UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de Marília

OFICINA UNIVERSITÁRIA
CULTURA ACADÊMICA Editora

Do Virtual ao Material:

Tendências da Ciberização das Relações Internacionais

Friedrich Maier

Como citar: MAIER, F. Do virtual ao material: tendências da ciberização das Relações Internacionais. *In*: AGUILAR, S. L.; ALONSO, I. Z. (org.). **Os Desafios da Política Externa e Segurança no século XXI.** Marília: Oficina Universitária; São Paulo: Cultura Acadêmica, 2018. p. 331-350.
DOI: https://doi.org/10.36311/2020.978-85-7983-968-9.p331-350

Do Virtual ao Material: Tendências da Ciberização das Relações Internacionais

Friedrich Maier

1 – Introdução

Fundamental para o desenvolvimento desse artigo é o argumento de Kremer e Müller (2014a) a respeito do processo de "ciberização" (*cyberization*) das relações internacionais, isto é, a crescente penetração do ciberespaço nas relações internacionais e a crescente dependência dos atores de relações internacionais dos instrumentos do ciberespaço. A "ciberização" indica, portanto, crescente importância das questões relacionadas ao ambiente cibernético.

Todavia, esse ainda é um processo que padece de teorização e discussões de casos. Estudiosos apontam certas dificuldades das teorias

https://doi.org/10.36311/2020.978-85-7983-968-9.p331-350

de Relações Internacionais em sua apreensão do novo ambiente. Alguns apontam a necessidade de estabelecer aparatos conceituais adequados ao novo contexto (CHOUCRI, 2012; GUIMARÃES JR, 2000; BELOW, 2014), ou preconizam a necessidade de novos vocabulários e tipologias (CROSSTON, 2014; GREATHOUSE, 2014; KREMER; MÜLLER, 2014b). Enquanto que Choucri & Goldsmith (2012) apontam que os estudos sobre ciberespaço padecem de lacunas de três tipos: teoria cibernética, dados empíricos e análise de políticas.

Nesse sentido, o presente capítulo intenta apresentar uma contribuição no debate sobre o ciberespaço e a questão dos ataques cibernéticos. Nosso objetivo é duplo: de um lado fornecer evidências que comprovam o processo de *ciberização* acima discutido e, doutro lado, apontar tendências dos impactos oriundos do ciberespaço. Para tanto, elencamos dois casos que, ao nosso ver, marcam pontos de inflexão na discussão sobre essa temática indicando tendências futuras: 1) o ataque à usina de enriquecimento de urânio em Natanz no Irã pelo vírus *Stuxnet*; 2) a interferência de hackers nas eleições presidenciais de 2016 dos Estados Unidos da América (EUA). Os dois casos demonstram como as ações no ciberespaço adquirem importância de dois modos bastante diferentes: o primeiro aponta como o uso de armas cibernéticas sofisticadas significa a possibilidade de *danos físicos*, no sentido de uma operação militar cibernética, enquanto o segundo aponta como a Internet e o ciberespaço podem ser utilizados para *influenciar processos eleitorais.*

A divisão do capítulo, para além da presente introdução contemplará uma seção com breve discussão acerca das definições do ciberespaço – cruciais para a compreensão desse novo ambiente –, uma seção referente a cada um dos casos elencados e, por fim, uma seção de considerações finais, onde tenta-se uma reflexão acerca da tendência de centralidade do "mundo *cyber*" nos próximos anos, sugerindo uma perspectiva teórica de engajamento com tal ambiente.

2 – O ciberespaço: em busca de definições

A reflexão sobre o ciberespaço deve levar em conta a relativa novidade desse ambiente. Os desenvolvimentos em tecnologias de produção,

transmissão e processamento de dados eletrônicos remete às décadas de 1970 e 1980. O começo da popularização da Internet nos Estados Unidos da América (EUA) se deu, principalmente, a partir da década de 1990; a segunda metade dessa década marca também o início de domínios que hoje são amplamente conhecidos e utilizados, tais como o "Yahoo.com", "Google.com" e "Amazon.com". Em junho de 2017 são 3,8 bilhões de pessoas acessando o maior componente do ciberespaço, a Internet[1].

Desde então o desenvolvimento das tecnologias de informação e comunicação, em conjunto com a popularização da Internet e o Computador Pessoal (PC) ampliaram sobremaneira o acesso ao ciberespaço; movimento que se intensifica nas duas décadas iniciais do século XXI, no qual o *smartphone* dita novos padrões de interação, cada vez mais intensa e cotidiana. Porém, permanece a questão: como definir esse novo ambiente?

Por perpassar e influenciar amplos aspectos da sociedade contemporânea, como bem observa Castells (2002) e sua análise sobre a "sociedade em rede", os pesquisadores que se debruçam sobre essa problemática pertencem a campos de estudos variados, tais como a cibercultura, as relações internacionais, a teoria da informação, a geografia e outros. A pluralidade de perspectivas diante do ciberespaço influenciam também a pluralidade de suas definições.

Quanto a etimologia do conceito, concordamos com Mayans e Planells (2002) acerca da melhor adequação do termo "ciberespaço" para identificar o fenômeno que é objeto desse artigo[2]. A partir daí, podemos encontrar posições que focam em determinados aspectos desse ambiente, tal como em Kuehl (2009) que aponta a especificidade do domínio cibernético na dependência dos meios eletrônicos e do campo eletromagnético para criar, processar e transmitir informação utilizada por seres humanos.

