Mural Internacional
V. 9 | N. 1
JAN-JUN 2018

O uso de ciberataques em eleições e as Relações Internacionais

The use of cyberattacks in elections and International Relations

THIAGO JACOBINO HONÓRIO[1]

Recebido em:
30 de Janeiro de 2018

Received on:
January 30, 2018

Aceito em:
27 de Novembro de 2018

Accepted on:
November 27, 2018

DOI: 10.12957/rmi.2018.32570

Resumo: Durante a campanha presidencial dos Estados Unidos no ano de 2016 o governo do país acusou agentes de inteligência russa de usarem ataques cibernéticos contra a empresa responsável pelos softwares que são usados no sistema eleitoral do país. O caso americano constitui apenas um entre vários outros ocorridos recentemente. Interferências externas em eleições não constituem algo novo, entretanto, o caso representa uma tendência na qual o meio cibernético torna-se um valioso recurso, pois, com o avanço da tecnologia da informação nos meios democráticos surgem novas vulnerabilidades advindas do ciberespaço. O trabalho tem por objetivo expor a questão do uso dos ataques cibernéticos em eleições. Sustenta que é necessário o desenvolvimento de tecnologias de proteção e privacidade para a garantia dos processos democráticos na era digital. Como estudo de caso o trabalho irá se baseará na exposição dos casos da eleição dos E.U.A em 2016 e eventos semelhantes ocorridos em outros países no mesmo período.

Palavras-chave: Relações Internacionais; ciberataques; eleições.

Abstract: During the United States presidential campaign in the year 2016, the US government has accused Russian intelligence agents of attacks against companies responsible for the use of software used in the country's electoral system. The American case its only one between several others occurred recently. External interference in elections are not new, but the case represents a trend in how cybernetics becomes a valuable resource because, with the advancement of technology in democratic circles, new vulnerabilities emerges from cyberspace. The paper aims to raise an issue about cyberattacks in elections. Sustains the need for the development of technologies for protection and privacy of democratic process in the digital era. As a case study the work will be based on the exposure of US election cases in 2016 and similar events that occurred in other countries in the same period.

Keywords: International Relations, cyberattacks; elections.

[1] Mestre em Estudos Estratégicos pela Universidade Federal Fluminense. Pesquisador associado ao Laboratório de Simulações e Cenários da Escola de Guerra Naval (EGN). **Endereço para correspondência:** Av. Pasteur, 480 - Urca, Rio de Janeiro - RJ, 22290-240, Brasil. **Email**: tjhonorio@gmail.com

Introdução

Sistemas eleitorais são parte essencial do funcionamento de sociedades democráticas. As eleições acabam sendo o veio condutor pelo qual não apenas se determina quem irá governar, mas como irá governar. No geral eleições tendem a ter disputas que refletem os diferentes matizes nas quais setores da sociedade reivindicam demandas, pautas e agendas. As políticas domésticas e externas adotadas nos anos vindouros serão influenciadas em grande parte pela vitória dos grupos e partidos que ganham tais disputas. Por essa razão outros Estados tentam influenciar processos democráticos em outros com base em seus interesses políticos, econômicos e ideológicos no intuito de obter ganhos. Para fins desse trabalho o fenômeno será aqui chamado como Intervenção Eleitoral Externa (IEE). Acerca do tema define Dov H. Levin que tal fenômeno constitui:

> " [...] uma situação em que um ou mais países soberanos intencionalmente realiza ações específicas para influenciar uma próxima eleição em outro país soberano, de maneira aberta ou encoberta, que eles acreditam que favorecerá ou ferirá um dos lados que contestam aquela eleição ou pode incorrer custos para os intervenientes ou o país intervenido" (Levin 2016a, p.3)[2]

