Faculdade Damas da Instrução Cristã

Curso de Relações Internacionais

João Aureliano Bezerra

A Intervenção Russa nas Eleições Americanas de 2016:

A Interferência nas Eleições Através das Mídias Sociais

Recife

2020

João Aureliano Bezerra

A intervenção Russa nas Eleições Americanas de 2016:

A Interferência nas Eleições Através de Mídias Sociais

Trabalho de conclusão de curso como exigência parcial para graduação no curso de Relações Internacionais sobre orientação do Prof. Charles Hodges

Recife

2020

Ficha catalográfica
Elaborada pela biblioteca da Faculdade Damas da Instrução Cristã

Bezerra, João Aureliano.
B574i A intervenção russa nas eleições americanas de 2016: a interferência nas eleições através das mídias sociais / João Aureliano Bezerra. – Recife, 2020.
42 f. : il. color.

Orientador: Prof. Charles Hodges.
Trabalho de conclusão de curso (Monografia – Relações Internacionais) – Faculdade Damas da Instrução Cristã, 2020.
Inclui bibliografia

1. Estados Unidos. 2. Rússia. 3. Eleições. 4. Mídias sociais. 5. Cybersecurity. I. Hodges, Charles. II. Faculdade Damas da Instrução Cristã. III. Título.

327 CDU (22. ed.) FADIC (2020.1-618)

FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ

CURSO DE RELAÇÕES INTERNACIONAIS

João Aureliano Bezerra

Trabalho de conclusão de curso como exigência parcial para graduação no curso de Relações Internacionais sobre orientação do Prof. Charles Hodges

Aprovada em:

BANCA EXAMINADORA

Pedro Paulo Procópio

Bianor Teodósio

Charles Hodges

Recife

2020

Resumo

Após as eleições de 2016, o cenário internacional foi apresentado novamente com um novo desafio, interferências em eleições através de campanhas e esforços de grupos internacionais em mídias sociais. Este novo desafio apresenta um grande perigo para os estados, devido ao uso de veículos de informação e comunicação recentes e a falta de conhecimento geral sobre os métodos utilizados e possíveis consequências dos ataques. Com os principais objetivos de identificar, mapear e analisar a interferência russa nas eleições americanas de 2016, seus precedentes e a resposta dos Estados Unidos, este trabalho procura explorar o perigo representado pelos métodos utilizados por *hackers* russos, para interferir nas eleições de 2016 e entendê-lo através de uma visão realista, aplicando a ideologia dentro do âmbito de *cybersecurity*.

Palavras Chave: Estados Unidos. Rússia. Eleições. Mídias Sociais. Cybersecurity.

Abstract

After the 2016 elections, the international scenario was presented again with a new challenge, interference in elections through campaigns and efforts of international social media groups. This new challenge presents a major danger for states due to the use of recent information and communication vehicles and the lack of general knowledge about the methods used and possible consequences of the attacks. With the main objectives of identifying, mapping and analyzing Russian interference in the 2016 U.S. elections, its precedents and the response of the United States, this paper seeks to explore the danger posed by the methods used by Russian hackers to interfere in the 2016 elections and understand it through a realistic vision, in which this ideology will be applied within the scope of cybersecurity.

Keywords: United States. Russia. Elections. Social Media. Cybersecurity.

Lista de Abreviaturas e Siglas

ARPANET	: *Advanced Research Projects Agency Network*
CIA	: *Central Intelligence Agency*
CPAC	: *Conservative Political Action Conference*
DNC	: *Democratic National Committee*
FBI	: *Federal Bureau of Investigation*
FSB	: *Russian Federal Security Service*
GRU	: Departamento Central de Inteligência
IRA	: *Internet Research Agency*
KGB	: Comité de Segurança do Estado
NSA	: *National Security Agency*
OTAN	: Organização do Tratado do Atlântico Norte
UFES	: Universidade Federal do Espírito Santo
US:	: Estados Unidos

Sumário

1. Introdução

A interferência russa nas eleições americanas de 2016 é um tema que é regularmente discutido por pessoas dentro da esfera política americana. O início do debate ocorreu durante a então campanha do atual presidente americano Donald J. Trump.

Durante o verão de 2016, o jornal americano *Wall Street Journal* revelou através de suas análises que várias contas falsas na rede social Twitter foram utilizadas pela *Internet Research Agency* (IRA), uma agência russa que utiliza mídias sociais para promover interesses russos em outros países.

Nessa época, o então candidato Trump passou a negar a necessidade de sanções direcionadas à Rússia e passou a promover políticas e ações mais amigáveis em direção ao país. Simultaneamente, hackers ligados à *Russian Federal Security Service* (FSB), ganharam acesso a servidores da *Democratic National Committee* (DNC) expondo informações consideradas confidenciais.

Mais tarde em 2017, em seus relatórios de janeiro, o FBI, a *National Security Agency*(NSA) e a *Central Intelligence Agency*(CIA) afirmaram que o presidente russo, Vladmir Putin, ordenou que suas agências iniciassem atividades online com os propósitos de prejudicar a campanha da candidata Hillary Clinton e interferir no processo democrático americano.

Como resultado várias críticas têm sido levantadas contra sites como Twitter e Facebook, devido à sua inabilidade de impedir a criação e uso de *bots* (Contas falsas criadas para disseminar ideias e narrativas especificas através de sites) em mídias sociais feitos por grupos russos com o objetivo de gerar desinformação e propaganda.

Bots criados e utilizados para fins políticos, porém, não são algo novo. A estratégia tem sido documentada tanto nos Estado Unidos quanto em outros países, muitos deles com o objetivo de apoiar partidos específicos. Em 2010 por exemplo, bots foram encontrados “conversando” favoravelmente sobre o

candidato John A. Boehner. A “conversa” incluía links para sites e blogs do candidato[1]. Outro uso comum para bots, é de aumentar o número de seguidores e de curtidas nas páginas de mídias sociais de certos candidatos, fazendo-os parecer mais populares.

No passado, devido ao fato de muitas das atividades relatadas por bots terem se originado dentro dos próprios países afetados(muitas vezes sendo promovidas por entidades governamentais ou por ativistas políticos), as questões securitárias relacionadas a esses ataques muitas vezes eram vistas como um problema interno. Além disso, estados raramente tomavam medidas preventivas ou procuravam regular atividades de bots, muitas vezes por falta de urgência e/ou conhecimento sobre o assunto. Essa inadimplência com questões securitárias permitiu a popularização e evolução dos bots, que devido a programas mais avançados, se tornaram capazes de ações mais complexas.

As atividades russas, devido a suas implicações, forçaram o governo americano a tomar medidas preventivas contra o uso de bots pela primeira vez. Essas medidas vão ter grandes consequências no mundo virtual, não só devido ao espaço detido pelos americanos on-line[2], mas também devido à sua possível influência na tomada de decisão de outros países, que provavelmente no futuro terão que lidar problemas similares.

Utilizando-se do método qualitativo, o presente projeto vai se utilizar de fontes e materiais secundários como base do estudo de caso e fará a revisão de documentos oficiais de instituições governamentais americanas e trabalhos e pesquisas feitas sobre a intervenção russa, análise histórica de ações e iniciativas tomadas pelo governo americano no âmbito de *cybersecurity* e, por fim, medidas tomadas pelo governo americano como forma de resposta a dita intervenção durante o período de 2016-2019.

---

[1]Indiana University Research Group. 2010. Disponivel em: https://truthy.indiana.edu/highlights/. Acesso em: 19 Dez. 2019

[2] J. Clement. 20 Aug 2019. Disponivel em: https://www.statista.com/topics/2237/internet-usage-in-the-united-states/. Acesso em: 19 Dez. 2019

1.1 Metodologia

O projeto tem como natureza de sua metodologia uma aproximação exploratória, em seu primeiro capítulo apresentando o histórico de ações dos EUA e Rússia no âmbito de *cybersecurity*. A apresentação desses dados é realizada através pesquisas feitas com relatos históricos e têm o objetivo de informar o leitor sobre os eventos precedentes à intervenção russa nas eleições americanas de 2016.

O segundo capítulo tem o intuito de identificar e analisar os eventos ligados às questões de cybersecurity que decorreram após a confirmação da interferência russa, as possíveis motivações dos russos e o crescente uso das mídias sociais como formas de afetar eleições (dentro do período de 2016-2019). A identificação e análise destes dados foram feitas através de relatos históricos, notícias e pesquisas previamente feitas por universidades e instituições governamentais.

O terceiro capítulo terá como objetivo apresentar as respostas imediatas dos EUA aos ataques cibernéticos orquestrados pela Rússia, e as alterações e impactos que estes eventos tiveram para questões de segurança cibernética para os Estados Unidos e para o resto do mundo.

Por fim, a conclusão tem como intuito avaliar os ataques, intenções e objetivos dos russos, como também avaliar as respostas tomadas pelos Estados Unidos. A avaliação será feita através da aplicação de uma perspectiva realista dentro do cenário internacional e virtual.

Utilizando-se do método qualitativo, o projeto vai se utilizar de fontes e materiais secundários para base do estudo de caso e fará a revisão de documentos oficiais de instituições governamentais americanas e trabalhos e pesquisas feitas sobre a intervenção russa, análise histórica de ações e

iniciativas tomadas pelo governo americano no âmbito de *cybersecurity* e, por fim, medidas tomadas pelo governo americano como forma de resposta a dita intervenção durante o período de 2016-2019.

Após a revisão, o projeto terá como objetivo identificar como a interferência e as medidas tomadas pelo governo americano impactaram as questões de *cybersecurity* para o governo americano.

2.1 Primeiro Capítulo

2.1.1 Guerra fria

Para entender as consequências causadas pela intervenção russa na securitização do ciberespaço americano, é importante primeiro entender a relação entre os dois países dentro do cenário tecnológico moderno.

Desde o começo da guerra fria, ambos os Estados Unidos e Rússia têm engajado em uma acirrada corrida tecnológica em que, o foco em computadores foi frequente. Esse foco ocorreu, devido ao grande potencial tanto ofensivo quanto defensivo proporcionado pela nova tecnologia, que poderia garantir àquele que estivesse na frente grandes vantagens em diversos cenários como comunicação, inteligência, conflitos militares, planejamento, entre outros.

Após os russos terem lançado o satélite Sputnik em 1957, os Estados Unidos responderam com a criação do Advanced Research Projects Agency Network (ARPANET). O projeto foi iniciado em 1966 e foi colocado em uso 3 anos mais tarde. O ARPANET foi uma rede de comutação de pacotes e foi a primeira rede a implementar o conjunto de protocolos TCP/IP, que permitiram a comunicação entre redes de computadores.

O principal uso da rede foi o de facilitar a troca de informações entre bases militares. Ambos a ARPANET e os protocolos TCP/IP foram essenciais para a criação da internet.