Existem abordagens mais simplistas, tais como em Kassab (2014) para quem as operações no ciberespaço não se distinguem em muito dos outros ambientes de ação, empregando apenas novos moldes, *eletrônicos*.

---

[1] De acordo com o *Internet World Stats* <http://www.internetworldstats.com/stats.htm>. Acesso em: 21 jul. 2017.

[2] A palavra se forma a partir do prefixo "ciber" utilizado pelos entusiastas e especialistas da informática para se referir aos fenômenos a ela relacionados. O termo remete à "cibernética" de Robert Wiener, uma tentativa de formação de campo científico no estudo da semelhança dos processos de retroalimentação informacional (*feedback eletrônico)* entre homens e máquinas. Para uma recuperação histórica do conceito ver: KIM, 2004.

Alguns autores apontam semelhanças entre o ciberespaço e o panorama internacional, focando no caráter evidentemente anárquico de ambos os sistemas (KIGGINS, 2014). As características únicas também servem para distinção. Assim Nye Jr (2010) define o ciberespaço como uma ambiente híbrido, composto por uma camada estrutural (cabos, servidores, computadores) e uma camada virtual (as trocas de informações), a hibridez do ambiente é crucial nesse autor para entender como ações podem provocar efeitos nas duas camadas.

Já Manjikian (2010) distingue o ciberespaço de outros ambientes de ação humana a partir de suas "qualidade únicas", de "mobilizar usuários [...] prover rapidamente grandes quantidades de informação de qualidade incerta ou não-regulada [... e] diminuir distâncias entre usuários" (p. 381). Enquanto o atual governo dos EUA define o ciberespaço como "uma rede interdependente de infraestruturas de tecnologia e informação, e inclui a internet, redes de telecomunicações, sistemas de computadores e conjuntos de processadores e controladores em indústrias críticas" (WHITE HOUSE, 2009, p. 01, trad. nossa).

Além de muitas outras definições opta-se nesse texto por aquela encontrada em Choucri (2012) por oferecer uma perspectiva multifacetada. Ao distinguir o ciberespaço em camadas, a autora permite observar esse ambiente com atenção tanto aos recursos técnicos, quanto aos recursos informacionais e humanos que o compõem – aspecto crucial para a discussão que desenvolveremos abaixo. Assim apreende: 1) as bases físicas, 2) os códigos por detrás da interação entre as máquinas, 3) a informação em suas distintas formas e 4) os atores (humanos) que interagem nesse espaço (p. 8). Ou seja, o ciberespaço não existe apenas pelas máquinas, os códigos que as movimentam são necessários e necessárias são também as informações trocadas entre as máquinas pelos códigos. Todavia, esse não seria um espaço de ação sem os humanos que o operacionalizam[3].

[3] Cabe notar como essa definição se aproxima da visão literária de Gibson ([1984], 2002) um dos primeiros a empregar o termo "ciberespaço"; no romance *cyberpunk* "Neuromancer" de 1984, escreve: "O ciberespaço. Uma alucinação consensual, vivida diariamente por bilhões de operadores legítimos, em todas as nações, por crianças a quem estão ensinando conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas que abrangem o universo não-espaço da mente; nebulosas e constelações infindáveis de dados. Como luzes de cidade, retrocedendo."

Cabe ainda desfazer alguns mal-entendidos do termo. O ciberespaço compreende a uma multiplicidade de tecnologias de criação, transmissão e processamento de informação e não fica restrito à Internet (que é seu maior componente[4]). Fazem também parte do ciberespaço redes locais (governamentais, empresariais, do terceiro setor), sistemas de tráfego aéreo, operadoras de telefonia e processos industriais controlados por computador (sistemas SCADA) – o que amplia sua importância. Tendo encontrado uma definição para trabalhar com esse ambiente seguimos em nossa proposta de observar seus efeitos nas relações internacionais. Assim, procedemos com a análise do primeiro caso elencado, o do vírus militar Stuxnet.

3 – O Stuxnet

Em 2009 uma série de defeitos nas centrífugas da usina de enriquecimento de urânio de Natanz colocou as autoridades iranianas em uma situação inédita: as constantes falhas que chegaram a danificar aproximadamente 1.000 centrífugas foram fruto de um sofisticado ataque cibernético por meio de um vírus especialmente desenhado para causar esse dano: o Stuxnet.

Não se sabe o exato momento em que os engenheiros nucleares iranianos descobriram que as falhas não tinham origem mecânica ou de programação, mas eram devidas a um *malware (malicious software)*. Já o resto do mundo, conheceu o Stuxnet somente em 2010. O vírus se reproduziu para além da usina de Natanz, se "proliferando" pela internet graças a uma atualização em seu código por parte de seus criadores. Uma empresa de segurança cibernética localizada na Bielorrússia foi a primeira a reportá-lo (KASPERSKY, 2011). Logo, as empresas líderes no mercado de cibersegurança – Kasperspy Lab e Symantec – não tardaram em emitir relatórios que eram unânimes em um ponto: o novo vírus possuía um nível de sofisticação nunca antes presenciado (FALLIERE; MURCHU; CHI, 2011; SHAHEEN, 2014).

[4] Isto é: o ciberespaço compreende a Internet e uma série de outras redes. Outra confusão comum é a utilização de "Internet" e "Web" como sinônimos. A última é apenas uma das tecnologias que permitem a navegação dentro da grande rede, a Internet.

