso sobre catástrofes cibernéticas para justificar a necessidade de se buscar previsões mais precisas e autorizar métodos mais eficazes e amplos de coleta e correlação de dados (AMOORE, 2014).

Políticas de segurança são construídas com base na diferenciação entre o que é seguro e o que consta na zona cinzenta do inseguro (GROS, 2012). O que as abordagens concorrentes identificadas nesse trabalho sugerem é que, para além de uma distinção clara entre ataque e defesa, abordagens que priorizam a defesa ativa se beneficiam da confusão entre ambos para oferecer um cardápio mais completo de soluções que não são apenas adaptáveis ao contexto para o qual se apresentam, como também expandem significativamente o sentido e os limites da cibersegurança, de modo a compreender práticas diversas, tais como a coleta e processamento de

dados para atividades inteligência - não somente a respeito da ameaça; o desenvolvimento de malwares e programas espiões para serem utilizados por agentes policiais e pelo setor de defesa dos países - acompanhado pela pouca ou inexistente preocupação com o modo como serão utilizados por esses clientes; ou mesmo o uso da expertise em cibersegurança e da arquitetura em rede da Internet reforçar essas atividades e/ou operar no limiar da legalidade.

O tipo de poder alocado a esta zona cinzenta onde se realizam as políticas de segurança, bem como as dinâmicas entre os atores que nela operam, requerem maior escrutínio na literatura das Relações Internacionais, particularmente por envolver a concessão de certos poderes a certos atores e a certos arranjos políticos, em cujos questões de legitimidade e responsabilização são bastante problemáticas. Pesquisas futuras devem considerar como essas dinâmicas operam em campos onde a agenda da cibersegurança possui pesos diversos e como contextos locais se comunicam com o aspecto transnacional do tema. À medida que a Internet desafia concepções rígidas de fronteiras políticas, disputas de poder no campo da cibersegurança facilmente se estendem para além delas.

Agradecimentos: FAPERJ.

Referências

ABRAHANSEM, R.; WILLIAMS, M. Security beyond the State: Global security assemblages in international politics. **International Political Sociology**, vol. 3, n. 1, 2009, p. 7-17.

AMOORE, L. Security and the incalculable. **Security Dialogue**, vol. 45, n. 5, 2014, p. 423-439.

AVANT, D. Private security companies. **New Political Economy**, vol. 10, n. 1, 2005, p. 121-131.

AVIRA. Disponível em: https://www.avira.com. Acesso em: 24 abr. 2019.

BANCO CENTRAL DO BRASIL. Risco cibernético e o exercício nacional de simulação de incidente de segurança cibernética. Relatório de Estabilidade Financeira, Outubro de 2018.

BATTACHARYA, A. Exclusive: Philippines to outsource all cyber security. GovInsider, 6 de dezembro de 2018. Disponível em: https://govinsider.asia/digital-gov/exclusive-philippines-to-outsource-all-cyber-security. Acesso em: 24 mai. 2019.

BBC BRASIL. NSO Group, a polêmica empresa israelense que está sendo vinculada a hackeamento do WhatsApp, 15 de maio de 2019. Disponível em: https://www.bbc.com/portuguese/geral-48279595 . Acesso em: 23 mai. 2019.

BERNDTSSON, J.; KINSEY, C. **The Routledge research companion to security outsourcing**. New York: Routledge, 2016.

BERNDTSSON, J.; STERN, M. Private security and the public-private divide: contested lines of distinction and modes of governance in the Stockholm-Arlanda security assemblage. **International Political Sociology**, vol. 5, n. 4, 2011, p. 408-425.

BEVIR, M. **Key concepts in governance**. New York: SAGE, 2009.

BIGO, D. Security: Analysing transnational professionals of (in)security in Europe. In: ADLER-NISSEN, R. (ed.). **Bourdieu in International Relations**: Rethinking key concepts of IR. New York: Routledge, 2013, p. 114-130.

BITDEFENDER. Disponível em: http://www.bitdefender.com. Acesso em: 24 abr. 2019.

BOEING. Disponível em: http://www.boeing.com/defense/cybersecurity-information-management. Acesso em: 26 mar. 2019.

BOOTH, K. **Theory of world security**. Cambridge: Cambridge University Press, 2007.

BOOZ ALLEN HAMILTON. Disponível em: http://www.boozallen.com. Acesso em: 26 abr. 2019.

BOURDIEU, P. **Science of science and reflexivity**. Cambridge: Polity Press, 2004.

BOURDIEU, P.; WACQUANT, L. **Réponses: Pour une anthropologie réflexive**. Paris: Éditions du Seuil, 1992.

BRITO, J.; WATKINS, T. Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. **Harvard National Security Journal**, vol. 3, 2011, p. 39-84.

BUZAN, B.; HANSEN, L. **The evolution of International Security Studies**. Cambridge: Cambridge University Press, 2009.
CASTELLS, M. **The rise of the network society**. Malden: Blackwell, 2010.

CARR, M. Public–private partnerships in national cyber-security strategies. **International Affairs**, vol. 92, n.1, 2016, pp. 43–62.