Em janeiro de 2017 o jornal *The Intercept* vazou um documento da Agência Nacional de Segurança dos Estados Unidos (N.S.A) que afirma que durante a campanha presidencial americana no ano de 2016 o governo russo executou um ataque cibernético a pelo menos uma empresa que produzia softwares usados no sistema eleitoral, além de enviar e-mails contendo vírus para pessoas que trabalhavam nos locais de votação (Cole *et al* 2017). Acredita-se que o governo russo possuía interesse em sabotar a campanha da candidata Hillary Clinton, em detrimento de seu concorrente Donald Trump e buscou nos meios digitais interferir no processo. Apesar de o caso americano ter conquistado maior cobertura por meios da imprensa, nos últimos anos outros casos que serão expostos abaixo apontam estratégias semelhantes em outros países.

Contudo, o caso referido apenas reflete uma tendência crescente. Em uma sociedade informacional, ou seja, uma

[2] Tradução nossa. Do original: "a situation in which one or more sovereign countries intentionally undertakes specific actions to influence an upcoming election in another sovereign country in an overt or covert manner which they believe will favor or hurt one of the sides contesting that election and which incurs, or may incur, significant costs to the intervener(s) or the intervened country".

sociedade estruturalmente permeada pelas tecnologias da informação e comunicação, conforme o sistema eleitoral ou qualquer outra atividade social é informatizada, ou seja, absorve e instrumentaliza o emprego dessas tecnologias, adquire conjuntamente suas vantagens e vulnerabilidades. Conforme nos lembra o filósofo francês Paul Virilio "*inventar o veleiro ou o barco a vapor é inventar o naufrágio"*[3] (Virilio 2007, p.10). Assim todos os acidentes e intempéries relativas ao ciberespaço tornam-se novas vulnerabilidades dos sistemas eleitorais, dos aparatos e estruturas democráticas dos países e por fim da segurança nacional.

O presente trabalho pretende abordar o uso de ciberataques como instrumentos de intervenção em processos democráticos e suas implicações para as Relações Internacionais. É importante enfatizar que o trabalho possuí caráter exploratório, de modo que não pretende apresentar nenhum resultado de investigação sistemática, mas sim, levantar novas questões para a pesquisa científica. Através da exposição dos casos intenta apontar novas possibilidades de emprego de força, neste caso, através do uso dos meios digitais em processos eleitorais. Sustenta que os processos de informatização trazem consigo novas oportunidades e vulnerabilidades e que devido a características referentes ao ciberespaço, o recurso a tais métodos como instrumentos de projeção de poder nos fazem repensar o papel e relevância da segurança dos meios informacionais, mas também a proteção dos meios democráticos.

Democracia, eleições e as e ingerências externas

Influenciar processos democráticos não constitui ineditismo. Durante a Guerra Fria por exemplo o 'terceiro mundo' sofreu constantes interferências diretas de potências, muitas das vezes apoiados ou demandados por Washington, que resultaram em eleições de candidatos desejados ou mesmo a deposição de governos democráticos gerando as ditaduras que perduraram por boa parte da segunda metade do século passado na América do Sul[4]. E mesmo após o fim do período bipolar alguns autores apontam a presença direta de influência eleitoral de potências na América Latina através de emprego de capital, mesmo durante o período de governos de esquerda na região (Garland e Biglaiser,

[3] Tradução nossa. Do original "To invent the sailing ship or the steamer is to invent the shipwreck".

[4] O caso mais notório no Brasil foi a CPI aberta em 1963 para investigar acerca do financiamento de políticos pelo Instituto Brasileiro de Ação Democrática (IBAD) que financiava e dava suporte a candidatos de postura anticomunista com capital advindo dos E.U.A.

2009). Acerca dos IEE Shulman e Bloom afirmam que os estudos empíricos e teóricos acerca do tema são "surpreendente fracos" (Shulman e Bloom 2012, p.446). Também assinalam que acadêmicos das Relações Internacionais prestam pouca atenção sobre como a tais ações influenciam o comportamento de Estados-nação e seus cidadãos (p.447). É possível que tal relação possa ser explicada devido a preponderância do realismo estrutural no campo e por conseguinte a posição defendida por alguns autores desta corrente na qual o Estado é visto uma caixa-preta, atendo-se distante das suas dinâmicas domésticas (Mearshimer 2007, p.72).