Com a criação e difusão da internet no mundo acadêmico no começo dos anos 80, vários grupos na então União Soviética e nos Estados Unidos passaram a ampliar o uso da internet para apoiar questões securitárias. Porém, ainda não se tinha conhecimento sobre o potencial ofensivo garantido pela internet.

Parte deste potencial foi descoberto em 1982, quando um software canadense foi adquirido por soviéticos. O software tinha o objetivo de controlar uma linha de gás siberiana. Porém, devido a um erro, o programa causou uma grande explosão. Acusações contra a CIA foram feitas[3], afirmando que a agência de segurança americana modificou o software com o objetivo de causar a explosão. As acusações ainda são disputadas[4], porém se forem confirmadas, este pode ser considerado o primeiro ato de *cyberwarfare* entre os dois países.

Apesar da corrida tecnológica ter começado nos anos 40, da criação dos primeiros computadores da primeira geração terem começado nos anos 50, e do primeiro ataque cibernético confirmado ter acontecido nos anos 80[5], a maior parte do mundo só começou a demonstrar maior interesse em *cyberwarfare* nos anos 2000.

2.1.2 Anos 90

Em seu trabalho *Rise of Cyber Militias*[6], o autor Robert S. Dudney afirma que houve várias operações feitas por grupos de *hackers* independentes que passaram a ocorrer no final dos anos 90. Esses *hackers* não eram apenas ativos, mas também tinham recebido suporte e encorajamento de certos países que se encontravam em conflitos ou disputas.

---

[3] Thomas C. Reed. 2004. Disponivel em:
At the Abyss*:* An Insider's History of the Cold War.
[4] Anatoly Medetsky. 18 mar 2004. Disponivel em:
http://oldtmt.vedomosti.ru/sitemap/free/2004/3/article/kgb-veteran-denies-cia-caused-82-blast/232261.html. Acesso em: 9 Mar 2020.
[5] Scott Shackelford. 1 nov 2018. Disponivel em:
https://theconversation.com/30-years-ago-the-worlds-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges-105449. Acesso em: 9 Mar 2020.
[6] Air Force Magazine. Robert S. Dudney. Rise of the Cyber Militias. 2011. Disponivel em:
https://jmw.typepad.com/files/dudney-cyber-militia-feb-2011.pdf Acesso em: 9 Mar 2020.

No ano de 1998 no México, o Exército Zapatista de Libertação Nacional, foi responsável por vários ataques cibernéticos. O grupo revolucionário tinha, em 1994, entrado em conflito com o governo mexicano e, quatro anos depois do início do conflito, passaram a se utilizar de ataques cibernéticos. Os *hackers* Zapatistas primeiro focaram em derrubar sites de instituições governamentais mexicanas, porém com o passar do tempo, decidiram incluir os EUA na sua lista de alvos, conseguindo paralisar a bolsa de valores de Frankfurt. Esse evento foi considerado o primeiro a envolver "milícias cibernéticas"[7].

> Ever since the Zapatista operations in 1998, virtually all regional conflicts have had a cyber component. Later in 1998, for example, India performed some nuclear tests, and nongovernment Pakistani ethnonationalists attacked Indian cyber targets. DUDNEY, 2011, p. 1[8]

Os Estados Unidos sofreriam outro ataque vindo de grupos independentes no ano seguinte, em 1999, desta vez como retaliação devido ao seu envolvimento na operação *Allied Force*, que ocorreu durante a intervenção militar na Iugoslávia. Durante o conflito, os Estados Unidos se utilizaram de ataques cibernéticos com o objetivo de apoiar as forças da OTAN. Esses ataques, por sua vez, foram respondidos por grupos de *hackers* independentes da Rússia.

Entretanto, apesar de conflitos cibernéticos terem se tornado inevitáveis, e grupos de *hackers* independentes passarem a participar mais ativamente em *cyberwarfare*, houve um grande atraso em relação à maioria dos países na fortificação de sua segurança *on-line*. De fato, apenas em 2006 a maior parte dos países passaram a investir em *cyber war*[9].

---

[7] Air Force Magazine. Robert S. Dudney. Rise of the Cyber Militias. 2011. Disponivel em: https://jmw.typepad.com/files/dudney-cyber-militia-feb-2011.pdf Acesso em: 9 Mar 2020.

[8] Desde as operações Zapatistas de 1998, virtualmente todos os conflitos regionais tiveram um componente cibernético. Mais tarde em 1998, por exemplo, Índia realizou alguns testes nucleares, e entidades neonacionalistas não governamentais do Paquistão atacaram alvos cibernéticos indianos. (Tradução livre do autor)

[9] Ron Kelson, Pierluigi Paganini, Benjamin Gittins, David Pace. 25 Jun 2012. Disponivel em: https://securityaffairs.co/wordpress/6776/security/the-cyber-war-era-began-long-ago.html Acesso em: 10 Mar 2020.

2.1.3 Anos 2000

Ambos os Estados Unidos e Rússia entraram nos anos 2000 com instituições dedicadas a questões ligadas à *cybersecurity*. A Rússia conta com cinco diferentes grupos (O Conselho de Segurança, o Serviço de Segurança Federal, o Serviço da Guarda Federal, Técnico Federal e Serviço de Controle de Exportação, e o Ministro de Informação, Tecnologia e Comunicação), enquanto os Estado Unidos contam com seis (Departamento de Segurança Interna, Departamento de Estado, Departamento de Defesa, o Escritório de Segurança Cibernética e Comunicações, Centro de Proteção da Infraestrutura Nacional e a Seção de Crimes de Computação e Propriedade Intelectual do Departamento de Justiça).

Além disso, os dois países veem o espaço cibernético e seus riscos de forma diferente. Dentre os dois, a Rússia demonstra ter uma visão mais ampla, preferindo se referir a elas como questões de "informação"[10].

> According to Russian experts, the U.S. terms *cybersecurity* and *cyberspace* are primarily technological, whereas the Russian terms for information security and information space are seen as having broader philosophical and political meanings. The technology is perceived as only one of many components in Russia's understanding of information security and is not considered to be the most important one. GADY, AUSTIN, 2010, p. 13[11]

[10] Gady, Austin. Russia, The United States, And Cyber Diplomacy. 2010. Disponivel em:https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf Acesso em: 27 Nov 2019.

[11] De acordo com especialistas russos, os termos *cybersecurity* e *cyberspace* utilizados pelos EUA, são de forma primária, tecnológicos, enquanto os termos russos para "segurança de informação" e "espaço de informação" são vistos como tendo um maior significado filosófico e político. A tecnologia é vista como apenas mais um dos vários componentes dentro do entendimento russo de segurança de informação, e não é visto como o mais importante. (Tradução livre do autor)

No ano de 2007, a Rússia iniciou ataques cibernéticos contra à Estônia. O motivo do ataque foi o deslocamento de uma estátua soviética. A estátua, chamada de Soldado de Bronze, tinha grande significado para a comunidade russa dentro do país e, após o governo ter anunciado planos para o seu deslocamento, vários protestos no país foram iniciados.

O ataque teve o objetivo de paralisar a infraestrutura do país: sites estavam fora de acesso, bancos fora de ação, instituições públicas não poderiam mais ser contactadas on-line. Como consequência, não só a Estônia, mas também vários outros países passaram a fortificar ainda mais as suas defesas no espaço virtual.

Mais tarde, em 2008, a Rússia conduziu mais 2 ataques, um contra a Lituânia em junho, e outro contra a Geórgia em agosto. Estes ataques (e outros que viriam a acontecer nos anos seguintes) demostraram mais uma vez as capacidades ofensivas do país, e estabeleceram a sua posição no cenário cibernético internacional. A Rússia passou a ser vista como um país não só agressivo militarmente, mas também ciberneticamente.

Atividades focadas em intervir em eleições também foram iniciadas por organizações russas. Durante as eleições da Ucrânia em 2014, *hackers* russos disseminaram e-mails privados e informações falsas contra candidatos nacionalistas, e candidatos com agendas não-favoráveis a interesses russos. A Rússia já havia tentado influenciar as eleições do país anteriormente em 2004, porém seu método havia sido drasticamente diferente, com maior foco em suporte político e investimentos financeiros de determinados candidatos.

Por outro lado, os Estados Unidos têm feito restruturações em suas instituições cibernéticas. Durante a segunda metade dos anos 2000, o governo americano admitiu não estar preparado para lidar com as maiores ameaças cibernéticas. Em 2008 o secretário da agência de segurança interna, Michael Chertoff afirmou: "É a área onde eu sinto que estamos atrás de onde eu gostaria que estivéssemos."[12] No ano seguinte, o então presidente, Barack Obama, também admitiu que o país ainda

[12] Original: “It's the one area in which I feel we've been behind where I would like to be.” Tradução livre do autor.

não estava pronto: “Nós falhamos em investir na segurança de nossa infraestrutura digital.”[13]

Também é importante notar que estas afirmações foram feitas depois de duas grandes ações tomadas pela administração do ex-presidente Bush. Em 2003 a administração revelou seu plano para aumentar a segurança cibernética do país. O plano envolveu maior participação do setor privado, melhorias na comunicação entre os setores públicos e privados e criação de melhores sistemas para fortalecer a segurança cibernética das agências ligadas diretamente ao governo.

A segunda grande ação tomada pela administração do ex-presidente Bush veio em 2008, quando foi anunciado um aumento em investimentos públicos nos setores que lidam com segurança cibernética. O aumento representou um acréscimo de 74% comparado com investimentos em 2004, algo considerado necessário devido ao grande aumento em ataques sofridos, com um aumento de 152% em incidentes reportados durante o período de 2007-2008.[14]

As capacidades ofensivas dos Estados Unidos no âmbito de *cyberwarfare* foram demonstradas em 2010 em um ataque feito contra o Iran. Os Estados Unidos criaram o programa malicioso(*malware*) chamado Stuxnet. Este *malware* foi criado com o objetivo de infiltrar computadores iranianos contendo dados referentes ao seu programa nuclear e destruir arquivos necessários para o seu avanço.

O ataque teve sucesso, e conseguiu destruir vários arquivos essenciais do projeto nuclear. Foi reportado que os danos causados pelo *malware*, retardaram a iniciativa do Irã em 2 anos[15].