NEWSWIRE. Cybersecurity Market Worth $248.26 Billion by 2023, 21 de setembro de. 2018. *Academic OneFile*. Disponível em: http://link-galegroup.ez370.periodicos.capes.gov.br/apps/doc/A555111328/AONE?u=capes&sid=AONE&xid=0e2c62e7. Acesso em: 20 mai. 2019.

CYBERSECURITY VENTURES. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics, 6 de fevereiro de 2019. Disponível em: https://cybersecurityventures.com/cybersecurity-almanac-2019/. Acesso em: 19 mai. 2019.

DEIBERT, R. **Black Code**: Inside the Battle for Cyberspace. Oxford: Signal, 2013.

DENNING, D. E. Framework and principles for active cyber defense. **Computers & Security**, vol. 40, 2014, p. 108-113.

DEWAR, R. S. The “triptych of cyber security": A classification of active cyber defence. In: International Conference on Cyber Conflict, 2014, Talin. IEEE Xplore, online. Disponível em: http://ieeexplore.ieee.org/document/6916392/?reload=true. Acesso em: 15 abr. 2019.

DITTRICH, D.; HIMA, K. Active response to computer intrusions. In: BIGDOLI, H. (ed.). **The handbook of information security**. Hoboken: John Wiley & Sons, 2005.

DUNN CAVELTY, M. **Cyber-security and threat politics**: US efforts to secure the information age. London: Routledge, 2008.

DUNN CAVELTY, M. The militarisation of cyberspace: Why Less May Be Better. International Conference on Cyber Conflicts, 4, 2012, Talin. Talin: NATO CCD COE, 2012, p. 141-153.

DUNN CAVELTY, M. Cyber-security and Private Actors. In: ABRAHANSEM, R.; LEANDER, A. (eds.). **Routledge Handbook of Private Security Studies**. New York: Routledge, 2016.

DUNN, J. Antivirus is 'dead' says Symantec security head as firm launches more services and cloud security. **Tech World**, 06 de maio de 2014. Disponível em: https://www.techworld.com/news/security/antivirus-is-dead-says-symantec-security-head-as-firm-launches-more-services-cloud-security-3515066. Acesso em: 15 abr. 2019.

DZIUNDZIUK, V. Stopping cyberterror: CountrieS muSt work together to thwart effortS of internet CriminalS. Per Concordiam: Journal of European Security and Defense Issues, vol. 2, n. 2, 2018.

ENDGAME: Endpoint protection for enterprises. Disponível em: https://www.endgame.com. Acesso em: 20 abr. 2019.

GREENBERG, A. Inside Endgame: A second act for the Blackwater of hacking. **Forbes**, fevereiro de 2014.

GROS, F. **Le Principe Sécurité**. Paris: Gallimard, 2012.

HACKING TEAM. Disponível em: http://www.hackingteam.it/. Acesso em: 23 abr. 2019.

HANSEN, L.; NISSENBAUM, H. Digital disaster, cyber security, and the Copenhagen School. **International Studies Quarterly**, vol. 53, n. 4, 2009, p. 1155–1175.

HARRIS, S. **@War**: The rise of the military-internet complex. Boston: Houghton Mifflin Harcourt, 2014.

HERRICK, D. The social side of 'cyber power'? Social media and cyber operations. In: 8th International Conference on Cyber Conflict. Talin: NATO CCDCOE, 2016. Disponível em: https://ccdcoe.eu/uploads/2018/10/Art-07-The-Social-Side-of-Cyber-Power.-Social-Media-and-Cyber-Operations.pdf. Acesso em: 18 mai. 2019.

HOFFMAN, W.; LEVITE, A. E. Private sector cyber defense: can active measures help stabilize cyberspace? Washington, D.C: Carnegie Endowment for International Peace, 2017. Disponível em: https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf. Acesso em 24 abr. 2019.

JABEE, R.; ALAM, A. Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). In: **International Journal of Computer Applications**, vol 144 n. 3, June 2016. Disponível em: https://pdfs.semanticscholar.org/b501/886f966f8cd7e47115d390afbbda017506e1.pdf . Acesso em: 23 mai. 2019.

KASPERSKY LAB. Disponível em: https://www.kaspersky.com/resource-center. Acesso em: 23 abr. 2019.

KRAUSE, K.; WILLIAMS, M. **Critical Security Studies**: Concepts and cases. Minneapolis: University of Minnesota Press, 1997.

LEANDER A. Commercial security practices. In: BURGESS, P. (ed.). **Handbook of new Security Studies**. New York: Routledge, 2010.

LEANDER A. Understanding US national intelligence: Analyzing practices to capture the Chimera. In: BEST, J.; GHECIU, A. (eds). **The return of the public in Global Governance.** Cambridge: Cambridge University Press, 2014, p. 197-220.

LEANDER, A. Regressive Rites of Passage: Certification Infrastructuring Liminality in Cybersecurity. In: EWIS: Performing World Politics through Rituals, 6-9 June 2018, Groningen.