Em um sistema globalizando e interligado, no qual aspectos econômicos, culturais e políticos interagem, os resultados de uma eleição tendem a ter efeitos que ultrapassam o território nacional impactando grupos de interesse internacionais, investidores ou mesmo minorias étnicas. Todavia devido as suas capacidades de projeção e interesses amplos grandes potências tendem a ter maior preponderância em intervenções. Segundo Dov. H Levin no artigo *When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results* (2016b), o mais completo estudo feito sobre o tema até o momento, o autor afirma que entre os anos de 1946 e 2000 os Estados Unidos e a União Soviética/Rússia intervieram 117 vezes diretamente em países democráticos. O que equivale, segundo o Levin, a 1 em cada 9 eleições realizadas durante esse período (p. 189). Os métodos utilizados tradicionalmente combinavam desde ajuda financeira para partidos ou políticos conhecido como Investimento Direto Estrangeiro (IDE), passando por pressões, ameaça de cortes de fundos de ajuda internacional e o emprego de agências de segurança para sabotagens. Nos anos recentes conforme será visto Estados encontraram no ciberespaço novos meios de ação que expandem as capacidades de intervenção eleitoral externa.

Os ciberataques nas eleições e política internacional.

As relações entre o país norte americano e a Rússia são historicamente conflitivas desde o período da Guerra Fria. Apesar de um breve arrefecimento das relações entre os dois países no início da década de 90, a partir da eleição de Vladimir Putin a presidência do país em 2000 houve uma retomada das tensões. Em 2011, como primeiro ministro do país, Putin havia acusado Hillary Clinton, então secretária de Estado, de incitar protestos na capital Moscou através de seus opositores políticos (Herszenhorn e

Barry, 2011). Em contrapartida Clinton no mesmo ano, teria levantado dúvidas acerca das eleições russas (Elder, 2011). Especula-se que a Rússia tenha visto no concorrente republicano, Donald Trump, maior possibilidade de obter ganhos em relação a Hillary. Além disso, durante a campanha o próprio Trump havia sugerido arrefecer as relações entre os dois países. Considerasse que o governo russo além dos ciberataques foi responsável por comprar propaganda na internet para interferir na campanha presidencial (Wakabayashi, 2017). Segundo Jacqueline Van De Velde (2017) a Rússia usou uma série de grupos hackers para diversos fins. O grupo conhecido como *Cozy Bear* foi responsável se encarregaram de atacar o Comitê Nacional do Partido democrata. Outro grupo conhecido como *Fancy Bear* teria se encarregado de atacar o partido republicano. Enquanto isso uma série de ataques foram conduzidos contra organizações não governamentais e sem fins lucrativos (Van de Velde 2017. p. 11). O primeiro sucesso da estratégia russa ocorreu quando as informações obtidas do partido democrata foram vazadas através do site Wikileaks, revelando que o partido vinha tentando sabotar o candidato que concorreu nas primárias contra Hillary, Bernie Sanders (Shear e Rosenberg, 2016), o escândalo acabou resultando na saída da presidente do comitê do partido Debbie Wasserman Schultz.

Entretanto o envolvimento mais direto ao processo eleitoral veio apenas mais a frente. Segundo oficiais do governo americano 21 estados americanos, quase metade do país, sofreram ciberataques direcionados aos sistemas eleitorais de votação. Segundo o documento vazado pelo *Intercept*, em novembro, dias antes da votação o GRU[5], um órgão de inteligência do governo russo conduziu uma série de operações no intuito de obter dados acerca do hardware e software usados nos locais de votação e produzidos pela empresa VR Systems baseada na Flórida. De acordo com o documento:

> Os atores da Diretoria de Inteligência Principal do Estado-Maior Russa ... executaram operações de ciberespionagem contra uma empresa americana nomeada em agosto de 2016, evidentemente para obter informações sobre soluções de software e hardware relacionadas a eleições. ... organizações de governo local dos EUA. Organizações governamentais locais dos EUA. Organizações governamentais locais dos EUA (Cole *et al*, 2017)[6].