Esse alto padrão de sofisticação do vírus levantou suspeitas, já em 2010, de que o ataque não tinha as marcas de um "cibercrime" comum e, portanto, deveria ser fruto de alguma equipe de desenvolvimento, financiada por alguma entidade (ADHIKARI, 2010). Somente em junho de 2012 o *The New York Times* publicou uma extensa reportagem apontando, por meio de fontes anônimas dentro do governo estadunidense, que o Stuxnet era parte de um grande programa secreto de armas cibernéticas desenvolvido em parceria com o governo de Israel: o *Olympic Games*. Iniciado em 2006 pela administração Bush e continuado nas administrações Obama, esse programa tinha por objetivo central atrasar o programa nuclear iraniano por meio do ciberespaço (SANGER, 2012).

Desse modo, o Stuxnet contou com uma arquitetura de programação especificamente desenvolvida para atuar na planta nuclear de Natanz. Composto por duas partes, uma capaz de inserir o vírus dentro da máquina (*trojan*) e outra cuja função é a inserção de códigos de programação alterados (*rootkit)* no sistema de comando das centrífugas, o *malware* chegou a contaminar cerca de 60.000 computadores relacionados a sistemas industriais– 60% deles no Irã (FARWELL; ROHOZINSKI, 2010). Empresas apontam que o vírus se aproveitou de quatro falhas no sistema operacional *Windows* para se proliferar[5] (BEAUMONT, 2010). Inicialmente, o código foi inserido a partir de um *pen drive* utilizado em um dos computadores da rede da usina (ADHIKARI, 2010). O alto nível de sofisticação do vírus garantia a autonomia em sua capacidade de proliferação para o resto da usina.

Após a invasão das máquinas e inserção dos códigos alterados no sistema de controle eletrônico das centrífugas, o Stuxnet emitia comandos para elevar a velocidade de rotação das centrífugas a fim de quebra-las[6]. Ao mesmo tempo, o vírus enviava dados aos controladores do equipamento apontando o funcionamento normal das máquinas disfarçando, assim, sua

[5] Esse é um dos maiores argumentos sobre a origem estatal do código: as falhas no código (ou *zero-day vulnerability*) de sistemas operacionais de uso global são raros e, quando descobertos, prontamente corrigidos por *patchs* de atualização. O número elevado de brechas aproveitadas pelo vírus demonstra que o mesmo foi fruto de um longo processo de programação – o que suscita problemas sobre os custos de tal empreitada.

[6] Dois documentos são essenciais para demonstrar a atuação do vírus: o dossiê sobre o Stuxnet elaborado pela Symantec oferece dados precisos sobre o código do vírus (FALLIERE; MURCHU; CHI, 2011) e o relatório que especifica a atuação desse vírus em relação ao sistema dos controladores industriais Siemens S7-315 (ALBRIGHT; BRANNAN; WALROND, 2010).

atuação. O vírus recebeu constantes atualizações até a data de sua descoberta em 2010[7] (ALBRIGHT; BRANNAN; WALROND, 2010).

Mesmo após a divulgação, uma onda de novos vírus continuou a assolar o Irã e a região do Oriente Médio. Principalmente focado na espionagem cibernética e roubo de dados confidenciais o vírus *Flame* foi responsável por perdas de dados no Ministério do Petróleo iraniano (CONSTANTIN, 2012a; 2012b). As empresas de cibersegurança supracitadas apontaram em seus relatórios sobre o *Flame* a semelhança com o código do Stuxnet, indício de que ambos os códigos ou foram desenvolvidos pela mesma equipe ou por equipes em cooperação (BEAUMONT, 2010; CONSTANTIN, 2012c).

Em 2012, mais um programa de espionagem foi descoberto. Denominado *miniFlame* o *malware*, diferentemente dos outros vírus focados na transmissão de informação roubada, tinha por objetivo o controle direto de computadores específicos de autoridades. O *miniFlame* atuava assim como um "módulo" entre os programas de espionagem *Flame* e uma outra variante, o *Gauss* (CONSTANTIN, 2012b).

Todas essas informações apontam na direção de uma sofisticada operação militar cujo objetivo era a penetração, espionagem e sabotagem de pontos industriais cruciais no Irã, como o setor de enriquecimento de urânio e de petróleo. A ofensiva cibernética dos EUA em conjunto com Israel possui, todavia, mais uma peculiaridade: a narrativa inédita de Farwell e Rohozinski (2010) aponta que partes do código do vírus vinham da comunidade hacker, isto é, eram "códigos de prateleira", amplamente conhecidos nos fóruns "ocultos" da camada mais anônima da Internet. Essa informação pode indicar uma colaboração dos governos com essas comunidades de "cibercriminosos". Os governos de Israel e dos EUA nunca comentaram ou confirmaram oficialmente a responsabilidade pelo ataque do Stuxnet, pelo projeto *Olympic Games* ou pelos outros ataques (*Flame, miniFlame*).

[7] A "culpa" da descoberta do vírus estaria em uma modificação do código original pela parte israelense do projeto. Arranjos de programação que objetivavam maior rapidez na proliferação permitiram o comportamento inesperado do vírus, que se replicou em máquinas conectadas à internet, levando à descoberta do projeto. Para além do Irã, Índia e Malásia foram países que reportaram danos em alguns sistemas industriais causados pelo Stuxnet (SANGER, 2012).

