DE OBAMA A TRUMP: O CONTÍNUO DA POLÍTICA CIBERNÉTICA ESTADUNIDENSE

FROM OBAMA TO TRUMP: THE CONTINUUM OF US CYBER POLITICS

Friedrich Maier[1]
UNESP

Resumo

A partir da crescente importância do ciberespaço e das tecnologias de informação e comunicação para a política, economia e sociedade contemporâneas, o artigo tem por objeto a política cibernética dos Estados Unidos da América e sua formulação dentro da agenda de política externa desse Estado. Posicionando a cibersegurança e demais problemas que emergem dessa temática como assuntos intermésticos, o trabalho adota a perspectiva estrutural da política externa norte-americana para avançar a hipótese de um *contínuo iterativo* entre as diversas ações e proposições das administrações sobre o tema. Nesse sentido, procedemos com uma análise documental e histórica das políticas em relação ao ciberespaço do governo Obama e do primeiro ano do governo Trump, procurando especificar se há elementos de continuidade ou de mudança. Nossas conclusões apontam para um posicionamento "especial" da política cibernética dentro do executivo norte-americano, representando uma permanência do objetivo de manutenção da condição hegemônica do Estado, também no "mundo cyber".

Palavras-chave

Ciberespaço. Política externa. Estados Unidos da América. Donald Trump.

Abstract

Regarding the increasing importance of cyberspace to contemporary politics, economics and society, the paper focuses on the United States of America's cybernetic policy and its formulation within its foreign policy agenda. Positioning cybersecurity and other issues that emerge from this theme as intermestic issues, the paper adopts the structural perspective of the North American foreign policy to advance the hypothesis of an iterative continuum between the various actions and propositions of the north american administrations on the subject. In this sense, we proceed with a documentary and historical analysis of policies regarding the cyberspace of the Obama

[1] Mestrando em Ciências Sociais (linha: Relações Internacionais e Desenvolvimento) - UNESP/FFC - Marília

administration and the first year of the Trump government, trying to specify if there are elements of continuity or change. Our conclusions point to a "special" positioning of cybernetic politics within the US executive, representing a permanence of the goal of maintaining the hegemonic condition of the state, also in the "cyber world".
Keywords
Cyberspace. Foreign Policy. United States of America. Donald Trump.

INTRODUÇÃO

Nas quase duas décadas do século XXI a presença do prefixo "ciber" (*cyber*) cresceu nas análises de Ciências Sociais. Neologismos como "cibercultura", "ciberguerra", "cibercrime" e "ciberdiplomacia" ilustram tentativas de compreensão dos fenômenos relacionados ao ciberespaço. No campo das Relações Internacionais (RRII), autores como Kremer e Muller (2014) destacam um processo de ciberização (*cyberization*), isto é, a crescente dependência e influência das relações internacionais com o novo ambiente.

Dada a sua própria natureza multidisciplinar, o conceito de ciberespaço pode ser compreendido por várias perspectivas. Numa definição sintética, é o ambiente gerado a partir da interconexão em rede dos diversos aparelhos de processamento eletrônico, desde computadores de mesa (*desktops*), passando por controladores de tráfego aéreo, até sistemas de controle industrial (SCADA); a partir de uma determinada infraestrutura física (cabos e satélites) e lógica (programação) no qual seres humanos criam, transmitem e operam informações. Portanto, o ciberespaço contempla a Internet, mas não se reduz a ela, abarcando todo o fluxo de informações eletrônicas do globo (Nye, 2010; Kuehl, 2009; Choucri, 2012).

Seja pelo dinamismo da "economia digital", seja pela importância nas infraestruturas críticas, o ciberespaço ganhou lugar nas agendas de política externa. Características como a ação anônima, o baixo custo de entrada e as grandes vulnerabilidades geradas pela ubiquidade dos sistemas eletrônicos são pontos politicamente exploráveis para os Estados. O mundo cibernético se

tornou, assim, um ambiente de ação estatal, de estadismo (*statecraft*) (Malagutti, 2017), cuja especificidade engendra novos problemas para as RRII. Conceitos cristalizados dentro dessa disciplina como atribuição, dissuasão e retaliação encontram dificuldades de aplicação ao "mundo cyber" (Choucri, 2012).

Além disso, casos como os ataques à Estônia (2007) e Geórgia (2008), o vírus Stuxnet na usina de Natanz no Irã (2010), as revelações de Snowden (2013) ou a influência russa nas eleições presidenciais de 2016 dos Estados Unidos da América (EUA) são exemplos variados e fortes dessa consideração, justificando atenção a um tema cuja necessidade de ser pensado como ferramenta de política externa é real (Maker, 2017).

A partir dessa contextualização, surge como problema deste trabalho avaliar como as ações dos primeiros meses do governo Trump a respeito do ciberespaço se relacionam com as definições estratégicas legadas pelo governo Obama (2009/2016). Partindo de uma visão estrutural da política externa dos EUA, nossa hipótese procura demonstrar que no caso da "política cibernética" as estratégias das diferentes administrações apresentam o que Howard e Da Cruz (2017) chamaram de "contínuo iterativo", relação de continuidade, expansão e intensificação das ações, de modo que a nova administração propõe políticas que se pautam nos avanços predecessores, sem a destruição do "legado" anterior. A visão estrutural, ao ponderar o desenvolvimento histórico da política externa estadunidense, permite compreender que as alterações táticas de política externa descendem tanto das diferentes percepções do objetivo estratégico de manutenção da hegemonia internacional quanto das pressões sociais internas da sociedade estadunidense (Pecequilo, 2017).

Nesse sentido, a "percepção de que os Estados Unidos têm a tarefa e o dever de manter a estabilidade global, garantindo a reprodução de um ambiente internacional propício à expansão de seus valores, princípios e objetivos" (Pecequilo, 2005, p. 458) baliza a ação internacional desse Estado cuja política externa

contemporânea reapresenta, sob novas percepções táticas, padrões de comportamento presentes desde a fundação da nação, em 1776 (com destaque à pendularidade uni e multilateral). Cabe ressaltar, isso não reduz todo o desenvolvimento histórico da ação internacional estadunidense a uma simples reiteração de linhas estratégicas do passado, uma vez que a própria processualidade histórica do desenvolvimento tanto do sistema internacional quanto da sociedade estadunidense geram dinâmicas que premem por alterações táticas. Mesmo assim, a visão estrutural indica a permanência do objetivo estratégico de manutenção da hegemonia internacional criada a partir de 1945, e permite dirimir avaliações que identificam excessivos rompimentos nas agendas de política externa dos EUA sobre a temática, considerando-os, como dito, ajustes táticos (idem, pp. 20-1).