Em 2013, o administrador de sistemas da CIA, Edward Snowden, revelou que os Estados Unidos conduziram diversas iniciativas contra a China com o objetivo de

---

[13] Original: “We've failed to invest in the security of our digital infrastructure.” Tradução livre do autor.
[14] Richard Wolf. Bush calls for tighter cybersecurity, 2008. Disponivel em: https://abcnews.go.com/Technology/story?id=4457451&page=1. Acesso em: 14 Mar 2020.
[15] Shalal-Esa. Business Insider, 2013. Disponivel em: https://www.businessinsider.com/us-general-irans-cyber-war-machine-a-force-to-be-reckoned-with-2013-1. Acesso em: 14 Mar 2020.

invadir centros de pesquisa e educação chineses, como também a companhia de telecomunicações Huawei. A empresa se tornou um alvo devido ao medo dos americanos, que acreditavam na possibilidade da Huawei criar “portas dos fundos” em seus aparelhos que permitiriam aos hackers aliados ao governo chinês terem acesso a dados de cidadãos americanos[16].

Outro motivo é o fato dos aparelhos serem vendidos em países que não são abertos a produtos americanos. Com acesso aos dados da empresa, as instituições dos EUA poderiam então invadir computadores de várias partes do mundo, tanto de nações rivais quanto aliadas[17].

Além de diferenças em agendas e objetivos, os Estados Unidos e Rússia têm outra grande diferença: a restrição de dados ao público, algo que pode ser visto nas restrições impostas ao acesso de conteúdo ao público pelos países. Os Estados Unidos acreditam no acesso mais irrestrito, vendo a imposição de barreiras que limitem acesso, como um ato diretamente oposto à liberdade de expressão, enquanto a Rússia acredita que restrições são necessárias para manter a segurança e estabilidade do estado.

Enquanto os dois países têm se desenvolvido de forma diferente quando se trata do espaço virtual, é possível observar que, devido ao seu status de países soberanos, avanços tecnológicos e possibilidades de conflito com outros estados, tanto os Estados Unidos quanto a Rússia, vêm incrementando esforços para fortalecer sua presença e segurança no espaço cibernético.

[16] Raposa. U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press, 2013. Disponivel em: https://www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked-china-universities-mobile-phones-snowden-tells-china-press/#5eedb9825340. Acesso em: 14 Mar 2020.
[17] Raposa. U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press, 2013. Disponivel em: https://www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked-china-universities-mobile-phones-snowden-tells-china-press/#5eedb9825340. Acesso em: 14 Mar 2020.

2.2 Capítulo 2

2.2.1 Trump, Política e Moscou

Com a aproximação do fim do governo de Barack Obama, o início das eleições americanas ocorreu como o esperado. Vários cidadãos americanos se apresentaram como candidatos para os partidos democrata e republicano. Dentre eles, temos os candidatos do partido democrata Hilary Clinton e Bernie Sanders, e o candidato do partido republicano Donald Trump.

A forma como as eleições americanas são conduzidas ocorre através da divisão de dois ciclos: as eleições primárias, que são feitas para eleger os representantes de cada partido, e as gerais, onde os representantes de cada partido e outros candidatos independentes competem pelo título de presidente.

Nesta eleição em particular, os candidatos de maior interesse são Donald Trump do partido republicano e, Hilary Clinton e Bernie Sanders, do partido democrata. Tanto Sanders quanto Clinton competiram nas eleições primárias, porém após a vitória de Clinton, Sanders saiu da corrida e passou a apoiar a candidata. Também é importante notar a divisão entre candidatos e eleitores democratas: Clinton demonstrou maior influência dentro do partido e tinha maior suporte do público mais próximo ao centro da esfera política, enquanto Sanders angariou a maior parte do público jovem e mais próximo da extrema esquerda.

Outro fator importante é entender o cenário político do país, onde é possível ver grandes divisões ideológicas dentro do país, onde grupos conservadores, liberais, sociais democratas, libertários e vários outros lutam por representação política. Essa luta tem ocorrida frequentemente no âmbito cibernético, com a maior parte dela sendo travada dentro das redes sociais.

Sites como Reddit, Youtube, Twitter, Facebook, Instagram e 4chan observaram grande aumento em atividade e engajamento de conteúdo político, uma vez que os

possíveis candidatos começaram a se apresentar. Dentre esses candidatos, uma das figuras mais populares e controversas a entrar no discurso online foi o candidato Donald Trump.

Trump já foi um candidato no passado, com o começo de sua carreira política no ano 2000, quando demonstrou certa popularidade no estado da Califórnia. No ano de 2011 chegou a considerar a possibilidade de se candidatar, e demonstrou bom desempenho de acordo com pesquisas feitas[18], porém, ao invés de participar das eleições, decidiu apoiar o então candidato representante do partido republicano Mitt Romney. Trump também se tornou extremamente vocal quanto à sua visão política e sua oposição ao presidente Barack Obama.

Ainda em 2011, Trump fez seu primeiro discurso na Conferência de Ação Política Conservativa (CPAC). Durante o evento, seu discurso focou em negociações com outros países, preços do petróleo e impostos, afirmando que outros países têm se beneficiado de trocas desvantajosas feitas pelos Estados Unidos durante a administração do presidente Obama.

> If I decide to run, I will not be raising taxes. We will be taking in hundreds of billions of dollars from other countries that are screwing us. We will be creating vast numbers of productive jobs, and we will rebuild our country so that we can be proud. TRUMP, 2011, CPAC[19]

Porém, apesar dos discursos apresentados terem um tom de confronto, quando se trata das relações econômicas dos Estados Unidos com outros países, em 2016, Trump demonstrou discursos mais diplomáticos, quando se referindo a certos estados, entre os mais notáveis a Rússia, Arábia Saudita, e mais tarde em sua

[18] Jonathan Weisman, Scott Greenberg. WSJ/NBC Poll: A Donald Trump Surprise, 2011. Disponivel em: https://blogs.wsj.com/washwire/2011/04/06/wsjnbc-poll-a-donald-trump-surprise/. Acesso em: 4 Abr 2020.

[19] Se eu decidir me candidatar, eu não vou aumentar impostos. Nós vamos receber bilhões de dólares de outros países que estão nos ferrando. Vamos criar um vasto número de trabalhos produtivos e reconstruir o nosso país para que possamos ser orgulhosos. (Tradução livre do autor)

campanha, Israel. É especulado, que o motivo da súbita mudança de tom, ocorre devido aos interesses econômicos e políticos do candidato nestes estados.

Apesar de suas posições em relação a Arábia Saudita e Israel sofrerem poucas críticas, seja da mídia, de outros políticos americanos ou do público em geral (em grande parte, devido a uma opinião pública positiva quanto ao relacionamento dos Estados Unidos com estes países), muitos dos discursos de Trump voltados à Rússia, sofreram repúdio de uma quantidade significativa da população americana, em especial daqueles dentro do círculo político.

O histórico da relação de Trump com Moscou começou em 1987, quando foi convidado pelo embaixador Yuri Dubinin a visitar a Rússia. Trump, aceitou o convite devido ao seu interesse em criar um hotel no país. Com o passar do tempo o relacionamento do candidato com o Kremlin aumentou devido a suas negociações imobiliárias. Durante o período de 2000 até 2006, Trump e seus filhos fizeram diversas viagens a Moscou, em busca de parceiros interessados em construir Trump Towers.

Em uma entrevista de 2015, Trump mencionou que em 2013, em suas tentativas de iniciar negócios com os russos, ele entrou em contato com diversos generais, oligarcas e políticos russos do alto escalão. Mais tarde Trump se referiu ao seu relacionamento com eles, como “extraordinário”[20].

O relacionamento entre Trump e Putin também foi questionado inúmeras vezes por jornalistas e analistas políticos, com o então candidato, em determinados momentos elogiando o russo e afirmando ter tido contato com ele durante as eleições. Porém, tempos depois, passou a negar a existência destas conversas.

Com o passar do tempo, a troca de elogios entre Trump e Putin, e os discursos onde Trump encorajava maior parceria com russos, levaram diversos democratas a acusar Trump de ser uma “marionete russa”. Alguns republicanos também

[20] Hugh Hewitt. Donald Trump Returns, 2015. Disponivel em: https://www.hughhewitt.com/donald-trump-returns/. Acesso em: 7 Abr 2020.

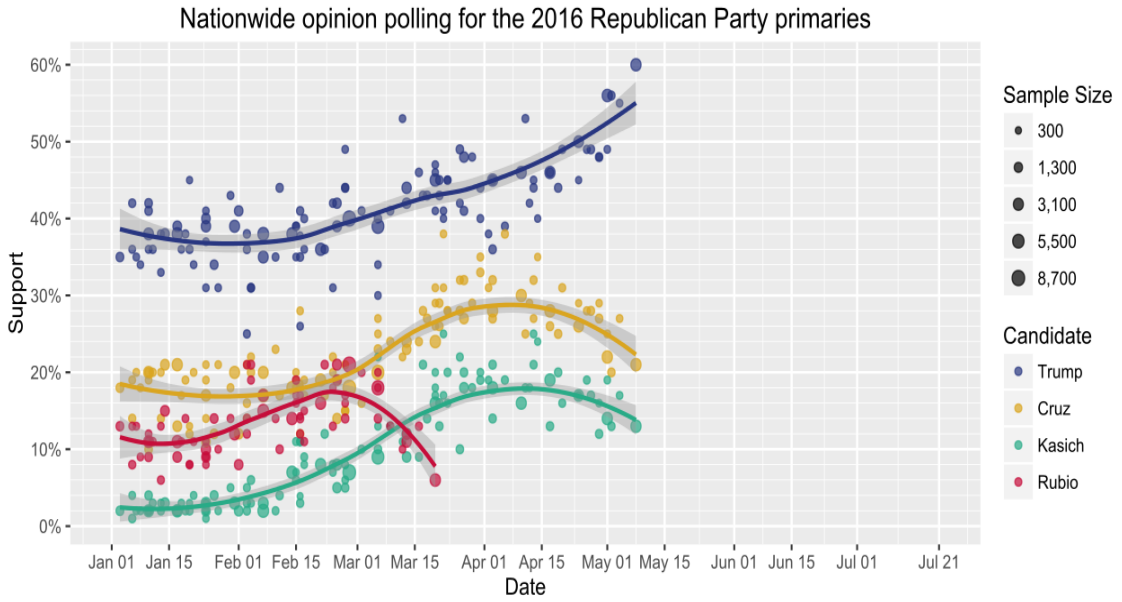
demonstraram insatisfação com discursos do presidente, demonstrando desconforto com o relacionamento entre os dois.

As posições de Trump em relação à Rússia viriam a mudar. Em resposta às constantes críticas levantadas pela sua oposição, Trump passou a fazer várias postagens na rede social Twitter. Muitas delas viriam a, mais uma vez, contradizer afirmações feitas por ele no passado. Em janeiro de 2017, Trump escreveu: “A Rússia nunca tentou me influenciar, não tenho nada com a Rússia, não tenho acordos, não tenho empréstimos, não tenho nada.”[21] Trump passou a se referir às acusações de coalisão com a Rússia feitas por sua oposição, como uma caça às bruxas (*witch hunt*).