Esse conjunto de informações demonstra algo crucial: presenciamos uma crescente militarização do ciberespaço. Governos estão se preparando para atuar nesse novo ambiente. O caso do Stuxnet é a mais nítida representação da potencialidade das armas cibernéticas: demonstrou a capacidade de destruição física por meio de códigos eletrônicos (BEAUMONT, 2010). Tal capacidade – inédita até então – marca, portanto, um ponto de inflexão acerca do uso de armas cibernética e do debate sobre cibersegurança[8], influenciado as discussões teóricas sobre a "ciberguerra"[9]. Além disso, o vírus escancarou operações que se desenvolviam em segredo há alguns anos em países como EUA, Grã Bretanha e Israel. No mesmo sentido, Mehmetcik (2014) aponta que "mais de 30 países já construíram ou estão construindo capacidades cibernéticas defensivas e ofensivas" (p. 126, trad. nossa).

Tal panorama indica uma das múltiplas possibilidades das tecnologias da informação: a capacidade de ofensiva militar, com *impactos físicos* por meio de armas cibernéticas. A *ciberização das relações internacionais* indica, portanto, que armamentos cibernéticos são uma opção de atuação dos Estados. Seus benefícios apontam para os custos – menores se comparados com a atuação militar direta – e para a "anonimidade" desses ataques; cabe ressaltar que a possibilidade de colaboração com grupos e organizações hackers pode dificultar ainda mais a possibilidade de atribuição. Passaremos agora para o outro caso selecionado, cujas características específicas também marcam tendências futuras.

[8] Recomendamos o documentário-filme *Zero Days* (ZERO..., 2016) para a compreensão da dimensão dos impactos do Stuxnet na comunidade de cibersegurança. Todos os responsáveis por empresas de cibersegurança entrevistados foram unânimes: tratava-se de algo inédito até então e altamente perigoso as infraestruturas dependentes de tecnologias de controle eletrônico.

[9] Ainda que em caráter de possibilidade, certa literatura defende a operacionalização do conceito de *ciberguerra* ou "guerra cibernética" para tratar de operações militares promovidas por Estados dentro do ciberespaço (ver: ARQUILLA; RONDFELDT, 1997; LOPES; TEIXEIRA JR, 2010; WENDT, 2011). Não defendemos esse ponto de argumentação por compreender que o conceito de "guerra" (tanto teoricamente quanto sobre as bases do direito internacional) necessita de certos condicionantes para ser utilizado. Estamos conscientes da possibilidade de uma "guerra cibernética" no futuro, mas apontamos que até então, tanto o Stuxnet quanto os casos de Ataques de Negação de Serviço Distribuído (DDoS, em inglês) utilizados na Guerra Russo-Georgiana de 2008 tratam de *operações militares no ciberespaço* ou de *ciberataques* promovidos por Estados e não propriamente de guerras cibernéticas.

4 – As eleições estadunidenses de 2016

Os efeitos do ciberespaço não se restringem aos vírus e armas cibernéticas. A centralidade da informação, cada vez maior nas sociedades do século XXI (NYE JR, 2010), permite uma série de ações cujos objetivos recaem na manipulação daquilo que comumente se chama de "opinião pública"[10]. As "notícias falsas" (*fake news*), vazamentos de documentos oficias e campanhas internacionais de difamação são alguns exemplos. O segundo caso elencado, que aponta para os impactos da *ciberização das relações internacionais* trata especificamente dessa forma de ação durante as eleições presidenciais de 2016 nos EUA.

Em 20 de junho de 2016, um usuário da rede social *Twitter*, chamado Guccifer 2.0, reivindicou a autoria de um ataque cibernético que teria atingindo o Comitê Nacional Democrata (CND) vazando uma série de e-mails relacionadas à campanha da então candidata à presidência e ex-Secretária de Estado, Hillary Clinton. Em 22 de julho de 2016, o reconhecido site de vazamentos de documentos oficiais, *Wikileaks*, publicou 44.053 e-mails com 17.761 anexos roubados do CND. Os vazamentos não pararam por aí: em 07 de outubro de 2016 – algumas semanas antes das eleições presidenciais – uma série de publicações do *Wikileaks* liberaria ao público 60.000 e-mails roubados da conta de John Podesta, presidente da campanha de Hillary Clinton (HARDING, 2016).

Em 13 dezembro de 2016, uma reportagem especial do jornal *The New York Times* aponta aquilo que seria "a arma perfeita": a invasão do comitê democrata por *hackers* supostamente ligados ao governo Russo. A notícia contou como dois grupos de hackers, ATP28 e ATP29, que agiram ao mesmo tempo – aparentemente sem coordenação – no acesso e roubo de informações. O grupo ATP29 teria acesso ao servidores do CND desde o verão de 2015 no hemisfério norte, enquanto o ATP28 desde a primavera do ano seguinte – ambos extraíram grandes volumes de informação, tais como os e-mails vazados (LIPTON; SANGER; SHANE, 2016). Cabe ressaltar, o presidente Obama colocou a cibersegurança como um dos pontos principais do seu governo, paradoxalmente, seu partido foi incapaz de

[10] Esfera de atuação que não é nova, vale lembrar que tanto a propaganda nazista e antinazista na Europa da 2ª Guerra Mundial, quanto as transmissões de rádio da USIA para o território da União Soviética foram casos de mobilização de ferramentas de informação com objetivos militares e políticos específicos.

implementar medidas básicas de cibersegurança que evitariam essa invasão (FIDLER, 2017).

