Artigos Selecionados REDE 2017
I Encontro da Rede de Pesquisa em Governança da Internet
Rio de Janeiro, 14 de Novembro de 2017

ATORES PRIVADOS E A PRODUÇÃO DA SEGURANÇA CIBERNÉTICA

Luísa Cruz Lobato
Doutoranda em Relações Internacionais – IRI/PUC-Rio
l.cruzlobato@gmail.com

RESUMO
Após pouco mais de duas décadas, o debate sobre segurança cibernética foi incorporado ao campo das Relações Internacionais. Uma parcela significativa da área tem apontado para a participação e influência de governos no campo da tecnologia da informação e, consequentemente, da insegurança proporcionada por isso. Em meio a este debate, o papel de atores privados na definição do que é segurança cibernética ainda requer debate aprofundado. Propõe-se, portanto, refletir a respeito disto, argumentando-se que estes atores participam diretamente na produção de segurança no ciberespaço principalmente a partir 1) do uso de parâmetros de segurança (p.ex., criptografia) em seus softwares; e 2) da comercialização de produtos e serviços voltados a proteger ou combater ameaças cibernéticas. Além da criação de companhias especializadas em segurança cibernética, a última década também presenciou maior envolvimento de companhias estabelecidas em ramos tradicionais da segurança no desenvolvimento e comercialização de produtos e serviços de vigilância e segurança cibernética, motivadas por um aumento no volume de recursos direcionados a estes esforços. A partir disto, reflete-se sobre as relações entre estes atores e governo a partir do caso dos Estados Unidos, onde se observa seu envolvimento em disputas envolvendo a definição do que é segurança cibernética e a constituição de alianças com o governo. Esses arranjos público-privados, voltados para reforçar uma visão de segurança nacional, afetam também o que se entende por segurança cibernética, agravando o alcance da vigilância e coleta de dados massiva em nome da “segurança” e enfraquecendo a posição do indivíduo enquanto sujeito a ser protegido.

PALAVRAS-CHAVE: SEGURANÇA CIBERNÉTICA, ATORES PRIVADOS, RELAÇÕES INTERNACIONAIS

Sugestão de citação (ABNT): SOBRENOME, Nome. **Título do artigo**. I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, NOVEMBRO DE 2017. Disponível em: <endereço na web>. Acesso em: mês. ano.

1. INTRODUÇÃO

A última década viu a normalização das interações e conflitos envolvendo o ciberespaço nas Relações Internacionais (R.I.), um processo marcado por tentativas de países de estabilizar interações políticas na e por meio da Internet, assim como pela inclusão da segurança cibernética em agendas de segurança ao redor do mundo (DEIBERT, 2013; DENARDIS, 2014; DUNN CAVELTY, 2015; CSIS, 2008; 2010). A distinção cada vez mais imprecisa entre atividades *online* e *offline* e o crescente uso de computadores para solucionar problemas corriqueiros ou cada vez mais complexos contribuíram para este processo (KITCHIN; DODGE, 2011; DUNN CAVELTY, 2016).

Debates sobre segurança cibernética se desenvolveram intensamente na interseção entre a disciplina das R.I e dos Estudos de Segurança (BARNARD-WILLS; ASHENDEN, 2012; DUNN CAVELTY, 2007; 2008; 2012; 2015; 2016; DEIBERT, 2011; 2013; DEIBERT; ROHOZINSKI, 2010; ERIKSSON; GIACOMELLO, 2009; HANSEN; NISSENBAUM, 2009). Um mapeamento desta literatura prontamente aponta para a maneira com a qual diferentes perspectivas trataram de diferentes aspectos do assunto: trabalhos produzidos por especialistas em “think tanks” ou orientados para a formulação de políticas públicas e de defesa (CSIS, 2008; 2010; ABLON et al., 2014; SEGAL, 2016); estudos críticos de segurança focando na relação entre poder e informação (DAY, 2001); estudos sobre a produção de insegurança *online* por meio de vigilância e censura (DEIBERT et al., 2010); e estudos sobre a securitização do espaço cibernético e sobre a constituição de ameaças cibernéticas (DUNN CAVELTY, 2008; HANSEN; NISSENBAUM, 2009; BETZ; STEVENS, 2011; 2013). Mas, conforme nota Dunn Cavelty (2016), essa extensa literatura ainda explora muito pouco a maneira como atores privados (e, acrescenta-se, companhias privadas) têm participado nesse campo.

Visando contribuir com esta literatura, a presente proposta explora o papel de atores privados, mais especificamente companhias privadas, na produção da segurança ou insegurança cibernética e tem por foco o caso dos Estados Unidos (EUA). O país tem sido central para o desenvolvimento de tecnologias da informação e comunicação (TICs) e da Internet, processos para os quais atores privados foram e têm sido centrais (CASTELLS, 2010). Partindo da importância desses atores para o desenvolvimento e difusão das tecnologias digitais, argumenta-se que os mercados de TICs participam na produção de seguranças e inseguranças na Internet a partir da forma como retratam ameaças digitais em anúncios, bem como na comercialização de seus produtos e serviços. Com um foco na parcela deste mercado que tem se voltado para responder a uma crescente demanda por segurança, busca-se compreender como essas práticas produzem e reforçam abordagens e entendimentos atraentes

sobre a segurança cibernética e indagamos sobre as implicações da participação do mercado na definição do que é segurança e insegurança *online*.

Compreender a participação das companhias privadas na produção da segurança cibernética a partir de uma discussão situada no campo das R.I. importa à literatura sobre governança da Internet, de modo mais amplo, e sobre segurança cibernética, de modo mais específico, de duas maneiras: em primeiro lugar, ao situar essa participação no contexto de disputas e alianças práticas e conceituais, chama-se a atenção para o papel que dinâmicas de mercados desempenham, de modo mais ou menos indireto, na definição dos elementos centrais nestas agendas. Para além de questões normativas (como deveria ser?), situar esses 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 tem na segurança cibernética seu principal ativo nesse processo.