Os discursos apresentados por Trump durante a CPAC em 2011, não mudaram em 2016, e demonstraram grande sucesso com grupos conservadores. Durante o período das eleições primárias, Trump conseguiu conquistar um número crescente de eleitores, rapidamente ultrapassando os outros candidatos. No fim das eleições primárias, Trump ganhou a nominação do partido republicano com margens significantes.

[21] Original: “Russia has never tried to use leverage over me. I HAVE NOTHING TO DO WITH RUSSIA - NO DEALS, NO LOANS, NO NOTHING!” Tradução livre do autor

Figura 1 – Sumário de Projeções Nacionais Para as Eleições Primárias Republicanas de 2016



Fonte:https://en.wikipedia.org/wiki/Nationwide_opinion_polling_for_the_2016_Republican_Party_presidential_primaries

A popularidade do candidato dentro do partido republicano também foi refletida no âmbito virtual. Durante o mês de setembro de 2016, Trump chegou a adquirir 11,9 milhões de seguidores no Twitter, a rede social onde ele se encontra mais ativo até hoje. Em comparação à sua adversária Hillary Clinton, que se encontrava com aproximadamente 3 milhões a menos de seguidores, contando com o total de 9,3 milhões durante o mesmo período.

2.2.2 Hackers vs DNC

Indícios de ataques cibernéticos foram detectados em setembro de 2015, quando o FBI identificou que hackers russos conseguiram acesso a um dos computadores do partido democrata. O aviso, porém, não foi executado de maneira apropriada, com o FBI apenas comunicando a um técnico de computação do partido, e deixando uma mensagem, em um telefone do centro de ajuda do Comitê Nacional Democrata (DNC).

O técnico afirmou ter escaneado os computadores, porém não encontrou indícios de uma infiltração cometida por fontes externas. No entanto, ele não informou a notificação do FBI à liderança da DNC.

A falha de comunicação interna dentro da DNC permitiu com que hackers ganhassem acesso a vários documentos, e-mails e mensagens de membros dentro do partido democrata. Dois meses depois, em novembro, o FBI contatou a DNC novamente para informar que um computador do partido democrata estava transmitindo informações para a Rússia.

O segundo ataque, ocorreu em março de 2016. O alvo foi John Podesta, que trabalhava como presidente da campanha presidencial da candidata Hillary Clinton. A tática do ataque foi relativamente simples: os hackers mandaram um e-mail para Podesta. No e-mail, eles se passaram pela empresa Google, avisando que alguém teria tentado acessar a sua conta e que ele deveria mudar a senha. O e-mail então direcionou Podesta para uma página falsa.

Essa página é semelhante à página que o Google utiliza para permitir que seus usuários mudem a sua senha de e-mail, enganando o usuário para que ele revele suas informações. Essa tática é conhecida como *spear-phishing* e é extremamente popular entre criminosos.

A estratégia dos hackers funcionou, devido a outro problema de comunicação entre membros da DNC. Desta vez, um dos técnicos de computação foi capaz de identificar a falta de legitimidade da mensagem, porém, mandou um comunicado ao time de Podesta, afirmando que o e-mail recebido era legítimo. Esta falha de

comunicação levou a assistente de Podesta a tentar alterar a senha, que, por sua vez, permitiu que os hackers ganhassem acesso aos dados presentes no e-mail.

Em abril do mesmo ano, hackers russos continuaram com a tática de *spear-phishing* e-mails de funcionários da campanha de Hilary Clinton. Depois do ataque, mais de trinta funcionários confirmaram ter recebido e-mails suspeitos. Dessa vez, os hackers enviaram um documento intitulado "hillaryclinton-favorable-rating.xlsx." O link direcionava os usuários a um site controlado pelos hackers.

No mesmo mês, os hackers utilizaram as informações obtidas, para acessar dados referentes à campanha de Clinton e do partido democrata, e conseguiram ganhar acesso a 33 computadores pertencentes à DNC. Por fim, de forma anônima, os hackers criaram o site “DCLeaks” para publicar os dados obtidos[22].

Firmas de cybersecurity afirmam que o site DCLeaks tem ligação direta com *Fancy Bear*, um grupo de hackers russos que trabalham com espionagem cibernética DCLeaks não apenas postou dados referentes à eleição de 2016, mas também dados obtidos do e-mail do general Philip Breedlove. Breedlove trabalhou como comandante da OTAN na Europa. Os dados obtidos alegam que, em 2014, o então comandante procurou aumentar as tensões militares com a Rússia, apesar da relutância do presidente Barack Obama[23]. Mais tarde, em agosto, o site publicou e-mails e números de telefone de senadores republicanos e democratas.

No dia 15 de junho, Crowdstrike, uma firma que trabalha com questões de *cybersecurity* e que havia sido contratada pela DNC, afirma acreditar que os grupos *Cozy Bear* e *Fancy Bear* foram responsáveis pelos ataques aos computadores da DNC. Esses são apelidos da Crowdstrike para os dois grupos de hackers russos que a firma encontrou no trabalho dentro da rede DNC.

O Grupo *Cozy Bear* pode ou não estar associado ao Serviço Federal de Segurança da Rússia (FSB), o principal sucessor da KGB, da era soviética, e

[22] Court of the United States of the district of Colombia. Indictment document. 2018. https://www.justice.gov/file/1080281/download. Acesso em: 10 Abr 2020.
[23] Lee Fang, Zaid Jilani. Hacked Emails Reveal NATO General Plotting Against Obama on Russia Policy, 2016. Disponivel em: https://theintercept.com/2016/07/01/nato-general-emails/. Acesso em: 10 Abr 2020.

acredita-se que *Fancy Bear* esteja associado à GRU, o principal serviço de inteligência militar da Rússia. Considera-se amplamente que seja uma operação exclusiva do governo russo[24].

Pouco tempo depois da acusação, um usuário anônimo chamado de Guccifer 2.0 diz ter sido o responsável pelos ataques e pelo vazamento de informações. Porém, devido às circunstâncias, muitos investigadores ainda acreditam que Guccifer foi uma persona criada pelos hackers, para diminuir a atenção atraída pelas acusações feitas por Crowdstrike.

Ainda em junho, grupos de hackers conseguiram executar o maior vazamento de informações na história da DNC. No dia 22, apenas alguns dias antes da Convenção Nacional Democrática, o site de notícias *WikiLeaks*, conhecido por publicar matérias que contêm informações confidenciais e restritas para o público, publicou quase 20.000 e-mails de servidores da DNC.

Os documentos incluíram diversas mensagens de membros do partido democrata demonstrando favoritismo à candidata Hilary Clinton, e apresentando repúdio a membros da campanha do candidato Bernie Sanders. Estas mensagens foram trocadas entre diretores e a presidente da DNC.

Investigações feitas pelo FBI apontam novamente para hackers russos como fonte de informações do *WikiLeaks*, que, por sua vez, foi acusado múltiplas vezes de favoritismo a Trump, devido aos interesses e posições políticas de seu criador, Julian Assange.

O vazamento de informações causou grandes danos à credibilidade da DNC, de sua liderança e da candidata Hilary Clinton. Sanders, mesmo depois de apoiar a campanha de Clinton durante as eleições gerais, não conseguiu acalmar muitos de seus eleitores, que durante a campanha utilizaram a hashtag “BernieOrBurst”, afirmando que não teriam intenções de votar em Clinton. O escândalo foi tão grande

[24] Time Editorial da Crowdstrike. CrowdStrike’s work with the Democratic National Committee: Setting the Record Straight. 2020. Disponivel em: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. Acesso em: 10 Abr 2020.

que Debbie Wasserman Schultz, presidente da DNC, deixou o seu cargo após o incidente.

Os próximos meses seriam marcados por mais tentativas de infiltração em servidores e usuários pertencentes a senadores americanos, com a maior parte delas demonstrando foco em políticos do partido democrata. O FBI e a CIA, novamente afirmaram acreditar que os ataques foram feitos por hackers russos, porém discordaram da intenção do ataque, com a CIA, acreditando que o objetivo dos hackers seria o de ajudar o candidato republicano, enquanto o FBI acredita que o objetivo seria o de criar desconfiança e desordem entre o público americano durante as eleições[25].

Mais tarde, em janeiro de 2017, após o final das eleições, Obama viria a afirmar que, depois de várias reuniões com oficiais de inteligência, ele acredita que a Rússia é provavelmente responsável pelos ataques à DNC, porém que o resultado da eleição não foi impactado, citando que as máquinas utilizadas para a contabilidade de votos não foram comprometidas.

O governo russo continuou a negar seu envolvimento nos ataques, afirmando a possibilidade de terem sido conduzidos por grupos de hackers independentes que vêm tanto de dentro, quanto de fora de seu país. Mais tarde, Putin viria a dizer numa entrevista que até mesmo uma criança poderia estar atrás dos ataques e que as acusações feitas à Rússia são resultados de brigas políticas internas dos Estados Unidos[26].

Porém, as acusações não terminaram com os russos. Devido a várias especulações que surgiram de encontros com membros da família Trump e oficiais do Kremlin, uma considerável parcela do público e da mídia, passaram a acreditar na possiblidade de uma troca de favores entre indivíduos na campanha presidencial

[25] Evan Perez, Manu Raju e Deirdre Walsh. Gap on Russia hacking conclusions between intelligence, FBI, 2016. Disponivel em: https://edition.cnn.com/2016/12/11/politics/russia-hacking-conclusions-donald-trump/index.html. Acesso em: 7 Mai 2020.
[26] Megyn Kelly quizzes Vladimir Putin if Russia affected U.S. elections, 2017. Disponivel em: https://www.nbcnews.com/video/megyn-kelly-quizzes-vladirmir-putin-if-russia-affected-u-s-elections-958769219830. Acesso em: 7 Mai 2020.

de Trump e agentes do governo russo, que teriam orquestrados os *cyberattacks* contra a DNC.

2.2.3 Social Media *Bots*

O uso de *bots* sociais é algo que originou em 1964 com o programa ELIZA, um programa de computador de processamento de linguagem natural criado no Laboratório de Inteligência Artificial dos Estados Unidos.

ELIZA foi criado com o propósito de demonstrar a superficialidade da comunicação entre humanos e máquinas. O programa utilizou uma metodologia de correspondência de padrões, roteiros e substituição que deu aos usuários uma ilusão de que o programa conseguia compreendê-los. Porém, o programa não tinha uma estrutura construída para contextualizar eventos. O programa foi essencial para o desenvolvimento de projetos relacionados a inteligência artificial e eventualmente a criação de *bots* que passariam a atuar em sites.