Os hackers utilizaram da técnica de *spear-phishing*, isto é, direcionamento de e-mails com o objetivo de roubar informações. Assim, funcionários do CND e de diversas instituições dos EUA recebiam e-mails com aparência legítima (e-mails que pareciam enviados de remetentes confiáveis) que continham ou *links* para a substituição de senhas, ou arquivos anexos contaminados. Ao clicar no *link*, ou abrir o documento anexo, os hackers conseguiam promover alterações no sistema operacional dos computadores e instalar outros *malwares*, obtendo amplo acesso tanto aos dados armazenados nos discos rígidos, quanto os dados disponíveis nas contas de e-mail[11].

Inicialmente, a atribuição desses ataques cibernéticos ao governo russo pautava-se em indícios tais como as semelhanças com outros ataques russos, a abertura de alguns documentos roubados em softwares no idioma russo e a relação entre os horários dos ataques e o horário comercial do fuso horário da Rússia, incluindo períodos de inatividade durante os feriados nacionais desse país. A primeira atribuição oficial dos ataques à Moscou por parte do governo dos EUA aconteceu em 7 de outubro de 2016, numa declaração conjunta do Departamento de Segurança Interior (*Department Of Homeland Security* – DHS) e do Escritório do Diretor de Inteligência Nacional:

> A Comunidade de Inteligência dos Estados Unidos confia que o governo russo dirigiu o recente comprometimento de e-mails de pessoas e instituições estadunidenses, incluindo organizações políticas dos EUA. As recentes divulgações de supostos e-mails hackeados em sites como DCLeaks.com e Wikileaks e pela personagem online Guccifer 2.0 são

[11] Trechos de um "documento secreto" da NSA vazados pelo site de notícias *The Intercept* em 05 de maio de 2017, especificam essa tática no caso das invasões às empresas fornecedoras de produtos relacionados às eleições (COLE, 2016): "Os atores de ameaça cibernética [oculto] executaram uma campanha de spear-pishing do endereço de e-mail noreplyautomaticservice@gmail.com em 24 de agosto de 2016 mirando vítimas que incluíram empregados da empresa estadunidense 1, de acordo com informações que se tornaram disponíveis, em abril de 2017" (ESTADOS UNIDOS DA AMÉRICA, 2017b, p. 2, trad. nossa) e "Os [oculto] atores estavam provavelmente tentando obter informações associadas com aplicações de hardware e software relacionadas com as eleições. É desconhecido se o desdobramento do spear-phising mencionado acima comprometeu com sucesso todas as vítimas pretendidas, e quais os dados potenciais das vítimas que puderam ser exfiltrados. Contudo, baseado no ato subsequente, é provável que ao menos uma conta foi comprometida" (ESTADOS UNIDOS DA AMÉRICA, 2017b, p. 3, tradução nossa).

> consistentes com os métodos e motivações de esforços direcionados russos (ESTADOS UNIDOS DA AMÉRICA, 2016b, trad. nossa).

A declaração continua apontando que os ataques focaram não somente os roubos de e-mails e dados, mas também atuaram sobre empresas que fornecem equipamentos de software e hardware para as eleições em diversos locais dos EUA, com o objetivo de obter acesso às suas estruturas – apesar disso afirma que não houve danos ao processo de contagem dos votos.

As informações desse pequeno comunicado de imprensa foram complementadas com uma declaração conjunta do DHS e do FBI (*Federal Bureau of Investigation*) de 29 de dezembro de 2016, cuja função era fornecer uma análise das "ferramentas e infraestruturas utilizadas pelos Serviços de Inteligência Russos (RIS) civis e militares para comprometer e explorar redes e *endpoints* associados com as eleições dos EUA" (ESTADOS UNIDOS DA AMÉRICA, 2016a, p. 1, trad. nossa). Deixando claro que as declarações anteriores desses órgãos não atribuíram os ataques "especificamente à países ou atores ameaçadores" o documento muda radicalmente o tom, afirmando que "a atribuição pública dessas atividades aos RIS [Serviços de Inteligência Russos] é suportada por indicadores técnicos da Comunidade de Inteligência dos EUA, DHS, FBI, setor privado e outras entidades" (idem, trad. nossa), ampliando a informação de 7 de outubro.

As declarações acima foram reforçadas com um versão pública "não-secreta" de um "relatório secreto" divulgado pelas principais agências de inteligência dos EUA – FBI, CIA (*Central Intelligence Agency*) e NSA (*National Security Agency*). Dentre os "julgamentos-chave" desse documento, há a clara menção da intenção russa de minar a democracia estadunidense por meio dos ataques cibernéticos:

> Os esforços russos para influenciar as eleições presidenciais dos EUA em 2016 representam a mais recente expressão do desejo de longa data de Moscou em enfraquecer a ordem liberal democrática liderada pelos EUA, mas essas atividades demonstraram uma significativa escalada na franqueza, nível de atividade e escopo e esforços comparados à operações prévias. (ESTADOS UNIDOS DA AMÉRICA, 2017a, p. ii).