Complementando nosso referencial teórico, partimos também da perspectiva de complexidade da formulação da política externa nos EUA, um processo "muito político", permeado por uma constante tensão de responsabilidades entre o Executivo e o Legislativo e sujeito às pressões dos *lobbies* e setores organizados da sociedade (Rosati, Scott, 2011). Nosso trabalho foca, portanto, apenas em um dos poderes – ressalte-se o fato de que na política cibernética historicamente a assertividade do Executivo é maior.

Além do panorama interno de múltiplas pressões, a profunda relação da ordem internacional atual com o Estado norte-americano (Ikenberry, 2011) reflete na divisão dos assuntos de política desse país como domésticos, internacionais e "intermésticos" (mescla entre doméstico e internacional) (Rosati, Scott, 2011, pp. 64-66). O ciberespaço e a cibersegurança, seguindo este raciocínio, são assuntos "intermésticos" por excelência, uma vez que políticas dessa área envolvem a necessidade de cooperação internacional e entre amplos setores da sociedade (empresarial, acadêmico, militar) para alcançarem efetividade (Hurwitz, 2014; Maker, 2017).

Deste modo, para atingir nossos objetivos, procedemos na primeira seção, com uma breve descrição do "legado"

estratégico da administração Obama para o ciberespaço, a partir dos documentos oficiais *"Cyber Policy Review"* (2009), *"International Strategy for Cyberspace"* (2011) e "*Cybersecurity National Action Plan*" (2016) e das principais ações do governo sobre o tema. Na segunda seção, apresentamos a compilação e análise de atos internos e externos da administração Trump sobre o ciberespaço entre os meses de janeiro e dezembro de 2017. Foram considerados como da administração Trump: a) os documentos oficiais e notícias divulgados sob responsabilidade da Casa Branca; b) as declarações oficiais do próprio presidente Trump, do Secretário Oficial de Imprensa Sean Spicer (até sua renúncia em julho de 2017), do vice-presidente Mike Pence e de conselheiros presidenciais sobre o assunto da cibersegurança (em conferências de imprensa). Por fim, na seção de considerações finais apresentamos nossa avaliação sobre o primeiro ano da administração Trump e seu relacionamento com o legado Obama, recuperando os principais pontos da argumentação.

A Política Cibernética da Era Obama

Barack Obama assumiu o cargo de presidente dos EUA em 2009, num contexto nacional marcado pela crise econômica e por profundas fraturas sociais (Pecequilo, 2012). A crise de 2007/2008 trouxe novamente à tona o debate sobre o declínio estadunidense, sobretudo em comparação com o panorama de ascensão da China. O novo presidente pautou sua campanha num ideário de esperança em relação ao futuro, sua tarefa era reunificar a sociedade estadunidense, contornar a crise e o desemprego e retomar o crescimento.

Internacionalmente Obama herdou um cenário de resignação; a crise econômica dos países desenvolvidos contribuiu para a estagnação nos fóruns multilaterais tradicionais. Soma-se o desafio de países emergentes e em desenvolvimento, cujas alianças de geometria variável acenavam para novos padrões de cooperação

e tomada de decisão (Pecequilo, 2012). Por fim, o unilateralismo agressivo de Bush filho no pós-11/09, somado às duas guerras no Oriente Médio e à errática postura intervencionista na América Latina causaram uma erosão na capacidade estadunidense de liderança, ao mesmo tempo que os "novos temas" premiam por medidas multilaterais – ciberespaço incluso.

Nesse breve cenário a postura de política externa do presidente alternou num padrão que poderemos chamar de "pendular": justapôs a assertividade multilateral na retórica com uma prática unilateral em muitos momentos. Como exemplo desse padrão, ao mesmo tempo que acenava aos países emergentes o "novo" espaço que teriam no panorama internacional, pautado na cooperação e reestruturação do sistema de governança, Obama negava o diálogo entre os EUA e as diversas alianças de geometria variável, numa estratégia de "dividir para conquistar" (Pecequilo, 2012, pp. 27-28). O mesmo padrão pendular pode ser utilizado para classificar a atuação do presidente para o ciberespaço, como mostraremos a seguir.

Ações para o ciberespaço

Obama posicionou o ciberespaço e a cibersegurança como objetivos centrais de sua administração. Pouco tempo após a posse estabeleceu uma comissão para avaliar a situação de toda a estrutura crítica de Tecnologia da Informação (TI) das redes federais, bem como a resiliência e a capacidade de resposta dos EUA à ataques e invasões cibernéticas em 60 dias. Os resultados dessa avaliação plasmaram-se no *"Cyberspace Policy Review"* (Estados..., 2009) e numa série de medidas de curto e médio prazo, com o objetivo de aperfeiçoar a estrutura institucional adequada à liderança dos EUA no campo cibernético.

Cabe ressaltar que as iniciativas de Obama não aconteceram no vácuo. Antes dele, Bush filho teria duas ações importantes no tema. Em 2003, lançava a primeira estratégia voltada exclusivamente ao ciberespaço e à cibersegurança do país, a "*National Strategy to Secure Cyberespace"*. Quase ao final de seu

mandato, em 2008, Bush lançou a "*Comprehensive National Cybersecurity Initiative"* texto que serviu de base para as ações de Obama e já previa a necessidade de construção de uma linha de defesa cibernética robusta (Pereira, 2013, pp. 45).

Nesse sentido, as constatações do *Policy Review* ressonavam documentos anteriores, ressaltando que a extrema dependência dos EUA para com suas redes cibernéticas gerava vulnerabilidades com grande capacidade disruptiva (Estados..., 2009). Além disso, apresentou uma sólida visão da própria natureza do ciberespaço, que engendra a necessidade de cooperação do governo tanto internacionalmente, quanto nacionalmente[2]. O documento ainda posicionava planos de ações de curto e médio prazo, como criação do cargo de "chefe de cibersegurança" no Conselho de Segurança Nacional, o estímulo à formação e contratação de pessoal especializado, bem como a criação de uma campanha nacional de conscientização (idem, pp. 37-8).

Às medidas apresentadas pelo *Policy Review* seguiram-se dois marcos importantes dessa administração. O primeiro é o lançamento, ainda em 2009, do Comando Cibernético dos EUA (*United States Cyber Command*, doravante USCYBERCOM), um subcomando do exército cuja missão era adquirir capacidade para condução de operações militares completas no ciberespaço, operacional desde outubro de 2010. O segundo ponto foi o lançamento da "*International Strategy for Cyberspace"* (Estados..., 2011), a primeira estratégia internacional de uma administração dos EUA para o ciberespaço.