[5]Do inglês *Russian General Staff Main Intelligence Directorate*.

[6] Tradução livre. Do original: "Russian General Staff Main Intelligence Directorate actors … executed cyber espionage operations against a named U.S. company in August 2016, evidently to obtain information on elections-related software and hardware solutions. … The actors likely used data

Segundo o próprio Intercept contas de e-mail ligadas ao fornecedor do software utilizado e mais de 100 oficiais que trabalhavam nos locais de votação sofreram ataques do tipo *phishing*[7].

O caso americano é apenas o noticiado: existem episódios semelhantes ocorridos na Alemanha e França. No caso alemão há suspeitas que o governo russo tenha utilizado estratégia semelhante para tentar interferir na eleição em 2017. Haveria interesse russo em evitar a reeleição da chanceler Angela Merkel, crítica da política russa na Síria e Ucrânia nos anos anteriores (Schwirtz, 2017). Hackers russos também são acusados de terem roubados dados sensíveis do governo alemão em 2015 o que teria levado as autoridades germânicas a temer algum vazamento durante a eleição (Eddy, 2016). A França também acusou os russos em 2017 de serem responsáveis por um ataque cibernético que gerou o vazamento de uma série de documentos relativos a campanha do então candidato Emmnuel Macron dias antes da votação. O vazamento do material foi na véspera da votação, algumas horas antes do horário limite no qual os candidatos podiam fazer campanha antes da votação, tornando a capacidade de mitigar danos de Macron limitada por causa do tempo (Breeden e Chan e Perloth, 2017). Em maio do mesmo ano o governo de Malta também acusou o governo russo de ciberataque nos mesmos moldes relatados acima (Doward, 2017)

O uso de ciberataques parece ter se tornado parte da estratégia russa. Conforme Charles E. Ziegler afirma em *International dimensions of electoral process: Russia, the USA, and 2016* que juntamente ao financiamento de grupos extremistas, a promoção de valores conservadores críticos do liberalismo ocidental, colocando-os na defensiva, o que aponta para o retorno a estratégias de desinformação que remontam a União Soviética, dessa vez munido do domínio informacional (Ziegler 2017, p.2). Em outras ocasiões o governo russo foi acusado de ter atacado a Geórgia e a Estônia respectivamente em 2007 e 2008 causando danos aos sistemas de comunicações e dificultando a operacionalidade estatal nesses países. No caso da guerra entre a Rússia e a Geórgia em 2008 o governo russo parece ter combinado o uso de ciberataques com os movimentos cinéticos feitos militarmente na antiga

obtained from that operation to… launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations".

[7] Tipo de ataque no qual e-mails falsos tentam obter dados atraindo os alvos para sites ou outros meios nos quais eles possam entregar informações. Este tipo de ataque geralmente é usado tanto para crimes cibernéticos quanto para espionagem.

república soviética (Deibert e Rohozinski e Nishihata, 2012).

Apesar dos casos mais recentes remeterem ao governo russo, vale lembrar, que após as revelações feitas pelo ex-prestador de serviços da CIA Edward Snowden em 2013 e dos respectivos esquemas de espionagem em massa que atingiram milhões de pessoas e incluía chefes de estado como os do Brasil e Alemanha, deixa claro que países do chamado 'Cinco Olhos' aliança formada por Austrália, Nova Zelândia, Reino Unido especialmente Estados Unidos possuem capacidade de realizar operações de ciberataque de nível extremamente avançado, assim como China, Israel e respectivamente a Rússia.