Contudo, esse relatório não aponta somente a culpa pelos ataques. Há uma clara menção ao desejo russo de *interferir no resultado das eleições*, favorecendo o presidente eleito Donald Trump em detrimento à ex-Secretária Hillary Clinton:

> Nós avaliamos que o presidente russo Vladimir Putin ordenou uma campanha de influência em 2016 visando a eleição presidencial dos EUA. Os objetivos russos deveriam minar a fé pública no processo democrático dos EUA, denegrir [sic] a Secretária Clinton e prejudicar sua elegibilidade e potencial presidência. Nós avaliamos ainda que Putin e o governo russo desenvolveram uma clara preferência pelo presidente eleito Trump. Nós temos alta confiança nesses julgamentos. (ESTADOS UNIDOS DA AMÉRICA, 2017a, p. ii, trad. nossa).

E ainda em:

> Nós também avaliamos que Putin e o governo russo aspiravam a ajudar as chances de eleição do presidente eleito Trump, quando possível, desacreditando a Secretária Clinton e publicamente contrastando ela desfavoravelmente a ele. Todas as três agências concordam com esse julgamento. A CIA e o FBI têm alta confiança nesse julgamento; a NSA tem uma confiança moderada. (ESTADOS UNIDOS DA AMÉRICA, 2017a, p. ii, trad. nossa).
>
> Quando parecia à Moscou que a Secretária Clinton provavelmente venceria as eleições, a campanha de influência russa começou a focar mais em minar sua futura presidência. (ESTADOS UNIDOS DA AMÉRICA, p. ii, trad. nossa).

Ligam-se, assim, os ataques cibernéticos e as ações midiáticas internacionais levadas à cabo pelo Departamento Central de Inteligência Russo (GRU). As agências apontam coordenação do GRU com sites de vazamento, tal como o *Wikileaks* e companhias ligadas ao setor da mídia. Uma campanha de ataques e interferências "sem precedentes" na história. Apesar disso, as agências não questionaram o resultado das eleições, nem o impacto dos vazamentos na opinião pública:

> Nós não fizemos uma avaliação sobre o impacto que as atividades russas tiveram no resultado da eleição de 2016. A Comunidade de Inteligência dos EUA é encarregada de monitorar e avaliar as intenções, capacidades, e ações de atores estrangeiros; ela não analisa os processos

> políticos dos EUA ou a opinião pública dos EUA. (ESTADOS UNIDOS DA AMÉRICA, p. i, trad. nossa).

Fica claro, a partir da discussão desenvolvida até agora, o caráter inédito das invasões e vazamentos durante o período eleitoral de 2016. A atuação de hackers russos – ligados ou não ao governo da Rússia – apontou a capacidade de influência estrangeira em um dos maiores "tesouros nacionais" dos EUA: a democracia. Roubo de informação e vazamentos de documentos oficiais acontecem às centenas, diariamente (ZERO..., 2016). Todavia, essa série de ataques em específico representou, ao nosso ver, um segundo ponto de inflexão na capacidade das ferramentas trazidas pelo ciberespaço. Seu objetivo era claramente o de *influenciar o pleito eleitoral*, por meio de ações que buscavam prejudicar um dos lados em disputa e pautou-se na ação coordenada de invasão de computadores, roubo de dados e midiatização dos mesmos dentro do ciberespaço.

A ciberização, nesse caso, indica a crescente dependência dos Estados em relação à informação – principalmente nas democracias liberais do ocidente, submetidas periodicamente à processos eleitorais nos quais a "opinião pública" é crucial para os resultados. No caso apresentado, os *bits* transmitidos à velocidade da luz foram capazes de desafiar o Estado mais poderoso do mundo durante seu processo eleitoral. Fato que agudamente demonstra a necessidade de atenção ao "mundo cyber" e ao processo de ciberização.

5 – Conclusões

Nosso texto teve por objetivo apontar dois casos que marcam pontos de inflexão no processo denominado por Kremer e Müller (2014a) de *ciberização das relações internacionais*, no sentido de ilustrarem os impactos reais que o ciberespaço pode trazer e, além disso, indicarem tendências. De um lado, apresentamos o Stuxnet que demonstrou pela primeira vez as capacidades de armas cibernéticas sofisticadas. Não queremos dizer, com isso, que ataques anteriores não tiveram sua importância: o amplo uso de hackers em ações de "negação de serviço" na Estônia em 2007 e na Geórgia em 2008 pelo governo russo são casos

marcantes do processo de crescimento das capacidades de ação por meio do ciberespaço (MEHMETCIK, 2014) e apresentam os primeiros casos de operações cibernéticas militares.

Contudo, o caso do ataque cibernético ao Irã apresentou características inéditas: a sofisticação do código do vírus e, principalmente, os danos materiais ocasionados. Ao revelar a possibilidade de destruição de infraestrutura física, o Stuxnet levantou debates em toda a comunidade internacional sobre como agir em relação aos ataques cibernéticos. Alguns autores, chegaram a discutir, inclusive, se o acontecimento poderia ser considerado um *ato de guerra*, por apresentar as características de uso da força (KNOEPFEL, 2014). Portanto, o ponto de inflexão causado pelo caso Stuxnet confirma a tendência de ciberização e nos diz muito a respeito da futura "ciberguerra".

Do outro lado, o segundo caso elencado, a interferência de hackers nas eleições presidenciais de 2016 apresentam como o ciberespaço é um elemento crucial na crescente dependência informacional das sociedades. As características inéditas desse caso estão no alvo, o Estado que se considera "a maior democracia do mundo" e nos métodos coordenados de invasão, roubo de dados e vazamentos para a mídia internacional para *influenciar especificamente* um processo eleitoral. Ressaltamos que é justamente o objetivo de i*nfluenciar um processo eleitoral* que distingue esse acontecimento de outros casos, tal como o conhecido vazamento dos dados da NSA por Edward Snowden em 2013.