Esse texto é uma grande exortação para a cooperação internacional e entre os setores nacionais para avançar medidas de securitização do ciberespaço. A premência da segurança da Internet é ressaltada a cada capítulo e balizada por preocupações: as políticas para o ciberespaço devem ser inteligentes o suficiente para garantir

[2] Dado que a maior parte das infraestruturas relacionadas ao ciberespaço são propriedade de empresas privadas, que também possuem grande *expertise* no campo da cibersegurança.

as características de liberdade de expressão, privacidade e propriedade intelectual; pontos considerados centrais para a continuidade da inovação proporcionada pelo mundo cibernético (Estados..., 2011, pp. 07-11). A retórica do excepcionalismo estadunidense, mais um elemento aqui considerado como de continuidade no desenvolver histórico da política externa estadunidense, também se faz presente nesse documento: a liderança pelo exemplo acontece também no ciberespaço[3].

No que se refere à cooperação, essa deve acontecer entre os Estados interessados na normatização do novo ambiente (*likeminded States*) e em organismos multilaterais (Hurwitz, 2014; Estados..., 2011, p. 12-3). A estabilidade do ciberespaço, portanto, deve se pautar por uma "garantia pelas normas" assim como acontece em "outras esferas das relações internacionais". A essa visão normativa, segue-se que as regras já em vigor do direito internacional e consuetudinário se aplicam ao ciberespaço, não obstante, "atributos únicos" do ambiente precisarão de novas regras, cuja base será a defesa das liberdades fundamentais, o respeito à propriedade, a valorização da privacidade, à proteção contra o crime e o direito à autodefesa[4].

Às exortações de cooperação seguem-se as ameaças contra todos aqueles que desejam atingir os EUA pelo ciberespaço. A dissuasão assume um importante papel. A administração compromete-se com a avaliação de todas as possibilidades de

[3] Como em: "[o]s Estados Unidos devem sinalizar ao mundo que estão sérios sobre como lidar com esse desafio com forte liderança e visão. A liderança deve ser elevada e fortemente ancorada na Casa Branca para fornecer orientação, coordenar ações e alcançar resultados." (Estados..., 2011, p. III, trad. nossa)

[4] Observa-se, claramente, a reposição do atual *status quo* internacional para o mundo cibernético, como em: "Os EUA trabalharão internacionalmente para promover uma infraestrutura de comunicação e informação aberta, interoperável, segura e confiável que apoie a economia internacional e o comércio, fortaleça a segurança internacional e estimule a liberdade de expressão e inovação. Para atingir esse objetivo, nós construiremos e sustentaremos um ambiente no qual normas de comportamento responsável guiarão ações estatais, sustentarão parcerias e suportarão o estado de direito no ciberespaço" (Estados..., 2011, p. 08, trad. nossa)

retaliação para responder à ataques, "quer a ameaça provenha de terroristas, cibercriminosos ou estados e seus mandatários (*proxies*)" (Estados..., 2011, p. 12, trad. nossa).

> Todos os Estados possuem um direito inerente à autodefesa, e reconhecemos que certos atos hostis realizados através do ciberespaço podem obrigar ações sob os compromissos que temos com nossos parceiros nos tratados militares. Reservamo-nos **o direito de usar todos os meios necessários** - diplomáticos, informativos, militares, e econômicos - conforme apropriado e consistente com o direito internacional aplicável, **para defender nossa nação, nossos aliados, nossos parceiros e nossos interesses** (idem, p. 14, negrito nosso)

A *International Strategy* lançava ao mundo os preceitos básicos de negociação internacional dos EUA para o campo do ciberespaço e cibersegurança. A ameaça da retaliação, em caso de ciberataques, é um ponto de inflexão numa tentativa de criação de padrões de comportamento pautados na dissuasão, por mais que sua eficácia ainda não seja provada[5].

Chegamos ao último documento selecionado para essa seção, o "*Cybersecurity National Action Plan*" (Estados..., 2016). Lançado no último ano da administração Obama o plano é

[5] A dissuasão no ciberespaço não é tão simples. Isso porque a atribuição de determinado ataque, elemento clássico dentro das teorias de dissuasão, é difícil de ser determinada, dados os inúmeros mecanismos de triangulação de navegação existentes. Normalmente atribuir o ataque a uma determinada nação envolve longos processos de contrainteligência, o que mina a capacidade de resposta rápida. Além disso, existem questões como proporcionalidade da retaliação (no ciberespaço é difícil determinar a exata amplitude de um ataque), bem como a profundidade dos efeitos secundários de um ataque (um ciberataque direcionado a determinada rede pode causar efeitos secundários em outras redes, ou ainda pode acontecer em ondas de impacto, com intervalos entre si) são problemáticas importantes. Para mais informações ver: Burns, Cohen, 2017; Nye 2011.

claramente uma base para a construção da política cibernética do próximo presidente, propõe robustos investimentos no campo da cibersegurança para o ano fiscal de 2017 – US$ 3,1 bilhões para um fundo de modernização de estruturas federais de TI e US$ 19 bilhões para gastos com cibersegurança em geral.

O documento toca ainda outras medidas importantes, como criar a "*Commission on Enhancing National Cybersecurity*" com integrantes do setor privado e especialistas de fora do governo, implementar medidas para contratação de pessoal qualificado bem como fortalecer a formação educacional de novos profissionais, dobrar o número de equipes de defesa cibernética no Departamento de Segurança Nacional (DHS, em inglês) e, mais importante, criar uma estrutura unificada para controles técnicos e de gestão de risco à cibersegurança (*Framework for Improving Critical Infrastructure Cybersecurity*, doravante "o *framework*").

Balanços da Era Obama

Conforme ressaltamos no começo dessa seção, a política externa de Obama marcou-se por uma atividade pendular, entre a retórica multilateralista e a ação unilateral. No ciberespaço esse movimento foi semelhante. Sua administração foi a mais profícua no lançamento de documentos, planos, relatórios e leis sobre o tema (Howard, Da Cruz, 2017). A cooperação internacional figurava como uma das bases dessas políticas, propondo uma normatização do mundo cibernético em aspectos muito próximos ao atual *status quo* internacional. Ao lado dessas questões, a segurança da rede deveria garantir tanto a privacidade quanto a liberdade. Porém, tais aspectos apresentaram contradição no plano prático.

A começar pela cooperação internacional, o governo Obama tentou avançar sua pauta em organismos multilaterais, como demonstra a participação dos EUA no "Grupo das Nações Unidas de Especialistas Governamentais em Desenvolvimento no

Campo das Comunicações e Telecomunicações no Contexto de Segurança Internacional" (doravante GGE, sigla em inglês). Contudo, alguns acontecimentos minaram parte da capacidade estadunidense de gerar consenso nos órgãos multilaterais. Em 2010 o vírus Stuxnet foi revelado e dois anos depois, uma reportagem do *The New Tork Times* (Sanger, 2012) revelou o *Olympic Games*, uma sofisticada operação cibernética conjunta com Reino Unido e Israel com o objetivo de atacar o Irã e seu programa nuclear. A administração Obama autorizou a destruição de infraestrutura física por meio de um ataque cibernético – até hoje não reconhecido oficialmente pelos perpetradores[6]. Argumentos apontam o ataque como um ato de guerra (Knoepfel, 2014).

