OBSERVARE
Universidade Autónoma de Lisboa

e-ISSN: 1647-7251
Vol. 13, Nº. 1 (Maio-Outubro 2022)

JANUS.NET
e-journal of International Relations

PROTEÇÃO DOS PROCESSOS DEMOCRÁTICOS E DOS ATOS ELEITORAIS CONTRA MEDIDAS ATIVAS DIGITAIS RUSSAS: 2016 COMO ANO DE REFERÊNCIA

RICARDO SILVESTRE
ricsilvestre@hotmail.com

Doutor em Filosofia pela Universidade de Connecticut, com *major* em fisiologia humana, e um mestrado em Relações Internacionais pela Universidade Lusófona de Humanidades e Tecnologia de Lisboa, com enfoque no futuro do debate político *online*. *International Officer* do *think tank* Movimento Liberal Social (Portugal). Coordenador de projetos de comunicação política com o European Liberal Forum, o *think tank* do Partido Aliança dos Liberais e Democratas pela Europa no Parlamento Europeu. Os seus principais interesses na área da investigação política são: o futuro da democracia, soluções digitais para problemas societais, e a transição e independência energética da União Europeia com a respetiva diminuição do dilema segurança para com países autoritários e iliberais.

Resumo

A Rússia tem sido acusada de forma credível de tentar enfraquecer as democracias liberais ocidentais com o uso de meios digitais. Peritos em cibersegurança, agências de informação e segurança, jornalistas de investigação e serviços governamentais, detalharam as ações do Kremlin no acesso ilegal a infraestruturas digitais, divulgando conteúdos roubados online, e influenciando o debate político sobre plataformas digitais para criar discórdia e polarização. Estas iniciativas estão incluídas numa estratégia mais ampla de alteração do equilíbrio de poder na ordem internacional através das chamadas "medidas ativas". Duas das mais consequentes aplicações recentes deste tipo de medidas tiveram lugar em 2016, nas Eleições Presidenciais dos Estados Unidos e no Referendo Brexit. Relatórios tornados públicos com as avaliações dos erros cometidos pelos governos dos Estados Unidos e do Reino Unido mostram que houve uma proteção insuficiente desses dois processos cruciais de consulta pública. Os erros cometidos por estes países na proteção da democracia contra agentes hostis com um elevado nível de proficiência digital, devem ser um ponto de interesse, e de urgência, para a União Europeia. É de esperar que este tipo de operação de influência continue, e se torne mais sofisticada, uma vez que podem visar eleições nos Estados-Membros da União, mas também para o Parlamento Europeu. A deteção precoce, a aplicação de contramedidas e a partilha de informação com os eleitores deste tipo de ataques por agências estrangeiras é um importante mecanismo de defesa que precisa de ser reforçado e expandido.

Palavras-chave

Democracia; agências de informação e segurança; plataformas digitais; Federação Russa; União Europeia

Como citar este artigo

Silvestre, Ricardo (2022). Proteção dos processos democráticos e dos atos eleitorais contra medidas ativas digitais russas: 2016 como ano de referência. In Janus.net, e-journal of international relations. Vol. 13, Nº 1, Maio-Outubro 2022. Consultado [em linha] em data da última consulta, https://doi.org/10.26619/1647-7251.13.1.2

Artigo recebido em 11 Maio 2021 e aceite para publicação em 3 Março 2022

PROTEÇÃO DOS PROCESSOS DEMOCRÁTICOS E DOS ATOS ELEITORAIS CONTRA MEDIDAS ATIVAS DIGITAIS RUSSAS: 2016 COMO ANO DE REFERÊNCIA[1]

RICARDO SILVESTRE

Introdução

O Kremlin tem tentado enfraquecer as democracias liberais ocidentais consideradas pelo regime, e pelo Presidente Putin, como ameaças à Federação Russa[2]. Peritos em cibersegurança, agências de informação e segurança, órgãos legislativos e jornalistas de investigação, detalharam algumas das iniciativas de Moscovo para se imiscuírem nos processos democráticos. Exemplos incluem a Geórgia, Estónia, Lituânia, Ucrânia, Holanda, França, Alemanha (Ténis, 2020). O comportamento russo, visto através da teoria dos "quatro mundos" de Robert Jervis, tem uma lógica interna: a preferência por ações ofensivas para inclinar o equilíbrio de poder na ordem internacional (Jervis, 1978). Além disso, a decisão de não assumir posturas defensivas pode ser vista como uma resposta às perceções políticas e sociais das ameaças vindas das fronteiras para o Ocidente (Rato, 2018). Tais preocupações conduzem a uma maximização do poder, em vez de cooperação (Baylis, Smith & Owens, 2019). Num sistema internacional anárquico, os Estados procuram a sua sobrevivência através do enfraquecimento dos adversários. Um exemplo é a criação de ações disruptoras nesses países (Mearsheimer, 2001). Uma destas disrupções é atingir os sistemas democráticos, eleições e organizações, com ferramentas digitais. Uma análise dos incidentes cibernéticos entre 2014 e 2018 (Galante & Ee, 2018) mostra que estes podem ser: exploração de infraestruturas através do acesso a redes informáticas com recolha ou alteração de dados; manipulação do recenseamento eleitoral, alteração da contagem dos votos ou dos votos expressos a fim de causar desconfiança nos resultados eleitorais; divulgação de informação obtida ilegalmente com materiais comprometedores para políticos ou partidos políticos; "frentes falsas" com perfis falsos de indivíduos e grupos, principalmente em redes sociais, com a intenção de provocar polarização; amplificação da dissensão com operações abertas ou encobertas; produção e difusão de informações falsas e desinformação.

Duas das ações mais consequentes, e mesmo impressionantes, da Rússia no interferir nos processos democráticos tiveram lugar durante 2016, nas eleições presidenciais dos

[1] Artigo traduzido por Cláudia Tavares.
[2] Para melhor compreender as motivações do Presidente Putin sugere-se a leitura de "*The Man Without a Face: The unlikely rise of Vladimir Putin*", de Masha Gessen.