Em segundo lugar, isto nos permite visualizar não apenas como se constituem dinâmicas de segurança no contexto da governança da Internet, como também a forma como dinâmicas de insegurança se constituem e se difundem para além desta agenda. Isto ocorre 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.

Com base nisto, o trabalho é estruturado em quatro partes. Em um primeiro momento, o artigo revisita o tratamento dado pela disciplina das R.I. aos atores privados e apresenta o conceito de campo (BOURDIEU, 1988; 2004) para fundamentar o argumento sobre o papel dos mercados na produção da segurança/insegurança cibernética. Tal participação pode ocorrer mediante o desenvolvimento e uso (ou não) de parâmetros de segurança, a exemplo da criptografia, em softwares; ou mediante a comercialização de produtos e serviços voltados à proteção contra ou combate a ameaças cibernéticas. Argumenta-se que isto ocorre no contexto de um campo dinâmico de disputas por recursos e por influenciar nas “regras do jogo”. O trabalho de Bourdieu tem sido utilizado nas R.I. para proporcionar uma perspectiva distinta a respeito das formas como o poder é exercido na vida internacional. Sugerir a existência de um campo de disputas sobre a segurança cibernética implica uma base analítica consistente para discutir de que forma a competição de mercado molda práticas e entendimentos sobre segurança cibernética, bem como quais são os resultados políticos das relações de poder e disputas em torno da definição do que é segurança na sociedade digital. Nesse

contexto, chama-se a atenção para o envolvimento de companhias privadas em arranjos políticos e econômicos por meio de disputas nesse campo.

Em seguida, analisa-se os produtos e serviços anunciados publicamente por contratantes de defesa, companhias antivírus e "fornecedores" de vulnerabilidades. A partir disso, identifica-se três abordagens distintas, porém não excludentes, para a segurança cibernética: defensiva, ofensiva e defesa ativa. Em um terceiro momento, analisa-se a predominância da defesa ativa nos mercados comercial e governamental nos EUA e suas implicações enquanto uma mudança de paradigma na segurança cibernética. Conclui-se com uma reflexão a respeito da maneira como determinados arranjos públicos-privados, em particular aqueles voltados para reforçar uma visão de segurança nacional, afetam também os elementos que ajudam a constituir o discurso sobre segurança cibernética para além dos elementos técnicos e humanos enfatizados por especialistas, podendo agravar o alcance da vigilância e coleta de dados massiva em nome da "segurança", mais amplamente compreendida, paralelamente enfraquecendo a ideia do indivíduo enquanto principal sujeito a ser protegido. Nota-se que apesar do foco no caso dos EUA, é possível, a princípio, generalizar esses resultados para outros casos, na medida que uma parcela considerável das companhias analisadas opera em um escopo global. Todavia, embora a dinâmica do mercado global de TICs permita vislumbrar como as disputas nos EUA reverberam para outros lugares, os termos precisos destas disputas, devem ser definidos com base na análise dos casos específicos, à medida que questões regulatórias podem alterá-los substancialmente.

2. ATORES PRIVADOS NO CAMPO DA SEGURANÇA CIBERNÉTICA

Debates sobre governança da Internet, de modo mais amplo, e segurança cibernética, de modo mais específico, encontraram nas R.I. terreno fértil para se desenvolver (EPSTEIN; KATZENBACH; MUSIANI, 2016), tendo sido este último campo abraçado pelas subdisciplinas dos estudos de segurança e estudos de defesa (DUNN CAVELTY, 2008; HANSEN; NISSENBAUM, 2009). O interesse pelo tópico da segurança cibernética nas R.I., entretanto, veio acompanhado pela histórica preocupação da disciplina com a figura do Estado (MCCARTHY, 2015; CARR, 2015). Enquanto válida, o foco resultante de tal orientação tem gerado uma cegueira disciplinar com relação ao papel dos atores privados na constituição daquilo que se entende por segurança e insegurança no ciberespaço (DUNN CAVELTY, 2016).

O estudo dos atores privados na segurança internacional pode contribuir para preencher essa lacuna na literatura sobre segurança cibernética. O campo se desenvolve no início dos anos 2000, favorecido por contestações anteriores das bases

teóricas da disciplina e por tentativas de expandir seu entendimento sobre poder, segurança e a realidade social (KRAUSE; WILLIAMS, 1997; KRAUSE, 1998; BOOTH, 2007; BUZAN; HANSEN, 2009), tendo por foco uma variedade de temas relativos à segurança e atores privados, como privatização da segurança e uso da força (SINGER, 2002; AVANT, 2005; LEANDER, 2008; ABRAHANSEN; WILLIAMS, 2009); o papel das companhias privadas de segurança/militares em criar (in)segurança (SINGER, 2002; AVANT, 2005) e a contestação da linha que divide público e privado na governança da segurança (BERNDTSSON; STERN, 2011; BIGO, 2013; 2015). Nesse campo de estudos, os atores com fins lucrativos são o foco principal, porém não exclusivo (ver, por exemplo, PETERSEN; TJALVE, 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 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). Segundo Leander (2010), uma atenção às mais diversas formas de privatização ilumina distintos arranjos políticos entre Estados e atores privados.

Atores privados desempenham um papel central no campo da segurança cibernética. Empresas disputam o mercado, a definição do que se constitui 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; qual problema de segurança é mais grave; a (i)legalidade de práticas como o hackeamento; a constituição da segurança enquanto valor central à rede, entre outros.

Por campo de segurança cibernética, nos referimos ao “espaço” onde disputas simbólicas ocorrem. Bourdieu (1988; 2004) retrata o mundo social como um terreno dinâmico de disputas, em torno de certas questões, em campos que frequentemente 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 (*habitus*) 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 (BERLING, 2012; BOURDIEU, 1988; BOURDIEU; WACQUANT, 1992).