Em mesmo diapasão, os milhares de documentos secretos vazados por Edward Snowden, ex-funcionário de uma empresa de serviços contratada pela *National Security Agency* (NSA), por meio do site *Wikileaks* revelaram a existência do PRISM, um programa de espionagem extensiva que a administração Obama utilizava para monitorar não somente seus cidadãos, mas também cidadãos de outros países. E-mails, telefonemas, mensagens de texto e metadados de milhões foram vigiados e armazenados. A espionagem em massa não poupou nem agentes governamentais e atingiu, como exemplos, as presidentas Angela Merkel e Dilma Roussef, além de altos funcionários da estatal brasileira Petrobrás (Greenwald, 2014).

Pertinente lembrar, o presidente Obama escreveu, ao introduzir a *International Strategy,* que os EUA enfrentariam os novos

[6] A República Popular Democrática da Coreia também foi alvo de ataques cibernéticos, dentro da lógica *"left of launch*" promovida pela gestão Obama, cujo objetivo era impedir o progresso norte-coreano nos mísseis balísticos intercontinentais antes destes sequer chegarem nas plataformas de lançamento. "O general Martin E. Dempsey, presidente do *Joint Chiefs of Staff*, anunciou o programa, dizendo que "guerra cibernética, energia dirigida e ataque eletrônico", uma referência a coisas como malware, lasers e bloqueio de sinal, tornaram-se importantes novos complementos às formas tradicionais de defletir ataques inimigos." (Sanger, Broad, 2017).

desafios de criminalidade e agressão no ciberespaço de uma "forma consistente com os princípios que defende[m]: **liberdade de expressão e associação, privacidade e livre fluxo de informações**" (Estados..., 2011, negrito e tradução nossos). Ponto de indício de uma "dupla padronização" que corriqueiramente acontece no comportamento de política externa dos EUA para os "novos temas": as regras direcionadas a outros Estados não recebem paralelo de cumprimento estadunidense (Pecequilo, 2012, p. 151).

Diante desses pontos, as revelações do caso Snowden dificultaram a capacidade de liderança dos EUA em relação ao ciberespaço e à cibersegurança, ao explicitarem uma postura unilateral e agressiva em operações de inteligência cujos objetivos poderiam ser militares, políticos, econômicos, científicos e tecnológicos. Burns e Cohen (2017) comentam como os vazamentos também pioraram as relações com o setor empresarial nos EUA. Entendemos, portanto, que esses fatores também foram decisivos para a falta de acordo em ações de normatização multilaterais para o ciberespaço[7].

Obama também avançou alguns pontos de entendimento bilateral. O maior deles foi com a China, em 2015. Ambos acordaram a aceitação mútua de que nenhum dos Estados promoveria ou permitiria a espionagem cibernética em alvos da outra parte – principalmente no setor privado, resguardando o direito de propriedade intelectual (Maker, 2017).

Em síntese, na administração Obama o ciberespaço foi um elemento de destaque. Suas estratégias foram importantes marcos no processo de securitização desse novo ambiente[8]. Além

[7] Além disso, cabe destacar o papel cada mais assertivo de países como China e Rússia (e também Brasil) em promover visões alternativas de regulação do ciberespaço, como veremos mais à frente.

[8] Nesse ponto destaco as contribuições de estudos pautados pela perspectiva da securitização, centrada na Escola de Copenhague. Pereira (2013) a partir de uma revisão dos documentos lançados por Obama em relação ao ciberespaço, conclui a associação do tema a uma gramática comum ao *status quo* internacional, pautada na visão estadocêntrica e na segurança internacional. Halvordsson (2012) ao

disso, suas linhas táticas avançaram uma perspectiva multilateral e de cooperação internacional positiva. Os acontecimentos dos anos de 2012 e 2013, todavia, minaram essa perspectiva ao revelarem o aspecto contraditório do governo Obama – dificultando entendimentos multilaterais para o assunto.

Em geral, seu legado para a área de cibersegurança é comumente avaliado de forma positiva (Howard, Da Cruz, 2017), dado os importantes passos para a consolidação de uma política cibernética nacional mais robusta, como demonstram o USCYBERCOM, o *framework*, as estratégias e o estabelecimento do CNAP. Contudo, críticos apontam certa "passividade" na tentativa de propor soluções de dissuasão/retaliação mais críveis (principalmente contra o *hacking* das eleições estadunidenses em 2016, perpetrado pela Rússia) (Groll, 2016; Maker, 2017). Veremos na próxima seção como as ações do primeiro ano de governo Trump atuam sobre esse legado.

Ações de Política Cibernética nos primeiros do governo Trump

Avançando na argumentação, essa seção ponderará os principais pontos da administração Trump em relação ao ciberespaço durante seus primeiros meses no governo dos EUA. Começando por uma contextualização mais geral, o presente trabalho corrobora a visão estrutural também no que se refere à política estadunidense, como afere Pecequilo (2017). Nessa perspectiva, Trump, ao invés de um "ponto fora da curva", representa a reposição das forças neoconservadoras na cena política estadunidense. Cabe lembrar que além do presidente, também o Senado e a Câmara eleitos em 2016 possuem maioria republicana,

refletir especificamente sobre o *Cyberspace Policy Review* chega à conclusões semelhantes, apontando o claro movimento de securitização que o documento contém.

partido que tende a agremiar as principais forças conservadoras do país. Portanto, podemos encontrar similaridades entre a atual administração e a era Bush Filho (2001/2008), também republicana (idem).

Desde sua campanha, Trump explicitava uma posição de política externa alinhada aos pressupostos neoconservadores, agressiva e unilateralista, como demonstram os slogans "América Primeiro" (*America First*) e "Torne a América Grande Novamente" (*Make America Great Again*). Propostas como a continuação da construção de um muro na fronteira com o México, o banimento de imigrantes de determinados países, a desconsideração ao regime internacional de proteção ao meio ambiente e o "retorno dos empregos roubados pela globalização" (caracterizada com feições chinesas) são pontos ilustrativos.

Quando questionado sobre o ciberespaço, o presidente, ainda em campanha, tinha resposta vagas, mas que apontavam para uma visão belicista do problema[9]. Em geral, apontava a necessidade de maior capacidade de resistência e dissuasão. Dentro de sua plataforma de governo, o ciberespaço se associava com a necessidade premente de reequipagem das Forças Armadas, "esquecidas" por administrações anteriores. O presidente atuou no assunto tanto internamente quanto externamente.

Internamente, ações como a nomeação de um especialista em cibersegurança para a Secretaria da Marinha, o encontro com representantes do setor privado de cibersegurança ainda na segunda semana do governo e uma campanha de conscientização sobre a segurança na Internet durante a "Semana Nacional de Proteção ao Consumidor" em março de 2017 davam indicativos de atenção ao tema nos primeiros meses de governo.