Estados Unidos e no Referendo sobre a permanência do Reino Unido na União Europeia. Voltando às teorias de Jervis e Mearsheimer, estas ações podem ser vistas como resultantes de um cálculo do Kremlin dos riscos e benefícios das referidas ações. Os riscos era um maior antagonismo pela comunidade internacional, com a possibilidade de sanções e respostas proporcionais. Quanto aos benefícios, contribuir para o colapso de um bloco económico e político vizinho, e ajudar a derrotar um candidato a Presidente dos Estados Unidos que se opunha manifestamente ao regime de Moscovo em favor de outro claramente mais amistoso, se não ansioso por aceitar as intenções do Presidente russo. Os resultados foram obviamente positivos para o Kremlin. O Reino Unido deixou a União Europeia, com divisões internas que podem levar à desagregação do Reino. Nos Estados Unidos, a administração Trump alienou aliados, tentou diminuir a importância da Organização do Tratado do Atlântico Norte (OTAN), ameaçando mesmo a saída da América da organização, privilegiou os interesses russos no Médio Oriente e colocou os Estados Unidos em "guerras" económicas e diplomáticas, que diminuíram o estatuto do país na comunidade internacional. A União Europeia foi também um alvo destas ações em alguns dos seus Estados-Membros, que levaram à implementação de medidas para combater a desinformação, as notícias falsas, os ciberataques, as operações de disrupção e polarização. O Vice-Presidente da Comissão Europeia para o Mercado Único Digital afirmou em 2019 que "temos de proteger as nossas eleições livres e justas. Esta é a pedra angular da nossa democracia. Para assegurar os nossos processos democráticos contra manipulações ou atividades cibernéticas maliciosas por parte de interesses privados ou de países terceiros" (ENISA, 2019).

Objetivos e métodos de investigação

O objetivo deste documento é produzir um corpo sistematizado de conhecimento, descrevendo como as medidas ativas digitais estão a ser implantados nas democracias liberais ocidentais com a intenção de causar discórdia, e disrupção. Do mesmo modo, serão propostas soluções sobre como melhor combater estas ameaças. A metodologia utilizada é uma estratégia de investigação qualitativa, com a recolha de informação com o objetivo de desenvolver um significado associado às referidas atividades e respostas (Unikaitė-Jakuntavičienė & Rakutienė, 2013). Esta estratégia permite a criação de uma narrativa construtivista, que visa desenvolver uma teoria de forma dedutiva, começando com factos específicos, observação empírica, e avançando para uma generalização teórica dos factos relacionados com a teoria. Do mesmo modo, será aplicada uma investigação científica qualitativa, com a análise do comportamento dos diferentes agentes envolvidos na construção da teoria, bem como dos valores, crenças e emoções. Isto será feito através da observação, análise de discursos, documentos e opiniões de organizações governamentais e da sociedade civil e artigos noticiosos. A lógica da investigação é assim indutiva, com um ponto de partida de conhecimento da realidade, conceitos flexíveis e generalizações analíticas com a ajuda de exemplos (Unikaitė-Jakuntavičienė & Rakutienė, 2013).

Revisão da literatura

A Federação Russa e as "medidas ativas"

O termo medidas ativas foi desenvolvido na União Soviética, a partir dos anos 50, para caracterizar operações secretas e subversivas de influência política que são facilmente refutáveis. Podem variar desde a criação de organizações de fachada, apoio a grupos políticos pró-russos e a disseminação da desinformação (Galeotti, 2019). Em 1982, o então líder do Comité de Segurança do Estado (KGB), Yuri Andropov, fez das medidas ativas uma das principais formas de intervenção do Kremlin durante a Guerra Fria (Andrew & Mitrokhin, 2006: 316). A utilização destas medidas abrandou quando a União Soviética mudou a sua abordagem à comunidade internacional, primeiro liderada por Gorbachev, e depois por Ieltsin, com tentativas de ter uma relação mais estreita com o Ocidente. Com a perda de influência da Rússia e com a ascensão de Vladimir Putin ao poder, Moscovo regressou às hostilidades com países, e blocos de países, que promovem os valores liberais e democráticos. Estes valores podem então chegar à Rússia e aos países situados nas suas fronteiras. Este foi o caso dos protestos de 2012 na Rússia por eleições livres, que Putin explicou como uma operação de influência americana (Crowley & Ioffe, 2016), ou no caso das "revoluções coloridas" nas suas fronteiras (Stewart, 2009). A esta preocupação juntam-se as debilitantes sanções económicas para os setores primários da economia russa, o bloqueio à venda de armas e materiais relacionados, o congelamento de ativos económicos e a aquisição de equipamento para a indústria petrolífera (Krausse, 2018). E depois há a OTAN, e em particular o Artigo 5º da carta da organização, onde um ataque a um dos membros é um ataque a todos (OTAN, 1949). Isto provoca uma perspetiva atraente para os países que a Rússia pensa como parte da sua esfera de influência. Todos estes fatores aumentam a perceção por Putin de um cerco à sua volta (Rato, 2018).

Com a diminuição das expetativas de compreensão Leste-Oeste, Moscovo voltou ao conjunto de ações já conhecidas, juntando-se às recentes levadas a cabo nos países "estrangeiro próximo" (Galeotti, 2019). Recentemente, em 2013, o General Valery Gerasimov, Chefe do Estado-Maior do Exército russo, defendeu a utilização de "métodos indiretos e assimétricos" para criar influência política (Bartles, 2016: 33). Isto inclui alterar o equilíbrio de poder nos países adversários (Bartles, 2016: 34), e o apoio dos partidos políticos que defendem uma relação amigável com Moscovo, como observado em Itália e na Alemanha (Apuzzo & Satarino, 2019), e em França (Turchi, 2017). É também atribuída a Gerasimov a proposta de que as táticas desenvolvidas durante o tempo da União Soviética deveriam ser atualizadas e incluídas no pensamento militar estratégico, para uma "nova teoria da guerra moderna - uma teoria que se assemelha mais a invadir a sociedade de um inimigo do que a atacá-la de frente" (McKew, 2017). As medidas estratégicas defendidas pelo General incluem combinações de ações tecnológicas, informativas, diplomáticas e militares (Galeotti, 2013). Em setembro de 2014, o General Philip Breedlove, durante uma reunião da OTAN, advertiu que a Rússia estava envolvida na "mais espantosa guerra de informação que alguma vez vimos na história da guerra de informação" (Vandiver, 2014).