Os tipos de *bots* mais utilizados nas mídias sociais são chamados de *social bot* (*bots* sociais), que têm o objetivo de influenciar o discurso público ou promover uma agenda. *Bots* sociais são capazes de comunicação autônoma limitada, permitindo que sejam disfarçados como pessoas se seu criador desejar.

O uso de *bots* em mídias sociais é algo que se tornou extremamente comum. Muitas vezes, *bots* são empregados por empresas para administrar seus perfis on-line no Twitter, Facebook e outros[27]. Certas empresas hoje em dia chegam a promover *bots* como mascotes da empresa, utilizando a inteligência artificial como marketing. O uso de *bots* também se popularizou devido ao crescente uso da

[27] Equipe The Brief. Conheça empresas brasileiras que utilizam *chatbots* para atendimento. 2017. Disponivel em: https://www.thebrief.com.br/mercado/118734-conheca-empresas-brasileiras-utilizam-chatbots-atendimento.htm. Acesso em: 10 Mai 2020

automação, em que, ao invés de empregar pessoas, empresas e grupos privados ou públicos passam a delegar tarefas a máquinas e programas de computador.

Os *bots* sociais que foram utilizados para interferir nas eleições americanas de 2016 foram empregados em diversos sites. Os mais predominantes foram Facebook e Twitter. Porém sua presença também pode ser notada em sites menores, como 4chan e Reddit.

Como citado anteriormente o objetivo dos *bots* foi promover agendas. As formas como essas agendas foram apresentadas variavam de site para site. No Facebook e Reddit, o objetivo era espalhar postagens; no Twitter era levantar *hashtags* (termos, frases ou palavras que são precedidas pelo símbolo "#", quando *hashtags* são utilizadas por um grande número de usuários, elas passam a ser mais facilmente visíveis para todos os usuários da plataforma) e postagens para que elas se tornassem mais visíveis através das opções de "retweet" e "gostar"; no 4chan era o de enviar mensagens em certas páginas on-line que estivessem com alta movimentação. Em todos os casos os bots eram empregados em táticas de *spam*.

O *spam* ocorre quando mensagens on-line são enviadas múltiplas vezes, de forma que a fonte das mensagens (também conhecido como *spammer*), possa garantir que o indivíduo ou público-alvo tenha recebido a mensagem. A maioria das mídias sociais têm políticas e regras contra o *spam* devido a ser uma grande fonte de estresse para os alvos. Porém, quando essas mensagens vêm de múltiplas fontes ao invés de apenas uma, sites apresentam dificuldade em lidar com o problema.

As mensagens variavam de acordo com certos fatores, seja a origem do *bot*, sua capacidade para conversar com outros usuários, o público alvo das mensagens, ciclo de notícias, sites onde eles estavam operando e o desenvolvimento das eleições, apenas para citar alguns. Porém, foi possível identificar padrões entre as mensagens e agendas puxadas pelos *bots*, entre estas, o frequente uso de notícias falsas (*fake news*) se tornou o mais infame.

A tática como forma de interferir ou influenciar eleições, porém, não nasceu em 2016. O uso de *bots* políticos pode ser observado nas eleições americanas de 2010, e mais tarde, durante o período de 2011 até 2013, a tática se tornou popular entre grupos políticos.

Vários países reportaram um aumento no uso de *bots* em mídias sociais durante ciclos eleitorais. No Brasil, por exemplo, o uso de *bots* foi frequente durante as eleições de 2014. Estudos feitos pela UFES (Universidade Federal do Espírito Santo), notaram que a movimentação de *bots* influenciou diversas discussões entre pessoas no Twitter e Facebook após debates entre os candidatos[28], algo que não foi considerado incomum em outros países, que também observaram o aumento de atividade de *bots* em mídias sociais.

Levando estas questões em consideração, é importante questionar: por que os bots políticos e sociais apenas receberam maior atenção após as eleições de 2016? A resposta se deve a dois grandes fatores: o primeiro seria a falta de conhecimento que várias pessoas têm sobre o assunto e o segundo seria devido ao fato dos *bots* terem surgido de fontes internas.

As maiores plataformas, Twitter e Facebook, foram criadas em 2006 e 2004 respectivamente. Sua grande popularidade levou muitas pessoas a adotá-las em seu cotidiano. Porém, devido à grande parte dessas pessoas apenas terem seu primeiro contato com mídias sociais durante esse período de popularidade, poucas delas chagariam a ter conhecimento da existência de “usuários falsos”, seu propósito e o perigo que eles podem trazer para o ambiente político nacional de seus países.

Outra questão importante vem do fato dos *bots* terem sido empregados não apenas por indivíduos simpatizantes de certos candidatos, mas também por pessoas em cargos políticos e seus partidos.

[28] Alexandre Aragão. Eu, robô. 2014. Disponivel em: https://www1.folha.uol.com.br/fsp/especial/188299-eu-robo.shtml. Acesso em: 12 Mai 2020

Durante as eleições primárias no ano de 2012 nos Estados Unidos, o candidato Mitt Romney foi acusado de comprar seguidores no Twitter[29] para aumentar seu número de seguidores. Nas eleições brasileiras de 2014, os partidos dos dois principais candidatos, Dilma e Aecio, foram acusados de utilizar *bots* para subir tópicos e inflar a popularidade dos seus candidatos[30]. No México, *bots* utilizados pelo governo estadual, ajudaram a campanha do candidato Enrique Pena Nieto, no ano de 2012, através da disseminação de *fake news* e *hashtags*[31].

Porém, certos países foram capazes de identificar o perigo que *bots* sociais representam e tomaram medidas para lidar com o novo desafio. Dentre estes países podemos identificar a Estônia, que, após ter sido vítima de ataques cibernéticos orquestrados pela Rússia em 2007, passou a investir em *cybersecurity*, e hoje é considerado um dos países mais preparados para lidar com "campanhas de desinformação" promovidas por *bots* e grupos on-line.

O sucesso da Estônia ocorre devido a um conjunto de esforços governamentais, industriais e públicos, em que instituições e agências relacionadas a questões de segurança on-line, identificam problemas atuais e comunicam-se com outras instituições que possam estar interessadas ou que possam ser vítimas de novos ataques. O país também conta com uma identidade digital segura apoiada pelo governo, um registro digital da população e uma camada robusta de intercâmbio de dados entre bases de dados e serviços[32].

Outros países que demonstraram estar preparados para lidar com o uso de *bots* políticos nas mídias sociais são a China e a Rússia, que avançaram suas

---

[29] Dara Kerr. Mitt Romney suspiciously gets 116K Twitter followers in one day. 2012. Disponivel em: https://www.cnet.com/news/mitt-romney-suspiciously-gets-116k-twitter-followers-in-one-day/. Acesso em: 12 Mai 2020

[30] Alexandre Aragão. Eu, robô. 2014. Disponivel em: https://www1.folha.uol.com.br/fsp/especial/188299-eu-robo.shtml. Acesso em: 12 Mai 2020

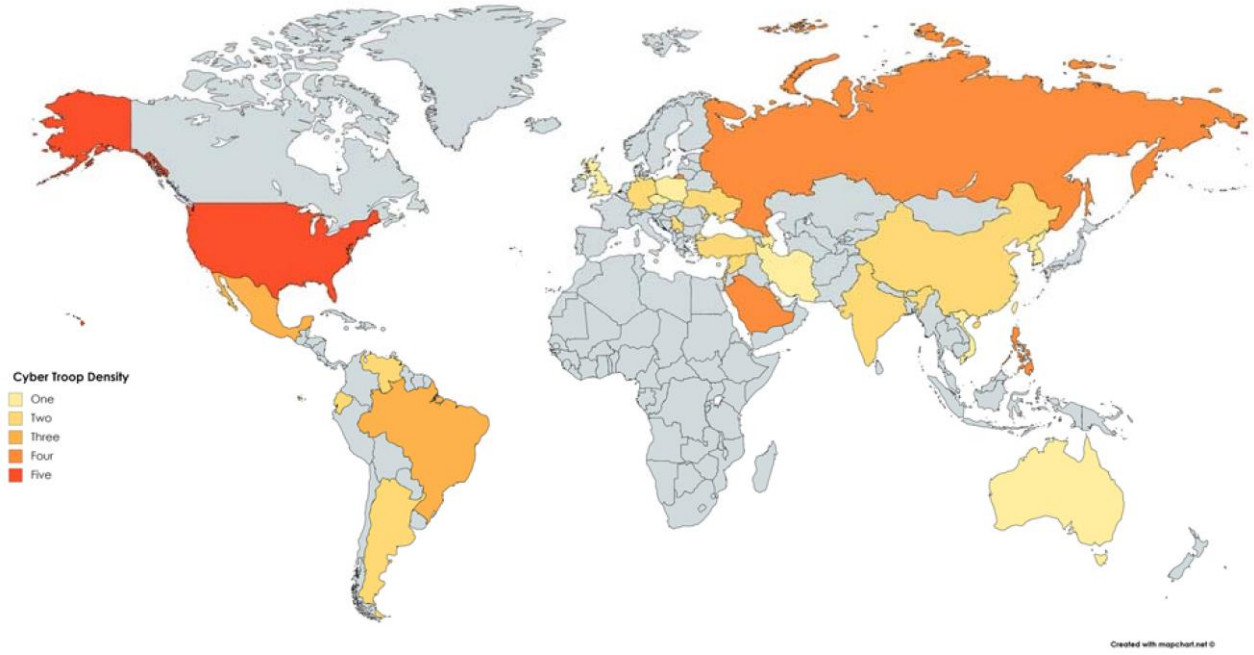
[31] Samantha Bradshaw & Philip N. Howard. Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. 2017. Disponivel em: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf. Acesso em 12 maio de 2020.

[32] Liisa Past & Keith Brown. Estonia is winning the cyber war against election meddling. 2019. Disponivel em: https://qz.com/1582916/estonia-is-winning-the-cyber-war-against-election-meddling/. Acesso em: 12 Mai 2020.

tecnologias devido à sua corrida tecnológica com outros estados, em particular os EUA. Porém, diferentemente da Estônia, ambos os países foram capazes de tomar atitudes mais extremas devido ao seu cenário político, em que o governo tem maior autoridade e pode tomar medidas que possam afetar a privacidade de seus cidadãos.

Porém, apesar do exemplo proporcionado pela Estônia, grande parte do mundo ainda se encontra atrasado em relação à sua segurança on-line, e, mesmo depois do crescimento na densidade de tropas cibernéticas (grupos de *bots* criados com o propósito de servir e cumprir objetivos designados pelo/s seu/s criador/es), não tomou os passos necessários para lidar com o problema.