Eleições na era da Sociedade da Informação.

Todas as sociedades em certa medida estruturam-se através de suas tecnologias. A moderna introdução de sistemas digitais em processos eleitorais é reflexo de um fenômeno profundo que funda raízes na penetração cada vez maior das tecnologias da informação nas atividades humanas. Esse construto social no qual a informatização se expande e torna-se peça chave da sociedade é conhecida como "Sociedade da Informação". O cientista político espanhol Manuel Castells define o conceito da seguinte forma:

> [...] o termo "informação" indica o atributo de uma específica forma de organização social na qual a geração da informação, processamento e transmissão tornam-se as fontes fundamentais de produtividade e poder por causa das novas condições tecnológicas emergentes neste período histórico (Castells 2010. p. 21)[8].

Conforme Castells aponta a nova tecnologia cria dimensões de interação e poder que transformam as estruturas sob as quais a sociedade se organiza tanto materialmente nas esferas de produção e troca, como no modo com o qual a política pode ser exercida tanto de modo doméstico como internacional. Os episódios acima são reflexos da sociedade da informação contemporânea e espelham as relações de poder decorrentes do emprego de meios efetivos da era informacional.

Ciberespaço e poder cibernético

De modo geral ciberespaço é uma abstração. Conforme nos explica o geógrafo Mark Graham a impossibilidade de atribuir dimensões espaciais faz com que a melhor forma

[8] Tradução livre "In contrast, the term "informational" indicates the attribute of a specific form of social organization in which information generation, processing, and transmission become the fundamental sources of productivity and power because of new technological conditions emerging in this historical period".

de definir o ciberespaço é como um domínio etéreo (Graham, 2013). Seu caráter ubíquo impede determinar onde o ciberespaço se encontra. Não nos é possível ir ou vir de tal domínio. Ele permeia todo o espaço físico mas não se encontra em nenhum lugar. Apesar disso os eventos ocorridos através desse domínio de modo algum podem ser considerados 'virtuais'. Ele é parte do universo cinético ao qual a vida política se estrutura, afinal como nos lembra Castells "informa e impõe, decisões econômicas poderosas a cada momento na vida em rede" (Castells 2010, p. 214). O ciberespaço é uma parte da realidade e como tal interage cada vez mais com eventos que existem aquém de sua existência. As rivalidades entre potências independem das redes de computadores, mas a sua presença abre novos domínios para o poder. O assim chamado poder cibernético pode ser definido como todo o tipo de relação ou expressão de poder através do ciberespaço. Este trabalho entede poder como a capacidade de um ator de transformar eventos e altera-los (Giddens, 1985). Se o poder constitui um fenômeno do âmbito da política, logo, nos leva a pensar que o poder cibernético existe no espectro da ciberpolítica, ou seja, a política que existe em decorrência e através do ciberespaço. John B. Sheldon resume a relação entre a fisicalidade e os fenômenos do ciberespaço:

> Ciberespaço é o domínio no qual as operações cibernéticas ocorrem; poder cibernético é a soma dos efeitos estratégicos gerados pelas operações cibernéticas a partir do ciberespaço. Estes efeitos podem ser sentidos no ciberespaço, bem como os outros domínios da terra, mar, ar e espaço, e também pode ser cognitivamente eficaz com os seres humanos individuais (Sheldon 2011, p.96)[9].

Importante para esse ponto do trabalho é compreendermos a noção do que é conhecido como ataque cibernético. O termo remete ao ataque que ocorre através do ciberespaço. De acordo com o glossário organizado por Richard Kissel um ataque cibernético pode ser entendido da seguinte forma:

> Um ataque, via ciberespaço, visando o uso do ciberespaço por um empreendimento com o objetivo de interromper, desativar, destruir ou controlar maliciosamente um ambiente/infraestrutura de computação; ou destruindo a integridade dos dados ou roubando informações controladas (Kissel 2014, p. 57)[10].