[9] Em um debate eleitoral (25/09/2017) Trump realizou um discurso confuso quando questionado sobre ciberataques, tornando-se alvo de sátiras (LAFRANCE, 2016). Em um evento de campanha (03/10/2017) afirmou "Como dissuasão contra ataques a nossos recursos críticos, os Estados Unidos devem possuir ... a capacidade inquestionável de lançar contra-ataques cibernéticos incapacitantes. Quero dizer, incapacitantes mesmo." (NEWMAN, 2016, tradução nossa).

Pouco tempo depois, a administração Trump lançava seu primeiro esboço de orçamento para o ano de 2018 (Estados..., 2017a). "*America First: A Budget Blueprint to Make America Great Again*" centra o foco de investimento do novo governo dos EUA em defesa e segurança, promovendo cortes em todos os outros departamentos do governo, propõe um adicional de US$ 54 bilhões com gastos de defesa, atingindo um total agregado de US$ 639 bilhões para o setor. Todo o orçamento tem por base os "núcleos duros" que a administração Trump escolheu: efetividade, eficiência, cibersegurança e responsabilidade fiscal (*accountability*).

O posicionamento da "cibersegurança" como núcleo duro do governo ressalta a centralidade da questão, com diretivas para vários departamentos. O departamento de Comércio deve representar o governo em fóruns e encontros sobre a governança da internet e comércio eletrônico. O Departamento do Tesouro, o Departamento de Energia e a NASA deverão reforçar suas infraestruturas de TI. Dentro do Departamento de Justiça, o FBI receberá US$ 61 milhões para o combate ao terrorismo e às ameaças cibernéticas (Estados..., 2017a) Já no Departamento de Defesa (DoD, em inglês) o orçamento garantirá que os EUA "permaneçam a força militar melhor comandada, melhor equipada e melhor preparada no mundo" (idem, p. 16). As somas extras de dinheiro: "Definem a base de uma força conjunta maior, mais capaz e mais letal, impulsionada por uma nova Estratégia de Defesa Nacional que reconhece **a necessidade de superioridade americana**, não só na terra, no mar, no ar e no espaço, mas **também no ciberespaço**." (idem, ibidem, ênfase e tradução nossas).

Enquanto isso, o DHS, único departamento que receberá aumentos além do DoD, deverá priorizar a operações de aplicação de lei, segurança fronteiriça e "financiar o desenvolvimento contínuo de fortes defesas de cibersegurança" (Estados..., 2017a, p. 23). Nesse sentido, receberá US$ 1,5 bilhões

para atividades de proteção das infraestruturas críticas e redes federais[10].

Todavia, é em maio de 2017 que o governo Trump lança uma de suas maiores medidas sobre o ciberespaço – certamente a mais publicizada pela administração – a Ordem Executiva 13800 "*Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*" (Estados..., 2017b). A medida é uma grande revisão da política cibernética estadunidense, estabelecendo prazos para que as principais agências e departamentos do governo produzam relatórios sobre o estado e a resiliência da estrutura cibernética em nível federal e sobre a capacidade de resposta em caso de ataques.

Além disso, a ordem torna os chefes das agências federais responsáveis pela cibersegurança de suas jurisdições e propõe estudos sobre a centralização das redes de TI. A adoção do *framework* para cibersegurança em todas as agências federais torna-se obrigatória. Por fim, menciona ainda a produção de uma estratégia de engajamento internacional para a cooperação em cibersegurança – o que indica a substituição da estratégia cunhada por Obama em 2011. A ordem executiva foi alvo de grande propaganda. Declarações de imprensa, notícias oficiais e falas de representantes do governo reforçaram a ação do presidente, pontuando-a sempre como um passo para o cumprimento da promessa de campanha de Trump (The White House, 2017a).

Enquanto a Ordem Executiva traz a impressão de uma administração que se mobiliza para lidar com as questões cibernéticas, em agosto a elevação do USCYBERCOM para um "Comando Combatente Unificado" representa um passo na consolidação do órgão que, talvez, seja o mais importante advindo da era Obama. Com a elevação, o comando ganha maior

[10] Agindo "[a]través de um conjunto de ferramentas avançadas de cibersegurança e de uma defesa mais assertiva das redes governamentais, o DHS compartilharia mais informações de incidentes de segurança cibernética com outras agências federais e o setor privado, levando a respostas mais rápidas aos ataques de segurança cibernética dirigidos a redes federais e infraestruturas críticas (Estados..., 2017a, p. 24, trad. nossa)

autonomia operacional e poder de compra, conferindo-lhe mais autoridade sobre as questões cibernéticas (The White House, 2017b). Apesar disso, continua ligado à NSA o que suscita problemas de operação[11].

Mais três ações de política interna são importantes para o trabalho que aqui se propõe. A declaração do mês de outubro enquanto "Mês de Consciência Nacional para a Cibersegurança", convida os cidadãos estadunidenses a aprender com a campanha "*Stop. Think. Connect*" criada pelo DHS em 2010, sob a gestão Obama. Ainda em outubro, o presidente escolhe Kirstien Nielsen para Secretária do DHS, aplaudida pela mídia especializada em cibersegurança, dado sua experiência no campo. Importante mencionar que Nielsen também foi funcionária do governo Bush filho.

Em novembro, Trump promove ação cuja significância avançaria questões centrais para a cooperação entre setor público e privado. Um documento sobre o processo de tomada de decisão entre publicação ou retenção de vulnerabilidades em *softwares* e sistemas operacionais descobertos por agências do governo (doravante VEP, sigla em inglês) foi bem recepcionado pelas empresas de tecnologia. Basicamente informa que o processo de avaliação de vulnerabilidades acontece a partir de um conselho compostos por especialistas de diversas áreas do governo e não

[11] NSA e USCYBERCOM compartilham o mesmo prédio e respondem ao mesmo chefe. Tensões operacionais surgem dado os propósitos divergentes dos dois no ciberespaço: coleta de informações e operações militares respectivamente. "Esta tensão veio à tona quando o presidente Barack Obama [...] ordenou ao Comando Cibernético que tomasse ações mais agressivas contra o Estado islâmico no ciberespaço. Enquanto os operadores militares podiam fechar facilmente a infraestrutura de comunicação do Estado islâmico, a NSA às vezes preferia bisbilhotar esses sistemas em vez de matar um servidor que poderia ser facilmente recriado em outro lugar longe dos olhos curiosos da agência." (Groll, 2017, trad. nossa).

somente funcionários das agências de inteligência[12]. Outra ação recepcionada positivamente pelo setor privado, principalmente na segurança digital, foi o anúncio pelo DHS do banimento de um programa antivírus desenvolvido pelo laboratório russo *Kaspersky Lab* (Department..., 2017; Marks, 2017a)

Como ressaltado em nossa introdução, o ciberespaço e as políticas de cibersegurança são assuntos intermésticos por excelência. As ações internas de Trump podem ser compreendidas dentro de um panorama de reforço do ciberespaço estadunidense com acenos à cooperação com o setor privado, apesar de um claro afã militarista. Porém, considerando a interoperabilidade das redes, ações internas não são suficientes para lidar com todos os problemas. Assim, a cooperação internacional revela-se ponto chave para um política cibernética efetiva (Maker, 2017). Cabe ressaltar, esse entendimento já estava presente nos documentos produzidos na era Obama e serão trabalhados no novo governo.