Figura 2 – Densidade organizacional das tropas cibernéticas, 2017



Fonte: Samantha Bradshaw & Philip N. Howard. Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. 2017

2.2.4 *Bots* e *Fake News* nas eleições americanas de 2016

De acordo com o antigo procurador especial, Robert Mueller, as investigações conduzidas pelo FBI sugerem que muitos dos ataques foram orquestrados por uma das instituições russas, a IRA (Internet Research Agency). De acordo com as informações encontradas por Mueller, as principais atividades da IRA foram de espalhar mensagens e *hashtags* em favor de Trump, aumentar os números de seguidores do candidato e causar maior divisão política no país. Todas estas operações teriam sido conduzidas por *bots*, que por sua vez passariam a disseminar notícias falsas (*fake news)*[33].

O termo *Fake News* foi inicialmente utilizado pela candidata Hillary Clinton em dezembro de 2016. Porém, com o passar do tempo, foi adotada por Trump e seus eleitores.

A candidata, mencionou *fake news* pela primeira vez, durante uma de suas manifestações políticas para se referir às informações falsas em favor da campanha de Trump, espalhadas nas mídias sociais durante 2016. Enquanto isso, Trump e seus eleitores adotaram o termo para criticar a chamada *mainstream media*, emissoras ou editoras tradicionais ou estabelecidas. De acordo com críticas levantadas por Trump, essas emissoras e editoras espalhavam notícias falsas com o objetivo denegrir a sua imagem.

A forma como *bots* disseminaram *fake news* durante as eleições de 2016 foi variada. Alguns foram programados para espalhar links de sites com informações falsas, outros, foram programados para escrever mensagens com notícias falsas junto a *hashtags* como forma de aumentar a sua visibilidade. Entre os casos mais notórios de *fake news*, foi possível observar artigos que afirmavam que Clinton

[33] Jacqueline Thomsen. Mueller: Russia sought to help Trump win but did not collude with campaign. 2019. Disponivel em: https://thehill.com/policy/national-security/439544-mueller-russia-sought-to-help-trump-win-2016-election-but-did-not. Acesso em: 18 Mai 2020.

vendeu armas para o grupo terrorista ISIS, deu milhões de dólares para o diretor do FBI, que o Papa Francisco apoia Trump[34], entre outros.

Estudos feitos pela Universidade Estadual de Ohio, revelaram que informações falsas como essas foram fatores importantes na derrota de Clinton. Durante o estudo os pesquisadores descobriram que números relativamente grandes de eleitores que votaram em Obama nas eleições de 2010 consideraram a possibilidade de certos exemplos de f*ake news* serem verdadeiros[35], comprovando o sucesso e impacto da tática apresentada pelos hackers.

Outro fator importante a ser considerado durante a avaliação do impacto do fenômeno de *fake news*, é a velocidade com que as notícias falsas foram espalhadas on-line pelos *bots* políticos. De acordo com um estudo da Universidade de Indiana, apenas seis por cento dos usuários do Twitter identificados como *bots* foram responsáveis por quase um terço das notícias falsas publicadas no site[36].

Porém, apesar de sua eficácia, a frequência com que os *bots* são vistos em atividade tende a variar, com picos e declínios altamente dependentes do período avaliado. Uma pesquisa conduzida por Alessandro Bessi e Emilio Ferrara, indica que o número de atividades conduzidas por *bots* tende a depender da atividade humana, eventos políticos relevantes à eleição e quais *hashtags* estão sendo usadas por diferentes grupos[37].

---

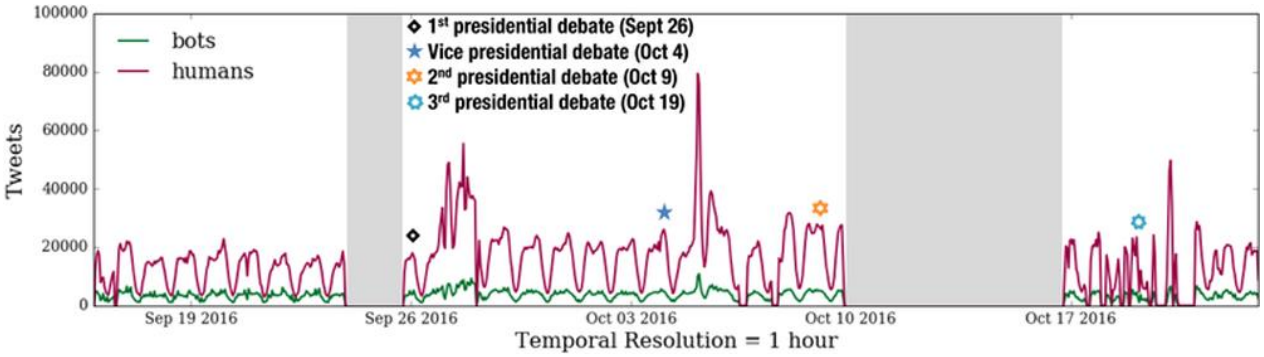
[34] Hannah Ritchie. Read all about it: The biggest fake news stories of 2016. 2016. Disponivel em: https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html. Acesso em: 18 Mai 2020.

[35] Richard Gunther, Paul A. Beck & Erik C. Nisbet. Fake News May Have Contributed to Trump's 2016 Victory. 2018. Disponivel em: https://www.documentcloud.org/documents/4429952-Fake-News-May-Have-Contributed-to-Trump-s-2016.html. Acesso em: 18 Mai 2020.

[36] Indiana University. Study: Twitter bots played disproportionate role spreading misinformation during 2016 election. 2018. Disponivel em: https://news.iu.edu/stories/2018/11/iub/releases/20-twitter-bots-election-misinformation.html. Acesso em: 18 Mai 2020.

[37] Alessandro Bessi e Emilio Ferrara. Social Bots Distort the 2016 Presidential Election Online Discussion. 2016. Disponivel em: https://firstmonday.org/article/view/7090/5653. Acesso em: 18 Mai 2020.

Figura 3 – Linha do tempo do volume de tweets gerados durante os períodos de observação (área cinza = sem dados).



Fonte: Alessandro Bessi e Emilio Ferrara. Social Bots Distort the 2016 Presidential Election Online Discussion. 2016

Pesquisas como esta podem ser conduzidas através dos principais métodos utilizados para identificação de bots: a frequência de atividades, descrição, nome e comportamento do usuário e aparência, com a maioria dessas características sendo randomizadas devido à natureza da programação dos *bots*. A avaliação dessas qualidades é normalmente feita através de um programa que, baseado nos dados citados anteriormente, produz uma pontuação que sugere a probabilidade da conta inspecionada ser de fato um *bot*.

Porém é importante notar que, devido ao alto avanço da tecnologia e dos métodos utilizados para a criação e configuração de *bots* políticos e sociais, a identificação de *bots* não é sempre garantida, e números apresentados em pesquisas podem ser acompanhados por grandes margens de erro.

Outro fator a ser levado em conta é que a dificuldade de identificar *bots* mais avançados, apenas permite com que eles continuem a interferir no cenário político do país. Em março de 2017, Clinton Watts, um membro sênior do Centro de Segurança Cibernética e Segurança de Estado da Universidade de George

Washington, disse acreditar que mesmo após as eleições, vários *bots* criados durante o período da eleição, continuam ativos[38].

[38] Kathryn Watson. Russian bots still interfering in U.S. politics after election, says expert witness. 2017. Disponivel em: https://www.cbsnews.com/news/russian-bots-still-interfering-in-u-s-politics-after-election-expert/. Acesso em: 28 de Maio de 2020.

2.3 Terceiro capítulo

2.3.1 Resposta Imediata

A confirmação da fonte dos ataques cibernéticos e das tentativas de influenciar as eleições ocorridas durante o ano de 2016, aconteceram no dia sete de outubro do mesmo ano, através das agências de inteligência. Em janeiro de 2017, o diretor do escritório de inteligência nacional, James Robert Clapper, confirmou mais uma vez, que as tentativas de interferência foram coordenadas pelos russos.

Estas confirmações levaram a administração de Obama, que se encontrava em seus últimos meses de mandato, a tomar medidas diplomáticas e políticas contra a Rússia. As medidas tomadas pela administração foram a expulsão de 35 diplomatas russos e a aplicação de sanções econômicas contra o país, porém, apesar de reconhecer o perigo das atividades dos russos, a administração do antigo presidente não tomou medidas significativas para fortalecer a segurança on-line do país.

A falha da administração do antigo presidente, em responder às operações russas, seria corrigida no ano de 2017, quando foi possível ver um maior número de políticos, especialmente aqueles que pertencem ao partido republicano, reconhecendo o perigo que as mídias sociais e a falta de maior infraestrutura e planejamento sobre questões de *cybersecurity* podem trazer para o país.

Após assumir o cargo de presidente, no dia 20 de janeiro de 2017, Trump afirmou que questões de *cybersecurity* se encontravam em sua lista de prioridades. No dia 11 de maio, o presidente assinou uma ordem executiva com o objetivo de fortalecer a infraestrutura cibernética dos Estados Unidos.

A ordem executiva reconhece as dificuldades tecnológicas e financeiras dos setores que lidam com tecnologia de informação (IT)[39], e exige que as agências de segurança identifiquem autoridades e tecnologias que possam aumentar a sua segurança virtual, planejem e calculem o orçamento necessário para empregar estas autoridades e tecnologias, aumentem a punição para indivíduos dentro de agências de segurança que pratiquem atividades ilegais e não autorizadas, e reportem todas as suas atividades para o presidente[40].

Entretanto, enquanto a ordem executiva demonstrou um passo na direção certa, ela não continha nenhuma forma de contramedidas que protegessem o país. Em casos de *cyberattacks* similares aos que ocorreram nas eleições, os Estados Unidos apenas começariam a tomar iniciativas que abordassem o problema, no final do mês de junho de 2017.

No dia 30 de junho, a administração do presidente Trump criou uma nova ordem executiva. Nela, a administração fez um maior apelo para o governo americano modernizar sua infraestrutura de IT, e utilizar a “nuvem”, um sistema que permite que usuários salvem seus arquivos em servidores on-line ao invés de seus computadores.

Esta medida aumentaria a segurança contra hackers, que por sua vez teriam maior dificuldade em acessar informações de seus alvos. A administração também anunciou uma cooperação bilateral com Israel com o objetivo de fortalecer a infraestrutura de *cybersecurity* de ambos os países. Deve ser notado que grupos dentro de Israel foram banidos da plataforma Facebook por tentar influenciar eleições através de mídias sociais. Num dos casos mais notórios, foi possível

[39] O termo "tecnologia da informação" (TI) tem o significado dado a esse termo na secção 11101(6) do título 40, do código dos Estados Unidos, e inclui sistemas de hardware e software de agências que monitoram e controlam equipamentos e processos físicos.
[40] Ordem executiva da Casa Branca. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 2017. Disponivel em: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/. Acesso em: 23 de Maio de 2020.

identificar uma firma de comunicações que foi acusada pelo site, de espalhar *fake news*[41].