[9] Tradução nossa: "Cyberspace is the domain in which cyber operations take place; cyberpower is the sum of strategic effects generated by cyber operations in and from cyberspace. These effects can be felt within cyberspace, as well as the other domains of land, sea, air, and space, and can also be cognitively effective with individual human beings".

[10] Tradução nossa: "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting,

A definição acima é ampla, todavia, ajuda a elucidar o grande número de táticas, estratégias e ferramentas podem ser empregadas em diferentes ações. Atualmente o emprego de ciberataques oferece-se um conjunto de vantagens se comparado ao emprego tradicional de meios cinéticos. Em primeiro lugar o ciberespaço é um ambiente no qual muitas vezes as ações perpetradas não permitem clara identificação dos atores envolvidos. A ocultação faz com que muitas vezes os verdadeiros interessados em um ataque cibernético não possam ser diretamente atribuídos. No caso americano Apesar de inicialmente ter negado qualquer relação, o presidente russo chegou a sugerir que hackers patriotas de seu país pudessem ter sido os responsáveis pelos ataques cibernéticos (McKirdy e Ilyushina, 2017). Qualquer atribuição direta torna-se difícil perante a imensa capacidade de disfarçar ataques cibernéticos através da rede. Ademais, Estados possuem recursos e capital para dispor dos custos de meios avançados para camuflar o ataque de origem, sendo assim por mais que na maioria dos casos existam fortes suspeitas a possibilidade de estabelecer relações diretas é extremamente difícil.

Ainda existe a questão da resposta adequada caso um Estado seja responsabilizado por uma IEE. Sob o ponto de vista jurídico Jacqueline Van de Velde problematiza a questão. Aponta que a maioria dos autores foca em respostas no âmbito de contra-ataques cibernéticos. Entretanto vê nos aparatos do Direito Internacional, especialmente no direito consuetudinário, o direito que surge dos costumes e práticas que criam jurisprudência, meios pelos quais os Estados podem recorrer em caso de agressão:

> No caso de danos físicos à infraestrutura, como equipamentos de votação, os estados têm a oportunidade de invocar a Carta da ONU e atacar o Estado hacker. E no caso de "roubar" informações, os estados podem ir ao tribunal nacional para lutar contra a espionagem. [...] Nem o direito internacional nem o direito interno falam claramente sobre a questão, mas desesperados por respostas os estudiosos provaram-se também dispostos a defender o uso do direito internacional consuetudinário e a aplicação da doutrina das contramedidas, como forma de remediar os estados

disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."

"prejudicados" (Van de Velde 2017. p. 38)[11].

O ineditismo do fenômeno pode fazer com que demore alguns anos para a formação de aparatos e mecanismos no âmbito jurídico internacional para lidar com IEE cibernéticas. Contudo, através do direito consuetudinário as práticas e costumes domésticos jurídicos podem ser incorporadas de modo a acelerar o processo de inserção deste fenômeno no campo do direito. Apesar da dificuldade de atribuição relatadas acima, a busca pelo desenvolvimento de meios de resposta aceitos pela comunidade internacional como legítimos é um importante mecanismo para os Estados-nação recorrem caso se sintam lesados.