Os sinais de campanha de uma política externa unilateral e agressiva permaneceram após a eleição de Trump. Alçado ao cargo, "enviou um relatório ao Congresso, no início de março, apresentando uma agenda que enfatiza a **preferência por acordos bilaterais, em detrimento dos multilaterais**." (Magnotta, 2017, p. 4, ênfase nossa). Na política cibernética, um indicativo dessa postura foi o fechamento do Escritório do Departamento de Estado para coordenação cibernética (*State Department cyber coordinator's office*), organismo responsável pela representação multilateral e bilateral dos EUA para negociações na temática (Marks, 2017a).

Seguindo a lógica mais unilateralista, há menção à cooperação no ciberespaço em declarações bilaterais dos EUA com 15 Estados, nos quais se destacam parceiros tradicionais (Reino Unido, Canadá, Austrália, Israel) e países asiáticos (China, Índia,

[12] A versão desclassificada do "*Vulnerabilities Equities Policy and Process for the United States Government*" (Estados…, 2017c) fez a administração Trump ser elogiada pela transparência no campo da política cibernética pela *American Civil Liberties Union* (ACLU) (Price, 2017).

Coreia do Sul, Malásia, Cingapura e Vietnã). Grupos de trabalho bilaterais em assuntos cibernéticos foram montados na Argentina e em Israel.

O entendimento bilateral também é utilizado em relação à China, um dos maiores perpetradores de espionagem cibernética do mundo. Em abril, data da visita do premiê chinês aos EUA, a administração Trump anunciou a elevação das conversas bilaterais entre os países para um "Diálogo Compreensivo" tendo por um dos pilares centrais o diálogo de "Aplicação da Lei e Cibersegurança" (The White House, 2017f). Além disso, quando da visita de Trump à China, em novembro, uma declaração conjunta reafirmou os compromissos acordados em 2015 por Obama (redução das operações cibernéticas entre si) (The White House, 2017e).

Refreando a participação estadunidense nos fóruns multilaterais mais amplos, a tática de Trump para avançar projetos de securitização e normatização do ciberespaço passa – assim como em Obama – pela cooperação com os "estados que pensam igual" (*likeminded States*). Tom Bossert funcionário do DHS e conselheiro para a área de cibersegurança, representando Trump na *CyberWeek* de 2017 em Israel, ressalta esse tom ao destacar que os EUA não veem mais o GGE como o ambiente ideal para as negociações do tema, buscando outras formas de trabalho[13].

Além disso, a retirada dos EUA da agência do sistema das Nações Unidas UNESCO reafirma essa tendência de

[13] O conselheiro disse: "Devemos nos mover de falas sobre normas para sua implementação. Mas também devemos responsabilizar os que violam essas normas. Isso pode não ser possível através de um esforço da ONU. Na semana passada, vimos os limites do Grupo de Especialistas Governamentais das Nações Unidas, que obteve bons resultados no passado, mas acabou cedo. Eles não conseguiram nem chegar a um consenso sobre o relatório final. É hora de considerar outras abordagens. Também trabalhamos com grupos menores de parceiros que pensam igual para apontar o mau comportamento e impor custos aos nossos adversários. Também perseguiremos acordos bilaterais quando necessário" (The White House, 2017d, trad. nossa)

esvaziamento dos fóruns multilaterais[14]. Em algumas avaliações, esse movimento cede espaço para a pressão de modelos não democráticos de governança da Internet e do ciberespaço, propostos por grandes competidores, como China e Rússia (Marks, 2017a). Tais pressões implicam, no caso da dissuasão, a centralidade da cooperação com estados parceiros[15].

Antes de concluir, nenhuma pesquisa sobre o governo Trump e as políticas cibernéticas pode deixar de lado os problemas com a Rússia. Desde os meses finais de 2016 investigações sobre a interferência russa nas eleições presidenciais levantam suspeitas sobre intenções do Kremlin de beneficiar Trump na corrida eleitoral. O presidente eleito apresentou comportamento pendular sobre o tema, colocando em descrédito a própria capacidade da Central Intelligence Agency (CIA, em inglês) sobre o assunto (Donald..., 2016). Posteriormente, aceitou a possibilidade de interferência russa e chegou a conversar com o presidente russo sobre o assunto, durante o encontro do G20 de 2017 (The White House, 2017c). Apesar do diálogo e das afirmações do secretário Tillerson e do conselheiro Bossert sobre a formulação de novos ambientes de negociação entre os países, nenhuma ação foi divulgada. Trump enfrenta desde sua posse forte oposição

[14] Cabe lembrar, em 2013 a UNESCO se tornou palco de pressão de países como China, Brasil e Rússia para uma atuação mais forte na promoção de debates e entendimentos multilaterais sobre o ciberespaço e governança da Internet (Lynch, Groll, 2017).

[15] Como a declaração de Bossert revela: "Embora não abandonem nossos esforços multilaterais, os Estados Unidos avançarão internacionalmente em esforços bilaterais significativos, como o que usufruem com a Grã-Bretanha e agora com Israel, enquanto continuam a construir uma coalizão de parceiros de interesses próximos que possa atuar em conjunto. O próximo passo deve ser ganhar cooperação internacional para impor consequências sobre aqueles que atuam contrariamente a esse crescente consenso. Para conseguir isso, os estados com ideias semelhantes devem trabalhar para desenvolver opções para impor consequências dentro de uma estrutura de coalizão, se possível. Até então, os Estados Unidos devem buscar parceiros bilateralmente." (The White House, 2017d, trad. nossa)

midiática e partidária (inclusive dentro do seu próprio partido), no qual a possibilidade de conluio com os russos é um agravante.

Críticas ao presidente surgiram ainda em outro caso. No final de agosto, mais de um quarto dos funcionários do Conselho Consultivo Nacional de Infraestrutura (do DHS), um dos órgãos de maior importância na proposição de políticas cibernéticas, pediram demissão acusando o presidente de "atenção insuficiente" às vulnerabilidades cibernéticas do país.[16] (Marks, 2017b). O acontecimento trouxe preocupações para o setor de cibersegurança que aproveitou-se do caso para apontar a falha do governo em entregar os relatórios previstos na Ordem Executiva 13800 (Newman, 2017; Ackerman Jr, 2017)[17].