Em suma, demonstramos a pertinência do argumento da ciberização e apontamos casos representativos, *marcos* no desenvolvimento desse processo que indicam tendências futuras. Cabe destacar ainda que ao nosso ver o ciberespaço não é um ambiente homogêneo, a rede apresenta *desigualdades* ao redor do globo. Existem pontos de extrema conectividade e pontos de semi-isolamento. Os padrões de acesso também são desiguais entre as nações e, mesmo dentro delas, entre as diversas instituições e classes sociais. Isso significa que um berbere do Marrocos, um estadunidense no Vale do Silício e um chinês sob o "Grande Firewall" conectam-se ao ciberespaço a partir de diferentes infraestruturas e padrões de acesso.

Essa é uma posição teórica que permite considerar o ciberespaço como um ambiente de complexidade ímpar cujas tendências apontadas neste texto são apenas alguns dos desdobramentos possíveis e deve ser desenvolvida. Se nem a Grande Rede pode ser pensada como um local homogêneo, o ciberespaço tampouco o é e exatamente por isso a preocupação com sua securitização tornar-se-á pauta central dentro das agendas políticas dos Estados.

Referências

ADHIKARI, R. Stuxnet: dissecting the worm. *Tech News World*, Encino, CA, 16 ago. 2010. Disponível em: <http://www.technewsworld.com/story/70622.html>. Acesso em: 20 jun. 2017.

ALBRIGHT, D.; BRANNAN, P.; WALROND, C. Stuxnet Malware and Natanz: update of ISIS December 22, 2010 Report. *Institute for Science and International Security*, Washington, DC, 15 fev. 2011.

ARQUILLA, J.; RONFELDT, D. Cyberwar is coming! In: ARQUILLA, J.; RONFELDT, D. *In Athena's Camp*: preparing for conflict in the Information Age. Santa Monica, CA/EUA: RAND Corporation, 1997. p. 23–60.

BEAUMONT, P. Stuxnet worm heralds new era of global cyberwar. *The Guardian*, London, 30 set. 2010. Disponível em: <http://www.guardian.co.uk/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar>. Acesso em: 20 jun. 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.-F.; MÜLLER, B. (Ed.). *Cyberspace and International Relations:* theory, prospects and challenges. Berlim Heidelberg: Springer, 2014. p. 95–116.

CASTELLS, M. *Sociedade em rede*. Tradução Roneide Venâncio Majer. São Paulo: Paz e Terra, 2002. (A era da informação: economia, sociedade e cultura, v. 1).

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

____; GOLDSMITH, D. Lost in cyberspace: harnessing the internet, international relations and global security. *Bulletin of the Atomic Scientists*, Chicago, IL, v. 68, n. 2, p. 70–77, 2012.

COLE, M. et al. Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election. *The Intercept*, 05 jun. 2017. Disponível em: <https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/>. Acesso em: 19 jun. 2017.

CONSTANTIN, L. Flame part of US-Israel cyber attack campaign against Iran. *InfoWorld*, San Francisco, CA, 20 jun. 2012a. Disponível em: <http://www.infoworld.com/article/2617357/government/report--flame-part-of-u-s--israeli-cyber-attack-campaign-against-iran.html>. Acesso em: 20 jun. 2017.

_____. Kaspersky discovers miniflame cyberespionage malware directly linked to flame and gauss. *ComputerWorld*, Framingham, MA, 15 out. 2012b. Disponível em: <http://www.computerworld.com/s/article/9232367/Kaspersky_discovers_miniFlame_cyberespionage_malware_directly_linked_to_Flame_and_Gauss>. Acesso em: 20 jun. 2017.

_____. Security researchers discover link between Stuxnet and Flame. *InfoWorld*, San Francisco, CA, 11 jun. 2012c. Disponível em: <http://www.infoworld.com/article/2617574/intrusion-detection/update--security-researchers-discover-link-between-stuxnet-and-flame.html>. Acesso em: 20 jun. 2017.

CROSSTON, M. Phreak the Speak: The Flawed Communications within Cyber Intelligentsia. In: KREMER, J.-F.; MÜLLER, B. (Ed.). *Cyberspace and International Relations*: theory, prospects and challenges. Berlim Heidelberg: Springer, 2014. p. 253–268.

ESTADOS UNIDOS DA AMÉRICA. Department of Homeland Security. Federal Bureau of Investigation. Joint Analysis Report GRIZZLY STEPPE – Russian Malicious Cyber Activity, 2016a. *US-Cert*: United States Computer Emergency Readiness Team. 29 Dec. 2016. Disponível em: <https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity>. Acesso em: 20 jun. 2017.

_____. Department Of Homeland Security. Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. *Department of Homeland Security*, 7 Oct. 2016b. Disponível em: <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>. Acesso em: 19 jun. 2017.

_____. Intelligence Community Assessment. *Assessing Russian Activities and Intentions in Recent US Elections*. 6 Jan. 2017a. Disponível em: <https://www.dni.gov/files/documents/ICA_2017_01.pdf >. Acesso em: 20 jun. 2017.

_____. National Security Agency. *Report on Russia spearpishing*, 5 May 2017b. Disponível em: <https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1>. Acesso em: 23 jun. 2017.