Entre as principais organizações russas, em termos de criação e aplicação de medidas ativas de intrusão nos processos democráticos dos países estrangeiros, destacam-se as agências de informação e segurança. Os exemplos mais conhecidos são: a Direção

Central do Estado-Maior General das Forças Armadas da Federação Russa, ou GRU; Serviço Federal de Segurança da Federação Russa, ou FSB[3]; e o Serviço de Informações Externas da Federação Russa, ou SVR[4]. O aparelho administrativo do Kremlin caracteriza-se por ser um sistema "não institucionalizado" com um elevado nível de coordenação entre agências para a aplicação de medidas ativas (Galeotti, 2017). Em seguida, reportam diretamente ao Kremlin e/ou ao Presidente Putin (DNI, 2017). A partir daí, são identificadas três formas conhecidas de interferência nas eleições: dirigidas pelo Estado com ações realizadas por operativos na sua qualidade de representantes do regime; encorajados pelo Estado, onde os operacionais não são diretamente responsáveis por iniciar medidas ativas, mas quem quer que seja responsável fá-lo com o conhecimento de que será bem recebido pela liderança; e aqueles alinhados com o Estado, onde indivíduos e/ou organizações atuam para a promoção das políticas do regime (Galante & Ee, 2018). Como extensão das agências de informação e segurança existem também instituições privadas, sob o controlo de oligarcas na órbita de Putin, que atuam para fazer avançar narrativas pró-russas, criando polarização na opinião pública dos países visados. É o caso da Internet Research Agency (IRA), com sede em São Petersburgo, que será apresentada detalhadamente mais à frente. Estas diferentes "frentes de ataque" criam um "tecido conjuntivo" de organizações que trabalham para o mesmo objetivo (Watts, 2018), no modelo de guerra moderna não convencional sugerido por Gerasimov. Este tipo de ações, as suas origens e aplicações, têm sido descritas extensivamente em relatórios tornados públicos por agências ocidentais de informação e segurança. Alguns destes exemplos serão agora apresentados.

O referendo sobre a permanência do Reino Unido na União Europeia

Antes do referendo de 2014 sobre o futuro das relações entre o Reino Unido e a União Europeia (Brexit), realizou-se outro referendo sobre a possível independência da Escócia em relação ao Reino Unido. Nesse processo democrático, foram detetados agentes sediados na Rússia a intrometer-se na consulta pública (Carrell, 2017). Através do Twitter, Facebook e YouTube, contas falsas espalham alegações de interferência no referendo para reforçar a manutenção da Escócia na União. Apesar da ausência de uma ligação direta a Moscovo, "relatos pró-Kremlin reforçaram comprovadamente essas acusações. A raiva e desilusão sentida por muitos eleitores "sim" [foi] alimentada por *trolls* pró-Kremlin, de uma forma característica das operações de influência russa" (Carrell, 2017). A perspetiva de uma dessegregação do Reino Unido corresponde aos objetivos do Kremlin de desestabilização do bloco ocidental de países, e um enfraquecimento dos adversários tanto na arena militar como política. A saída da Escócia do Reino Unido representa um desafio à segurança nacional e a capacidade económica para todos os países envolvidos. Uma diminuição da posição da Grã-Bretanha no mundo leva a negócios comerciais menos vantajosos, uma vez que a Escócia representa um terço da massa terrestre e cerca de 8% dos consumidores. Do mesmo modo, uma desagregação do Reino levaria a questões militares. Uma saída da Escócia da União poderia "desarmar unilateralmente o Reino Unido da sua dissuasão nuclear", uma vez que essas defesas estão " atualmente localizadas em Faslane e Coulport, mas um

[3] *Federal'naya sluzhba bezopasnosti*, no original.
[4] *Sluzhba Vneshney Razvedki*, no original.

governo SNP independente exigiria a sua remoção da Escócia" (Daisley, 2020). Deve acrescentar-se que Nicola Sturgeon, que assumiu a posição de Primeiro-ministro após o referendo, negou que tais influências tivessem existido na consulta pública, e a Comissão Eleitoral, que como autoridade para a realização de eleições e referendos, garantiu que não tinha encontrado provas de fraude. O mesmo foi assegurado, após o referendo do Brexit, pelo Gabinete da Primeira-ministra Theresa May, assegurando que não havia provas para apoiar a conclusão de que o referendo no Reino Unido e a relação com a União Europeia tinha sido alvo de interferência de governos estrangeiros (Syal, 2017).

No entanto, provas de que o Governo de Sua Majestade poderia ter subestimado, ou pior, minimizado possíveis medidas ativas durante o referendo de Brexit, suscitaram o pedido de uma avaliação das ações empreendidas pelas instituições responsáveis pela proteção da democracia no Reino. Após o que foi considerado um atraso excessivo para a publicação da avaliação, e acusações de tentativas de minimizar a importância do seu conteúdo pelo Gabinete do Primeiro-ministro Boris Johnson (Murphy, 2020), a Comissão de Informação e Segurança do Parlamento publicou o relatório intitulado "Rússia" (ISCP, 2020). Esta Comissão supervisiona a atividade das agências de informação e segurança; os Serviços de Segurança (MI5), o Serviço Secreto de Informação e Segurança (MI6) e a Sede de Comunicações do Governo, ou GCHQ. Uma das justificações para a produção do relatório afirma que "tem sido credível a informação pública sugerindo que a Rússia empreendeu campanhas de influência em relação ao referendo sobre a independência da Escócia em 2014" (ISCP, 2020: 13). Relativamente ao referendo na relação entre o Reino Unido e a União Europeia, "as provas escritas que nos foram fornecidas pareciam sugerir que HMG [o Governo de Sua Majestade] não tinha visto ou procurado provas de interferência bem-sucedida nos processos democráticos do Reino Unido ou de qualquer atividade que tivesse tido um impacto material sobre uma eleição, por exemplo, influenciando os resultados" (ISCP, 2020: 13). Indo mais longe, a Comissão afirma que "não nos foi fornecida qualquer avaliação pós-referendo das tentativas de interferência russas. Esta situação contrasta fortemente com o tratamento dado pelos EUA às alegações de interferências russas nas eleições presidenciais de 2016" (ISCP, 2020: 14). A Comissão determinou que o Governo de Sua Majestade subestimou seriamente a ameaça russa e negligenciou as contramedidas, não protegendo, portanto, o processo referendário (ISCP, 2020a).

No relatório é descrito que a Federação Russa tende a ver a política externa como uma "soma zero", onde cada ação prejudicial para o Ocidente é favorável a Moscovo. Isto resulta de uma apreciação "alimentada pela paranoia, acreditando que instituições ocidentais como a OTAN e a UE têm uma postura muito mais agressiva em relação [à Rússia] do que na realidade têm" (ISCP, 2020: 1). O centro de decisão "está concentrado em Putin e num pequeno grupo de consultores de confiança (muitos dos quais partilham o passado de Putin nos RIS [serviços de informação russos])" (ISCP, 2020: 29) fazendo com que essas decisões tenham uma aplicabilidade e flexibilidade que as organizações ocidentais não podem igualar. Principalmente, e tal como avaliado pelo GCHQ, a Rússia tem uma elevada capacidade na área digital e é capaz de realizar operações cibernéticas com uma vasta gama de impactos em vários setores da sociedade.