Nesse campo, 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; BETZ; STEVENS, 2011; DUNN CAVELTY; JAEGER, 2015). 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 segurança cibernética 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).

Governos e companhias de tecnologia são atores particularmente poderosos por combinarem conhecimento técnico em TICs e poder econômico, o que lhe proporciona 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 também produzem caracterizações de ameaças cibernéticas por meio de anúncios, análises técnicas e estudos veiculados em mídia própria, como blogs, websites, relatórios e revistas. Uma estratégia do setor de antivírus, por exemplo, tem sido questionar o valor e utilidade desta tecnologia em relação ao crescente universo das coisas conectadas e dos complexos desafios de segurança que se seguem, sugerindo alternativas envolvendo a segurança do Endpoint ("ponto final") 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 segurança cibernética, à medida que o "poder" no âmbito do mercado se vê fortemente associado ao número e natureza (governamental, comercial, usuários) de seus clientes e, fundamentalmente, ao lucro gerado com seus produtos e serviços[1].

Parcerias público-privadas (PPPs) e a terceirização de serviços de segurança são dois arranjos resultantes das dinâmicas do campo da segurança cibernética. Nesse caso específico, justifica-se o recurso às PPPs com base (1) nas especificidades das TICs, ao serem tecnologias predominantemente desenvolvidas e operadas pelo setor privado; e (2) nas demandas que surgem dadas as novas dinâmicas de segurança,

1 O processo descrito se insere na noção Bourdieusiana de estratégia. Ver: Swartz (1997)

quando ataques cibernéticos e programas maliciosos passam a, cada vez mais, serem 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 (LEANDER, 2009; 2014; BIGO, 2013; BERNDTSSON; STERN, 2011). A segurança de sistemas de computador civis e militares, bem como o desenvolvimento de novas soluções de segurança cibernética 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 segurança cibernética, 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, 2011; 2013; HARRIS, 2014). A cristalização deste tipo de arranjo no campo da segurança cibernética 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 nos EUA (DUNNE; SKÖNS, 2011; DEIBERT, 2011; 2013; HARRIS, 2014). Tais dinâmicas levam as companhias a adotar estratégias de mercado agressivas de modo a ganhar mais espaço para a comercialização de suas soluções. Outros arranjos complexos ainda incluem os esforços da Agência de Segurança Nacional dos EUA (NSA) para desenvolver, junto a companhias de tecnologia, produtos que facilitem a vigilância, o que tem levado a conflitos substanciais com algumas delas (COOK, 2016; HERN, 2015).

3. ANÁLISE EMPÍRICA DO CAMPO DA SEGURANÇA CIBERNÉTICA NOS EUA

O campo da segurança cibernética nos EUA é altamente dinâmico e, com frequência, suas dinâmicas tem efeitos que ultrapassam suas fronteiras e afetam as dinâmicas e termos do debate sobre segurança cibernética em outros países[3]. Isto se

2 Complexos industriais são alianças público-privadas de natureza híbrida por meio das quais governos incentivam acordos institucionais com o setor privado (ADAMS, 1968), podendo ser de natureza militar (ADAMS, 1968) ou distinta (DEIBERT, 2011; 2013).

3 O caso brasileiro é ilustrativo disto. Diversos movimentos legislativos e políticos se seguiram às revelações feitas por Edward Snowden acerca do programa de espionagem dos EUA, no ano de 2013, a exemplo da imediata aprovação do Marco Civil da Internet (o projeto tramitava no Congresso Nacional desde 2009 e do encontro NETMundial, em 2014, além da instauração de uma Comissão Parlamentar de Inquérito para investigar denúncias de espionagem pelos EUA, da apresentação, pelo país, junto à ONU, de uma proposta de resolução sobre privacidade na era digital, dentre outros.

deve, dentre outros fatores, à centralidade do país no desenvolvimento das TICs e à sua vanguarda (e relativo sucesso) nos esforços de securitização do espaço cibernético (DUNN CAVELTY, 2008). Os EUA ainda concentram grande parte das companhias de tecnologia mais poderosas do mundo, servindo de *hub* para inúmeras outras companhias estrangeiras. Por estas razões, concentraremos a análise empírica ora proposta no caso dos EUA.

Cabe salientar que o rótulo “companhias privadas” abarca uma ampla categoria de atores no mercado, desde companhias não especializadas em TICs, como bancos, até provedores de Internet e redes sociais. Nosso foco consiste na categoria denominada companhias de segurança cibernética, que compreende aquelas que anunciam e comercializam produtos e serviços que oferecem proteção e análise de risco contra softwares maliciosos, intrusões e ataques cibernéticos. A fim de prover uma análise mais consistente, categoriza-se essas companhias conforme a natureza das soluções por elas oferecidas e seu público alvo. Assim, no caso dos EUA, identifica-se três grupos:

(1) Empresas de antivírus ou proteção de *endpoints*, 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 segurança cibernética variam no mercado, assim como seus efeitos. Por vezes, parcerias com governos ou mercados são benéficas e resultam em mais proteção para usuários, mas por vezes essa relação pode conduzir a práticas de violação de privacidade e crescente insegurança na Internet.

Empresas de antivírus / proteção de *Endpoint*

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. (MCDONALD, 2012; KASSNER, 2012; YADRON, 2014; MCAFEE, 2015).