FALLIERE, N.; MURCHU, L. O; CHIEN, E. *W32.* Stuxnet Dossier: version 1.4. *Symantec*, fev. 2011, 69 p.

FARWELL, J. P; ROHOZINSKI, R. Stuxnet and the Future of Cyber War. *Survival:* Global Politics and Strategy, London, v. 53, n. 1, p. 23–40, Feb.–Mar. 2011.

FIDLER, D. P. The U.S. Election hacks, cybersecurity, and international law. *AJIL Unbound*, Washington DC, v. 110, p. 337–342, 15 Feb. 2017. doi:10.1017/aju.2017.5.

GIBSON, W. *Neuromancer*. Tradução Abdulie Sam Boyd e Lumir Nahodil. São Paulo: Aleph, [1984], 2002.

GREATHOUSE, C. B. Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? In: KREMER, J.-F.; MÜLLER, B. (Ed.). *Cyberspace and International Relations*: theory, prospects and challenges. Berlim Heidelberg: Springer, 2014. p. 21–40.

GUIMARÃES JR, M. J. L. O ciberespaço como Cenário para as Ciências Sociais. *ILHA*: Revista de Antropologia, Florianópolis, v.2, n. 1, p. 139–154, dezembro 2000.

HARDING, L. What we know about Russia's interference in the US election. *The Guardian*, London, 16 dez. 2016. Disponível em: <https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election>. Acesso em: 19 jun. 2017.

KASPERSKY, E. The Man Who Found Stuxnet: Sergey Ulasen in the Spotlight. *Nota Bene*, 2 nov. 2011. Disponível em: <https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/>. Acesso em: 19 jun. 2017.

KASSAB, H. S. In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. In: KREMER, J.-F.; MÜLLER, B. (Ed.). *Cyberspace and International Relations:* theory, prospects and challenges. Berlim Heidelberg: Springer, 2014. p. 59–76.

KIGGINS, R. D. US Leadership in Cyberspace: Transnational Cyber Security and Global Governance. In: KREMER, J.-F.; MÜLLER, B. (Ed.). *Cyberspace and International Relations*: theory, prospects and challenges. Berlim Heidelberg: Springer, 2014. p. 161–180.

KIM, J. H. Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural. *Horizontes Antropológicos*, Porto Alegre, ano 10, n. 21, p. 199–219, jan/jun 2004.

KNOEPFEL, S. Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War. In: KREMER, J.-F.; MÜLLER, B. (Ed.). *Cyberspace and International Relations*: theory, prospects and challenges. Berlim Heidelberg: Springer, 2014. p. 117–124.

KREMER, J.-F.; MÜLLER, B. (Ed.). *Cyberspace and International Relations*: theory, prospects and challenges. Berlim Heidelberg: Springer, 2014a.

_____. A Framework to Understand Emerging Challenges to States in an Interconnected World. In: _____. *Cyberspace and International Relations*: theory, prospects and challenges. Berlim Heidelberg: Springer, 2014b. p. 41–58.

KUEHL, D. From cyberspace to cyberpower: Defining the Problem. In: KRAMER, F.; STARR, H.; WENTZ, L. (Ed.). *Cyberpower and national security.* Washington D.C.: Potomac, 2009. p. 24–42.

LIPTON, E.; SANGER, D. E.; SHANE, S. The Perfect Weapon: How Russian Cyberpower Invaded the U.S. *The New York Times*, New York, 13 dez. 2016. Disponível em: <https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html>. Acesso em: 19 jun. 2017.

LOPES, G.; TEIXEIRA JR, A. *O Ciberespaço é o novo front*: implicações para o pensamento estratégico. In: CONFERÊNCIA NACIONAL DA ILA (International Law Associations), 1., Brasil, 2010.

MANJIKIAN, M. M. E. From global village to virtual battlespace: the colonizing of the Internet and the extension of Realpolitik. *International Studies Quarterly*, Oxford, n. 54, p. 381–401, 2010.

MAYANS, J.; PLANNELS, I. Ciberespaço: notas para a utilização de um conceito analítico em Ciências Sociais. In: ALVES, G.; MARTINEZ, V. (Org.). *Dialética do ciberespaço*. São Paulo: Práxis, 2002.

MEHMETCIK, H. A new way of conducting war: cyberwar, is that real? In: KREMER, J.-F.; MÜLLER, B. (Ed.). *Cyberspace and International Relations*: theory, prospects and challenges. Berlim Heidelberg: Springer, 2014. p. 125–140.

SANGER, D. E. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*, New York, 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.

SHAHEEN, S. Offense–Defense Balance in Cyber Warfare. In: KREMER, J.-F.; MÜLLER, B. (Ed.). *Cyberspace and International Relations:* theory, prospects and challenges. Berlim Heidelberg: Springer, 2014. p. 77–95.

WENDT, E. Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos. *Revista Brasileira de Inteligência*, Brasília: ABIN, n. 6, abr. 2011, p. 15–26.

WHITE HOUSE. *Cyberspace Policy Review:* Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington, D.C.: Executive Office of the President of the United States, 2009.

ZERO Days. Direção: Alex Gibney. Estados Unidos, Magnolia Pictures, 11 de fevereiro de 2016. Colorido. 116 minutos. Disponível em: <https://www.amazon.com/Zero-Days-Colonel-Gary-Brown/dp/B01I2EKYTC>. Acesso em: 20 de jun. 2017.

Governança e Imigrações