Resumindo a argumentação até aqui, comentamos nessa seção os principais pontos de ação da administração Trump sobre o ciberespaço. Desde as primeiras semanas no governo o presidente deu indicativos da importância do tema para seu governo. Nesse sentido, apontamos como os problemas cibernéticos associaram-se com a premência de modernização e reforço das forças armadas dos EUA, uma das bandeiras da administração Trump, como o esboço de orçamento para 2018 demonstra. Tal visão preocupa especialistas, pois posiciona o ciberespaço excessivamente dentro da lógica militar (Maker, 2017). Mesmo assim, houve acenos à cooperação com o setor privado,

[16] Os funcionários citaram ainda a falta de capacidade de Trump para lidar com as questões morais da nação, referência à declarações erráticas de Trump sobre os acontecimentos de Charllotesville, quando um jovem negro morreu num embate entre manifestantes neo-nazistas e supremascistas brancos e militantes antifascistas. O conteúdo completo da carta de resignação, obtido pelo site de notícias Nextgov, se encontra em:
<http://www.nextgov.com/media/gbc/docs/pdfs_edit/082417jm1.pdf>
Acesso em: 01 dez 2017.

[17] O posicionamento oficial da administração sobre esse assunto é de que os relatórios continuam a ser produzidos e entregues dentro dos prazos e que a publicação futura variará no tempo (NEWMAN, 2017).

como nos casos da publicação do *VEP* e no banimento do antivírus russo *Kaspersky* das redes governamentais.

Enquanto atuava no reforço da infraestrutura crítica e institucional interna para lidar com problemas cibernéticos, Trump imprimiu às políticas externas dessa temática seu caráter unilateral, presente nas declarações de Bossert em Israel e nos múltiplos entendimentos bilaterais que tocam, mesmo que de relance, no tema. Pontuando um aparente imobilismo dentro das soluções multilaterais para o ciberespaço, a administração volta-se para parceiros tradicionais e estados parceiros, na busca de mecanismos de dissuasão e normatização.

Diante desse quadro, resta-nos a pergunta central de nossa pesquisa. Na temática do ciberespaço, como Trump se relaciona com o legado deixado por Obama?

CONCLUSÕES FINAIS

A manutenção do objetivo estratégico no ciberespaço

Desfazendo as visões que encontram rupturas excessivas, o presente artigo corrobora, com uma base factual mais ampla, o argumento lançado por Howard e Da Cruz (2017) sobre o histórico de "contínuo iterativo" das políticas cibernéticas dos sucessivos governos dos EUA. Para os autores, a preocupação com a segurança das redes e infraestruturas críticas aparece desde a administração Clinton, com o Ordem Executiva 13011 em 1996 e se desenvolve desde então (idem, p. 08-09).

Nesse sentido, Obama construiu seu legado cibernético sob as diretivas da "*Comprehensive National Cybersecurity Initiative"* de Bush filho. Da mesma forma, observamos em Trump a continuidade de muitas das políticas de seu antecessor. A implementação obrigatória do *framework* para todas as agências do governo, a elevação do USCYBERCOM e a adoção da campanha de conscientização *"Stop. Think. Connect*" são indicativos dessa

continuidade. Ademais, a cooperação com os setores nacionais, prevista nas principais políticas de Obama, também apresentou avanços como vimos no caso do VEP.

Até mesmo no campo da cooperação internacional não podemos mencionar uma ruptura com a postura anterior. Não devemos esquecer que enquanto Obama buscava a liderança dos EUA no campo cibernético por meio de ambientes multilaterais, também lançava operações de espionagem cibernética contra seus parceiros; uma clara contradição entre a retórica multilateral e a ação unilateral e agressiva. Ponto que ressalta o padrão comumente ambíguo da política externa estadunidense, pendular entre o uni e o multilateralismo (Pecequilo, 2012, p. 178), como já mencionado.

Nesse sentido, as movimentações de Trump para o entendimento bilateral e com grupos de estados com interesses compatíveis são frutos da percepção tática de que os EUA ainda não possuem capacidade de avançar sua agenda sobre o ciberespaço apenas no campo multilateral, principalmente pela existência de grandes competidores nesses ambientes, como China e Rússia, e pela imagem negativa que as revelações do caso Snowden trouxeram.

Mesmo assim, a cooperação dentro do ciberespaço é necessária ao país. Apesar de certamente possuírem o arsenal militar cibernético mais sofisticado do mundo (Manson, 2011) os EUA também têm grande parte de suas infraestruturas críticas dependentes do ciberespaço, o que gera grandes problemas de vulnerabilidade. Numa imagem: o país, dentro do ciberespaço, é uma grande casa de vidro repleta de armas dentro (Groll, 2016).

Sendo assim, identificamos que a temática cibernética se desenvolve dentro das administrações dos EUA como um assunto *especial*, dada a sua crescente importância para a segurança nacional e, portanto, é menos vulnerável às oscilações políticas do bipartidarismo, como acontece com temáticas como direitos humanos, meio ambiente e saúde pública.

As alterações táticas, portanto, não representam mudança do objetivo principal dos EUA nesse campo – a perpetuação da condição hegemônica, agora também no ciberespaço – mas sim alternativas de movimentação internacional para atingi-lo, responsivas tanto às pressões internas da sociedade estadunidense quanto ao novo contexto internacional. Desse modo, a relação de Trump com o legado de Obama para o campo cibernético repõe as linhas estratégicas básicas do segundo, de reforço da resiliência interna e de liderança no processo de securitização, mesmo que com um tom mais agressivo e militarista. Resta saber como as profundas modificações do sistema internacional já em curso influirão nesse objetivo.

BIBLIOGRAFIA

ACKERMAN JR, B. The Trump team has failed to address the nation's mounting cybersecurity threats. **TechCrunch**, 17 de outubro de 2017.

BELOW, K. C. The Utility of Timeless Thoughts: Hannah Arendt's Conceptions of Power and Violence in the Age of Cyberization, 2014. In: KREMER, J; MÜLLER, B (org). **Cyberspace and International Relations**: Theory, Prospects and Challenges. Berlim Heidelberg: Springer, 2014, pp. 95-116.

BURNS, W J.; COHEN, J. The Rules of the Brave New Cyberworld. **Foreign Policy**, 16 fev. 2017.

CHOUCRI, N. **Cyberpolitics**. Cambrigde/Londres: The MIT Press, 2012.

DEPARTMENT of Homeland Security (DHS). **DHS Statement on the Issuance of Binding Operational Directive 17-01**, 13 de setembro de 2017.

DONALD Trump rejects CIA Russia hacking report. **BBC News**, 11 de dezembro de 2016.

ESTADOS UNIDOS DA AMÉRICA. **America First:** A Budget Blueprint to Make America Great Again. Washington: Office of Management and Budget, 2017a.