Conclusão

O trabalho expôs dois distintos fenômenos e sua relação contemporânea. Por um lado os processos de Intervenção Externa Eleitoral que conforme mostrado possuem longo histórico. Por outro a conjunção entre esse fenômeno e outro mais recente, ou seja, os ataques cibernéticos que remonta a uma nova dimensão. As exposições de caso atentaram apontar como através de novas formas de tecnologia como a tecnologia da informação foi possível influenciar processos eleitorais em Estados-nação. Todavia, a ocorrências de tais eventos apenas foi possível devido a existência do domínio que constitui o ciberespaço e concomitantemente o processo de informatização da sociedade que apesar de trazer grandes vantagens como a velocidade e redução de custos, abre caminho para novas vulnerabilidades como os ataques cibernéticos e novas formas de poder, ou seja, o poder cibernético. Também é importante ressaltar que apesar dos eventos relatados, tais episódios não mudam dinâmicas tradicionais das Relações Internacionais como as relações de poder exercidas entre potências para com outros Estados. Contudo é necessário observar que conforme foi visto o tema das IEE ainda é escassamente pesquisado no campo das R.I's. Apesar de serem necessários mais estudos acerca, os trabalhos existentes delineiam algumas formas pelas quais o emprego do poder externo consegue interagir nos fenômenos intra-estatais. Em contraposição a preceitos da teoria realista e o respectivo distanciamento das dinâmicas internas (caixa preta), os estudos sobre IEE abrem espaço para

[11] Tradução nossa. Do original: "In the case of physical damage to infrastructure, such as voting equipment, states have the opportunity to invoke the UN Charter and attack the hacking state. And in the case of "stealing" information, states can go to domestic court to fight espionage. [..] Neither international law nor domestic law clearly speaks to the issue, but—desperate for answers—scholars have proven all-too-willing to argue for the use of customary international law, and the application of countermeasures doctrine, as a way to remedy states' harms".

novas questões e explorações para pesquisa científica no campo do internacional.

Os processos eleitorais têm papel decisivo em sistemas democráticos. Conforme visto interferência externa por meio de ataques cibernéticos gerou debates e repercussões nos países atingido. Apesar dos exemplos apresentados serem de países desenvolvidos, muitos países em desenvolvimento, inclusive o Brasil, possuem processos eleitorais e plataformas digitalizadas. É necessário repensar o papel que o desenvolvimento e investimento em meios de proteção de dados e redes deve ocupar devido a importância dos instrumentos democráticos. Conforme vimos por motivos de natureza do ciberespaço é extremamente difícil a atribuição dos ataques ocorridos e os países atingidos ainda encontram pouco respaldo no Direito Internacional ou mesmo um aparato de resposta legitimamente aceito pela comunidade internacional.

O futuro na era digital pode proporcionar novas experiências de democracia direta aos indivíduos. Poderá reduzir custos dos processos eleitorais e reduzir o tempo das atividades relacionadas. Porém a garantia da autonomia nesses sistemas dependerá do desenvolvimento e investimento em tecnologias que garantam a proteção de dados e privacidade. Os processos de informatização se expandem consistentemente em várias áreas das atividades humanas, mas não se manterão aquém da Política Internacional e de seus revezes. Os fenômenos advindos do ciberespaço são uma das facetas pelas quais a tecnologia hoje interage com a sociedade. Nesse contexto a defesa e proteção dos meios digitais transcende a tecnicidade pura e torna-se em si própria uma defesa dos instrumentos democráticos e soberanos de uma nação.

Referências Bibliográficas

Breeden, Aurelien; Chan, Sewell; Perloth Nicole (2017) Macron Campaign Says It Was Target of ‘Massive’ Hacking Attack. *The New York Times*, 5 de maio. Disponível em: <https://www.nytimes.com/2017/05/05/world/europe/france-macron-hacking.html>. [Acesso em: 01 Nov. 2017]

Castells, M. (1996). *The information age: Economy, society, and culture*. Volume I: The rise of the network society.

Castells, M. (2010). *End of millennium* (Vol. 3). John Wiley & Sons.

Cole, M. (2017). Top-Secret NSA Report Details Russian Hacking Effort Days before 2016 Election. *The Intercept*, 5 de junho. Disponível em: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ [Acesso em: 01 Nov. 2017]

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). 'Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war'. *Security Dialogue*, 43(1), 3-24.