Desde 2014, a Federação Russa tem "levado a cabo atividades cibernéticas maliciosas a fim de se afirmar agressivamente em várias esferas, incluindo a tentativa de influenciar

as eleições democráticas de outros países (…) A GCHQ também aconselhou que os agentes do GRU russo orquestraram tentativas de *phishing*[5] contra departamentos governamentais" (ISCP, 2020: 5), algo que foi observado no Reino Unido, na Alemanha e nos Países Baixos (Silvestre, 2019). De facto, no dia 3 de outubro de 2018, o Ministro dos Negócios Estrangeiros, na altura liderado por Jeremy Hunt do Partido Conservador, anunciou publicamente que o Reino Unido e os seus aliados tinham identificado uma campanha do GRU que é "imprudente e indiscriminada: eles tentam minar e interferir nas eleições noutros países" (NCSC, 2018).

Relativamente às propostas para combater as ameaças observadas durante o referendo, a Comissão Parlamentar expressou que o "extremo cuidado" das agências de informação para se envolverem em processos democráticos é "ilógico". A interferência em atos eleitorais por países hostis deve ser vista como uma prioridade em relação à proteção do Estado e que esta deve ser da responsabilidade das agências de informação e segurança (em particular, o MI5) (ISCP, 2020: 11). Outra recomendação importante no relatório é que o Governo deve estabelecer protocolos com plataformas de meios de comunicação social para assegurar que detetam medidas ativas por parte de atores hostis, com um tempo claramente definido para a remoção de tais conteúdos. Como recomendações legislativas, a Comissão Digital, Cultura, Meios de Comunicação Social e Desporto pediu ao Governo para avaliar se a legislação atual para proteger os processos eleitorais da influência maligna é suficiente, e que "a legislação deve estar em conformidade com os últimos desenvolvimentos tecnológicos" (DCMS, 2019: 71). Propõem também que a Comissão Eleitoral tenha o poder de "intervir ou impedir alguém que aja ilegalmente numa campanha se viver fora do Reino Unido" (DCMS, 2019).

As eleições para a Presidência Americana

Em fevereiro de 2018, o então Conselheiro Especial Robert Mueller entregou provas de facto a um grande júri federal no Distrito de Columbia, o que resultou na acusação de treze indivíduos russos e três organizações russas por interferirem nas eleições presidenciais americanas de 2016 (USDJ, 2018). A acusação mostra o alcance e a natureza sistemática dos ataques que começaram em 2014. Particularmente ativa foi a empresa Internet Research Agency (IRA), com as suas explorações de *troll*[6]. Ao roubar identidades americanas, criar relatos falsos em plataformas de meios de comunicação social, e disseminar conteúdos inflamatórios, tanto raciais como sociais, o IRA tentou causar disrupção e polarização política. As operações desta empresa não se limitaram a ações remotas a partir de São Petersburgo, mas também em cooperação com os membros da campanha Trump "no terreno" (USDJ, 2018: 4). Utilizando perfis falsos no Facebook e Twitter, os membros do IRA organizaram comícios e reuniões nos Estados Unidos, através da sedes locais da campanha, e compraram anúncios online para promove-los (USDJ, 2018: 21-28).

[5] O ato de *phishing* é o envio de e-mails fraudulentos para induzir os utilizadores a partilhar dados pessoais, tais como palavras-passe.

[6] Uma exploração *troll* é um grupo de utilizadores da Internet que pretende interferir na discussão política online com propósitos (na sua maioria) nefastos.

Tal como o Conselheiro Especial Mueller, a Comissão Especial do Senado dos EUA sobre Informação e Segurança e Segurança também foi clara nas suas conclusões: Os agentes russos, através do IRA, utilizaram plataformas de meios de comunicação social digitais para conduzir campanhas de guerra informativas, difundindo a desinformação e criando divisões nos Estados Unidos (SSCI, 2019: 3). Estas campanhas foram realizadas sob a direção do Kremlin, e com o objetivo de reduzir as chances de sucesso da candidata Hillary Clinton em favor do candidato Trump (SSCI, 2019: 4), uma vez que a primeira foi vista como mais hostil aos interesses russos (SSCI, 2019: 6). Embora Moscovo rejeite as conclusões do Senado americano, o proprietário do IRA, Yevgeniy Prigozhin, tem ligações diretas com o Presidente Putin, o que aponta para uma " direção, apoio e autorização significativa do Kremlin nas operações e objetivos do IRA" (SSCI, 2019: 5). Tal como o IRA, o GRU também foi acusado de explorar plataformas de comunicação social para difundir informações obtidas ilegalmente. Isto foi feito através da divulgação de e-mails da campanha Clinton, informação que foi obtida pelas Unidades 26165 e 74455 dentro do GRU (USDJ, 2018a). De facto, o Conselheiro Especial Mueller acusou o Coronel Aleksandr Osadchuk, comandante da Unidade 74455, por ajudar "na divulgação de documentos roubados através do DCLeaks e do Guccifer 2.0 personas, na promoção dessas divulgações e na publicação de conteúdo anti-Clinton em contas de meios de comunicação social operadas pelo GRU" (USDJ, 2018a: 5). Numa declaração conjunta do Department of Homeland Security e Director of National Intelligence (DHS, 2016) foi anunciado que a comunidade de informação e segurança americana estava confiante de que o governo russo tinha interferido nas eleições, através do uso indevido de e-mails obtidos ilegalmente de organizações políticas americanas. Para o efeito, recorreram à ajuda de organizações externas, principalmente o WikiLeaks e o Guccifer 2.0, sendo a segunda uma outra frente dos serviços secretos militares russos (Sanger & Schmitt, 2016). As agências de informação e segurança americanas que contribuíram para esta investigação incluíram o *Federal Bureau of Investigation* (FBI), a *Central Intelligence Agency* (CIA) e a *National Security Agency* (NSA). Naturalmente, o grau de confiança entre as agências nos resultados dos processos analíticos não foi uniforme. Contudo, a maioria das conclusões são apresentadas com um "elevado grau de confiança" (DNI, 2017).