ESTADOS UNIDOS DA AMÉRICA. **CYBERSPACE POLICY REVIEW:** Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington: Executive Office of the President of the U.S, 2009.

ESTADOS UNIDOS DA AMÉRICA. **EXECUTIVE ORDER 13.800** - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 2017 b.

ESTADOS UNIDOS DA AMÉRICA. **FACT SHEET: Cybersecurity National Action Plan.** The White House, Office of the Press Secretary, 2016. Disponível em: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan. Acesso em: 15 nov. 2017

ESTADOS UNIDOS DA AMÉRICA. **International Strategy for Cyberspace:** Prosperity, Security and Openness in a Networked World. Washington: Executive Office of the President of the U. S., National Security Council, 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Acesso em: 10 nov. 2017.

ESTADOS UNIDOS DA AMÉRICA. **Vulnerabilities Equities Policy and Process for the United States Government – Unclassified.** The White House, 2017c. Disponível em: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. Acesso em: 20 nov. 2017

GREENWALD, G. **NO PLACE TO HIDE:** Edward Snowden, the NSA and the Suveillance State. London: Penguin, 2014.

GROLL, E. Trump and His Lieutenants Are Cyber Hawks. Will They Play Hardball With Putin? **Foreign Policy**, 16 de dezembro de 2016.

GROLL, E. Trump Elevates Cyber Command. **Foreign Policy**, 18 de Agosto de 2017.

HOWARD, T. D.; DA CRUZ, J. de A. Stay the course: Why trump must build on obama's cybersecurity policy. **Information Security Journal: A Global Perspective**, v. 26, n. 6, p. 276–286, 2 nov. 2017.

HURWITZ, R. The Play of States: Norms and Security in Cyberspace. **American Foreign Policy Interests**, v. 36, n. 5, p. 322–331, 3 set. 2014.

KAVANAGH, C. Cybersecurity, Sovereignty, and U.S. Foreign Policy. **American Foreign Policy Interests**, v. 37, n. 2, p. 100–112, 4 mar. 2015.

KLIMBURG, A. Mobilising Cyber Power. **Survival**, v. 53, n. 1, p. 41–60, fev. 2011.

KNOEPFEL, S. Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War, 2014. In: KREMER, J; MÜLLER, B (org). **Cyberspace and International Relations**: Theory, Prospects and Challenges. Berlim Heidelberg: Springer, 2014, pp. 117-124.

KREMER, Jan-Frederik; MÜLLER, Benedikt (Edit.). **Cyberspace and International Relations:** Theory, Prospects and Challenges. Berlim Heidelberg: Springer, 2014.

KUEHL, D. From cyberspace to cyberpower: Defining the Problem, pp. 24–42, 2009. In KREMER, F., STARR, H., WENTZ, L. (org.), Cyberpower and national security, Washington D.C.: Potomac Books Inc, 2009.

LAFRANCE, A. Trump's Incoherent Ideas About "the cyber". **The Atlantic**, 27 set. 2016.

LYNCH, C.; GROLL, E. As U.S. Retreats From World Organizations, China Steps in to Fill the Void. **Foreign Policy**, 06 de outubro de 2017.

MAGNOTTA, F. As expectativas para a era Trump e o papel do Congresso na formulação da política comercial. **Pontes**, v. 13, n. 6, p. 4–6, 2017.

MAKER, S. R. **New Frontier in Defense: Cyberspace and U.S. Foreign Policy**. Nova Iorque: National Committee on American Foreign Policy, maio 2017.

MALAGUTTI, M. **Ciberespaço: Instrumento Geopolítico com Implicações para o Brasil**. Anais do 6º Encontro da Associação Brasileira de Relações Internacionais. **Anais**...Belo Horizonte: ABRI, 25 jul. 2017

MANSON, G. P. Cyberwar: The United States and China Prepare For the Next Generation of Conflict. **Comparative Strategy**, v. 30, n. 2, p. 121–133, 3 maio 2011.

MARKS, J. Continuity on most cyber policies masks a growing erosion of global cyber norms. **Nextgov**, 29 nov. 2017a.

MARKS, J. "Trump's Lack of 'Moral Infraestructure' Causes Cyber Advisers to Resign. **Nextgov**, 24 de Agosto de 2017b.

NEWMAN, L. H. Taking Stock of Trump's Cybersecurity Executive Order So Far. **Wired**, 30 de setembro de 2017.

NEWMAN, L. H. Trump calls for 'crippling' cyber war capabilities. **Wired**, 03 de outubro de 2016.

NYE JR, Joseph S. **Cyber Power**. Cambridge: Harvard Kennedy School, 2010.

NYE JR, Joseph S. Nuclear Lessons for Cybereseucirty? *Strategic Studies,* v. 19, pp. 18-38, 2011.

PECEQUILO, C. S. A política externa de Trump e a Cooperação Sul-Sul: impactos e potencialidades. **Pontes**, v. 13, n. 6, p. 12–15, 2017.

PECEQUILO, C. S. **A política externa dos Estados Unidos**. 2a ed. Porto Alegre: Editora da UFGRS, 2005

PECEQUILO, C. S. **Os Estados Unidos e o século XXI**. Rio de Janeiro: Elsevier, 2012. p. 151–178.

PEREIRA, J. M. G. **O Ciberespaço e a Mutação da Realidade**: ou como este novo campo de atuação modifica as relações internacionais. 2013. 84 f. Dissertação (Mestrado em Relações Internacionais – Estudos de Paz e Segurança) – Faculdade de Economia, Universidade de Coimbra, Coimbra – Portugal.

PRICE, G. Trump is better than Obama on cybersecurity rules, ACLU says. **Newsweek***,* 27 nov. 2017.

SANGER, D. E.; BROAD, W. J. Trump Inherits a Secret Cyberwar Against North Korean Missiles. **The New York Times**, 4 mar. 2017.

SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. **The New York Times**, 01 jun. 2012. Disponível em: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?ref=global-home. Acesso em: 19 jun. 2017.

THE WHITE HOUSE. **President Trump Protects America's CYBER Infrastructure**. Office of the Press Secretary, 12 de maio de 2017a.

THE WHITE HOUSE. **Presidential Memorandum for the Secretary of Defense**. Office of the Press Secretary, 18 de Agosto de 2017b.

THE WHITE HOUSE. **Press Briefing on the President's Meetings at the G20**. Office of the Press Secretary, 07 de julho de 2017c.

THE WHITE HOUSE. **Remarks by Homeland Security Advisor Thomas P. Bossert at CYBER Week 2017**. Office of the Press Secretary, 26 de junho de 2017d.

THE WHITE HOUSE. **Remarks by President Trump and President Xi of China in Joint Press Statement Beijing, China**. Office of the Press Secretary, 09 de novembro de 2017e.

THE WHITE HOUSE. **Statement from the Press Secretary on the United States-China Visit**. Office of the Press Secretary, 07 de abril de 2017f.