As plataformas de proteção Endpoint modernas compreendem uma variedade de modelos de proteção: detecção baseada em assinaturas ou sem a necessidade das mesas; direcionada a usuários corporativos, domésticos ou governamentais (KASPERSKY, 2017; INTEL SECURITY, 2017; SYMANTEC, 2017); ofertando serviços de gestão de risco (AVIRA 2017; BITDEFENDER 2017). A maioria desses modelos utiliza uma abordagem defensiva para proteger dispositivos, redes e atividades online, como compras e trocas de e-mail, de ameaças cibernéticas. Suas atividades incluem 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, que consiste em 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 Endpoint 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, gradativamente, 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 (ANDERSON, 1996; ANDERSON et al., 1999; SYMANTEC, 2017; KASPERSKY, 2017). 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"[4]. Devido ao uso dessas vulnerabilidades para fins ofensivos e de vigilância, este é um mercado que, na superfície, é 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 visarem 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 segurança cibernética, 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, 2017), 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 vazados, sugerem o contrário (HERN, 2015). O Citizen Lab, da Universidade de Toronto, reportou que um "backdoor"[5] foi utilizado para vigiar um jornalista marroquino (THE CITIZEN LAB, 2012) e que 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 (antes denominada VUPEN[6]). O envolvimento inicial 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 inteligência que analisa a informação do

4 Uma vulnerabilidade zero-dia é uma falha em um computador ou software, geralmente desconhecida pelo programador ou companhia responsável por seu desenvolvimento. Um estudo empírico deste fenômeno pode ser encontrado em: Bilge and Dumitras (2012).

5 Falhas ou brechas mediante as quais um sistema pode ser explorado por terceiros.

6 A companhia ficou conhecida por servir como fornecedora de vulnerabilidades para a NSA e abertamente anunciava seu envolvimento no negócio de desenvolvimento de exploits.

sistema do cliente, comparando-a com a pesquisa da companhia sobre programas maliciosos (GREENBERG, 2014). Sua estratégia comercial, o “Hunting Cycle” visa (sorrateiramente) identificar e eliminar adversários das redes, bem como proceder à coleta de inteligência para elaboração de estratégias de resposta (ENDGAME, 2017).

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).

Pressões para tornar o ciberespaço mais seguro contribuíram para criar um mercado com opções defensivas e ofensivas para a segurança cibernética, guerra cibernética e tecnologias de vigilância (BRITO; WATKINS, 2011). Reformulações como as vislumbradas nos casos da Endgame e Zerodium, indicam que fornecedores de vulnerabilidades têm buscado expandir suas atividades para além do setor governamental. O envolvimento no mercado para vulnerabilidades zero-dia vem acompanhado de uma maior abertura a medidas ofensivas para lidar com ameaças cibernéticas[7]. Ancorada 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 do setor de defesa se voltaram para o mercado de segurança cibernética em atenção ao seu crescimento exponencial[8] e motivados por restrições no orçamento de defesa do governo dos EUA (MORGAN, 2016). Estas 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. Ademais, há evidências de seu envolvimento no mercado de vulnerabilidades, muito embora os detalhes de tal envolvimento ainda não sejam muito claros[9] (BRITO; WATKINS, 2011; SCHNEIER, 2012; 2013; DEIBERT, 2013; HARRIS,

7 O que não implica na adoção automática da estratégia ofensiva por todas as companhias no ramo. A solução comercial da Engdame indica que alguns optam por uma “terceira via”, cujo foco é a antecipação de ameaças.

8 Dados de 2016 apontam que o governo dos EUA investiu cerca de 100 bilhões de dólares no mercado de segurança cibernética na última década. Ver: Morgan (2016).

9 As atividades de empresas contratantes de defesa tendem a ser sigilosas e seu envolvimento no mercado de vulnerabilidades é ainda mais obscuro que o de empresas que se dedicam apenas a ele. Anúncios de empregos, combinados com as descrições das

2014). Apesar disso, essas companhias reconhecem publicamente a aliança com setores da segurança nacional (LOCKHEED MARTIN, 2017; BOEING, 2017; GENERAL DYNAMICS, 2017; NORTHROP GRUMMAN, 2017; RAYTHEON, 2017; BOOZ ALLEN HAMILTON, 2017).

Os serviços oferecidos por essa categoria incluem: proteção à infraestrutura crítica, vigilância, análise de dados, segurança da informação, capacidades operacionais, segurança na nuvem, 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, 2017), e, assim, 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 Endpoint.

Com soluções que buscam detectar e analisar para prever, essa categoria invoca uma abordagem complexa à segurança cibernética, que mescla elementos ofensivos e defensivos[10]. A chamada defesa ativa concerne um conjunto de medidas para conter intrusões, podendo servir a fins investigativos, defensivos e punitivos. A implementação destas medidas ocorre sem o consentimento de (pelo menos) uma das partes envolvidas ou afetadas pela intrusão e podem impactar sistemas de terceiros. Dittrich e Hima (2005) notam que essas táticas incluem desde medidas "benignas" de coleta de informações até medidas mais agressivas que visam inibir/impedir o funcionamento de sistemas remotos. 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; NORTHROP GRUMMAN, 2015).

Assim, além de investirem no campo da segurança cibernética, essas companhias também contribuem para promover uma abordagem de segurança que

---

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 agencias de espionagem.

10 Algumas companhias inseridas nas categorias anteriores passaram a se inclinar nessa direção, como a Endgame, Symantec e Kaspersky.

pode adquirir contornos ofensivos. De um modo geral, companhias de segurança cibernética 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, e mesmo a abordagens abertamente ofensivas, ilustra o modo como essas companhias produzem noções de segurança por meio de suas práticas.

4. DEFESA ATIVA: PARADIGMA PARA SEGURANÇA CIBERNÉTICA?

O recurso crescente à defesa ativa resulta de uma disputa relativa a qual abordagem para a segurança cibernética é mais benéfica ou prejudicial a alianças no campo. Uma das principais questões em jogo é a possibilidade de conferir a atores privados autorização para "hackear de volta" quando um sistema se encontre sob ataque. Argumenta-se que uma abordagem meramente defensiva é insuficiente na proteção contra ataques cibernéticos, ao mesmo tempo em que se observa claras restrições legais quanto à adoção de medidas abertamente ofensivas por atores privados. A defesa ativa se torna atraente, por compreender medidas que incluem, mas não se restringem, à possibilidade de hackear de volta (DENNING, 2014; DEWAR, 2014; STRAND, 2015).