LEANDER, A.; WÆVER, O. Introduction. Em: Anna Leander and Ole Wæver (eds.). **Assembling Exclusive Expertise**: Knowledge, Ignorance and Conflict Resolution in the Global South. Oxon: Routledge: 2019.

LIBICKI, M. C.; SENTY, D.; POLLAK, J. **H4CKER5 wanted**: An examination of the cybersecurity labor market. Santa Monica: RAND, 2014.

LOBATO, L. C. "Anotações". LAAD Defence & Security, 3 de abril de 2019.

LOBATO, L. C. "Anotações". Private Sector 'Hack Back': Where is the Limit? Workshop no Fórum de Governança da Internet, 12 de novembro de 2018.

LOCKHEED MARTIN. Disponível em: http://cyber.lockheedmartin.com. Acesso em: 20 abr. 2019.

MCAFEE. Disponível em: http://www.mcafee.com/us/index.html. Acesso em: 25 abr. 2019.

MARCZAK, B.; GUARNIERI, C.; MARQUIS-BOIRE, M.; SCOTT-RAILTON, J. Mapping Hacking Team's "untraceable" spyware. **Citizen Lab research brief**, n.33, 2014.

MARCZAK, B.; SCOTT-RAILTON, J.; MCKUNE, S.; RAZZAK, B. A.; DEIBERT, R. Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Citizen Lab, 28 de setembro de 2018. Disponível em: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/. Acesso em: 14 mai. 2019.

MCCARTHY, D. **Power, information technology and international relations theory**: The power and politics of US foreign power and the Internet. Londres: Palgrave MacMillan, 2015.

MEDAIRY, B. The future of cybersecurity: The best defense is a good offense. Booz Allen Hamilton, s.d. Disponível em: https://www.boozallen.com/s/insight/blog/future-of-cybersecurity.html. Acesso em: 25 mai. 2019.

MCAFEE, J. The death of antivirus and what comes next. **Silicon Angle**, 22 de junho de 2015. Disponível em: https://siliconangle.com/blog/2015/06/22/the-death-of-antivirus-and-what-comes-next. Acesso em: 5 mai. 2019.

MEDVETZ, T. **Think tanks in America**. Chicago: University of Chicago Press, 2012.
MORGAN, S. Top five U.S. Defense contractors bungle commercial cybersecurity market opportunity. CSO: Cybersecurity Business Report, 28 de janeiro de 2016. Disponível em: https://www.csoonline.com/article/3027383/security/top-five-u-s-defense-contractors-bungle-commercial-cybersecurity-market-opportunity.html. Acesso em: 5 mai. 2019.

NEWMAN, L. H. A top-shelf IPhone hack now goes for $1.5 million. Wired, 29 de setembro de 2016. Disponível em: https://www.wired.com/2016/09/top-shelf-iphone-hack-now-goes-1-5-million. Acesso em: 15 mai. 2019.

NORTHROP GRUMMAN. Disponível em: http://www.northropgrumman.com. Acesso em 25 abr. 2019.

NSO Group. Disponível em: https://www.nsogroup.com/. Acesso em 24 abr. 2019.

PALANTIR. Disponível em: https://www.palantir.com/. Acesso em 25 abr. 2019.

RAYTHEON. Disponível em: http://www.raytheoncyber.com/. Acesso em 25 abr. 2019.

ROSENQUIST, M. How offensive cyber security is changing the industry. **IT Peer Network**, 8 de outubro de 2013. Disponível em: https://itpeernetwork.intel.com/how-offensive-cyber-security-is-changing-the-industry/. Acesso em: 28 abr. 2019.

SCHWARTZ, M. NSA contracted with Zero-Day vendor VUPEN. **DarkReading**, setembro de 2013. Disponível em: https://www.darkreading.com/risk-management/nsa-contracted-with-zero-day-vendor-vupen/d/d-id/1111564. Acesso em: 27 abr. 2019.

SILVA, K. K. How industry can help us fight against botnets: notes on regulating private-sector intervention, International Review of Law, Computers & Technology, vol. 31, n. 1, pp. 105-130, 2017. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13600869.2017.1275274. Acesso em: 20 mai. 2019.

SNOW, J. Pegasus: o spyware perfeito para iOS e Android. Kaspersky Lab, 8 de abril de 2017. Disponível em: https://www.kaspersky.com.br/blog/pegasus-spyware/7237/. Acesso em: 20 mai. 2019.

STEPTOE. The Hackback Debate. *Steptoe Cyberblog,* 2 de novembro de, 2012. Disponível em: https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate. Acesso em 29 abr. 2019.

SYMANTEC. Disponível em: https://www.symantec.com/. Acesso em: 24 abr. 2019.

CITIZEN LAB. Backdoors are Forever: Hacking Team and the Targeting of Dissent, **Citizen Lab Research Brief,** n. 12, 2012.

YADRON, D. Symantec develops new attack on cyberhacking. **The Wall Street Journal**, 4 de maio de 2014. Disponível em: https://www.wsj.com/articles/symantec-develops-new-attack-on-cyberhacking-1399249948. Acesso em: 16 mai. 2019.