Relativamente à utilização de plataformas de comunicação social por agentes russos, o Facebook confirmou à Comissão Especial que a atividade atribuível ao grupo Fancy Bear (Unidade 26165 do GRU) foi observada (Graff, 2018). Tal como o IRA, Fancy Bear também criou perfis falsos na plataforma e através da organização DCLeaks para distribuir a informação obtida ilegalmente a jornalistas (Stretch, 2018). No relatório minoritário de 2017 da Comissão de Seleção Permanente de Informação e Segurança da Casa dos Representantes dos EUA (elaborado por membros do Partido Democrata), com os resultados de uma investigação no Facebook sobre a disrupção e polarização nas eleições de 2016, as ações do IRA incluíram a compra de 3.393 anúncios políticos, e a criação de 470 páginas no Facebook que atingiram 126 milhões de utilizadores (HSCI, 2017). Na outra plataforma "gigante" de comunicação social onde há um debate político dinâmico, Twitter, entre 1 de setembro e 15 de novembro de 2016, mais de 36.000 *tweets* sobre as eleições presidenciais foram gerados por *bots*[7] ligados às contas russas.

[7] Um *bot* é um programa autónomo que interage com sistemas e utilizadores digitais.

Estes *tweets* geraram cerca de 228 milhões de interações[8]. Além disso, mais de 130.000 *tweets* eram de contas diretamente ligadas ao IRA (HSCI, 2017).

As medidas ativas implementadas pela Rússia não são um fenómeno recente. O KGB foi responsável pela autoria e divulgação de histórias falsas, bem como de cartas fraudulentas, visando os presidentes John Kennedy e Ronald Reagan, e o ativista Martin Luther King, Jr. (SSCI, 2019: 11). Contudo, nas eleições de 2016, este tipo de ação foi aperfeiçoado através da utilização de plataformas de comunicação social, com especial incidência na supressão do voto, especialmente da comunidade negra (SSCI, 2019: 39), promovendo narrativas políticas, nomeadamente, para atrair os seguidores do senador Bernie Sanders (Timberg & Harris, 2018); e visando a coligação que apoiava o Secretário de Estado Clinton (Kim, 2018).

Proteger a democracia na União Europeia contra ciberataques digitais

Nos relatórios apresentados acima, existe a preocupação de como proteger os processos democráticos e atos eleitorais de medidas ativas por parte de agências de informação de países hostis. Na era digital, e de acordo com a máxima de Thomas Jefferson que "a vigilância eterna é o preço da liberdade" (TJM, 2020), compete à União Europeia não subestimar o que aconteceu nos Estados Unidos e no Reino Unido. Os Estados-Membros da União Europeia, juntamente com o Parlamento Europeu e a Agência Europeia para a Segurança Cibernética (ENISA), organizaram um exercício em 2019 para "testar a resposta da UE e os planos de crise para potenciais incidentes de cibersegurança que afetem as eleições da UE" (ENISA, 2019). Este exercício visava aumentar a cooperação entre as autoridades nacionais nas áreas da cibersegurança, proteção de dados e cibercriminalidade. Além de trabalhar "no terreno", a ENISA também produz documentos práticos para garantir a segurança nos processos eleitorais. Para a Comissão Europeia, os objetivos são a proteção dos sistemas democráticos nos Estados-Membros, mas também a salvaguarda dos valores europeus (Comissão Europeia, 2020). Há um conjunto de instrumentos que já existem com objetivos semelhantes, incluindo o Plano de Ação Contra a Desinformação[9], o Plano de Ação para a Democracia Europeia[10], a rede europeia de cooperação em matéria eleitoral[11], o Compêndio sobre Segurança Cibernética da Tecnologia Eleitoral[12], a Lei de Cibersegurança da UE[13], a Diretiva revista sobre a segurança das redes e dos sistemas de informação (NIS2)[14], assim como instrumentos para combater as ameaças híbridas e aumentar a cibersegurança[15].

---

8 As interações incluem ações de utilizadores como retoques, respostas, seguimentos, inclusão de *hashtags* e expansão de *tweets*.

9 https://ec.europa.eu/info/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en.

10 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250.

11 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.

12 https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf.

13 https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

14 https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2.

15 https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193.

Contudo, existe uma ausência visível nos sistemas de proteção na União Europeia, seja por inação, seja por falta de comunicação com os cidadãos da União: qual é a capacidade de recolher informações e analisar ameaças aos processos democráticos por parte de agências de informação hostis? Isto aplica-se tanto nas eleições em que os Estados-Membros (se acordado), como nas eleições para o Parlamento Europeu. Atualmente, existe o Centro de Informação e Situação da UE (INTCEN)[16] que tem a missão de criar alertas atempados para ameaças, e avaliar ameaças nas áreas da segurança, defesa e contraterrorismo. Este trabalho é realizado através da recolha de informações em colaboração com as agências dos Estados-membros, autoridades militares e diplomatas (Estevens, 2020). Recomenda-se a inclusão da INTCEN numa estratégia de defesa mais ampla e integrada, servindo como um sistema avançado de deteção de sinais, quer a partir de fonte aberta, meios digitais ou através de recursos humanos. A atribuição desta missão seria da responsabilidade da Comissão Europeia: através de uma resolução com definições claras sobre o tratamento e partilha de informação entre agências nos Estados-Membros: tipos de desenvolvimento e aplicação de respostas rápidas; relação com os legisladores tanto no Parlamento Europeu como nos governos locais; e com os eleitores, quando possível ou aconselhável. Naturalmente, as ações das agências de informação e segurança na deteção de ameaças e na aplicação de contramedidas para defender processos eleitorais, que por vezes não podem ser do domínio público. Há necessidade de encontrar um equilíbrio entre a proteção de fontes e processos, e que ameaças podem ser partilhadas com os eleitores, para que estes sejam informados e possam tomar decisões políticas sem influências externas maliciosas.