Seu crescimento enquanto opção mais 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). O debate coexiste com a adoção *ad hoc* destas medidas por parte das companhias sem a autorização necessária, em virtude do ritmo dos ataques contra suas redes ou de preocupações com a reputação da companhia (DITTRICH; HIMA, 2005).

No campo da segurança cibernética, ataques cibernéticos não são simplesmente prováveis: são, sobretudo, iminentes – uma questão de tempo (RAYTHEON, 2017). A certeza da ocorrência de um ataque esconde as incertezas que cercam o exato momento de sua ocorrência, as consequências para o alvo, e a identidade do perpetrador[11]. Riscos cibernéticos são enquadrados em termos de um futuro calculável, porém desconhecido, no qual a probabilidade desempenha papel fundamental em determinar seu potencial de realização (BERNDTSSON; KINSEY, 2016).

Especulações sobre uma possível guerra cibernética são parte de um imaginário coletivo repetidamente debatido por especialistas e acadêmicos (ARQUILLA;

11 Também conhecido como problema da atribuição, refere-se às dificuldades em se precisar a identidade da pessoa que orquestrou um ataque.

RONFELDT, 1992; DUNN CAVELTY, 2012; BARNARD-WILLS; ASHENDEN, 2012; CARAFANO, 2015). Tal risco, de alto impacto político e baixa probabilidade, é reforçado por meio de especulações sobre o que pode acontecer de pior (BERNDTSSON; KINSEY, 2016), e representa uma oportunidade para aquelas companhias dispostas a expandir sua parcela do mercado para segurança cibernética (BRITO; WATKINS, 2011). A defesa ativa se beneficia da associação entre riscos prováveis e improváveis, ao propor uma abordagem antecipatória, baseada em tentativas de impedir que tais riscos se concretizem – ou, ao menos, mitiga-los, com base no estudo de eventos passados, – permitindo a atores privados defender-se nos limites da lei e a atores governamentais uma reação dinâmica contra intrusões e potenciais inimigos, com retaliação e medidas ofensivas constituindo seu portfólio. Ao atender a ambos os mercados, a defesa ativa se torna dominante no contexto de soluções de segurança mais sofisticadas.

Na prática, essa abordagem envolve atividades de detecção, identificação e reação a ataques por meio de uma série de movimentos sobrepostos e, às vezes, pouco coordenados, o que inclui medidas para aperfeiçoar técnicas de detecção; coleta de inteligência sobre o comportamento da ameaça; o uso de “honeypots”, mecanismos que simulam falhas em um computador, sistema ou redes para coletar informações sobre um ataque (ver: HOEPERS; STEDING-JESSEN; CHAVES, 2007); uso de DNS falsos, também conhecido como sequestro de Sistemas de Nomes de Domínios[12]; identificação de IP; geolocalização; websites falsos com programas maliciosos embutidos; acesso remoto ao sistema do agressor e outras formas de hackeamento. Os dados coletados mediante tais processos são utilizados para desenhar estratégias para prevenir ataques futuros.

Ao se apoiarem no uso de segurança por obscuridade e envolverem ações que afetam sistemas de terceiros e vigilância, algumas destas medidas passam a serem vistas como politicamente e eticamente problemáticas (ANDERSON, 2001; DEWAR, 2014). A legalidade dúbia percebida em algumas práticas típicas de defesa ativa torna-se uma preocupação diante da forma como atos de vigilância e intrusão podem ser exacerbados pela arquitetura da Internet. Na prática, isto implica uma dificuldade em se distinguir entre ações ofensivas e preventivas.

Enquanto paradigma de segurança cibernética, a defesa ativa autoriza a adoção de medidas invasivas em nome da antecipação de riscos, servindo como resposta à crescente complexidade dos riscos cibernéticos. Ao reconhecer que tecnologias digitais são inerentemente vulneráveis, esse paradigma propõe medidas para se lidar

12 Essa subversão do Sistema de Nomes de Domínio pode servir tanto a fins maliciosos, quanto ser utilizada por provedores de serviço de Internet para redirecionamento do tráfego para seus servidores, com fins de coleta de estatísticas, servir para fins de anúncios e ser utilizada por provedores para censurar o acesso a um determinado domínio.

com o que não se pode prever com precisão. As contradições próprias ao paradigma, porém, afetam diretamente a forma que adquire a segurança, caracterizada não como uma condição objetiva, marcada pela ausência de perigos, mas sim uma tentativa de se exercer controle sobre certos tipos de fluxo (GROS, 2010; 2012). Ao ganhar vida própria, esse modelo de segurança antecipatória invoca diversas formas de controle disponíveis: práticas de vigilância, por exemplo, são postas como fundamentais para manter o cidadão seguro diante dos riscos iminentes e inerentes do espaço virtual – cuja arquitetura, argumenta-se, favoreceria as atividades de criminosos e terroristas. Tentativas de controle de fluxos ruins são validadas e expandem o alcance da "segurança".

O problema do denominado "comércio de armas digitais" (DEIBERT, 2013:348) de soluções de defesa ativa é seu impacto na real segurança da Internet. O mercado que o sustenta se alimenta da competição em torno da definição do que se constitui como ameaça e, por consequência, segurança cibernética. A reflexão sobre o papel da defesa ativa na configuração contemporânea da segurança cibernética chama a atenção para a maneira com a qual a segurança contemporânea lida com o incalculável (AMOORE, 2014). O recurso à estratégia da defesa ativa como meio para lidar com ataques cibernéticos é sintomático de uma longa preocupação com a busca por possibilidades para lidar com ameaças futuras em um contexto de informação limitada e insuficiente. Seu apelo pela defesa para além do "ponto final" 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 – com cenários nos quais um ataque cibernético teria consequências societais catastróficas – 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).