2.3.2 Resposta Privada

Devido às mídias sociais serem todas de origem privada, foi necessário que vários processos burocráticos fossem executados antes do congresso tomar decisões sobre quais ações deveriam ser tomadas por empresas que controlam os sites de mídia social afetados por *bots*. Como resultado, as audições do senado começaram em novembro de 2017. As empresas responsáveis pelos sites selecionados para a audição terminaram de testemunhar perante o congresso, mais de um ano depois da fonte dos ataques ter sido confirmada.

Também é importante notar que nem todos os sites afetados estavam presentes nos inquéritos. Apenas Google, Twitter e Facebook foram questionados. Isto provavelmente, ocorreu devido à maior popularidade dos sites em questão.

Antes dos inquéritos, Twitter fez postagens em seus blogs revelando informações relacionadas a *bots* e ao governo russo encontradas pela empresa ao longo do ano. Os blogs surgiram como resposta a demandas de transparência feitas por políticos americanos, jornalistas e usuários da plataforma.

Em seus blogs, Twitter afirmou que contas automatizadas ligadas à Rússia, constituíram menos de um por cento do total dos tweets relacionados às eleições entre 1º de setembro e 15 de novembro de 2016.

A empresa também reconheceu ter encontrado 2.752 contas associadas à instituição russa, IRA, e que em 2016 foram pagos duzentos e quarenta mil dólares

[41] Isabel Debre and Raphael Satter. Facebook busts Israel-based campaign to disrupt elections. 2017. Disponivel em: https://apnews.com/7d334cb8793f49889be1bbf89f47ae5c. Acesso em 27 Mai 2020.

em troca de anúncios pelo grupo Russia Today (RT)[42], um canal de televisão estatal russo com emissão em inglês focado em transmissões globais. Twitter mais tarde viria a deletar todos os anúncios comprados por RT e outros grupos russos.

Durante os inquéritos, Twitter afirmou que menos de cinco por cento das contas em sua plataforma pertencem a *bots*. A afirmação contradiz um estudo publicado em março do mesmo ano pela Universidade do Sul da Califórnia (USC) e Universidade de Indiana. O estudo afirma que até quinze por cento dos usuários são operados por *bots*, porém também reconhece que, devido aos avanços em inteligência artificial, vários *bots* podem estar se passando por humanos, o que pode tornar estes quinze por cento uma estimativa prudente[43].

Por outro lado, Facebook começou sua operação para remover *bots* em abril, quando removeu trinta mil contas falsas; mais tarde a empresa viria a afirmar que o número subiu para setenta mil. Representantes da empresa também passaram a enviar exemplos de anúncios comprados por grupos russos e mensagens enviadas por *bots* para o congresso americano no mês de setembro.

Durante sua audiência com o senado, a empresa afirmou que menos de dois por cento de seus usuários são *bots*; porém, admitiu que, em sua plataforma Instagram, 20 milhões de usuários foram expostos a propaganda criada com o objetivo de influenciar as eleições.

Google, a terceira empresa a ter sua presença requerida pelo senado, afirma que tem trabalhado em programas para proteger jornalistas contra táticas de *spear-phishing* durante os primeiros meses das eleições francesas. Porém, não fez maiores comentários.

---

[42] Twitter Public Policy. Update: Russian interference in the 2016 US presidential election. 2017. Disponivel em: https://blog.twitter.com/official/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html. Acesso em: 25 Mai 2020.

[43] Onur Varol, Emilio Ferrara, Clayton A. Davis, Filippo Menczer & Alessandro Flammini. Online Human-Bot Interactions: Detection, Estimation, and Characterization. University of Indiana & University of South California. 2017. Disponivel em: https://arxiv.org/pdf/1703.03107.pdf. Acesso em: 25 de Mai de 2020.

Todas as empresas presentes na audiência se comprometeram a trabalhar com o governo americano e suas agências de segurança, e aumentar sua vigilância contra futuras tentativas externas de influenciar as eleições de 2020.

Durante os anos de 2018 a 2019, as três empresas viriam a tomar algumas medidas controversas, que surgiram devido a demandas e críticas feitas pelo público em geral. A mais notável foi a introdução de *fact checking*, demandando que as empresas verifiquem e removam notícias e postagens que contêm informações falsas de seus sites.

Representantes do Facebook repetidamente afirmaram que não teriam intenções de se tornar árbitros da verdade[44], acreditando que notícias não devem passar por análises internas. Twitter afirmou que irá proibir propaganda política em sua plataforma, e Google criou a iniciativa Google News, que promete demonstrar notícias verídicas em seu site de pesquisa.

Além destas iniciativas e esforços, as três empresas assinaram o Código de Práticas Sobre Desinformação (*Code of Practice on Disinformation*). O código foi criado pela União Europeia e estabelece quais passos devem ser tomados para lidar com casos de *fake news*[45]. Porém, mesmo após a assinatura do código, a União Europeia acredita que as empresas têm que apresentar maior diligência em seus esforços, e políticos europeus acreditam em aumentar regulações e punições caso as três empresas falhem em manter seus compromissos com o código[46].

Com a aproximação das eleições gerais de 2020, muitos especialistas acreditam que os Estados Unidos não se encontram preparados para combater tentativas de interferência em suas eleições. As análises dos especialistas, porém, devem não apenas preocupar os americanos. Devido à natureza global da ameaça,

---

[44] Adam Mosseri. Addressing Hoaxes and Fake News. 2016. Disponivel em: https://about.fb.com/news/2016/12/news-feed-fyi-addressing-hoaxes-and-fake-news/. Acesso em: 30 Mai 2020.
[45] European Commission. Code of Practice on Disinformation. 2018. Disponivel em: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation. Acesso em: 30 Mai 2020.
[46] Elizabeth Schulze. EU tells Facebook, Google and Twitter to take more action on fake news. 2019. Disponivel em: https://www.cnbc.com/2019/10/29/eu-tells-facebook-google-and-twitter-to-take-more-action-on-fake-news.html. Acesso em: 30 Mai 2020.

é de se acreditar que, se mesmo com toda a sua infraestrutura e recursos, os Estados Unidos se encontram vulneráveis a ataques organizados por outros estados, quais os perigos que países menos desenvolvidos em termos de *cybersecurity* podem encontrar?

3.0 Conclusão

É possível observar que, durante o desenvolvimento do cenário virtual, as capacidades de *cybersecurity* de cada estado, têm avançado devido à necessidade de se defender de ameaças externas e internas. Desde elementos que permitiram a criação da internet até os dias atuais, o comportamento apresentado pelos estados procede de forma similar.

Porém, recentemente, devido à falha de vários estados de reconhecerem e se adaptarem às ameaças cibernéticas atuais, muitas das dificuldades e desafios apresentados neste trabalho, continuam a representar uma grande ameaça à sua segurança.

Outro fator a ser considerado ao se tratar da segurança cibernética dos estados, é a constante evolução dos métodos utilizados por *hackers* em seus *cyberattacks*. Com *bots* se tornando apenas um dos mais recentes métodos, é de se esperar que, em alguns anos, suas táticas mudem novamente, e se tornem mais perigosas.

Estas ameaças ocorrem devido ao cenário caótico do mundo cibernético. Onde é possível observar estados e grupos privados e independentes constantemente em conflito, este conflito por sua vez, forçam os atores a não apenas aumentar suas seguranças, mas também aumentem suas capacidades ofensivas.

Como resultado, o *status quo*, dos estados em no cenário virtual, não é diferente de seu *status quo* dentro do âmbito de segurança. Onde avanços tecnológicos que proporcionem maiores capacidades ofensivas e defensivas, devem ocorrer, para garantir sua segurança.

Os métodos utilizados pelos Estados Unidos e pela União Europeia, para avançar suas capacidades defensivas, serão testados, nas eleições de 2020, e têm a expectativa de alterar o cenário virtual através de suas colaborações com as empresas privadas que controlam os sites de mídia social.

Referências

ARAGÃO, Alexandre**. Eu, Robo.** Folha de São Paulo, 2014. Disponivel em: https://www1.folha.uol.com.br/fsp/especial/188299-eu-robo.shtml. Accesso em 21 de Maio de 2020.

BARNES, Julian. **U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections.** The New York Times, 23 de outubro de 2018. Disponivel em: https://cyber-peace.org/wp-content/uploads/2018/10/U.S.-Begins-First-Cyberoperation-Against-Russia-Aimed-at-Protecting-Elections-The-New-York-Times.pdf. Acesso em: 19 de novembro de 2019.

BESSI, Alessandro & FERRARA, Emilio. **Social Bots Distort the 2016 Presidential Election Online Discussion.** First Monday, 2016. Disponivel em: https://firstmonday.org/article/view/7090/5653. Accesso em 21 de Maio de 2020.

BHATTACHARYYA, Suman. **Cyberattacks Against the US Government Up 1,300% Since 2006.** The Fiscal Times, 2016. Disponivel em: http://www.thefiscaltimes.com/2016/06/22/Cyberattacks-Against-US-Government-1300-2006. Accesso em 21 de Maio de 2020.

BRADSHAW, Samantha & HOWARD, **Philip. Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.** Oxford, 2017. Disponivel em: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf. Accesso em 21 de Maio de 2020.

CAPLAN, Nathalie. **Cyber War: The Challenge to National Security.** 2013. Disponivel em: http://globalsecuritystudies.com/Caplan%20Cyber.pdf. Acesso em: 27 de novembro de 2019.

C-SPAN. **Facebook, Google, and Twitter Executives on Russia Election Interference.** C-SPAN, 2017. Disponivel em: https://www.c-span.org/video/?436360-1/facebook-google-twitter-executives-testify-russias-influence-2016-election&start=3484. Acesso em: 29 Maio 2020.

CROWDSTRIKE'S EDITORIAL TEAM. **CrowdStrike's work with the Democratic National Committee: Setting the record straight.** Crowdstrike, 2020. Disponivel em: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. Accesso em 21 de Maio de 2020.

DUDNEY, Robert. **Rise of the Cyber Militias.** 2011. Disponivel em: https://jmw.typepad.com/files/dudney-cyber-militia-feb-2011.pdf. Acesso em: 7 de março de 2020.

EUROPEAN UNION. **EU Code of Practice on Disinformation**. Europa: 2018.

GADY, Stefan e AUSTIN, Greg. **Russia, The United States, And Cyber Diplomacy.** 22 de dezembro de 2009. Disponivel em: https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf. Acesso em: 27 de novembro de 2019.

GAMBINO, Lauren; SIDDIQUI, Sabrina; WALKER, Shaun. **Obama expels 35 Russian diplomats in retaliation for US election hacking.** Disponivel em: https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack. Acesso em: 30 Maio de 2020.

GUNTER, Richard; BECK, Paul; NISTBET, Erick. *Fake News May Have Contributed to Trump's 2016 Victory. 2018. 6f*. *Pesquisa*- Ohio State University: 2018.

GUMBEL, Andrew. **Why US elections remain 'dangerously vulnerable' to cyber-attacks.** The Guardian, 2018. Disponivel em: https://www.theguardian.com/us-news/2018/aug/13/us-election-cybersecurity-hacking-voting. Acesso em: 30 Maio de 2020.

HIGGINS, Tucker. **Obama response to 2016 Russian election meddling had 'many flaws,' Senate report finds**. CNBC, 2020. Disponivel em: https://www.cnbc.com/2020/02/06/obama-response-to-2016-russian-meddling-had-many-flaws-senate-report.html. Acesso em: 30 Maio de 2020.

HOWARD, Philip; WOOLLEY, Samuel; CALO, Ryan. **Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration.** The Journal of Information Technology and Politics, 2018. Disponivel em: https://www.tandfonline.com/doi/pdf/10.1080/19331681.2018.1448735?needAccess=true. Acesso em: 30 Maio de 2020.

INDIANA UNIVERSITY. **Study: Twitter bots played disproportionate role spreading misinformation during 2016 election.** Indiana University, 2018 Disponivel em: https://news.iu.edu/stories/2018/11/iub/releases/20-twitter-bots-election-misinformation.html. Accesso em 21 de Maio de 2020.

KELLY, Megyn. **Megyn Kelly quizzes Vladimir Putin if Russia affected U.S. elections.** NBC News, 2017. Disponivel em: https://www.nbcnews.com/video/megyn-kelly-quizzes-vladirmir-putin-if-russia-affected-u-s-elections-958769219830. Accesso em 21 de Maio de 2020.

KELSON, Ron, PAGANINI, Pierluigi, GITTINS, Benjamin, PACE, Dave. **The 'cyber war' era began long ago**. Security Affairs, 2012. Disponivel em: https://securityaffairs.co/wordpress/6776/security/the-cyber-war-era-began-long-ago.html. Acesso em: 6 de março de 2020.

KERR, Dara. **Mitt Romney suspiciously gets 116K Twitter followers in one day:** A new report shows that 15 percent of the Republican presidential hopeful's Twitter

followers may be from paid fake accounts. C Net, 2012. Disponivel em: https://www.cnet.com/news/mitt-romney-suspiciously-gets-116k-twitter-followers-in-one-day/. Accesso em 21 de Maio de 2020.

LANGNER, Ralph. **Cracking Stuxnet, a 21st-century weapon.** TED, 2011. Disponivel em: https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber_weapon. Acesso em: 7 de março de 2020.

LEMOS, Robert. **Bush unveils final cybersecurity plan.** Cnet 2003. Disponivel em: https://www.cnet.com/news/bush-unveils-final-cybersecurity-plan/. Acesso em 7 de março de 2020.

LIPTON, Erick; SANGER, David and SHANE, Scoot. **The Perfect Weapon: How Russian Cyberpower Invaded the U.S.** New York Times, 2016. Disponivel em: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html. Accesso em 21 de Maio de 2020.

MARTINEZ, Marcos. **Mexico election: Concerns about election bots, trolls, and fakes.** BBC, 2018. Disponivel em: https://www.bbc.com/news/blogs-trending-44252995. Accesso em 21 de Maio de 2020.

MCGUINNESS, Damien. **How a cyber-attack transformed Estonia.** BBC News, 2017. Disponivel em: https://www.bbc.com/news/39655415. Acesso em 8 de março de 2020.

MOSSERI, Adam. **Addressing Hoaxes and Fake News**. Facebook, 2016. Disponivel em: https://about.fb.com/news/2016/12/news-feed-fyi-addressing-hoaxes-and-fake-news/. Acesso em: 28 Maio de 2020.

MULLER, Robert. **Report on The Investigation into Russian Interference in the 2016 Presidential Election.** CNN, março de 2019. Disponivel em: https://cdn.cnn.com/cnn/2019/images/04/18/mueller-report-searchable.pdf. Acesso em: 9 de setembro de 2019.

NAKASHIMA, Ellen. **U.S. government officially accuses Russia of hacking campaign to interfere with elections.** The Washington Post, 7 de outubro de 2016. Disponivel em: https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html. Acesso em: 9 de setembro de 2019.

National Security Agency. **NSA Report on Russia Spearphishing.** 5 de maio de 2017. Disponivel em: https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1. Acesso em: 13 de outubro de 2019.

OBAMA, Barack. **Text: Obama's Remarks on Cyber-Security.** New York Times, 2009. Disponivel em: https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html?auth=login-google. Acesso em: 7 de março de 2020.

Office of the Director of National Intelligence. **Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.** New York Times, 6 de janeiro de 2017. Disponivel em: https://www.nytimes.com/interactive/2017/01/06/us/politics/document-russia-hacking-report-intelligence-agencies.html. Acesso em: 9 de setembro de 2019.

ORSI, Davide; AVGUSTIN, J.R.; NURNUS, Max. **Realism in Practice: An Appraisal**. Bristol, Inglaterra: E-International Relations Publishing, 2018.

PAST, Lisa & BROWN, Keith. **Estonia is winning the cyber war against election meddling.** Quartz, 2019. Disponivel em: https://qz.com/1582916/estonia-is-winning-the-cyber-war-against-election-meddling/. Accesso em 21 de Maio de 2020.

RAPOSA, Kenneth. **U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press.** Forbes, 2013. Disponivel em: https://www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked-china-universities-mobile-phones-snowden-tells-china-press/#6f9d80353405. Acesso em: 7 de março de 2020.

RITCHIE, Hannah. **Read all about it: The biggest fake news stories of 2016.** CNBC, 2016. Disponivel em: https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html. Accesso em 21 de Maio de 2020.

SCHULZE, Elizabeth. **EU tells Facebook, Google and Twitter to take more action on fake news.** CNBC News. Disponivel em: https://www.cnbc.com/2019/10/29/eu-tells-facebook-google-and-twitter-to-take-more-action-on-fake-news.html. Acesso em: 30 Maio de 2020.

SCIUTTO, Jim. **How one typo helped let Russian hackers in.** CNN, 2017. Disponivel em: https://edition.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html. Accesso em 21 de Maio de 2020.

SHANE, Scott & MAZZETTI, Mark. **The Plot to Subvert an Election Unraveling the Russia Story So Far.** The New York Times, 2018. Disponivel em: https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html. Accesso em 21 de Maio de 2020.

SHANE Scott. **The Fake Americans Russia Created to Influence the Election.** The New York Times, 7 de setembro de 2017. Disponivel em: http://cs.brown.edu/people/jsavage/VotingProject/2017_09_07_NYT_TheFakeAmericansRussiaCreatedToInfluenceTheElection.pdf. Acesso em: 12 de setembro de 2019.

SULLIVAN, Donie. **Russian bots retweeted Trump nearly 500,000 times in final weeks of 2016 campaign.** CNN, 2018. Disponivel em: https://money.cnn.com/2018/01/27/technology/business/russian-twitter-bots-election-2016/. Acesso em: 30 Maio de 2020.

TIMBERG, Graig e ROOM, Tony. **Bipartisan Senate report calls for sweeping effort to prevent Russian interference in 2020 election.** The New York Times, 8 de outubro de 2019. Disponivel em: https://www.washingtonpost.com/technology/2019/10/08/bipartisan-senate-report-calls-sweeping-effort-prevent-russian-interference-election/. Acesso em: 13 de outubro de 2019.

U.S. Department of Homeland Security. Office of the Director of National Intelligence. **Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security.** 7 de outubro de 2016. Disponivel em: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national. Acesso em: 9 de setembro de 2019.

VAROL, Onur; FERRARA, Emilio; DAVIS, Clayton; MENCZER, Filippo; FLAMMINI, Alessandro. *Online Human-Bot Interactions: Detection, Estimation, and Characterization. 2017. 11f. Pesquisa*- Indiana University & University of Southern California, 2017.

VOLZ, Dustin. **U.S. spending bill to provide $380 million for election cyber security.** Reuters, 2018. Disponivel em: https://www.reuters.com/article/us-usa-fiscal-congress-cyber/u-s-spending-bill-to-provide-380-million-for-election-cyber-security-idUSKBN1GX2LC. Acesso em: 30 Maio de 2020.

WALKER, Shawn & LUHN, Alec. **Petro Poroshenko wins Ukraine presidency, according to exit polls.** The Guardian, 2014. Disponivel em: https://www.theguardian.com/world/2014/may/25/petro-poroshenko-ukraine-president-wins-election. Acesso em: 8 de março de 2020.

WATSON, Kathryn. **Russian bots still interfering in U.S. politics after election, says expert witness.** CBS News, 2017. Disponivel em: https://www.cbsnews.com/news/russian-bots-still-interfering-in-u-s-politics-after-election-expert/. Acesso em: 30 Maio de 2020.

WEISMAN, Jonathan & GREENBERG, Scott. **WSJ/NBC Poll: A Donald Trump Surprise.** Wall Street Journal, 2011. Disponivel em: https://blogs.wsj.com/washwire/2011/04/06/wsjnbc-poll-a-donald-trump-surprise/. Accesso em 21 de Maio de 2020.

WHITE HOUSE. **residential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.** Estados Unidos: 2017.

WINDREM, Robert. **Timeline: Ten Years of Russian Cyber Attacks on Other Nations**. 2016. NBC News, Disponivel em: https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111. Acesso em: 10 de março de 2020.

WOLF Richard. **Bush calls for tighter cybersecurity.** ABC News, 2008. Disponivel em: https://abcnews.go.com/Technology/story?id=4457451&page=1. Acesso em: 10 de março de 2020.

WONG Julia. **Facebook discloses operations by Russia and Iran to meddle in 2020 election.** The Guardian, 21 de outubro de 2019. Disponivel em: https://www.theguardian.com/technology/2019/oct/21/facebook-us-2020-elections-foreign-interference-russia. Acesso em 19 de novembro de 2019.

WOOLEY, Samuel & HOWARD, Philip. **Computational Propaganda Worldwide: Executive Summary.** Oxford 2017. Disponivel em: http://www.philosophyofinformation.net/wp-content/uploads/sites/93/2017/06/Executive_Summary.pdf. Accesso em 21 de Maio de 2020.

WOOLEY, Samuel. **Automating Power: Social Bot Interference in Global Politics.** 4 de abril de 2016. Disponivel em: https://uncommonculture.org/ojs/index.php/fm/article/view/6161/5300. Acesso em 13 de outubro de 2019.