Outra exigência crescente, por parte de organizações como a Comissão Europeia, a Comissão Especial do Senado dos EUA e a Comissão de Informação e Segurança e Segurança do Parlamento do Reino Unido, é que as plataformas dos meios de comunicação social mudem as suas políticas para um maior trabalho conjunto com as autoridades, incluindo as agências de informação e segurança e os órgãos legislativos. Este trabalho conjunto deve incluir uma partilha atempada e abrangente de informação, principalmente de atividades maliciosas que exploram a arquitetura digital das plataformas, manipulação de algoritmos e disseminação de conteúdos para subversão de processos eleitorais. A Lei dos Serviços Digitais (DSA), proposta pela Comissão Europeia e aceite pelo Parlamento Europeu, aborda algumas destas necessidades. Na DSA, os fornecedores de serviços intermediários da Internet precisam de produzir relatórios de transparência com informações sobre interação com as autoridades, descrição de conteúdos ilegais, tempo necessário para a remoção de conteúdos, ações tomadas e justificações legais (Comissão Europeia, 2020a). Se forem detetados maus agentes ou medidas ativas, as agências de informação e segurança devem poder agir de forma precisa e oportuna em colaboração com plataformas digitais para a aplicação de medidas apropriadas. Este processo deve ser coordenado através da supervisão das estruturas governamentais, e, se necessário, dos órgãos legislativos sempre que houver necessidade de alterações nas leis para resolver problemas estruturais. Da mesma forma, deve haver um trabalho conjunto com os partidos políticos e/ou candidatos a posições governamentais. Exemplos bem sucedidos de tal colaboração têm tido lugar em França e no Reino Unido. Em França, a *Agence Nationale de la Sécurité des Systèmes*

[16] https://eeas.europa.eu/sites/default/files/2021_-_01_-_02_-_eeas_2.0_orgchart.pdf.

d'Information, a agência responsável pela proteção das infraestruturas governamentais contra ciberataques, organizou sessões de informação sobre cibersegurança para todos os partidos políticos (embora nem todos tenham demonstrado interesse em participar) (Daniels, 2017). No Reino Unido, foi a vez de o Centro Nacional de Cibersegurança Britânico, parte do GCHQ, oferecer ajuda no reforço das redes de comunicação dos partidos políticos (Reuters, 2017).

Conclusões

Uma questão provocadora levantada por Persily é "Poderá a Democracia Sobreviver à Internet?" (Persily, 2017). Alguns autores alertam para a ingenuidade de pensar que a Internet é um caminho para uma utopia de debate, compreensão e consenso, numa perspetiva Madisoniana de governação[17]. Ao mesmo tempo, ferramentas digitais ainda mais poderosas, como a recuperação de dados pessoais, grandes dados, aprendizagem de máquinas, função algorítmica, podem abrir o espaço para as empresas, que são de aluguer, para gerar publicidade política dirigida ao nível individual, criando "bolhas digitais", "câmaras de eco" que levam à polarização política e à ação política contraproducente.

A Comissão Especial do Senado dos EUA para Informação e Segurança adverte que medidas ativas, tendo o Kremlin como epicentro, e com uma alegada ligação direta a Vladimir Putin, "representam a mais recente expressão do desejo de longa data de Moscovo de minar a ordem democrática liberal liderada pelos EUA" (SSCI, 2019: 11). É preocupante que países com democracias estabelecidas, agências de informação e segurança sofisticadas, uma imprensa livre e uma sociedade civil vibrante, como o Reino Unido e os Estados Unidos, não se tenham apercebido, ou ignorado, as ameaças da Federação Russa de perturbar os processos eleitorais de 2016. No relatório da Comissão de Informação e Segurança do Parlamento, há um aviso perturbador de que o governo do Reino Unido se encontrava num "estado de negação" da influência russa, de modo a não questionar a legitimidade do executivo associado ao resultado de Brexit (Ellehuus & Ruy, 2020). Isso não foi exclusivo de Whitehall. Nos Estados Unidos, o Presidente Trump passou parte do seu mandato a negar, ou a minimizar, as ações da Rússia nas eleições de 2016, entrando mesmo em conflito com as agências americanas de informação e segurança sobre se Putin tinha autorizado alguma delas. De facto, Trump iria despedir, em 2017, o Diretor do FBI James Comey por causa, nas palavras do Presidente, da "questão da Rússia". Isto resultaria na nomeação do Advogado Especial Robert Mueller e no processo de *impeachment* do Presidente (Balsamo, 2019). Ainda no relatório do Parlamento, outra observação importante foi a falta de definição dentro do governo do Reino Unido sobre quais os mecanismos de defesa a utilizar contra medidas estrangeiras ativas nos processos democráticos. Isto fez com que a assunção de responsabilidades parecesse uma "batata quente" (ISCP, 2020: 5).

Os agentes russos continuarão a testar estas medidas ativas nos países ocidentais. Em 2018, na véspera das eleições intercalares para o Senado e Casa dos Representantes dos Estados Unidos, outra queixa criminal contra o IRA, na pessoa de Elena Khusyaynova,

[17] Alguns destes avisos podem ser encontrados em livros escritos por Timothy Garth Ash, Rebecca MacKinnon, Cass Sustein, Clay Shirky e Evgeny Morozov.

foi apresentada no Distrito Oriental da Virgínia por um Procurador Federal, por conspirar para interferir com o processo político e eleitoral americano nas eleições de 2018 (USDC, 2018). No mesmo ano, a CIA avaliou que Vladimir Putin era "provavelmente" responsável por outra campanha para desacreditar o Vice-Presidente Joe Biden, então candidato a Presidente (e eventual vencedor) (Rogin, 2020). Ações semelhantes foram observadas na Europa, onde, no período entre 2017 e 2018, campanhas de desinformação utilizando meios de comunicação estatais e meios de comunicação social patrocinados pela Rússia ocorreram em Itália, Países Baixos, Espanha (o referendo sobre a independência da Catalunha), República Checa e Suécia (Tennis, 2020).

Se as motivações para Presidente Putin e o Kremlin parecem óbvias à luz das teorias de Jervis e Mearsheimer, de tentar maximizar uma postura ofensiva, interferindo nos processos democráticos e eleições no Ocidente, o "preço" a pagar não parece ser dissuasor. A Federação Russa é um (quase) Estado pária no que diz respeito às relações com o Ocidente (exacerbadas por intervenções militares no "estrangeiro próximo"), pelo que a ameaça de isolamento não é operacional. Da mesma forma, as sanções devidas a interferências eleitorais e ciberataques continuam a concentrar-se em indivíduos e organizações que se crê estarem relacionados com o centro do poder em Moscovo (Turak & Macias, 2021). No entanto, o governo russo continuará a negar qualquer responsabilidade, enquanto dá abrigo a pessoas e grupos indiciados, tornando-os imunes à perseguição no Ocidente. Desta forma, será difícil infligir golpes graves a estas estruturas que promovem medidas ativas.