Por mais poderosa que a ideia possa ser, é importante atentar para sua expansão inobservada. Este é um conceito amplamente utilizado para justificar a suspensão de liberdades e direitos, autorizar práticas antiéticas e realocar recursos para setores específicos do mercado. Uma preferência pela defesa ativa, aliada à intensa competição mercadológica, conduz à adoção de medidas de coleta ampla de dados – em oposição a medidas de coleta direcionada – por companhias, a fim de aumentar as chances de sucesso de uma possível predição. Em outras palavras, essa articulação tem resultado em mais vigilância por parte de atores do mercado. Concomitantemente, ela também tem adicionado alguma pressão nos legisladores de modo a e permitir a adoção de medidas de natureza mais ofensiva pelo setor privado como forma de reagir mais efetivamente contra agressões, como é o caso do argumento a favor da retaliação a partir do "*hacking back*".

5. CONSIDERAÇÕES FINAIS

Prover segurança não é mais domínio de ação exclusivo dos Estados. Atores privados têm servido como fornecedores diretos de segurança, além de influentes produtores de (in)segurança. Vislumbra-se uma crescente legitimidade em torno da 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 (DEIBERT, 2013). Seu papel em definir a segurança cibernética, mediante a definição de padrões para o comércio de soluções do gênero, se torna, assim, fundamental. Entretanto, companhias privadas são diferentes de governos, particularmente ao atuarem movidas primordialmente por interesses econômicos próprios, alguns dos quais não se ajustam bem à dinâmica dos problemas de segurança. Esses atores tendem a compreender a segurança com base em uma avaliação permanente, não em termo de garantias. Não é de se surpreender que a participação direta destas no campo da segurança chame a atenção para problemas relativos ao acumulo de poder e à responsabilização politica e legal.

O tipo de poder alocado a atores privados no campo da segurança cibernética requer maior escrutínio na literatura das R.I, 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. À medida que o ciberespaço desafia concepções rígidas de fronteiras politicas, disputas de poder no campo da segurança cibernética facilmente se estendem para além delas.

Tal poder pode se tornar problemático se não devidamente monitorado e submetido a interesses de segurança de governos, às custas dos indivíduos. Políticas de segurança tendem a ser construídas com base na diferenciação entre o que é seguro e o que consta na zona cinzenta do inseguro (GROS, 2012). Esta é uma decisão tipicamente arbitrária ou resultante de disputas de poder entre grupos específicos.

No campo da segurança cibernética analisado neste trabalho, o discurso predominante é dominado pelo foco de Estados e corporações em sua própria segurança, o que serve para afastar decisões urgentes sobre o assunto dos interesses da sociedade civil e indivíduos. Mas enquanto aquela tem se afirmado de modo mais presente no campo, estes ainda são vistos como meros usuários, carecendo do conhecimento técnico necessário para adentrar propriamente o campo. Sua participação em processos decisórios sobre segurança cibernética deixa a desejar (COMINOS; SENEQUE, 2014). O usuário, diretamente afetado pelas dinâmicas das disputas de poder no campo da segurança cibernética, i.e., enquanto alvo de vigilância em massa por parte de governos e companhias, ainda permanece distante de

instâncias decisórias relativas a aspectos importantes de segurança e governança da Internet.

O paradigma de segurança antecipatória que alicerça apelos em favor da defesa ativa gera um problema difícil para a segurança cibernética, dadas as relações especificas com o futuro que alimenta. Se, por um lado, sustenta-se que a falta de conhecimento sobre o futuro pode ser suprida cientifica e tecnicamente, o reconhecimento do ciberespaço enquanto terreno inerente de incertezas, bem como a persistência de riscos improváveis de alto impacto e potencialmente catastróficos sugerem a necessidade de vigilância e estado de preparação constantes, indicando uma profunda ansiedade em relação ao desconhecido e ao improvável (DIPROSE et al., 2008).

Nos EUA, essa ansiedade, alimentada pela intensidade de ataques cibernéticos e por preocupações com sua escalada para cenários imaginados, como ciberguerra e ciberterrorismo, possibilitou o desenvolvimento de um campo no qual as disputas mais intensas são aquelas em torno da constante expansão de um mercado altamente lucrativo, às custas de problemas de segurança mais tangíveis. Apesar do foco no caso dos EUA, é possível, a princípio, generalizar esses resultados para outros casos, na medida que uma parcela considerável das companhias analisadas opera em um escopo global. Os termos precisos destas disputas, entretanto, devem ser definidos com base na análise dos casos específicos, na medida em que a dinâmica dos atores envolvidos e questões regulatórias podem alterá-los substancialmente.

REFERÊNCIAS

ABLON, L, LIBICKI, M; GOLAY, A. **Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.** Santa Monica: RAND, 2014.

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.

ADAMS, W. The Military-Industrial Complex and the New Industrial State. **The American Economic Review**, vol.58, n.2, 1968, p.652-665.

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

ANDERSON, R. H. **Risks to the U.S Infrastructure from Cyberspace**. Santa Monica: RAND, 1996.

ANDERSON, R. Why information security is hard - an economic perspective. COMPUTER SECURITY APPLICATIONS CONFERENCE, 17, 2001, Nova Orleans. IEEE Xplore, online, 2002. Disponível em: < http://ieeexplore.ieee.org/document/991552/>. Acesso em: 23 fevereiro 2017.

ARQUILLA, J.; RONFELDT, D. **Cyberwar Is Coming!** Santa Monica: RAND, 1993.

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

AVIRA. Download the free antivirus for PC & Mac. Avira Antivirus. 2017. Disponível em: <https://www.avira.com/>. Acesso em: 24 de julho de 2017.

BARNARD-WILLS, D.; ASHENDEN, D. Securing Virtual Space: Cyber War, Cyber Terror and Risk. **Space and Culture**, vol.15, n.2, 2012, p.110-123.