Doward, Jamie (2017). Malta accuses Russia of cyber-attacks in run-up to election. *The Guardian*. 27 de maio. Disponível em: < https://www.theguardian.com/world/2017/may/27/russia-behind-cyber-attacks-says-malta-jseph-muscat>. [Acesso em: 01 Nov. 2017]

Eddy, M. (2016). After a cyberattack, Germany fears election disruption. *The New York Times*. 8 de dezembro. Disponível em: < https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html>. [Acesso em: 01 Nov. 2017]

Elder, M. (2011). Vladimir Putin Accuses Hillary Clinton of Encouraging Russian Protests. *The Guardian*, 8 de dezembro. Disponível em: <https://www.theguardian.com/world/2011/dec/08/vladimir-putin-hillary-clinton-russia>. [Acesso em: 01 Nov. 2017]

Garland, M. W., & Biglaiser, G. (2009). 'Do electoral rules matter? Political institutions and foreign direct investment in Latin America'. *Comparative Political Studies*, 42(2), 224-251.

Graham, M. (2013). 'Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities?'. *The Geographical Journal*, 179(2), 177-182.

Herszenhorn, D. M., & Barry, E. (2011). Putin contends Clinton incited unrest over vote. *New York Times*, 8 de dezembro. Disponível em:

http://www.nytimes.com/2011/12/09/world/europe/putin-accuses-clinton-of-instigating-russian-protests.html [Acesso em: 01 Nov. 2017]

Kissel, R. (Ed.). (2011). *Glossary of key information security terms*. Diane Publishing

Levin, D. H. (2016a). 'Partisan electoral interventions by the great powers: Introducing the PEIG Dataset'. *Conflict Management and Peace Science*. p.1-19, 2016.

Levin, D. H. (2016b). 'When the great power gets a vote: The effects of great power electoral interventions on election results''. *International Studies Quarterly*, 60(2), 189-202.

Mearsheimer, J. J. (2007). 'Structural realism. International relations theories': *Discipline and diversity*, 83.

McKirdy, Euan; Ylyushina, Mary (2017). Putin: 'Patriotic' Russian hackers may have targeted US election". *CNN*, 2 de junho. Disponível em: < http://edition.cnn.com/2017/06/01/politics/russia-putin-hackerselection/index.ht-ml >. [Acesso em: 01 Nov 2017]

Schwirtz, Michael (2017). "German Election Mystery: Why No Russian Meddling?". The *New York Times*, 21 de setembro. Disponível em: <https://www.nytimes.com/2017/09/21/world/europe/german-electionrussia.htm-l>. [Acesso em: 01 Nov 2017]

Shear, M. D., & Rosenberg, M. (2016). Released Emails Suggest the DNC Derided the Sanders Campaign. *New York Times*, 22 de julho. Disponível em: <https://www.nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html>. [Acesso em: 01 Nov 2017]

Sheldon, J. B. (2011). 'Deciphering cyberpower: Strategic purpose in peace and war'. *Strategic Studies Quartely*, v5, n 2. p. 95-112, 2011.

Shulman, S., & Bloom, S. (2012). 'The legitimacy of foreign intervention in elections: the Ukrainian response'. *Review of International Studies*, 38(2), 445-471.

Van De Velde, J. (2017). 'The Law of Cyber Interference in Elections'. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=304 3828>. [Acesso em: 01 Nov 2017]

Virilio, P. (2007). *The original accident*. Polity.

Wakabayashi, Daisuke (2017). Google Finds Accounts Connected to Russia Bought Election Ads. *New York Times*, 9 de outubro. Disponível em < https://www.nytimes.com/2017/10/09/technology/google-russian-ads.html?smid=fb-nytimes&smtyp=cur > [Acesso em: 01 Nov 2017]

Wojtasik, W. (2013). 'Functions of elections in democratic systems'. *Political Preferences*, 4, 2013.

Ziegler, C. E. 'International dimensions of electoral processes: Russia, the USA, and the 2016 elections'. *International Politics*, 1-18.