O Vice-Presidente do Parlamento Europeu, Rainer Wieland, afirmou em 2019 que "os ciberataques são uma ameaça recente, mas muito real para a estabilidade da União Europeia e dos seus Estados-Membros. Um ataque cibernético às eleições poderia minar dramaticamente a legitimidade das nossas instituições. A legitimidade das eleições baseia-se no entendimento de que podemos confiar nos seus resultados. Esta mesma confiança tem estado sob pressão de ciberataques e outros novos tipos de fraude eleitoral na era digital, e nós temos de responder!" (ENISA, 2019). Uma das necessidades mais importantes é detetar, o mais rapidamente possível, quem está por detrás destes ataques, como começaram, como são dirigidos e os efeitos destas medidas ativas nos processos democráticos, devido às influências na forma como as sociedades funcionam. Especialmente, as agências de informação e segurança adversária são conhecidas por serem um "perigo claro e presente", como atestado pela informação de domínio público. Agências como o GRU, FSB e SRV continuarão a testar os sistemas e contramedidas ocidentais. É aconselhável que um bloco de países, com um poder centralizado no Parlamento Europeu, como a União Europeia, utilize todos os instrumentos disponíveis nesta linha de defesa, incluindo a exploração do potencial de alguns dos instrumentos já existentes.

Este trabalho visava sistematizar algumas das informações de domínio público sobre medidas ativas digitais, o seu *modus operandi*, e dar algumas contramedidas para combater estas ameaças. No entanto, o campo de batalha está a alargar-se e a tornar-se progressivamente perigoso. As respostas setoriais, como as observadas na União Europeia, nos Estados Unidos, no Reino Unido, poderiam ser os pontos de entrada para uma estratégia coordenada, multifacetada e proporcional para reforçar as democracias liberais ocidentais, e as inspiradoras em todo o mundo, contra estas ameaças.

Referências

Andrew, C & Mitrokhin, V (2006). *The Mitrokhin Archive: The KGB in Europe and the West.* New York: Penguin Press History.

Apuzzo, M & Satariano, A (2019). Russia Is Targeting Europe's Elections. So Are Far-Right Copycats. [Consultado a 15 de abril 2021]. Disponível em: https://www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html.

Balsamo, M (2019). Trump depicted in Mueller report feared being called a fraud. [Consultado a 15 de abril 2021]. Disponível em: https://apnews.com/article/677b7b2f0c184e65921afe2314e468ac.

Bartles, C.K (2016). «Getting Gerasimov Right». *Military Review*. 96(1): 30-38.

Baylis, J, Smith, S, & Owens. P (2019). *The Globalization of World Politics. An Introduction to International Relations*. Eighth Edition. Oxford: Oxford University Press.

Carrell, S (2017). Russian cyber-activists 'tried to discredit Scottish independence vote'. [Consultado a 15 de abril 2021]. Disponível em: https://www.theguardian.com/politics/2017/dec/13/russian-cyber-activists-tried-to-discredit-scottish-independence-vote-says-analyst.

Crowley, M & Ioffe, J (2016). Why Putin hates Hillary. Behind the allegations of a Russian hack of the DNC is the Kremlin leader's fury at Clinton for challenging the fairness of Russian elections. [Consultado a 15 de abril 2021]. Disponível em: https://www.politico.com/story/2016/07/clinton-putin-226153.

Daisley, S (2020). Why Putin wants Scottish independence. [Consultado a 15 de abril 2021]. Disponível em: https://www.spectator.co.uk/article/why-putin-wants-scottish-independence.

Daniels, L (2017). How Russia hacked the French election. [Consultado a 15 de abril 2021]. Disponível em: https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

DCMSC [Digital, Culture, Media and Sport Committee] (2018). Russian Influence in Political Campaigns. Disinformation and "fake news": Interim Report. [Consultado a 15 de abril 2021]. Disponível em: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm.

DHS [Department of Homeland Security] (2016). Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. [Consultado a 15 de abril 2021]. Disponível em: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

DNI [Director of National Intelligence] (2017). *Assessing Russian Activities and Intentions in Recent US Elections*. Intelligence Community Assessment, [Consultado a 15 de abril 2021]. Disponível em: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Ellehuus, R & Ruy, D (2020). Did Russia Influence Brexit? [Consultado a 15 de abril 2021]. Disponível em: https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit.

ENISA [European Union Agency for Cybersecurity] (2019). EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections. [Consultado a 15 de abril 2021]. Disponível em: https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-their-cybersecurity-preparedness-for-fair-and-free-2019-eu-elections.

Estevens, J (2020). «Building intelligence cooperation in the European Union». *Janus.net*, *e-journal of International Relations.* 11(2)

European Commission (2020). Tackling online disinformation. [Consultado a 15 de abril 2021]. Disponível em: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation.

European Commission (2020a). Proposal for a Regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. [Consultado a 15 de abril 2021]. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en.

Galante, L & Ee, S (2018). *Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents*. Atlantic Council, [Consultado a 15 de abril 2021]. Disponível em: https://www.atlanticcouncil.org/wp-content/uploads/2018/09/Defining_Russian_Election_Interference_web.pdf.

Galeotti, M (2013). The 'Gerasimov Doctrine' and Russian Non-Linear War. [Consultado a 15 de abril 2021]. Disponível em: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war.

Galeotti, M (2017). Controlling Chaos: How Russia Manages its Political War in Europe. ECFR Briefing. [Consultado a 15 de abril 2021]. Disponível em: https://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe.

Galeotti, M (2019). Active Measures: Russia's Covert Geopolitical Operations. [Consultado a 15 de abril 2021]. Disponível em: https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0.

Gessen, M (2012). *The man without a face. The unlikely rise of Vladimir Putin*. New York: Riverhead Books.

Graff. G.M (2018). Indicting 12 Russian Hackers Could Be Mueller's Biggest Move Yet. [Consultado a 15 de abril 2021]. Disponível em: https://www.wired.com/story/mueller-indictment-dnc-hack-russia-fancy-bear.

HSCI [House Select Committee on Intelligence] (2017). Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements. [Consultado a 15 de abril 2021]. Disponível em: https://intelligence.house.gov/social-media-content.

ISCP [Intelligence and Security Committee of Parliament] (2020). *Russia*. Intelligence and Security Committee of Parliament, [Consultado a 15 de abril 2021]. Disponível em: https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.

ISCP [Intelligence and Security Committee of Parliament] (2020a). *Press Notice. Intelligence and Security Committee of Parliament publish predecessor's Russia Report.* [Consultado a 15 de abril 2021]. Disponível em: https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDoxMmRkZmU2MjQ4ZWEzNDI0.