BERLING, T. V. Bourdieu, International Relations, and European Security. **Theory and Society,** vol.41, n.5, 2012, p.451-478.

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.

BETZ, D.; STEVENS, T. **Cyberspace and the State: Toward a Strategy for Cyber-power**. New York: Routledge, 2011.

_____. Analogical reasoning and cyber security. **Security Dialogue**, vol.44, n.2, 2013, p.147-164.

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.

_____. International Political Sociology: Internal Security as Transnational Power Fields. In: M. RHINARD M.; BOSSONG, R. (eds.). **Theorising Internal Security Cooperation in the European Union**. Oxford: Oxford University Press, 2015.

BILGE, L.; DUMITRAS, T. Before We Knew It: An Empirical Study of Zero-Day Attacks in The Real World. ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 19, 2012, Raleigh. Disponível em: < https://dl.acm.org/citation.cfm?id=2382284>. Acesso em: 24 março 2017.

BITDEFENDER. Bitdefender Soluções de Segurança. 2017. Disponível em: <http://www.bitdefender.com>. Acesso em: 24 fevereiro 2017.

BOEING. Cybersecurity & Information Management. 2017. Disponível em: <http://www.boeing.com/defense/cybersecurity-information-management/>. Acesso em: 26 fevereiro 2017.

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

BOOZ ALLEN HAMILTON. Consulting, Analytics, Digital Solutions, Engineering, Cyber. 2017. Disponível em: <http://www.boozallen.com/>. Acesso em: 26 fevereiro 2017).

BOURDIEU, P. Vive la Crise! For Heterodoxy in Social Science. *Theory and Society*, 17, n.5, 1988, p.773-787.

_____. **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**. Cambrigde: Cambridge University Press, 2009.

CARAFANO, J. J. The New Arms Race Is About Bytes, Not Bombs. **The Daily Signal**, 8 de fevereiro de 2015. Disponível em: < http://dailysignal.com/2015/02/08/the-new-arms-race-is-about-bytes-not-bombs/>. Acesso em: 23 março 2017.

CASTELLS, M. **The Rise of the Network Society**. Malden: Blackwell, 2010.

CARR, M. Power Plays in Global Internet Governance. **Millennium: Journal of International Studies**, vol. 46, n.2, 2015, p.640-659.

COMNINOS, A.; SENEQUE, G. (2014) Cyber security, civil society and vulnerability in an age of communications surveillance. In: **Global Information Society Watch 2014**: Communications Surveillance in The Digital Age, 2014, p.32-40.

COOK, T. A Message to Our Customers. Apple Inc., 2016. Disponível em: <http://www.apple.com/customer-letter/>. Acesso em: 05 março 2017.

CSIS. **Securing Cyberspace for the 44th Presidency**: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington DC: Center for Strategic and International Studies, 2008.

____. **Cybersecurity Two Years Later**: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Washington DC: Center for Strategic and International Studies, 2010.

DAY, R. **The Modern Invention of Information**: Discourse, History and Power. Carbondale: Southern Illinois University Press, 2001.

DEIBERT, R. Tracking the Emerging Arms Race in Cyberspace. **Bulletin of the Atomic Scientists**, vol.67, n.1, 2011, p.1-8.

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

DEIBERT, R.; ROHOZISNKI, R. Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, vol.4, n.1, 2010, p.15-32.

DENARDIS, L. **The Global War for Internet Governance.** New Haven: Yale University Press, 2014.

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, 6, 2014, Talin. IEEE Xplore, online. Disponível em: <http://ieeexplore.ieee.org/document/6916392/?reload=true>. Acesso em: 15 julho 2017.

DIPROSE, R.; STEPHENSON, N.; MILLS, C.; RACE, K.; HAWKINS, G. (2008). Governing the Future: The Paradigm of Prudence in Political Technologies of Risk Management. **Security Dialogue**, vol.39, n.2-3, 2008, p.267-288

DITTRICH, D.; HIMMA, K. Active Response to Computer Intrusions. In: BIGDOLI, H. (ed.). **The Handbook of Information Security**. Hoboken: John Wiley & Sons, 2005.

DUNN CAVELTY, M. (2007) Critical Infrastructures: Vulnerabilities, Threats, Responses. **CSS Analysis in Security Policy**, vol.2, n.16, 2007, p.1-3.

_____. **Cyber-Security and Threat Politics**: US Efforts to Secure the Information Age. London: Routledge, 2008.

_____. The Militarisation of Cyberspace: Why Less May Be Better. NTERNATIONAL CONFERENCE ON CYBER CONFLICTS, 4, 2012, Tallin. Tallin: NATO CCD COE, 2012, p.141-153.

_____. The Normalization of Cyber-International Relations. In: THRÄNERT, O.; ZAPFE, M. (eds.). **Strategic Trends 2015**: Key Developments in Global Affairs. Zurich: CSS, 2015.

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

DUNN CAVELTY, M.; JAEGAR, M. (In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous. **International Political Sociology**, June, vol.9, n.2, 2015, p.176-194.

DUNNE, J.; SKÖNS, E. The Changing Military Industrial Complex. Working Papers from Department of Accounting, Economics and Finance, março de 2011.

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 março 2017.

ENDGAME. Endgame: Endpoint Protection for Enterprises. 2017. Disponível em: <https://www.endgame.com/>. Acesso em: 20 fevereiro 2017.

EPSTEIN, D.; KATZENBACH, C.; MUSIANI, F. Doing internet governance: practices, controversies, infrastructures, and institutions. **Internet Policy Review**, vol.5, n.3, 2016. Disponível em: <http://policyreview.info/articles/analysis/doing-internet-governance-practices-controversies-infrastructures-and-0>. Acesso em 28 janeiro 2017.

ERIKSSON, J.; GIACOMELLO, G. Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State. **International Studies Review**, vol.11, n.1, 2009, p.205-230.

GENERAL DYNAMICS. General Dynamics. 2017. Disponível em: <http://www.gd.com/>. Acesso em: 20 de fevereiro 2017.

GREENBERG, A. Inside Endgame: A Second Act For The Blackwater Of Hacking. **Forbes**, February, 2014.

GROS, F. **States Of Violence: An Essay on the End of War**. London: Seagull Books, 2010.

_____. **Le Principe Sécurité**. Paris: Gallimard, 2012.

HACKING TEAM. Hacking Team. 2017. Disponível em: <http://www.hackingteam.it/>. Acesso em: 23 fevereiro 2017.

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.

HERN, A. Apple's Encryption Means it Can't Comply with US Court Order. **The Guardian**, 8 de setembro de 2015.

HOEPERS, C.; STEDING-JESSEN, K.; CHAVES, M. H. C. P. Honeypots e Honeynets: Definições e Aplicações. NIC.br, 2007. Disponível em: <https://www.cert.br/docs/whitepapers/honeypots-honeynets/>. Acesso em: 1 janeiro 2018.

INTEL SECURITY. McAfee: Antivirus, Encryption, Firewall, Email Security, Web Security, Network Security. 2017. Disponível em: <http://www.mcafee.com/us/index.html>. Acesso: 25 fevereiro 2017.

KASSNER, M. Endpoint Security: What Makes it Different from Antivirus Solutions. **TechRepublic**, 7 de março de 2012. Disponível em: <https://www.techrepublic.com/blog/it-security/endpoint-security-what-makes-it-different-from-antivirus-solutions/>. Acesso em: 23 março 2017.

KASPERSKY LAB. Cyber-security Resource Center for Threats & Tips, Kaspersky Lab. 2017. Disponível em: <https://www.kaspersky.com/resource-center>. Acesso em: 23 fevereiro 2017.

KITCHIN, R.; DODGE, M. **Code/Space**: Software and Everyday Life. Cambridge: The MIT Press, 2011.

KRAUSE, K. Critical Theory and Security Studies: The Research Programme of 'Critical Security Studies'. **Cooperation and Conflict**, vol.33, n.1, 1998, p.298-333.

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

LEANDER A. Chimeras with Obscure Powers: Hybrid States and the Public-Private Distinction. In: THE INTERNATIONAL STUDIES ASSOCIATION WORKSHOP: THE CHIMERICAL STATE AND THE PUBLIC-PRIVATE HYBRIDIZATION OF THE 21ST CENTURY, New York, 2009.

_____. Commercial Security Practices. In: BURGESS, P. (ed.). **Handbook of New Security Studies**. New York: Routledge, 2010.

_____. 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.

LIBICKI, M. C.; SENTY, D.; POLLAK, J. **H4CKER5 Wanted**: An Examination of the Cybersecurity Labor Market. Santa Monica: RAND, 2014.

LOCKHEED MARTIN. Cyber Solutions – Lockheed Martin. Disponível em: http://cyber.lockheedmartin.com/>. Acesso em: 20 fevereiro 2017.

MARCZAK, B.; GUARNIERI, C.; MARQUIS-BOIRE, M.; SCOTT-RAILTON, J. Mapping Hacking Team's "Untraceable" Spyware. **The Citizen Lab Research Brief** n.33, 2014.

MCCARTHY, D. **Power, Information Technology and International Relations Theory**: The Power and Politics of US Foreign Power and the Internet. Londres: Palgrave MacMillan, 2015.

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

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 março 2017.

MCDONALD, N. Is Antivirus Obsolete? **Gartner**, 13 de setembro de 2012. Disponível em: <https://blogs.gartner.com/neil_macdonald/2012/09/13/is-antivirus-obsolete/>. Acesso em: 5 março 2017.

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 março 2017.

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 de fevereiro de 2017.

NORTHROP GRUMMAN. Northrop Grumman Corporation. 2017. Disponível em: <http://www.northropgrumman.com/Pages/default.aspx>. Acesso em 25 fevereiro 2017.

PETERSEN, K.; TJALVE, V. (Neo)Republican Security Governance? US Homeland Security and the Politics of "Shared Responsibility". **International Political Sociology**, vol.7, n.1, 2013, p.1-18.

RAYTHEON. Raytheon Cyber. 2017. Disponível em: <http://www.raytheoncyber.com/>. Acesso em 25 fevereiro 2017

ROSENQUIST, M (2013) 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 janeiro 2017.

SCHNEIER, B. The Vulnerabilities Market and the Future of Security. **Forbes**, 30 de maio de 2012. Disponível em: <https://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/ - 395e728f7536>. Acesso em: 28 janeiro 2017.

_____. The Battle for Power on the Internet. **The Atlantic**, 24 de outubro de 2013. Disponível em: <https://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/>. Acesso em: 28 janeiro 2017.

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 janeiro 2017.

SEGAL, A. The Hacked World Order: How Nations Fight, Trade, Maneuver and Manipulate in the Digital Age. Council of Foreign Relations. New York: PublicAffairs, 2016.

SINGER, P. Corporate Warriors: The Rise and Ramifications of the Privatized Military Industry. **International Security**, vol.26, n.3, 2002, p.186-220.

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 janeiro 2017.

STRAND, J. How I Learned to Love Active Defense. **DarkReading**, *25* de julho de 2015. Disponível em <https://www.darkreading.com/attacks-breaches/how-i-learned-to-love-active-defense/a/d-id/1321361?>. Acesso em: 21 março 2017.

SWARTZ, D. **Culture & Power**: The Sociology of Pierre Bourdieu. Chicago: University of Chicago Press, 1997.

SYMANTEC. Global Leader in Next-Generation Cyber Security. 2017. Disponível em: <https://www.symantec.com/>. Acesso em: 19 fevereiro 2017.

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 fevereiro 2017.