Jervis, R (1978). «Cooperation Under the Security Dilemma». *World Politics.* 30(2): 167-214.

Kim, Y.M (2018). *Uncover: Strategies and Tactics of Russian Interference in US Elections. Russian Groups Interfered in Elections with Sophisticated Digital Campaign Strategies*. University of Wisconsin, [Consultado a 15 de abril 2021]. Disponível em: https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/09/Uncover.Kim_.v.5.0905181.pdf.

Krausse, C (2018). Exxon Mobil Scraps a Russian Deal, Stymied by Sanctions. [Consultado a 15 de abril 2021]. Disponível em: https://www.nytimes.com/2018/02/28/business/energy-environment/exxon-russia.html.

McKew, M.K (2017). The Gerasimov Doctrine its Russia's new chaos theory of political warfare. And it's probably being used on you. [Consultado a 15 de abril 2021]. Disponível em: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538.

Mearsheimer, J.J (2001). *The tragedy of great power politics*. New York: W.W. Norton & Company.

Murphy, S (2020). UK report on Russian interference: key points explained. [Consultado a 15 de abril 2021]. Disponível em: https://www.theguardian.com/world/2020/jul/21/just-what-does-the-uk-russia-report-say-key-points-explained.

NCSC [National Cyber Security Center] (2018). Reckless campaign of cyber attacks by Russian military intelligence service exposed. [Consultado a 15 de abril 2021]. Disponível em: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

OTAN [Organização do Tratado do Atlântico Norte] (1949). Tratado do Atlântico Norte. [Consultado a 15 de abril 2021]. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt

Persily, N (2017). «Can Democracy Survive the Internet? ». *Journal of Democracy*, 28: 63-76.

Rato, V (2018). «Romper o cerco: a Rússia de Putin e a Nova Guerra Fria». *Nação e Defesa*. 150: 116-148.

Reuters (2017). UK political parties warned of Russian hacking threat: report. [Consultado a 15 de abril 2021]. Disponível em: https://uk.reuters.com/article/us-britain-russia-cybercrime-idUKKBN16J0OE.

Rogin, J (2020). Secret CIA assessment: Putin 'probably directing' influence operation to denigrate Biden. [Consultado a 15 de abril 2021]. Disponível em: https://www.washingtonpost.com/opinions/2020/09/22/secret-cia-assessment-putin-probably-directing-influence-operation-denigrate-biden.

Sanger, D & Schmitt, E (2016). Spy Agency Consensus Grows that Russia Hacked D.N.C. [Consultado a 15 de abril 2021]. Disponível em: https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html.

SSCI [Senate Select Committee on Intelligence] (2019). *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume2: Russia's use of Social Media with Additional Views*. 116th Congress, [Consultado a 15 de abril 2021]. Disponível em: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf .

Silvestre, R (2019). «A Rússia e os ciber ataques a instituições democráticas europeias». *ResPublica*. 19: 83-107.

Stewart, S (2009). «Democracy Promotion before and after the 'color revolutions'». *Democratization*. 16(4): 645-660.

Stretch, C (2018). *Written responses from Facebook's General Counsel to U.S. Senate Select Committee on Intelligence*. U.S. Senate, [Consultado a 15 de abril 2021]. Disponível em: https://www.intelligence.senate.gov/sites/default/files/documents/Facebook%20Response%20to%20Committee%20QFRs.pdf.

Syal, R (2017). Brexit: foreign states may have interfered in vote, report says. [Consultado a 15 de abril 2021]. Disponível em: https://www.theguardian.com/politics/2017/apr/12/foreign-states-may-have-interfered-in-brexit-vote-report-says.

Tennis, M (2020). Russia Ramps up Global Elections Interference: Lessons for the United States. [Consultado a 15 de abril 2021]. Disponível em: https://www.csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states.

Timberg, C & Harris, S (2018). Russian operatives blasted 18.000 tweets ahead of huge news day during the 2016 presidential campaign. Did they know what was coming? [Consultado a 15 de abril 2021]. Disponível em: https://www.washingtonpost.com/ellipsis/russian-operatives-blasted-18000-tweets-ahead-of-a-huge-news-day-during-the-2016-presidential-campaign-did-they-know-what-was-coming/2018/07/20/6715a547-91db-43f0-b21a-a75ff3d9205a_story.html.

TJF [Thomas Jefferson Encyclopedia] (2020). Eternal vigilance is the price of liberty (Spurious Quotation). [Consultado a 15 de abril 2021]. Disponível em:

https://www.monticello.org/site/research-and-collections/eternal-vigilance-price-liberty-spurious-quotation.

Turak, N & Macias, A (2021). Biden administration slaps new sanctions on Russia for cyberattacks, election interference. [Consultado a 15 de abril 2021]. Disponível em: https://www.mediapart.fr/journal/international/300317/marine-le-pen-signe-nouveau-pour-de-l-argent-russe.

Turchi, M (2017). Marine Le Pen Signe à Nouveau Pour de l'Argent Russe. [Consultado a 15 de abril 2021]. Disponível em: https://www.mediapart.fr/journal/international/300317/marine-le-pen-signe-nouveau-pour-de-l-argent-russe.

Unikaitė-Jakuntavičienė, I, & Rakutienė, S (2013). Writing a Bachelor's Thesis in the Field of Political Science. Didactical Guidelines. [Consultado a 15 de abril 2021]. Disponível em: https://www.esparama.lt/es_parama_pletra/failai/ESFproduktai/2013_metodine_priemone_Writing_a_Bachelors_Thesis.pdf

USDC [United States District Court] (2018). 1:18-MJ-464. [Consultado a 15 de abril 2021]. Disponível em: https://www.justice.gov/usao-edva/press-release/file/1102591/download.

USDJ [United States Department of Justice] (2018). Case 1:18-cr-00032-DLF. [Consultado a 15 de abril 2021]. Disponível em: https://www.justice.gov/file/1035477/download.

USDJ [United States Department of Justice] (2018a). Case 1:18-cr-00032-DLF. [Consultado a 15 de abril 2021]. Disponível em: https://www.justice.gov/file/1080281/download.

Vandiver, J (2014). SACEUR: Allies must prepare for Russia 'hybrid war'. [Consultado a 15 de abril 2021]. Disponível em: https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464.

Watts, C (2018). Russia's Active Measures Architecture: Task and Purpose. [Consultado a 15 de abril 2021]. Disponível em: https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose.