UNIVERSIDADE CATÓLICA PORTUGUESA

RÚSSIA, CAMBRIDGE ANALYTICA E AS ELEIÇÕES PRESIDENCIAIS NORTE-AMERICANAS DE 2016: O CIBERESPAÇO COMO O MAIS RECENTE DOMÍNIO DA CONFLITUALIDADE POLÍTICA

Dissertação apresentada à Universidade Católica Portuguesa para obtenção do grau de Mestre em Ciência Política e Relações Internacionais

Por

João António França de Oliveira

Número de aluno: 100518002

Instituto de Estudos Políticos

Dezembro, 2020

UNIVERSIDADE CATÓLICA PORTUGUESA

RÚSSIA, CAMBRIDGE ANALYTICA E AS ELEIÇÕES PRESIDENCIAIS NORTE-AMERICANAS DE 2016: O CIBERESPAÇO COMO O MAIS RECENTE DOMÍNIO DA CONFLITUALIDADE POLÍTICA

Dissertação apresentada à Universidade Católica Portuguesa para obtenção do grau de Mestre em Ciência Política e Relações Internacionais

Por

João António França de Oliveira

Número de aluno: 100518002

Sob orientação do General Luís Vasco Valença Pinto

Instituto de Estudos Políticos

Dezembro, 2020

Resumo

A Eleição Presidencial dos Estados Unidos em 2016 ficará para sempre marcada pela interferência da Rússia e pelo envolvimento da Cambridge Analytica. Nesta eleição, a ideia de que a tecnologia digital, as redes sociais, a internet e o ciberespaço fariam do mundo um lugar mais aberto e livre foi desafiada, dado que Rússia e Cambridge Analytica instrumentalizaram estes meios para, através de desinformação, prejudicarem um candidato e enaltecerem outro, conduzindo o eleitorado a votar, não com base em factos, mas com base em narrativas criadas.

Neste trabalho, procuraremos mostrar como é que o Estado soberano e autoritário da Rússia, bem como a firma Cambridge Analytica, usaram a liberdade de expressão e a livre circulação de informação, que tão queridos são às democracias liberais, para veicular desinformação, numa tentativa de manipular a escolha democrática dum novo líder político através da tecnologia digital.

Tendo em conta que estes esforços de manipulação ocorreram sobretudo no ciberespaço, um domínio cada vez mais acessível e presente na vida das populações, em que a evolução tecnológica é extraordinariamente veloz, e que já quatros anos passaram desde a eleição, procuraremos, também, tecer considerações acerca do que será possível fazer no ciberespaço no futuro, que capacidades cibernéticas existirão e que riscos comportarão, bem como acerca de qual será o papel do ciberespaço enquanto quinto domínio de conflito, ao lado dos domínios da Terra, do Mar, do Ar e do Espaço.

Contagem de palavras da dissertação: 36 826

Abstract

The 2016 United States Presidential Election will forever be tainted with Russia's interference and Cambridge Analytica's involvement. In this election, the idea that digital technology, social media, the internet and cyberspace would make the world a freer and more open world was challenged, since Russia and Cambridge Analytica harnessed these means to, through disinformation, harm one candidate's chances and boost another's, steering the electorate to vote based not on facts, but on made-up narratives.

In this work, we will endeavour to show how the sovereign and authoritarian state of Russia, as well as the firm Cambridge Analytica, used freedom of expression and the free circulation of information, which democracies so dearly hold, to disseminate disinformation, in an attempt to manipulate the democratic choice of a new political leader, through digital technology.

Taking into account that these manipulation efforts took place primarily in cyberspace, a domain ever more accessible and present in the lives of populations, in which technological evolution is extraordinarily fast, and that four years have passed since the election, we will also endeavour to make considerations about what will be possible to do in cyberspace in the future, what cybernetic capabilities will exist and what risks they will bear, as well as considerations on what role of cyberspace will be the as the fifth domain of conflict, alongside the domains of Land, Sea, Air and Space.

Dissertation word count: 36 826

Agradecimentos

Em primeiro lugar, deixo o meu agradecimento ao Instituto de Estudos Políticos da Universidade Católica Portuguesa, minha *alma mater*, por toda a formação académica, desde a Licenciatura até esta fase final do Mestrado, e por não se coibir de me conceder a oportunidade de investigar um tema novo no leque de dissertações do Instituto.

Deixo um agradecimento muito especial ao meu Orientador, General Luís Valença Pinto, por tão prontamente ter aceitado embarcar neste projeto e por ter sido tão atencioso durante todo o processo. Bem-haja.

Em terceiro lugar, agradeço à minha amiga e colega de licenciatura Francisca Casais, pelas sugestões bibliográficas dadas quando primeiro lhe falei do interesse pelo tema desta dissertação e, claro, pelos anos de amizade.

Agradeço, também, à minha amiga Francisca Maria, cuja ajuda foi indispensável para que não tivesse de esperar indefinidamente pela entrega de algumas das obras aqui citadas.

À Carolina Tavares, a minha profunda gratidão pelas conversas infindáveis, sobre todos os temas e mais alguns, mas, principalmente, por todas as palavras de apoio, de conforto e de encorajamento quando a falta de vontade, a incerteza ou as dúvidas se instalavam.

Por fim, aos meus pais, pelo amor, carinho e apoio incondicionais dados em tudo, desde sempre.

É graças a vós que esta dissertação existe.

Índice

Índice de Ilustrações

Gráficos:

Quadros:

Metodologia

Nesta dissertação, pretende-se investigar a interferência nas eleições presidenciais dos Estados Unidos para, a partir da mesma, se analisar a importância do ciberespaço enquanto domínio de conflito político e militar. Uma vez que partimos dum caso específico para fazer conclusões gerais, o método utilizado é o indutivo.

Para realizar esta investigação, estabeleceram-se três questões às quais se procurará responder:

1. Qual o interesse da Rússia na eleição de Donald Trump como Presidente dos Estados Unidos da América?
2. De que forma é que Rússia e Cambridge Analytica usaram as redes sociais para recolher dados dos utilizadores e disseminaram, nas mesmas redes, conteúdo direcionado a utilizadores específicos, com bases nesses dados, com o intuito de persuadir a sua intenção de voto?
3. Quão importante é (ou virá a ser) o ciberespaço nos palcos de conflito político e militar?

Para responder a estas questões, os métodos investigativos utilizados foram maioritariamente qualitativos, por serem também os mais disponíveis. A investigação deste trabalho baseou-se sobretudo na leitura de documentos fundamentais como o Relatório do Procurador Especial Robert Mueller, o dossier de Christopher Steele, e nos relatos de dois denunciantes do caso da Cambridge Analytica, contando ainda com o importante contributo da investigação feita por Kathleen Hall Jamieson acerca da interferência russa.

Os métodos quantitativos presentes nesta dissertação são apenas a análise da quantificação das perceções dos eleitores face aos candidatos no mês de outubro, contida no trabalho de Jamieson, na tentativa de demonstrar que houve de facto perceções alteradas no

mês de outubro de 2016, e que essa alteração teve um saldo positivo para Donald Trump e um negativo para Hillary Clinton.

Indicam-se, de seguida, as metodologias utilizadas em cada capítulo:

Capítulo	Metodologia utilizada
1. Ciberespaço: uma introdução	Métodos qualitativos: Análise textual/documental
2. Rússia	-
2.1. O fim da História (adiado) – explicação da doutrina Putin	Métodos qualitativos: Análise textual/documental
2.2. O interesse na eleição de Donald Trump	Métodos qualitativos: Análise textual/documental
2.3 *Sharp power* russo e a campanha de desinformação: intrusão, divulgação, conteúdo, redes sociais, anúncios, *bots*, comícios	Métodos qualitativos: Análise textual/documental
3. Cambridge Analytica	-
3.1. O que era a Cambridge Analytica?	Métodos qualitativos: Análise textual/documental
3.2. A estratégia da Cambridge Analytica	Métodos qualitativos: Análise textual/documental
3.2.1.Os cinco tipos de personalidade	Métodos qualitativos: Análise textual/documental
3.2.2.Recolha de dados pessoais no Facebook	Métodos qualitativos: Análise textual/documental
3.2.3.Transformação da informação em arma política e PSYOPs	Métodos qualitativos: Análise textual/documental
3.3. Ligação com a Rússia	Métodos qualitativos: Análise textual/documental
4. O impacto da interferência: realidade ou exagero?	Métodos qualitativos: Análise textual/documental Métodos quantitativos: Análise quantitativa de mudanças nas perceções do eleitorado face aos candidatos durante o mês de outubro de 2016
5. Lições aprendidas/ilações retiradas	Métodos qualitativos: Análise textual/documental
6. Ciberespaço, evolução tecnológica e o futuro do conflito	Métodos qualitativos: Análise textual/documental
7. Conclusão	-

Introdução

As eleições presidenciais dos Estados Unidos da América em 2016 ficariam para sempre envolvidas em polémica, mesmo antes do dia da votação.

Tanto quanto se sabe, esta terá sido a primeira vez na História em que a Rússia tentou interferir em eleições presidenciais americanas, tendo, para o efeito, recorrido a ataques informáticos para obter e-mails e informações sensíveis acerca do partido, campanha e candidata Democrata, Hillary Clinton, bem como a uma campanha de desinformação e de difamação para prejudicar Clinton face ao seu oponente, o nomeado Republicano, Donald J. Trump.

Essa campanha de desinformação foi disseminada através das redes sociais mais utilizadas pelo eleitorado americano, com o intuito de influenciar o seu sentido de voto. As tentativas de interferência por parte da Rússia foram primeiro denunciadas pelo Congresso dos Estados Unidos a 22 de setembro de 2016, tendo sido posteriormente confirmadas pelos serviços de informação a 7 de outubro desse ano. A 8 de novembro de 2016, dia da votação, Donald Trump emergia como o 45º Presidente dos Estados Unidos, derrotando Hillary Clinton, antiga Primeira Dama e antiga Secretária de Estado da administração Obama.

Às eleições de 2016 juntar-se-ia nova polémica em março de 2018, quando os jornais *The Guardian* e *The New York Times* publicaram simultaneamente artigos sobre o trabalho da firma Cambridge Analytica ao serviço da campanha Trump, sobre a sua recolha indevida de dados pessoais de utilizadores de Facebook, a utilização desses dados para traçar perfis psicográficos e, através deles, ajustar e direcionar conteúdos de campanha de acordo com os traços psicológicos dos utilizadores, tornando-os mais eficazes no seu propósito de influenciar o voto dos eleitores. Pelo menos, era isso que a Cambridge Analytica alegava ser capaz de fazer.

A novidade desta tentativa de interferir com o processo eleitoral não está nem no furto de informação nem na campanha de desinformação. Está, sim, na utilização da tecnologia digital, das redes sociais, e na instrumentalização do ciberespaço para a executar.

Cada vez mais, o ciberespaço torna-se um domínio incontornável da vida quotidiana. Muitos de nós servimo-nos dele todos os dias, para estudo, trabalho e lazer. Mas muitos outros servem-se também dele de maneiras perversas, para importunar outros, roubar informações sensíveis, ou tentar condicionar escolhas que deveriam ser feitas de modo livre e independente. E da mesma maneira que há conflito político e militar nos domínios da Terra, do Mar, do Ar e do Espaço, há também conflito político e militar no domínio do ciberespaço, o mais recente entre estes.

É por isso que pretendemos, nesta dissertação, usar a interferência eleitoral russa e as ações da Cambridge Analytica nas eleições de 2016 como um caso de estudo, para compreender como estas atuaram no ciberespaço, recorrendo a vírus informáticos, figuras fictícias, ataques cibernéticos, obtenção ilícita de informação e propagação de desinformação para influenciar o eleitorado americano, para depois tecermos considerações acerca do futuro do ciberespaço enquanto domínio de conflito, bem como o futuro das tecnologias digitais que mais diretamente se relacionam com o mesmo, e a relação dos mesmos com os mundos político e militar.

Para tal, abordaremos de forma introdutória o ciberespaço, passando depois para a questão da Rússia, onde investigaremos as razões de inimizade entre a Rússia e os Estados Unidos, por que motivo a Rússia de Putin estaria interessada na eleição de Donald Trump, seguindo para a estratégia utilizada na interferência e o modo como essa estratégia foi executada.

Depois, analisaremos as ações da Cambridge Analytica ao serviço da campanha Trump, a alegada utilização de perfis psicográficos para tornar mais eficazes os conteúdos de campanha e como isso se assemelha às operações psicológicas aplicadas em contexto militar, bem como a possibilidade de existirem ligações entre a Cambridge Analytica e a Rússia.

Uma vez que o impacto das ações da Rússia e da Cambridge Analytica é algo contestado, procuraremos, de seguida, mostrar que esse impacto é, no mínimo, plausível.

De seguida, passaremos às lições que retiramos dos esforços russos e das ações da Cambridge Analytica, avançando depois para considerações acerca do futuro da tecnologia, do ciberespaço, do conflito, e do ciberespaço enquanto domínio de conflito, após as quais chegaremos, finalmente, à conclusão deste trabalho.

1. Ciberespaço: uma introdução

a) Origem do termo

"Ciberespaço" é, como tantos outros, um termo para o qual há diversas definições. Comecemos então pela etimologia do termo e, depois, sigamos para como o termo tem sido definido e usado.

"Ciberespaço" tem a sua origem na palavra grega "*κυβερνήτης*" (*kubernētēs*), que pode ser traduzida para "dirigir", "guiar", "comandar", "governar"[1]. Porém, o uso moderno da palavra "ciber" chegou com Norbert Wiener, um matemático da II Guerra Mundial autor do livro "*Cybernetics: Or, Control and Communication in the Animal and the Machine*" (1948)[2]. Foi assim que o termo manteve a ligação à sua origem grega ("*control*" remetendo para "dirigir") e que passou também a implicar uma interação entre aquilo que é biológico e aquilo que é mecânico. O termo cairia em desuso rapidamente porque a tecnologia deste período ainda não era desenvolvida o suficiente para se falar em integração entre homem e máquina[3].

O termo "ciber" acabaria por ser recuperado, 36 anos mais tarde, pela ficção científica, no romance "*Neuromancer*" (1984) de William Gibson. Nesta obra, Gibson explorou as interações dos seres humanos dentro duma rede global, completada com Inteligência Artificial e *hackers*, ou seja, explorou um "ciberespaço". Gibson acabaria por definir o seu ciberespaço como "uma 'alucinação consensual', (…) um ambiente virtual no qual humanos interagem entre si e entre máquinas"[4].

[1] Vassilys Fourkas, "What is 'cyberspace'?", março de 2004, https://www.researchgate.net/publication/328928631_What_is_'cyberspace'.
[2] Damien Puyvelde e Aaron Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Cambridge: Polity, 2019), 25.
[3] Puyvelde e Brantly, *Cybersecurity*, 25.
[4] Puyvelde e Brantly, *Cybersecurity*, 26.

b) Definição de ciberespaço

Em 2009, Daniel Kuehl, professor na Universidade de Defesa Nacional dos Estados Unidos, definiu o ciberespaço como "um domínio operacional modelado pelo uso da eletrónica e do espetro eletromagnético para criar, armazenar, modificar, trocar, e explorar informação via sistemas de informação interconectados e respetivas estruturas associadas"[5].

Desconstruamos, primeiro, esta definição.

Kuehl introduz o conceito de eletrónica, uma classe de dispositivos físicos que dependem da eletricidade para funcionarem, desde simples resistências a avançados computadores. Depois introduz o espetro eletromagnético, uma variedade de frequências e radiações, comprimentos de onda e energias fotónicas. Este é um espetro que vai desde a Wi-Fi, às ondas rádio ou aos infravermelhos dum comando de televisão. Por último, evidencia que o ciberespaço não é somente o uso de equipamentos eletrónicos ou o espetro eletromagnético isolado, mas sim a capacidade para funcionarem em conjunto para criar, modificar, trocar e explorar informação. Além disso, não se trata unicamente dos atributos da informação (de criar, armazenar, modificar e trocar dentro dum sistema), mas sim da capacidade de a transmitir através dos sistemas conectados e das suas infraestruturas associadas que constituem o ciberespaço.

Já o Estado-Maior Conjunto dos Estados Unidos define o ciberespaço do seguinte modo:

"O ciberespaço consiste em muitas redes que frequentemente se sobrepõem, bem como nodos (qualquer dispositivo ou localização lógica com um protocolo de endereço de Internet ou outro identificador análogo) nessas redes e o sistema de dados que os suportam. O ciberespaço pode ser descrito em termos de três camadas: rede física, rede lógica e ciberpessoa. A camada da rede física do ciberespaço compraz-se dos componentes geográficos e dos componentes da rede física. São o meio por onde os dados viajam. A camada da rede lógica consiste nos elementos da rede que estão relacionados entre si duma forma abstraída da rede física, ou seja, tudo aquilo que não está ligado a um caminho individual específico ou nodo. Um exemplo simples é qualquer website que está hospedado em

[5] Daniel Kuehl, citado em *Cyberpower and National Security*, ed. Franklin Kramer, Stuart Starr e Larry Wentz (Washington, D.C.: National Defense University Press, 2009), 4.

servidores em múltiplas localizações físicas onde todo o conteúdo pode ser acedido através dum único localizador uniforme de recursos [Uniform Resource Locator/URL]. A camada da ciberpessoa representa um nível de abstração ainda mais elevado da rede lógica no ciberespaço; esta usa as regras que se aplicam na camada da rede lógica para desenvolver uma representação digital dum indivíduo ou identidade duma entidade no ciberespaço. A camada da ciberpessoa consiste nas pessoas que estão realmente na rede"[6].

Não havendo uma definição consensual ou unânime do ciberespaço, a definição dada por Kuehl é um ponto de partida para compreender que o ciberespaço é um espaço físico onde a informação é criada, armazenada, modificada e onde circula, através de dispositivos eletrónicos e do espetro eletromagnético. A definição do Estado-Maior Conjunto dos Estados Unidos, por sua vez, vem acrescentar a esta definição os conceitos da lógica e da pessoa humana que existe também no ciberespaço.

Estudiosos de áreas diferentes tendem a focar aspetos diferentes daquilo que é o ciberespaço quando tentam defini-lo, porque definir um termo de acordo com a área de estudo simplifica o trabalho. Enquanto os programadores tendem a focar-se mais na camada lógica, os engenheiros informáticos tendem a focar-se mais na camada física. Já quem é das ciências sociais e a maioria dos utilizadores comuns/consumidores tende a focar-se na camada da ciberpessoa.

Contudo, a realidade é que o ciberespaço não é mais duma camada do que é doutra. Os atributos físicos, lógicos e da ciberpessoa estão profundamente interligados e a forma como interagem entre si são a base do ciberespaço.

"O ciberespaço é um domínio físico e virtual. É o produto da criação e do engenho humano. É um domínio que, enquanto obra humana, ainda é impactado pelas suas interações com outros domínios, como a terra, o mar, o ar e o espaço"[7].

[6] Estado-Maior Conjunto dos Estados Unidos, "Cyberspace Operations", *Joint Publication* 3-12 (2018): 3-5.
[7] Puyvelde e Brantly, *Cybersecurity*, 28.

Adicionalmente, o ciberespaço tem-se tornado, cada vez mais, sobretudo desde o advento das redes sociais, um mediador das relações sociais. No ciberespaço:

"Barreiras geográficas são transpostas. Quase tudo é registável. Os limites da 'privacidade' são mais complexos. As interações sociais podem ser síncronas, assíncronas, ou algo no meio. Sob o anonimato parcial ou quase total, as pessoas podem ficar mais desinibidas do que o costume, ou podem experimentar identidades diferentes. Experiências sensoriais podem ser reduzidas a comunicação somente textual ou expandida para experiências de multimédia, com as imagens e sons de fantasia altamente criativa. (…)

Os novos meios de comunicação forneceram não só um novo veículo para as pessoas interagirem umas com as outras, mas introduziu também novos fatores psicológicos na fórmula. Por exemplo, a capacidade de os utilizadores escolherem livremente entre modalidades alternativas de comunicação síncronas e assíncronas, a combinação de comunicação baseada em texto e anonimato, não identificabilidade, e a falta de contacto visual, ou privacidade percebida, são componentes novas, desconhecidas e inexplicadas [que carecem de estudo]"[8].

c) A vulnerabilidade da camada da ciberpessoa

Sendo este um trabalho de ciências sociais, mais concretamente de Ciência Política e Relações Internacionais, também aqui nos debruçaremos mais sobre a camada da ciberpessoa. Neste trabalho, é esta que mais importa estudar para compreender de que modo Rússia e Cambridge Analytica (contratada por Steve Bannon, diretor executivo da campanha Trump) tentaram influenciar os eleitores norte-americanos nas Eleições Presidenciais de 2016 no domínio do ciberespaço.

As ciberpessoas não têm necessariamente de corresponder a pessoas individuais. Pode tratar-se de indivíduos, pode tratar-se de empresas, ou mesmo de *bots* (programas criados para simular comportamentos humanos online). Ou seja, as ciberpessoas podem ser efetivamente

[8] Azy Barak e John Suler, "Reflections on the Psychology and Social Science of Cyberspace" (2008): 4-6.

pessoas, híbridos (juntando pessoa e empresa) ou falsificações completas que emulam o comportamento humano.

Uma vez que ninguém tem de fazer corresponder a identidade pessoal à da sua ciberpessoa enquanto navegador no ciberespaço, é possível ocultar quem somos ou mesmo fazermo-nos passar por outros usando outro nome, outra fotografia, mascarando o endereço do Protocolo de Internet (ou IP), ou quaisquer outros mecanismos que nos permitam esconder a nossa verdadeira identidade ou localização.

Uma vez que os comportamentos no ciberespaço podem ficar dissociados de quem os tem, os seres humanos podem agir neste domínio de formas que não poderiam/quereriam nos domínios da terra, do mar, do ar ou do espaço.

Nesses outros domínios, os seres humanos continuam a poder forjar documentos ou a ocultar a sua identidade, mas o grau até onde podem alterar a sua natureza fundamental permanece restringido por limitações físicas, limitações essas que, no geral, não se encontram no ciberespaço.

A possibilidade de criar ciberpessoas falsas tem múltiplas aplicações, muitas das quais são inofensivas ou até mesmo benéficas. As personagens que se criam em jogos online, por exemplo, são apenas isso: personagens dum jogo. Nem toda a ciberpessoa falsa é um operacional russo a divulgar propaganda para tentar influenciar uma eleição.

A capacidade de manipular quem somos, o que somos e "onde estamos" no ciberespaço tem, naturalmente, um lado negro. O anonimato e a baixa probabilidade de atribuição de responsabilidades permitem e impelem os Estados a utilizar a espionagem e os ataques cibernéticos como meios para atingir os seus fins.

O ciberespaço é então um domínio onde também existe conflito, tal como nos outros domínios já referidos (Terra, Mar, Ar e Espaço). Contudo, apesar das características físicas que constituem o ciberespaço, o que se pode fazer nele insere-se mais no domínio virtual do que no físico.

"Muitos dos sistemas de armas usados nos domínios de guerra mais convencionais andam à volta de explosivos e projéteis concebidos para usar impacto ou força para causar dano. (…) À medida que os Estados começam a potenciar o ciberespaço para operações militares, que tipos de armas utilizarão? (…) A doutrina militar dos EUA, desde junho de 2018, refere-se à habilidade de potenciar meios cibernéticos como 'capacidade no ciberespaço'"[9].

A "capacidade no ciberespaço", pode, então, ser entendida como as "armas" utilizadas no ciberespaço. Estas costumam ter como alvo uma de três áreas nucleares associadas com a segurança de computadores e redes. Estas áreas nucleares são a confidencialidade, a integridade e a disponibilidade dos computadores, redes e os seus dados residentes ou em trânsito[10].

Quando o alvo é a confidencialidade dum dispositivo, procura-se violar a privacidade dos dados em trânsito na rede ou armazenados num computador. Quando o alvo é a integridade dos computadores, rede ou dados, o objetivo é violar o estado pretendido dos dados ou dos sistemas (operativos e de rede). Por último, quando se procura atacar a disponibilidade dos computadores, rede ou dados, o propósito é impedir o acesso a estes pelos utilizadores pretendidos. Todos os ciberataques, quer sob a forma de espionagem, sabotagem ou roubo, incidem sobre um ou mais destes três atributos.

Ao contrário da terra, do ar, do mar e do espaço, o ciberespaço constitui um substrato que facilita muitos dos sistemas de armas utilizados nestes domínios. Como já foi referido, o ciberespaço tem características físicas, mas é também um domínio virtual, com camadas de interação lógicas e pessoais. Um soldado, um espião ou um criminoso que pretenda atuar no ciberespaço para atingir os seus objetivos terá de pensar o ciberespaço de forma holística.

É comum que um ciberataque procure explorar uma camada do ciberespaço para ganhar a acesso a uma outra camada, como nos esquemas de "*phishing*". Um esquema de *phishing* consiste numa tentativa fraudulenta de obter os dados confidenciais de alguém, como nomes de

[9] Puyvelde e Brantly, *Cybersecurity*, 57.
[10] Puyvelde e Brantly, *Cybersecurity*, 57.

utilizador, palavras-passe e detalhes de cartão de crédito. Através de mensagens instantâneas ou e-mails falsos que procuram imitar entidades confiáveis, os utilizadores são levados a confirmar os seus dados num site também falso, mas idêntico ao verdadeiro, através do qual cedem, sem saber, os seus dados ao atacante. Neste caso, o alvo do ataque é a camada da ciberpessoa, induzida em erro para fornecer dados de acesso a informação sensível, possivelmente armazenada em servidores.

Voltando às "armas", o arsenal usado para ataques no ciberespaço consiste em software mal-intencionado. A este tipo de software dá-se o nome de malware. Existem diversos tipos de malware, que podem ser usados de forma independente ou combinada, consoante o efeito pretendido.

Importa ainda ressalvar que apesar das múltiplas capacidades de interferir com outros dispositivos remotamente, a empresa IBM estimou que "o erro humano era um fator contributivo em mais de 95% de todos os incidentes de segurança com computadores"[11].

Tanto quanto se sabe, a interferência russa nas eleições americanas por via do ciberespaço fez-se sobretudo através de spear-phishing[12] para ganhar acesso aos servidores e aos e-mails dentro da campanha e do Congresso Nacional Democrata e de *bots* que se faziam passar por alguém ligado ao partido Republicano, mas que não existia, que divulgavam informações falsas nas redes sociais, informações essas que depois eram partilhadas por perfis reais, desde apoiantes do partido sem cargos públicos a senadores.

[11] Puyvelde e Brantly, *Cybersecurity*, 61.
[12] Esquemas de phishing, como já vimos, são ataques em massa que têm como objetivo obter os dados de indivíduos ao acaso, não havendo seleção prévia ou conhecimento de quem se está a atacar. O *spear-phishing*, por outro lado, é direcionado a indivíduos específicos, cujos atacantes julgam detentores de informações sensíveis.

d) Algoritmos, aprendizagem automatizada e Inteligência Artificial

Para melhor compreendermos o que se passou no ciberespaço durante estas eleições, sobretudo na parte respeitante à Cambridge Analytica, da qual falaremos em detalhe mais à frente, temos ainda de compreender o que são algoritmos, aprendizagem automatizada (*machine learning*) e inteligência artificial.

Na matemática e na ciência de computadores, um algoritmo é um "conjunto de regras e operações bem definidas e não ambíguas, que, aplicadas a um conjunto de dados e num número finito de etapas, conduzem à solução de um problema"[13]. Uma ilustração simples para o que é um algoritmo é, por exemplo, uma receita de culinária, com os ingredientes e passos até se obter aquilo que se pretendia confecionar. Naturalmente, os algoritmos são, por norma, mais complexos do que isto, podendo repetir passos (iteração) ou até mesmo tomar decisões, com base na lógica ou comparação, de modo a completar a tarefa.

Por sua vez, a aprendizagem automatizada consiste na capacidade dos ditos algoritmos melhorarem através da experiência[14].

Partindo dum conjunto de dados e alguns parâmetros de distinção, como a cor e a forma, entre outros, o algoritmo vai ter meios para distinguir entre elementos diferentes. Isto é o treino do algoritmo. Depois, é necessário testar o algoritmo e o quão bem desempenhou a sua função. No início é normal que erre, e é necessário identificar esses erros para que o algoritmo não os volte a distinguir incorretamente. A isto chama-se *feedback*. Com esse feedback, será possível voltar a testar o algoritmo, que à partida terá menos erros no segundo teste, e no terceiro, e no quarto, e assim sucessivamente. Quando já não houver erros na distinção daquele conjunto de dados, pode-se testar o mesmo algoritmo com um conjunto de dados diferente, tornando-o cada vez mais eficiente.

[13] "algoritmo", in Dicionário Priberam da Língua Portuguesa, 2008-2020, https://dicionario.priberam.org/algoritmo (consultado a 29-06-2020).
[14] Tom Mitchell, *Machine Learning* (Nova Iorque: McGraw Hill, 1997), 1.

Exemplos comuns desta aprendizagem automática são o reconhecimento de imagens, desde padrões simples, à distinção entre animais ou entre plantas, à deteção de caras quando se está a tirar uma fotografia e aos álbuns automáticos que se geram nos telemóveis com fotos duma pessoa específica, sendo nós próprios ou amigos nossos; o reconhecimento de discurso para o passar automaticamente a escrito; ou a classificação de informação, como classificar uma pessoa num determinado perfil psicográfico depois de fazer um teste de personalidade na internet, tal como fez a Cambridge Analytica, que através dum desses testes e usando o modelo de categorização OCEAN (acrónimo nascido de: *Openness*, *Conscientiousness*, *Extraversion*, *Agreeableness*, e *Neuroticism/Negativity*), categorizou os utilizadores de acordo com os seus traços psicológicos predominantes no grupo correspondente, para mais tarde ajustar o conteúdo propagandístico às características psicológicas mais proeminentes e jogar com as emoções e discernimento dos eleitores. Explicar-se-á isto em detalhe no capítulo dedicado à Cambridge Analytica.

Por fim, temos a Inteligência Artificial, um termo muitas vezes usado alternadamente com o que se quer dizer por aprendizagem automatizada. A aprendizagem automatizada é uma subcategoria da Inteligência Artificial e, atualmente, o seu principal motor. Pode-se dizer que enquanto a aprendizagem automatizada é a capacidade dos algoritmos melhorarem através da experiência, Inteligência Artificial é a capacidade duma máquina mimetizar comportamento humano, como um assistente de voz no telemóvel (como a Siri da Apple, a Bixby da Samsung ou a Alexa da Amazon) responder corretamente a uma pergunta que se lhes faça, ou veículos autónomos, que não requerem um condutor.

Este primeiro capítulo foi necessariamente mais técnico para explicitar alguns conceitos que são imprescindíveis para compreender as ações empreendidas pela Rússia e Cambridge Analytica para influenciar o comportamento dos eleitores norte-americanos. No capítulo seguinte, debruçar-nos-emos sobre a questão da Rússia, evidenciando o que a levou a interferir e como interferiu no processo eleitoral americano em 2016.

2. Rússia

2.1. O fim da História (adiado) – explicação da doutrina Putin

É comum duvidar-se do fim de grandes potências enquanto estas vigoram, sobretudo quando se trata de grandes potências autoritárias, que assentam grande parte do seu controlo na manipulação de informação, tanto a nível de política interna como de externa. Tal era o caso da União Soviética. Estabelecida em 1922, seguindo os eventos da Revolução Russa de 1917, a União Soviética duraria 69 anos, durante os quais existiram mais certezas da sua duração do que esperanças da sua extinção. Mesmo durante a década de 80, já perto da queda do Muro de Berlim e do colapso da União Soviética, muitos ainda acreditavam na sua continuidade. Crê-se, aliás, que o colapso da URSS não surpreendeu só o Ocidente, mas até os próprios soviéticos, tal era a manipulação da informação.

Regressado duma viagem à URSS em 1984, o economista John Kenneth Galbraith disse que a economia soviética tinha tido "grande progresso material" e que as pessoas na rua "aparentavam um bem-estar sólido"[15]. O prémio Nobel da Economia de 1970, Paul Samuelson, acrescentaria na edição de 1989 (ano da queda do Muro) do seu livro "*Economics*" (recomendado em inúmeras universidades do Ocidente) que "ao contrário daquilo em que muitos céticos acreditaram anteriormente, a economia soviética é prova de que uma economia de comando socialista pode funcionar e até mesmo prosperar"[16].

Também a CIA falharia em prever o fim da URSS, apesar de vários documentos produzidos na década de 80 identificarem isoladamente traços do que conduziria a União Soviética ao seu colapso. Reunir informação de várias fontes em relação ao mesmo assunto era uma tarefa bem mais difícil do que é hoje (não havia motores de busca como os que temos agora, em que é possível pesquisar por temas e palavras chave e obter os resultados mais

[15] Milo Jones e Philippe Silberzahn, *Constructing Cassandra: Reframing Intelligence Failure at the CIA, 1947–2001*, (Stanford: Stanford University Press), 2013, 121.
[16] Jones e Silberzahn, *Constructing Cassandra*, 121.

relevantes em poucos segundos), pelo que, apesar da identificação dos traços de declínio em documentos dispersos, a análise global falhou.

Stansfield Turner, ex-diretor da CIA, em 1991, disse:

"Nunca ouvi uma sugestão da CIA, ou dos ramos de informação dos Departamentos de Defesa ou de Estado, de que vários soviéticos reconheciam um problema económico sistémico e crescente. Hoje ouvimos alguns revisionistas dizerem que afinal a CIA previu o iminente colapso soviético. Se alguns analistas da CIA estavam mais cientes disto do que outros na Agência, as suas ideias foram filtradas no processo burocrático; e visão da Direção é que conta porque é a que chega ao Presidente e aos seus conselheiros"[17].

Apesar da crença generalizada na continuidade da URSS, a chegada de Mikhael Gorbachev a Secretário-Geral da URSS em 1985 e as suas políticas de abertura económica (*perestroika*) e de alívio da repressão social (*glasnost*), ainda que não indicassem o fim da União Soviética, apontavam para o fim do regime comunista e autoritário que vigorara desde a Revolução Russa.

Estes acontecimentos levariam Francis Fukuyama a escrever o seu célebre artigo (e subsequente livro, com um pequeno acréscimo ao título) "O Fim da História?", publicado na revista *The National Interest* no verão de 1989, no qual expunha a ideia de que o duelo entre democracia liberal e comunismo terminara, com uma vitória inequívoca do liberalismo económico e político, vitória essa que "ocorreu primariamente no reino das ideias ou da consciência e está, por enquanto, incompleta no mundo real ou material"[18]. Essa vitória ganharia expressão material pouco tempo depois, com a queda do Muro de Berlim em novembro desse ano e dois anos mais tarde, com o colapso da União Soviética em 1991.

Com o fim da URSS houve, durante algum tempo, a crença de que os Estados que a formavam se tornariam mais liberais económica e politicamente. Havia, sobretudo, grandes

[17] Jones e Silberzahn, *Constructing Cassandra*, 127-128.
[18] Francis Fukuyama, "The End of History?", *The National Interest*, n.º 16 (Verão de 1989): 3.

expectativas de democratização e de liberalização política e económica para o maior Estado da extinta União: a Rússia. A nova Constituição aprovada em 1993 alimentava essa esperança. Postula o artigo 1.º que "A Federação da Rússia - a Rússia é um estado democrático, federativo, de direito, com forma republicana de governo"[19] e o artigo 8.º que postula que:

"1. Na Federação da Rússia é garantida a unidade do espaço económico, a livre circulação de mercadorias, serviços e meios financeiros, o fomento da concorrência e a liberdade da atividade económica.

2. Na Federação da Rússia são reconhecidas e protegidas de igual forma, a propriedade privada, estatal, municipal e outras"[20].

Contudo, a História ensina-nos que, quando um regime cai, a sua queda não é desejada por todos. Existem sempre os saudosistas, os que simpatizavam ou concordavam com o regime, os que beneficiavam dele, os que detinham poder, os que sentiam orgulho no poderio da nação na cena internacional, os que desejam um regresso ao *satus quo* anterior. Vladimir Putin, o atual Presidente russo, era, e é, uma das figuras que nunca desejou o fim da União Soviética.

Para compreendermos a interferência russa nas eleições, temos de compreender (ou, pelo menos, tentar) o que levou o Chefe de Estado russo a intervir no processo eleitoral americano.

Putin era um agente secreto dos quadros médios da carreira quando a União Soviética colapsou. Vladimir Putin ingressou nos Serviços Secretos russos (também designados Comité de Segurança do Estado ou KGB) em 1975, aos 23 anos. Porém, no ano em que Gorbachev chegou ao poder, Putin partiu para Dresden, na Alemanha Oriental, para chefiar o Departamento de Fronteiras. Apesar de Dresden estar sob o controlo soviético, Putin não assistira de perto à perestroika e à glasnost. Quando regressou à Rússia, o KGB já não existia, a União Soviética já não existia. Ainda houve tentativas de golpes de Estado para restabelecer a União, das quais Putin fez parte, mas todas sem sucesso. Putin acabaria por renunciar a uma nova patente e

[19] Art. 1.º, Constituição da Federação da Rússia, 1993.
[20] Art. 8.º, Constituição da Federação da Rússia, 1993.

emprego nos novos serviços secretos (o atual FSB) e em 1995 organizou o ramo de São Petersburgo do partido do governo chefiado por Viktor Chernomyrdin, o *Nash Dom*, partido que se identificava como liberal e do centro-Direita. Depois, seria gestor de campanha nas legislativas de 1996, assessor do Presidente russo Boris Yeltsin e à medida que foi subindo na carreira política pelo ramo da Presidência Administrativa da Rússia nos anos de 1997 e 1998, foi depois eleito Primeiro Ministro em 1999 e eleito Presidente em 2000, devido à renúncia de Boris Yeltsin por doença avançada. Era o início da Doutrina Putin.

Em 2005, num discurso do Estado da Nação ao parlamento russo, Putin classificou o fim da URSS como "a maior catástrofe política do século XX" e, desde que assumiu a Presidência em 2000, as políticas por si adotadas têm tido o objetivo de recuperar muito do que a Rússia perdeu aquando da dissolução da URSS em 1991. Contudo, a ambição de Putin não passa por restabelecer a União Soviética tal como esta era.

"Putin não está interessado numa restauração total: Putin não deseja ressuscitar o controlo completo da Economia pelo Estado nem recriar a União Soviética no espaço pós-soviético"[21].

Putin está interessado, sim, em recuperar muitas das mais-valias que conferiam à União Soviética a sua importância geopolítica e geostratégica, que lhe permitiram ombrear com os Estados Unidos durante a Guerra Fria.

Para recuperar essa importância, Putin entendeu que a política externa russa teria de cumprir três imperativos geostratégicos: (1) a Rússia teria de permanecer uma superpotência nuclear; (2) continuar uma grande potência em todos os aspetos da atividade internacional e (3) manter-se o líder político, militar e económico da sua região[22]. "Este consenso marca uma linha

[21] Leon Aron, "Putinology", *The American Interest*, 30 de julho de 2015, https://www.the-american-interest.com/2015/07/30/putinology/.
[22] Leon Aron, "The Putin Doctrine: Russia's Quest to Rebuild the Soviet State", *Foreign Affairs*, 8 de março de 2013, https://www.foreignaffairs.com/articles/russian-federation/2013-03-08/putin-doctrine.

da qual a Rússia não se pode retirar sem perder o seu orgulho ou mesmo a sua identidade nacional"[23].

A doutrina Putin é então o cumprimento destes imperativos. Para a doutrina ou os imperativos se cumprirem, Putin tem, gradualmente, a nível interno:

"… reocupado o que Lenine apelidara de alto comando da economia; estabelecido controlo firme dos processos políticos, do sistema de justiça, e da comunicação social para prevenir algum desafio significante ao regime (…)"[24].

A nível externo, os três imperativos geostratégicos supramencionados explicam o sentido que as políticas de Putin têm tomado.

A necessidade de se manter superpotência nuclear a par dos Estados Unidos tem guiado a política externa russa num duplo sentido, em que esta tanto se dispõe a negociar com Washington sobre redução de armamento, como se opõe a fortemente a qualquer iniciativa da NATO (como um sistema de defesa de mísseis na Europa) que, no entender russo, possa enfraquecer o seu estatuto enquanto superpotência nuclear.

A manutenção da Rússia como uma superpotência nuclear é fundamental porque permite cumprir o segundo imperativo. A Rússia não produz tecnologia nuclear exclusivamente para si – a Rússia exporta tecnologia nuclear para vários países na América Latina, Médio Oriente e Ásia, dentre os quais se podem contar China, Turquia, Índia, Bielorrússia, Bangladesh e Irão. A presença da Rússia em diversos pontos-chave da política internacional, alicerçada no mercado nuclear, tem-lhe garantido a sua continuidade como grande potência, concretizando os desígnios de Vladimir Putin.

O terceiro imperativo da Doutrina Putin – a hegemonia regional – tem guiado a política externa russa no sentido de "reintegrar política, económica, militar e culturalmente o antigo

[23] Aron, "The Putin Doctrine".
[24] Aron, "Putinology".

bloco soviético sob a liderança russa"[25]. Esta reintegração, que Putin identifica como o "coração da nossa política externa"[26] tem sido o principal motor das intervenções militares da Rússia noutros países, sobretudo quando estes se tentam aproximar do Ocidente. Reintegrar o antigo bloco soviético consiste num domínio semelhante ao que a URSS exerceu sobre a política externa da Finlândia durante a Guerra Fria: o pressuposto é o de que o Kremlin permite aos países pós-soviéticos vizinhos escolherem os seus próprios sistemas políticos e económicos, desde que tenha a última palavra nas decisões de segurança e política externa. Esta busca pela reafirmação da hegemonia regional russa foi precisamente o que levou a Rússia a intervir militarmente na Geórgia em 2008, ao constatar a sua aproximação ao Ocidente primeiro com a participação na Coligação liderada pelos Estados Unidos na Guerra do Iraque em 2003 e com a tentativa de entrada na NATO que começou em 2005; e na Ucrânia em 2006 e 2009 durante a presidência de Viktor Yushchenko e governo de Yulia Tymoshenko, que advogavam a adesão à União Europeia e eventualmente à NATO. Em 2014, suceder-se-ia a intervenção na Crimeia, que acabaria formalmente anexada à Federação Russa em 2015.

Durante o seu o tempo no poder, fosse como Presidente ou como Primeiro-Ministro, Putin tem logrado a implementação dum conservadorismo russo, baseado em 5 elementos: "nacionalismo emotivo; conservadorismo social intrusivo; recuperação da mitologia soviética legitimadora (maioritariamente acerca da Segunda Guerra Mundial e Estaline); a Igreja Ortodoxa Russa como árbitra e executora de costumes nacionais; e etnicidade russa como a espinha dorsal do Estado Russo"[27]. A este conservadorismo russo Putin tem aliado a retórica duma Rússia com uma "civilização única", com uma missão histórica, cujos valores são moralmente superiores aos ocidentais, e dum Ocidente que repetida e perpetuamente lhe é hostil[28].

[25] Aron, "The Putin Doctrine".
[26] Aron, "The Putin Doctrine".
[27] Aron, "Putinology".
[28] Aron, "Putinology".

"Numa linguagem assustadoramente similar à de Mussolini e de Hitler, a Rússia era imaginada como nunca estando errada, mas perenemente prejudicada pelas democracias ocidentais. O fim da Guerra Fria tornou-se para a Rússia o que Tratado de Versalhes foi para a Alemanha: uma fonte inesgotável de adversidades e humilhação. Elevando a retórica a níveis da Segunda Guerra Mundial, Putin insiste que a terra-mãe está sob cerco e própria soberania da Rússia em perigo. (…) Nestes corolários geostratégicos, incluem-se as retificações destas injustiças históricas através da 'reunião das terras russas' e da criação do 'Mundo Russo'. Inclui-se também a recuperação do estatuto da ex-União Soviética como o outro polo no atual mundo unipolar – controlado pelos Estados Unidos. A Rússia não deve ser apenas uma superpotência eurasiática, mas sim o único contrapeso mundial à alegada supremacia do Ocidente liderada pelos EUA"[29].

A oposição de Putin ao Ocidente e aos EUA é ainda explicada pelo seu desprezo publicamente conhecido por Gorbachev e pelas suas políticas de abertura e aproximação ao Ocidente. Na ótica de Putin, Gorbachev e as suas medidas aceleraram exponencialmente o que considera a grande catástrofe do século passado, o fim da União Soviética[30], cuja essência Putin tanto tenta recuperar. Na doutrina de Putin, seguir modelos ou valores ocidentais é, em última análise, enfraquecer a Rússia, que é precisamente o oposto do que Vladimir Putin pretende.

[29] Aron, "Putinology".
[30] Aron, "Putinology".

2.2. O interesse na eleição de Donald Trump

No subcapítulo anterior tentou-se evidenciar que o grande desígnio de Putin é devolver à Rússia o estatuto da antiga União Soviética enquanto contrapeso do mundo ocidental liderado pelos Estados Unidos, ou seja, regressar a uma ordem mundial de equilíbrio bipolar, como a que vigorou durante a Guerra Fria. Mas um equilíbrio bipolar coloca duas superpotências em competição porque uma quer sempre derrotar a outra, buscando sempre o seu momento unipolar[31]. Em 1991, o colapso da URSS determinou a vitória dos EUA e do bloco ocidental. Agora, Putin busca uma nova competição, para lograr o resultado que o bloco soviético não conseguiu no século passado. Para obter esse resultado, interessava a Putin a eleição de Donald Trump em vez da de Hillary Clinton. Procuraremos aqui explicar porquê.

Durante o período da Guerra Fria, o KGB controlava todos os estrangeiros que entrassem na União Soviética (especialmente os americanos)[32] através da *Intourist*, a agência de viagens estatal soviética[33] por três motivos: o primeiro era conseguir identificar e monitorizar agentes secretos/espiões que procurassem informações sobre a URSS; o segundo era recrutar estrangeiros para trabalharem para o KGB levantando menos suspeitas e o terceiro era obter informações comprometedoras sobre figuras influentes de outros países para, nos momentos oportunos, as poder difamar, chantagear ou extorquir, o tipo de informação a que os russos chamam *kompromat*. O KGB tinha particular interesse em "pessoas jovens e ambiciosas … gente com futuro. (…) O objetivo é apenas um. Recolher informação e manter essa informação sobre ele[s] para o futuro"[34]. Naturalmente, milionários, congressistas e senadores (ou candidatos a esses cargos e ao de Presidente) eram alvos de eleição para o KGB.

[31] Dana-Marie Seepersad, "The politics of bipolarity and IPE in contemporary times", *E- International Relations*, 17 de fevereiro de 2011, https://www.e-ir.info/2011/02/17/the-politics-of-bipolarity-and-ipe-in-contemporary-times/.
[32] Luke Harding, *Collusion: How Russia Helped Trump Win the White House* (Londres: Guardian Faber, 2017), 16.
[33] Harding, *Collusion*, 221.
[34] Harding, *Collusion*, 221.

Donald Trump viajou até Moscovo pela primeira vez em julho de 1987[35]. Porém, é possível que a Rússia tenha registos sobre Trump desde 1977, o ano de casamento de Trump com a sua primeira mulher, Ivana Zelnickova (hoje conhecida como Ivana Trump), oriunda da antiga Checoslováquia, que não pertencia à URRS, mas era de regime comunista[36]. Todavia, em relação à primeira viagem de Trump a Moscovo pouco se registou. O momento que terá realmente posto os olhos do KGB em Donald Trump terá sido alguns meses depois da sua visita, quando surgiu no *The New York Times* de 2 de setembro desse ano a notícia de que "Trump dá vaga sugestão de candidatura". No corpo da notícia, lia-se:

> "Donald J. Trump, um dos maiores e mais vocais promotores de Nova Iorque, disse ontem que não estava interessado em concorrer para cargos públicos em Nova Iorque, mas indicou que a Presidência era um assunto à parte. Trump, um republicano, comprou anúncios de página inteira em três dos maiores jornais do país para divulgar as suas visões sobre política externa. E um assessor revelou que Trump planeia uma viagem em outubro a New Hampshire, local da primeira [eleição] primária presidencial"[37].

Disto, nada resultaria a nível político durante vários anos. Trump voltaria a Moscovo posteriormente em mais do que uma ocasião em busca de oportunidades de negócio imobiliário, mas que nunca se concretizaram. Trump convivia com personalidades da política americana frequentemente, mas envolvia-se pouco com a política em si. Ainda assim, o KGB e o pós-soviético FSB continuaram a sua prática da busca de *kompromat* sobre figuras públicas estrangeiras, o que acabaria, alegadamente, por jogar a seu favor em 2016.

O dossier de Christopher Steele, um ex-agente do britânico MI6, acerca da ligação de Trump com a Rússia foi divulgado ao público na íntegra pelo site *Buzzfeed* a 10 de janeiro de 2017, dez dias antes da sua tomada de posse como 45.º Presidente dos Estados Unidos da América.

---

[35] Harding, *Collusion*, 222.
[36] Harding, *Collusion*, 216.
[37] Harding, *Collusion*, 224.

O dossier de Steele afirma que:

"– O regime russo tem cultivado, apoiado e assistido TRUMP durante pelo menos os últimos 5 anos [desde 2011]. O objetivo, endorsado por PUTIN, tem sido encorajar divisões na aliança ocidental (…)

– Um antigo oficial de informação de topo afirma que o FSB comprometeu TRUMP através das suas atividades em Moscovo o suficiente para o poder chantagear. De acordo com diversas fontes fidedignas, a sua conduta em Moscovo inclui atos sexuais perversos preparados e monitorizados pelo FSB

– Um dossier de material comprometedor sobre Hillary CLINTON tem sido compilado pelos Serviços de Informação Russos ao longo de vários anos e compraz-se principalmente de escutas telefónicas de conversações tidas em várias visitas à Rússia e chamadas telefónicas intercetadas ao invés de qualquer conduta embaraçosa. O dossier é controlado pelo porta-voz do Kremlin, PESKOV, sob ordens diretas de PUTIN. Contudo, [o dossier] ainda não foi distribuído no estrangeiro, nem mesmo a TRUMP. Intenções russas para a sua divulgação ainda desconhecidas"[38].

A estratégia de obter *kompromat* sobre todos os visitantes por parte dos Serviços Secretos russos parece compensar. Em 2016, chegou-se ao ponto em que a Rússia detinha material comprometedor sobre dois candidatos presidenciais americanos para usar como entendesse. Se o objetivo para o *kompromat* acerca de Donald Trump era chantageá-lo enquanto Presidente dos Estados Unidos em benefício da Rússia, o objetivo do *kompromat* obtido sobre Hillary era denegrir a sua imagem para prejudicar as suas chances de ser eleita Presidente. Parece redundante, mas Putin não quereria apenas eleger Trump. Putin quereria, a todo o custo, evitar uma Presidência de Hillary Clinton. Veremos agora porquê.

Quando Putin chegou ao poder, tanto como Primeiro-Ministro em 1999 ou como Presidente em 2000, já sabia quem era Hillary Clinton. Hillary fora a Primeira Dama dos Estados Unidos durante a administração do seu marido Bill Clinton, de 1993 a 2001. Em 1993,

[38] Christopher Steele, "US Presidential Election: Republican Candidate Donald Trump's Activities in Russia and Compromising Relationship with the Kremlin", Fusion GPS, Company Intelligence Report 2016/080, dezembro de 2016, https://assets.documentcloud.org/documents/3259984/Trump-Intelligence-Allegations.pdf.

no seguimento do fim da URSS, esperava-se uma reviravolta nas relações entre EUA e Rússia, que parecia estar a concretizar-se nos primeiros anos, mas que azedaram rapidamente.

Os desentendimentos começaram a surgir logo em 1995. Enquanto os EUA se opunham à agressão russa na Chechénia e à venda de material nuclear ao Irão, a Rússia opunha-se às intervenções dos países ocidentais na Bósnia e à expansão da NATO a países do leste europeu. Estes desentendimentos manter-se-iam até ao final da administração Clinton em 2001, com a qual o primeiro governo de Putin e a sua primeira presidência ainda coincidiriam.

Putin reencontrou Hillary Clinton no primeiro mandato de Obama, sendo Putin, na altura, Primeiro Ministro da Rússia. Foi como que um interregno da Presidência para Putin, dado que já tinha cumprido dois mandatos presidenciais consecutivos, pelo que teria de aguardar a conclusão dum mandato exercido por outrem até se poder recandidatar à Presidência.

Barack Obama convidou Hillary para ser sua Secretária de Estado na nova administração depois de ter vencido as Primárias Democratas e as Presidenciais em 2008.

Também a administração Obama pretendia um recomeço para as relações entre os dois países.

> "… em 2009, Obama chegou à Presidência determinado em restabelecer as relações com a Rússia. A ideia principal … é deixar para trás todos os desentendimentos anteriores, erradicar a mentalidade da Guerra Fria, e restabelecer uma nova relação amigável mútua"[39].

Entre 2009 e 2011, a administração Obama reclamou vários sucessos na cooperação com a Rússia a nível económico, social e da segurança internacional, mas a relação russo-americana deteriorar-se-ia novamente. Quando Obama iniciou o seu segundo mandato, as relações entre EUA e Rússia estavam tensas uma vez mais. Desentendimentos acerca da posição de cada Estado nas questões da Líbia, Síria, Geórgia e, sobretudo, da Ucrânia, foram-se acumulando

[39] Maria Ezzeldin, "US-Russia Relations after the Crisis in Ukraine" (diss. Mestrado, Universidade Americana do Cairo, 2015), 28.

durante o primeiro mandato, comprometendo o segundo. A anexação da Crimeia terá sido a última gota para os EUA da administração Obama, que juntamente com a União Europeia, Canadá, Noruega e Austrália rapidamente aplicaram sanções económicas que em meados de 2016 já tinham custado à Rússia cerca de 170 mil milhões de dólares, acrescendo cerca de 400 mil milhões perdidos nas receitas de petróleo e gás natural[40].

Enquanto Secretária de Estado, Hillary Clinton criticara Putin abertamente. No seguimento das eleições legislativas russas de 2011, que receberam várias críticas de observadores internacionais, sobretudo da UE e dos EUA, e geraram protestos em Moscovo e São Petersburgo, Hillary falou em defesa dos protestantes:

"O povo russo, tal como os povos de todo o lado, merecem o direito de terem as suas vozes ouvidas e os seus votos contados. Isso significa que merecem eleições livres, justas e transparentes e líderes responsáveis perante as mesmas"[41].

Putin, por sua vez, fez acusações a Hillary e ao Departamento de Estado de terem fomentado os protestos da oposição:

"Ela [Hillary] deu o tom a certos atores dentro do país, ela deu o sinal. (…) Eles [protestantes] ouviram este sinal e, com o apoio do Departamento de Estado dos Estados Unidos, começaram ativamente a fazer o seu trabalho"[42].

No entanto, esta não foi a primeira vez que Putin ficou furioso com Hillary Clinton. Na primavera de 2011, os EUA tinham começado a pressionar a ONU para permitir uma intervenção da NATO na Líbia para impedir o regime de Muaamar Kadafi de massacrar as forças rebeldes e os seus apoiantes civis. A resolução não poderia passar no Conselho de

[40] Trude Pettersen, "Russia loses $600 billion on sanctions and low oil prices", *The Barents Observer*, 5 de fevereiro de 2016, https://thebarentsobserver.com/ru/node/414.
[41] Simon Shuster, "Vladimir Putin's Bad Blood with Hillary Clinton", *Time*, 25 de julho de 2016, https://time.com/4422723/putin-russia-hillary-clinton/.
[42] Shuster, "Vladimir Putin's Bad Blood with Hillary Clinton".

Segurança da ONU se a Rússia a tivesse vetado, mas na altura o Presidente era Dmitri Medvedev, não Putin. A pressão americana sobre Medvedev funcionou e a Rússia permitiu a aprovação da resolução, que acabaria por resultar na queda do regime líbio e do seu líder Kadafi[43].

A tensão entre os dois países manteve-se desse ano em diante. Putin foi adotando várias medidas anti-Estados Unidos, como expulsar a USAID[44], remover a transmissão de rádio da Radio Liberty e perseguir o embaixador americano na Rússia, Michael McFaul. Depois, face às sanções a oficiais russos aprovadas pelo Congresso americano na sequência da morte do delator Sergei Magnitsky, Putin retaliou proibindo a adoção de crianças russas por casais americanos[45].

Hillary acabaria por abandonar o cargo em 2013 por motivos de saúde, sendo substituída pelo Senador John Kerry, que acompanharia Barack Obama até ao fim do mandato. Quando questionado acerca do desempenho de Hillary, Putin recordou a presidência de Bill Clinton e das suas tentativas falhadas de conduzir a Rússia a políticas mais ocidentais, respondendo que "como dizemos por cá, 'marido e mulher são o mesmo Satanás'"[46].

Ao deixar o Departamento de Estado, Hillary aconselhou Obama a ser mais duro com Moscovo. Na ótica de Hillary Clinton, Putin não era merecedor de confiança e deveria ser combatido pela força[47]. Quando ressurgiu na cena política para ser a candidata presidencial Democrata, o discurso de dureza contra a Rússia manteve-se. Quando durante as Primárias Democratas Hillary propôs uma zona de exclusão aérea na Síria, o Kremlin via nesta proposta que a candidata estava pronta para começar uma guerra com a Rússia[48].

---

[43] Shuster, "Vladimir Putin's Bad Blood with Hillary Clinton".
[44] Agência dos Estados Unidos para o Desenvolvimento Internacional
[45] Will Englund, "The roots of the hostility between Putin and Clinton", *The Washington Post*, 28 de julho de 2016, https://www.washingtonpost.com/world/europe/the-roots-of-the-hostility-between-putin-and-clinton/2016/07/28/85ca74ca-5402-11e6-b652-315ae5d4d4dd_story.html.
[46] Englund, "The roots of the hostility".
[47] Molly O'Toole, "From Reset to Realpolitik, Clinton's New Hard Line on Moscow", *Foreign Policy*, 22 de setembro de 2016, https://foreignpolicy.com/2016/09/22/hillary-clintons-new-colder-cold-war-russia-putin-election/.
[48] O'Toole, "From Reset to Realpolitik".

Do outro lado, estava Donald Trump como candidato Republicano. Para além do *kompromat* que o Kremlin já detinha sobre o candidato, Trump praticamente não revelava hostilidade em relação à Rússia de Putin durante a campanha, antes pelo contrário.

"Em contraste com Clinton, os anos de experiência com a Rússia de Trump consistem largamente num concurso Miss Universo em Moscovo, uma séria admiração pelas táticas autoritárias de Putin, e ligações obscuras amigos do Kremlin (…).

[Trump:] 'A Rússia quer derrotar o ISIS tanto quanto nós (…). Não seria maravilhoso se pudéssemos trabalhar nisso juntos e derrotar o ISIS? Não seria uma coisa maravilhosa?'"[49].

O facto de Trump ter pedido publicamente à Rússia para encontrar os 30 mil e-mails do servidor privado de Hillary Clinton, bem como as declarações de que analisaria os contributos financeiros para a NATO dum aliado antes de decidir defendê-lo contra um ataque russo demonstravam não só a ausência de hostilidade, como também servia o desígnio russo de "encorajar divisões na aliança ocidental"[50].

Os dois candidatos presidenciais eram diametralmente opostos. Dum lado tínhamos alguém com uma ampla experiência política a nível interno e externo, que em múltiplas ocasiões já tinha antagonizado as pretensões do Kremlin e que prometia uma Presidência com uma política externa de forte oposição à Rússia; do outro tínhamos alguém que o Kremlin considerava poder manipular, que não lhe era hostil, que possivelmente levantaria as sanções, e que ainda colocava em causa o artigo 5.º do Tratado do Atlântico-Norte, a pedra angular da defesa coletiva. A escolha russa entre estes é óbvia. Porém, se o candidato republicano fosse outro que não Trump, sobre o qual não tivesse *kompromat*, e mesmo que se mostrasse mais duro quanto à Rússia, é muito possível que o Kremlin tivesse concretizado esforços semelhantes para evitar a presidência de Hillary Clinton.

[49] O'Toole, "From Reset to Realpolitik".
[50] Steele, "US Presidential Election".

Conhecidos os candidatos republicano e democrata, a escolha da Rússia tornou-se clara. Com o objetivo de eleger Donald Trump e evitar uma presidência de Hillary Clinton, rapidamente os objetivos da campanha Trump se tornaram os mesmos objetivos do Kremlin. Kremlin e campanha Trump procuraram ganhar o apoio de todas as franjas da direita americana e encorajar a ida às urnas da sua massa apoiante e, simultaneamente, procuraram convencer partes do eleitorado tradicionalmente democrata, como os eleitores negros e latinos, a não comparecer nas mesas de voto como compareceram nas eleições em que Obama tinha sido candidato, ou a não votar na Democrata nomeada se nas Primárias tinham apoiado qualquer outro candidato Democrata.

Procuraremos, agora, evidenciar qual foi o modo de atuação da Rússia.

2.3. *Sharp power* russo e a campanha de desinformação: intrusão, divulgação, conteúdo, redes sociais, anúncios, *bots*, comícios

A interferência russa nas eleições presidenciais de 2016 foi denunciada no Congresso americano pela primeira vez a 22 de setembro desse ano. Foi depois confirmada pelas agências de informação americanas a 7 de outubro, com detalhes sendo acrescentados pelo gabinete do Diretor Nacional de Informação em janeiro de 2017. A investigação do FBI à interferência foi encabeçada pelo Procurador Especial Robert Mueller em maio de 2017 e o relatório da investigação foi tornado público em abril de 2019. O relatório concluiu que:

"O governo russo interferiu na eleição presidencial de 2016 de forma abrangente e sistemática.

(…) A Rússia interferiu (…) principalmente através de duas operações. Primeiro, uma entidade russa executou uma campanha nas redes sociais que favoreceu o candidato presidencial Donald J. Trump e denigriu a candidata presidencial Hillary Clinton. Segundo, um serviço de informação russo conduziu operações de intrusão de computadores contra entidades, empregados e voluntários trabalhando na campanha Clinton e depois vazando documentos roubados.

(…) A Agência de Pesquisas de Internet [Internet Research Agency/IRA] executou as primeiras operações de interferência russa identificadas pela investigação – uma campanha nas redes sociais planeada para provocar e amplificar discórdia política e social nos Estados Unidos.

(…) A IRA mais tarde usou contas de redes sociais e grupos de interesses para semear discórdia no sistema político dos Estados Unidos através do que chamou 'guerra de informação'. A campanha evoluiu dum programa generalizado em 2014 e 2015 para fragilizar o sistema eleitoral dos Estados Unidos, para uma operação direcionada (…). A operação da IRA também incluiu a compra de anúncios políticos nas redes sociais em nome de pessoas e entidades dos Estados Unidos, bem como encenações de comícios políticos dentro dos Estados Unidos. Para organizar esses comícios, empregados da IRA fizeram-se passar por entidades e pessoas baseadas nos Estados Unidos e estabeleceram contacto com apoiantes e oficiais da campanha de Trump nos Estados Unidos.

(…) O serviço de informação russo conhecido como Departamento Central de Inteligência do Estado-Maior das Forças Armadas da Rússia (GRU) executou estas operações [de *hacking*]. (…) O GRU roubou e-mails de voluntários e empregados da campanha Clinton, incluindo o diretor de campanha John Podesta. (…) O GRU entrou nas redes de computadores do Comité de Campanha Congressional Democrata (DCCC) e do Comité Nacional Democrata (DNC). O GRU roubou dezenas de documentos … e quando o DNC anunciou o papel do GRU na intrusão na sua rede, o GRU começou

a disseminar os materiais roubados através das personas online fictícias 'DCLeaks' e 'Guccifer 2.0'. O GRU mais tarde vazou materiais adicionais através da organização WikiLeaks"[51].

A utilização deste tipo de táticas por parte da Rússia condiz também com o exercício de "*sharp power*", um termo recente nas Relações Internacionais, cunhado apenas em 2017, por Christopher Walker e Jessica Ludwig. "*Sharp power*" difere dos clássicos "*soft power*" e "*hard power*" na medida em que não se baseia na atratividade das políticas dum país, da sua cultura ou dos seus ideais políticos (*soft power*) nem na coerção através do poderio militar ou económico (*hard power*). O exercício de *sharp power* verifica-se, sobretudo, em estados autocráticos e consiste, principalmente, na manipulação de informação e na projeção de poder no estrangeiro de forma furtiva, passando frequentemente pela interferência em processos eleitorais de países democráticos.

"Os esforços de influência autoritária são 'afiados' [*sharp*] no sentido em que furam, penetram ou perfuram os ambientes político e informativo nos países alvo. Na nova implacável competição entre estados autocráticos e democráticos, as técnicas de '*sharp power*' dos regimes repressivos devem ser vistas como a ponta da adaga. Estes regimes não estão necessariamente a procurar ganhar 'mentes e corações', a referência comum do *soft power*, mas estão garantidamente a procurar manipular os seus públicos-alvo distorcendo a informação que chega até eles.

Sharp power permite aos [estados] autoritários entrar no tecido da sociedade, acicatando e amplificando divisões existentes. A Rússia tem sido particularmente habilidosa ao explorar falhas dentro de democracias (…). E ao contrário do impacto contundente do *hard power*, o *sharp power* envolve um grau de furtividade. Aproveitando-se do ambiente político e informativo aberto das democracias, os esforços de *sharp power* dos autoritários são tipicamente difíceis de detetar, o que significa que podem beneficiar de alguma latência até que as democracias se apercebam de que existe um problema"[52].

[51] Robert Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election", Departamento de Justiça dos Estados Unidos, março de 2019, 1-4.
[52] Christopher Walker e Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence" *Foreign Affairs*, 16 de novembro de 2017, https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.

a) Intrusão

Comecemos então por verificar como é que a Rússia ganhou acesso aos computadores da campanha de Hillary e outros órgãos do partido Democrata.

O GRU encarregou duas unidades militares – Unidade 26165 e Unidade 74455 – de executarem as intrusões nos computadores da campanha, do DNC e do DCCC. A Unidade 26165 foi a principal responsável pelo roubo de e-mails e material confidencial destas entidades. Já a Unidade 74455 deu assistência à primeira no vazamento dos documentos roubados, promovendo-o, e foi a principal responsável pela publicação de conteúdo difamatório para Hillary Clinton nas redes sociais. Adicionalmente, esta unidade ainda entrou furtivamente em computadores de comissões eleitorais, secretários de Estado e de empresas que forneceram software e outras tecnologias relacionadas com a administração do processo eleitoral[53].

O GRU utilizou primeiro *sites* como democrats.org, hillaryclinton.com, dnc.com e dccc.org para obter informações acerca dos empregados e voluntários democratas. Depois, o GRU enviou centenas de e-mails de *spearphishing* para os endereços de e-mail de trabalho e pessoais desses empregados e voluntários. A estratégia de *spearphishing* foi bem-sucedida por dois motivos. Não só deu ao GRU acesso a dezenas de milhares de e-mails, incluindo os de altas figuras da campanha, como o diretor John Podesta e assessores de campanha informais, como lhe deu acesso à rede de computadores. Podendo circular pela rede, o GRU foi roubando credenciais de acesso até chegar aos administradores informáticos, com acesso irrestrito a todo o sistema. Aqui chegado, o GRU pôde implantar dois tipos de malware – o "X-Agent" e o "X-Tunnel" – e o Mimikatz, uma ferramenta que serve para recolher credenciais. O "X-Agent" era um vírus multifunctional, que permitia registar cada tecla premida, tirar capturas de ecrã e recolher outros dados dos computadores infetados. O "X-Tunnel", por sua vez, era o que criava a ligação encriptada entre os computadores infetados e os computadores do GRU fora da rede

[53] Mueller, "Report On The Investigation Into Russian Interference", 36-37.

dos órgãos democráticos, com capacidade para transferir dados em grande escala, capacidade que o GRU depois usou para extrair dados dos computadores infetados[54].

b) Divulgação

Para publicar as informações roubadas, o GRU registou o domínio dcleaks.com através dum serviço que anonimizava o registador. A página inicial apontava para diferentes tranches de documentos roubados, organizados por "vítima" ou assunto. Outras páginas do dcleaks.com continham índices dos e-mails roubados que estavam a ser divulgados, contendo remetente, destinatário e data do e-mail. Para controlar os tempos das divulgações, havia ainda páginas temporariamente protegidas por palavras-passe, que eram depois desbloqueadas para acesso do público.

O GRU publicou milhares de documentos, incluindo dados de identificação pessoal e informação financeira, correspondência interna relacionada com a campanha Clinton e empregos políticos anteriores. O GRU criou ainda uma página de Facebook da DCLeaks, uma conta de Twitter e uma conta GMail para comunicar privadamente com repórteres e outras personalidades americanas.

Usando a persona DCLeaks, o GRU deu a vários repórteres acesso antecipado a arquivos e documentos vazados através de links e passwords para as páginas que ainda não eram públicas. O site dcleaks.com esteve operacional até março de 2017[55].

O GRU criou ainda uma outra persona – Guccifer 2.0 – como se fosse um *hacker* que agia por conta própria, para a qual foi criado um blog no WordPress, no qual foram publicados milhares de documentos roubados do DNC e do DCCC entre junho e outubro de 2016. Estes

[54] Mueller, "Report On The Investigation Into Russian Interference", 38.
[55] Mueller, "Report On The Investigation Into Russian Interference", 42.

documentos incluíam investigação à oposição (incluindo um memorando sobre potenciais críticas a Trump), documentos de medidas internas (como recomendações de como abordar temas políticos sensíveis) e de angariações de fundos.

Os documentos obtidos pelas unidades do GRU não foram logo publicados todos duma vez por razões estratégicas: primeiro, porque tornar públicos os documentos roubados teria mais impacto em momentos-chave da corrida eleitoral, como pela altura dos debates presidenciais ou nos dias próximos da votação, e, segundo, porque poderiam servir para contra-atacar o que pudesse danificar a imagem de Donald Trump.

Um bom exemplo do segundo caso foi o que aconteceu no dia 7 de outubro de 2016, dois dias antes do segundo debate presidencial entre Clinton e Trump.

Pelas 15:00 horas, foi feita uma declaração conjunta pelo Departamento de Segurança Interna dos EUA e pelo gabinete do Diretor de Informação Nacional que anunciava que o governo russo tinha ordenado as operações que comprometeram os e-mails de personalidades e instituições americanas, acrescentando que o modo divulgação dos e-mails nas plataformas DCLeaks, WikiLeaks e pela persona Guccifer 2.0 era "consistente com os métodos e motivações dos esforços ordenados pela Rússia"[56].

Cerca de uma hora depois, o Washington Post publicou a história e o vídeo conhecido como "Access Hollywood tape" em que se ouvia Donald Trump gabar-se de beijar mulheres sem o seu consentimento e de que, graças ao seu estatuto mediático, podia fazer o que quisesse, incluindo a infame frase de "agarrá-las pela c***".

Passada mais meia hora, foram divulgados os primeiros e-mails do diretor de campanha de Hillary Clinton, John Podesta, via WikiLeaks.

As contas controladas por operacionais russos começaram a trabalhar ativamente para desviar as atenções do vídeo com a voz de Trump, sobretudo no Twitter, partilhando e

[56] "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security", Departamento de Segurança Interna dos Estados Unidos, 7 de outubro de 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

partilhando o que era difamatório para Hillary, enquanto Donald Trump menosprezava o vídeo e classificava as suas declarações como "conversa de balneário", em que alguém se gaba de coisas que na realidade nunca fez[57].

As divulgações continuariam a ser feitas até ao final da corrida presidencial, sempre procurando denegrir Clinton face ao eleitorado americano.

c) Conteúdo da campanha de desinformação

Para maior eficácia na propagação das suas mensagens, a Rússia explorou vulnerabilidades do sistema americano, como a liberdade de expressão e de imprensa e a falta regulação em novas tecnologias da comunicação, bem como as capacidades das plataformas digitais para ocultar a identidade, recolher dados pessoais, de partilha fácil de conteúdo e de publicidade direcionada[58], bem como dos algoritmos que apresentam conteúdo semelhante àquele com que mais se interage, "desenvolvidos para ganhar e suster atenção"[59].

A campanha de Donald Trump e os intervenientes russos seguiram a mesma estratégia para influenciar os votos dos eleitores americanos. Apresentaram sempre a eleição presidencial como um jogo de soma-zero, numa lógica de "nós-versus-eles", de modo a ilustrar os Democratas, no geral, e Hillary, em particular, como inimigos da população[60]. Se Clinton ganhasse, o "nós" americano (cristãos, pró-vida, veteranos, polícia, cidadãos que se consideravam esquecidos pelo poder político) ficaria a perder e "eles" (imigrantes, refugiados, pessoas de cor) ficariam a ganhar. Apresentar a escolha eleitoral nestes moldes permitia usar os medos e receios da população como impulsionadores para votar em Donald Trump. A

[57] Kathleen Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President – What We Don't, Can't, And Do Know* (Oxford: Oxford University Press, 2018), 155.
[58] Jamieson, *Cyberwar*, 11.
[59] Jamieson, *Cyberwar*, 13.
[60] Jamieson, *Cyberwar*, 38.

campanha e a Rússia concentraram-se então nos temas que mais mexiam com os medos do eleitorado que conduziriam a votar em Trump e dissuadiriam de votar em Hillary Clinton[61]. Esses temas passavam pelas questões da imigração ilegal, da presença de muçulmanos na América (tema que se tornou mais sensível desde o 11 de setembro de 2001), pelos ataques à liberdade religiosa, pela falta de respeito pelas forças de segurança e veteranos, pela criminalidade associada a outras raças, sobre os quais Trump afirmava que teria uma mão firme; e pelos temas que desacreditavam Hillary enquanto candidata, como rumores de desonestidade e corrupção, de que não se preocupava com os veteranos, de que era responsável pela elevada taxa de presos negros, de que estava alinhada com os interesses de Wall Street e de que tinha viciado o resultado das Primárias Democratas contra o seu adversário Bernie Sanders[62]. A campanha girou então em torno do reforço das mensagens de que a administração Democrata dos últimos oito anos tinha beneficiado "os outros" e prejudicado o "nós", e de que quatro anos de Hillary apenas prolongariam essa situação.

> "Para os que temiam mobilidade social descendente e deslocação cultural, a retórica de Trump prometia não só empregos, como também que, como Presidente, esmagaria a imigração ilegal e restauraria a 'lei e ordem' (…). Veteranos deveriam ir votar nele porque ele restauraria o respeito por eles, protegeria os seus interesses e desenvolveria as forças militares. Ele apoia a polícia e, por implicação, não aqueles que protestam contra as suas ações. No entanto, negros e latinos não têm razão para aparecer em grandes números por Hillary. Trump promete fazer mais por ambos do que Clinton. E para aqueles preocupados com as revelações no "Access Hollywood", reafirmou o seu respeito pelas mulheres"[63].

As mensagens da campanha de desinformação foram dirigidas a cinco grupos principais que Trump precisava de influenciar, tanto para os impelir a votar em si, e, na impossibilidade de os convencer, dissuadi-los de votar em Hillary. As mensagens eram então intencionadas para

[61] Jamieson, *Cyberwar*, 38.
[62] Jamieson, *Cyberwar*, 102.
[63] Jamieson, *Cyberwar*, 78.

a mobilização de veteranos e cristãos brancos (com ênfase nos evangélicos) e para a desmobilização de negros, de apoiantes de Bernie Sanders e para mover os votos de liberais e democratas céticos de Hillary para Jill Stein.

Nos Anexos (página 133) encontram-se alguns exemplos das mensagens partilhadas pelas contas russas abordando as questões da imigração ilegal, do crime, da religião, dos veteranos e da alegada corrupção de Hillary Clinton.

d) Redes sociais, anúncios e *bots*

As redes sociais tiveram um papel preponderante na campanha de desinformação contra Hillary Clinton. Como já vimos, a estratégia russa não se limitava a roubar e a divulgar documentos confidenciais do lado Democrata. Passava também por chegar ao maior número de eleitores possível, por alinhar as mensagens com os interesses da campanha Trump de modo a mobilizar grupos menos participativos em eleições anteriores, através de mensagens persuasivas e direcionadas para os grupos pretendidos[64].

Falemos então do alcance e da direção das mensagens.

Devemos primeiro salientar que a Rússia dispõe dum canal televisivo que transmite em inglês ativo em todo o mundo, inclusive nos Estados Unidos, que dispõe duma audiência considerável, o Russia Today[65]. Em 2013 foi o primeiro canal de notícias a atingir mil milhões de visualizações no YouTube e contava em 2018 com 2,2 milhões de subscritores, tendo agora (julho de 2020) 3,9 milhões. A sua existência e o seu alcance potencial são relevantes tendo em conta que em 2016 o canal concentrou grande atenção no conteúdo disponibilizado via

[64] Jamieson, *Cyberwar*, 67-131.
[65] Jamieson, *Cyberwar*, 68.

WikiLeaks, tal como noticiou segmentos de que Hillary recebia financiamento de apoiantes do Estado Islâmico, estava mal de saúde e de que era corrupta[66].

Histórias destas eram depois amplificadas nas redes sociais, com o auxílio de anúncios, publicações e *bots*[67]. Existiam pelo menos três contas de Twitter direcionadas ao público americano, com um número combinado de 6 milhões de seguidores, que gastaram cerca de 274 mil dólares para promover tweets em 2016[68]. O Twitter encontrou pelo menos 3814 contas associadas à IRA e cerca de 50 mil *bots*, que partilharam tweets de Donald Trump 470 mil vezes. Adicionalmente, o Twitter confirmou que "1,4 milhões pessoas nos EUA que seguiam uma das contas potencialmente ligadas a um esforço de propaganda russo" estavam a receber notificações por e-mail de publicações dessas contas[69]. Em novembro de 2017, o Twitter reportou cerca de 1,4 milhões de tweets relacionados com as eleições gerados automaticamente por operacionais russos, que terão chegado a aproximadamente 288 milhões de utilizadores[70].

Contudo, a Rússia não operava apenas no Twitter ou no Facebook. A partir de novembro de 2017, gigantes da tecnologia como Facebook, Twitter, Instagram, YouTube, Reddit, 9GAG começaram a confirmar atividade russa pró-Trump nas suas plataformas digitais.

No Facebook, a IRA atuou através da publicação de conteúdo favorável a Trump e danoso para Hillary. Inclusive, foram criadas contas falsas para enviar mensagens privadas a membros de grupos pró-Trump. Para chegar a mais eleitores, a IRA comprou anúncios que promoviam os grupos por si criados. Foram comprados mais de 3500 anúncios, com gastos até perto dos 100.000 dólares, que se dividiam entre anúncios que promoviam Trump e que denegriam a imagem de Hillary Clinton.

Coletivamente, os anúncios chegaram a dezenas de milhões de pessoas. Alguns grupos chegaram a ter centenas de milhares de membros, como o grupo "Being Patriotic", com mais

[66] Jamieson, *Cyberwar*, 68.
[67] Programas criados para simular comportamentos humanos online.
[68] Jamieson, *Cyberwar*, 68.
[69] Jamieson, *Cyberwar*, 70.
[70] Jamieson, *Cyberwar*, 69.

de 200 mil seguidores, ou o "Secured Borders", com mais de 130 mil. Pelo que o Facebook conseguiu apurar, as contas pertencentes à IRA fizeram mais de 80 mil publicações até à sua desativação em agosto de 2017, chegando a, pelo menos, 29 milhões de americanos, podendo ter chegado a uns estimados 126 milhões.

Quanto ao Instagram, Jonathan Albright, um investigador da Universidade Columbia, ao analisar 28 de 170 contas criadas pela IRA, entretanto eliminadas, concluiu que houve cerca de 2,5 milhões de interações registadas com as publicações destas contas e estima 145 milhões de interações passivas com as mesmas publicações[71].

Deve-se, no entanto, questionar se o conteúdo publicado foi visualizado por utilizadores das redes sociais ao acaso ou se por utilizadores que eram sensíveis a este conteúdo. O conteúdo terá certamente passado por pessoas sobre as quais não teve qualquer efeito persuasivo ou dissuasor. Existe eleitorado fixo, existem eleitores que ora votam republicano, ora votam democrata, investigadores ou apenas curiosos que procuram o máximo de informação acerca de todos os candidatos numa eleição. Mas isso não significa que a mensagem não chegue principalmente a quem se pretendia, até porque as redes sociais têm os seus algoritmos construídos para esse mesmo efeito.

"Uma vez que as plataformas dos gigantes da tecnologia foram criadas para eficientemente alcançar os consumidores cobiçados pelos anunciantes, não surpreende que tenham capacidades únicas e meios amigos do utilizador para chegar à audiência pretendida. Entre outras formas, o Facebook permite aos mensageiros identificar utilizadores por ideologia (ex: muito liberal, moderado, conservador, muito conservador), afiliação política, atividade política, assuntos a que se é sensível (ex: controlo de armas), consumo de notícias, distrito, código postal, localização num raio de oito quilómetros, perfil pessoal, demografia e interesses.

Os russos exploraram estas capacidades. Por exemplo, o anúncio de Facebook que mostra Jesus em braço de ferro com Hillary estava direcionado para alcançar 'pessoas dos 18 aos 65+, interessados em Cristandade, Jesus, Deus, Ron Paul e personalidades dos *media* como Laura Ingraham, Rush

[71] Sheera Frenkel, "For Russian 'Trolls,' Instagram's Pictures Can Spread Wider Than Words", *The New York Times*, 17 de dezembro de 2017, https://www.nytimes.com/2017/12/17/technology/instagram-russian-trolls.html?auth=login-facebook.

Limbaugh, Bill O'Reilly e Mike Savage'. Por contraste, 'pessoas dos 18 aos 65+ interessadas em veteranos militares, incluindo aqueles do Iraque, Afeganistão e Guerra do Vietname' eram a audiência para o anúncio do Instagram com a viúva de luto sobre o caixão do marido. Anúncios apresentando muçulmanos que apoiavam a candidatura de Clinton 'eram direcionados a utilizadores de Facebook que pudessem temer muçulmanos'"[72].

Na divulgação nas redes sociais, a Rússia só tinha de criar as mensagens que pretendia difundir. O sistema de distribuição eficaz e preciso que permitia interferir com as escolhas dos eleitores tinha sido criado pelas empresas do próprio país onde a Rússia estava a tentar influenciar o resultado eleitoral.

e) Comícios políticos

A IRA serviu-se também das redes sociais para convocar comícios políticos para apoiar o partido e o candidato republicanos, fazendo-se passar por personalidades americanas. A IRA usava as suas personas das redes sociais, como nos grupos de Facebook ou contas de Twitter, para anunciar e promover os eventos. Depois de vários eleitores manifestarem o seu interesse em participar, eram-lhes enviadas mensagens privadas a confirmar o evento e a pedir a sua participação no mesmo. Dos interessados, a IRA selecionava depois alguém para coordenar o evento, argumentando que quem tinha organizado o evento não poderia estar presente por algum imprevisto ou porque estava noutra parte dos Estados Unidos. A IRA comunicava ainda o evento à comunicação social e dirigia-a para falar com o coordenador do evento, publicando, no final, fotos e vídeos do mesmo nas redes sociais. Foram criados pelo menos 129 eventos por 13 páginas da IRA e, segundo uma investigação do Wall Street Journal, pelo menos 22 foram realizados[73].

[72] Jamieson, *Cyberwar*, 140.
[73] Mueller, "Report On The Investigation Into Russian Interference", 29.

A forma como a Rússia operou permite-nos já ver muitas das potencialidades do ciberespaço como domínio de conflito. Sem necessidade de ter operacionais em território dos Estados Unidos, conseguiu roubar e divulgar documentos oficiais e conduzir uma campanha de desinformação de acordo com os seus interesses na eleição presidencial dum país estrangeiro. Com exceção dos dois vírus criados, praticamente não teve de desenvolver praticamente nada que requeresse conhecimento técnico especializado. A infraestrutura para a disseminação orientada do conteúdo propagandístico estava já criada pelas plataformas digitais de origem americana e os custos das operações foram relativamente baixos (sendo a maior fatia o custo dos anúncios nas redes sociais).

Veremos de seguida qual foi o modo de atuação da empresa Cambridge Analytica e, depois, analisaremos a plausibilidade da eficácia da campanha de desinformação no comportamento eleitoral dos cidadãos americanos.

2. Cambridge Analytica

2.1. O que era a Cambridge Analytica?

A Cambridge Analytica (CA) era uma das subsidiárias do SCL Group (Strategic Communication Laboratories), uma empresa especializada em contratos governamentais e militares, atuando em diversas áreas, desde segurança alimentar e antiterrorismo a campanhas políticas, dentre os quais se contavam colaborações com o Ministério da Defesa britânico e com a NATO em operações de informações. Segundo o relato do denunciante Christopher Wylie, Alexander Nix, o CEO da Cambridge Analytica ter-lhe-á dito que "a maioria do trabalho da firma era para agências militares e de informação (*intelligence*), em projetos que os governos não podiam oficialmente executar"[74], tendo de seguida passado a mostrar um relatório daquilo que era o ponto de partida para a maior parte dos contratos da CA – a Análise do Público Alvo (Target Audience Analysis/TAA)[75] – enquanto folheava outros relatórios idênticos.

Quando a CA foi criada em 2013, o seu objetivo seria combater a radicalização online.

"Depois de os aliados ocidentais estarem a ter problemas com como lutar contra a radicalização online, a firma quis que eu formasse uma equipa de cientistas de dados para criar novas ferramentas para identificar e combater o extremismo online. (…) Estávamos prestes a abrir novos caminhos para as ciberdefesas do Reino Unido, dos EUA e dos seus aliados e confrontar insurgências fervilhantes de extremismo radical com dados, algoritmos e narrativas direcionadas online"[76].

No entanto, o seu rumo alterar-se-ia no outono desse ano, e alterar-se-ia na direção exatamente oposta. Se a Cambridge Analytica tinha sido criada com o intuito de combater extremismos, os eventos no final de 2013 pô-la-iam a fazer precisamente o contrário: a fomentar

[74] Christopher Wylie*, Mindf*ck: Inside Cambridge Analytica's Plot to Break the World* (Londres: Profile Books, 2019), 40.
[75] Wylie, *Mindf*ck*, 40.
[76] Wylie, *Mindf*ck*, 5-6.

o extremismo na Direita americana, também com "dados, algoritmos e narrativas direcionadas online".

Essa mudança de rumo concretizou-se com a chegada de Steve Bannon, (futuro Diretor Executivo da campanha e estratega da administração Trump) e com a promessa duma injeção de capital a ser feita por Robert Mercer, um multimilionário gestor de fundos de cobertura e um apoiante do conservadorismo republicano americano.

Não nos adensaremos na biografia de Bannon ou de Mercer. Contudo, é importante referir que antes de se envolver na campanha de Donald Trump, Steve Bannon fora o sucessor de Andrew Breitbart, fundador e editor sénior da Breitbart News – um site de notícias, opiniões e comentários da extrema-direita americana – após a sua morte inesperada em 2012. Importa também referir que, segundo uma investigação do New York Times, o site é financiado pelo património da família Breitbart, Larry Solov (co-fundador) e pela família de Robert Mercer[77]. Por fim, o conteúdo do site tinha já sido alvo de controvérsia antes da candidatura de Trump, com liberais e até mesmo conservadores republicanos a classificarem-no como "misógino, xenófobo e racista"[78].

Antes do contacto com Bannon, a CA ainda não tinha trabalhado nos Estados Unidos, pelo que Bannon pediu prova de conceito do que a Cambridge Analytica era capaz de fazer. Sob alegada sugestão de Steve Bannon, a CA começou com testes no Estado da Virgínia, um "bom microcosmo da América"[79].

"É um pouco nortenho e um pouco sulista. Tem montanhas e áreas costeiras, cidades militares, subúrbios ricos de [Washington] DC, áreas rurais e quintas, e tem secções cruzadas de ricos e pobres, negros e brancos"[80].

[77] Michael Grynbaum e John Herrman, "Breitbart Rises From Outlier to Potent Voice in Campaign", *The New York Times*, 26 de agosto de 2016, https://www.nytimes.com/2016/08/27/business/media/breitbart-news-presidential-race.html.
[78] Grynbaum e Herrman, "Breitbart Rises".
[79] Wylie, *Mindf*ck*, 69.
[80] Wylie, *Mindf*ck*, 69.

Segundo Wylie, o trabalho na Virgínia tinha obtido resultados promissores. Teriam ficado provadas relações entre traços de personalidade e inclinação política, que se podia prever certos comportamentos e que era possível mudar algumas atitudes adequando a linguagem das mensagens ao perfil psicométrico dos alvos. Porém, a CA sabia que precisaria de mais dados e o seu trabalho de investigação nos Estados Unidos continuou. A Cambridge Analytica, uma firma com um orçamento anual entre os 7 e os 10 milhões de dólares, acabaria por conseguir 15 milhões dólares vindos unicamente de Robert Mercer no ano de 2013, bem como contratos para as campanhas de Ted Cruz, senador Republicano pelo Estado do Texas e candidato presidencial nas primárias Republicanas de 2016, e de Donald Trump, recebendo pelo menos 5 milhões de dólares de cada uma. Acabaria, também, por se tornar numa firma que combinava mineração, apropriação indevida, análise e corretagem de dados com análise psicográfica e publicidade direcionada para tornar a sua comunicação política o mais eficaz possível.

Veremos, de seguida, em que consistiu a estratégia e o *modus operandi* da Cambridge Analytica na campanha de Donald Trump.

3.2. A estratégia da Cambridge Analytica

A estratégia da Cambridge Analytica e a estratégia da Rússia não tinham muitas diferenças entre si. Aliás, se se viesse a descobrir que a Rússia usou os modelos de categorização psicográfica para adequar as diferentes mensagens propagandísticas aos diferentes perfis psicológicos dos eleitores americanos, poder-se-ia dizer que eram a mesma estratégia, mas executada por mais do que um ator, porque a principal diferença é essa: o alegado uso de categorização psicográfica para tornar as mensagens mais eficazes. Ainda assim, explicaremos a estratégia da Cambridge Analytica isoladamente.

O primeiro ponto da estratégia da CA foi recolher informação sobre os eleitores para depois poder traçar o seu perfil psicográfico, não só para os poder classificar em diferentes grupos, mas também para compreender que eleitores eram persuadíveis ou não. Tenhamos em atenção que esta persuasão não se cingiu somente a "votar em Trump". A persuasão consistiu, tal como na estratégia russa, na lógica "nós versus eles", em convencer os indecisos a optarem por Trump e a incentivar a participação eleitoral de todos os que preferissem Trump e em desacreditar Hillary junto do seu eleitorado mais provável, demovendo-o de ir votar. Mesmo com o auxílio da categorização psicográfica, é pouco provável que se convença alguém que sempre votou Democrata a de repente votar Republicano, pelo que seria insensato despender esforços nesse sentido. Daí que a(s) estratégia(s) tenha(m) assentado na mobilização dum lado e na desmobilização do outro.

O segundo ponto passava por fazer o tipo de mensagem corresponder ao perfil psicográfico traçado, de modo a levar os utilizadores a interagirem com elas ("gostar", partilhar, comentar). A interação com as publicações servia o propósito de confirmar que a mensagem recebia a "aprovação" de alguém, ou seja, de que estava a funcionar, e ainda fazia com que a publicação chegasse a mais utilizadores, uma vez que os "*feeds*" nas redes sociais também são alimentados por aquilo de que alguém com quem estamos conectados "gostou", partilhou ou

comentou. A Cambridge Analytica chegou, nalguns casos, a experimentar 30 versões diferentes da mesma mensagem[81].

O terceiro e último ponto da estratégia prende-se com o facto de não se ter feito, por parte da Cambridge Analytica, uma campanha massificada, mas antes uma campanha dirigida a indivíduos que se acreditavam ser persuadíveis, quer fosse no sentido da mobilização, quer no da desmobilização.

Segundo Christopher Wylie, denunciante do caso, a Cambridge Analytica não precisava de chegar a todos os utilizadores por duas razões.

Primeiro, porque o sistema eleitoral americano torna as eleições em jogos de soma-zero. Com a exceção do Maine e do Nebraska, todos os outros Estados atribuem a totalidade dos seus delegados do Colégio Eleitoral ao candidato mais votado. Ou seja, se no Estado da Califórnia existem 55 delegados para atribuir, o candidato mais votado nesse Estado recebe todos os 55 delegados, e o outro candidato recebe zero, não importando o quão renhida tenha sido a votação.

Depois, os próprios algoritmos do Facebook contribuíam para a propagação do conteúdo, embora os alvos principais fossem aqueles identificados e categorizados pela Cambridge Analytica.

"Muito do reportado sobre a Cambridge Analytica deu a impressão de que toda a gente era alvo [de propaganda]. De facto, não houve assim tanta gente a ser visada. A CA não precisava de criar um grande universo de alvos, porque a maioria das eleições são jogos de soma-zero. Se tiver mais um voto do que o outro, ganha a eleição. A Cambridge Analytica só precisava de infetar uma pequena parte da população e depois podia observar a narrativa espalhar-se"[82].

[81] Brittany Kaiser, *Targeted: My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy* (Londres: Harper Collins, 2019), 87.
[82] Wylie, *Mindf*ck*, 121.

A Cambridge Analytica terá chegado a 70,6 milhões de eleitores americanos, o que num universo de 250 milhões de eleitores corresponde a menos de 30% (28,24%, de acordo com os dados disponíveis).

Depois de analisarmos como se traçaram os perfis psicográficos, como se concretizou a recolha de dados pessoais no Facebook e como os perfis psicográficos e dados pessoais foram alegadamente transformados em arma política, procuraremos mostrar se os esforços propagandísticos russos e da Cambridge Analytica tiveram ou não os efeitos desejados.

3.2.1. Os cinco tipos de personalidade

Para a Cambridge Analytica adequar as suas mensagens políticas aos perfis psicográficos dos utilizadores, precisava de recolher vários dados, sobretudo dados que permitissem compreender a perceção que o eleitorado americano tinha acerca de vários assuntos. Só depois poderia a CA gerar as perguntas corretas para distinguir corretamente os traços de personalidade dominantes através dum teste de personalidade online. Por isso, primeiro foi necessário observar e interagir com cidadãos americanos no terreno, conversando, convivendo com eles e entrevistando-os. Quando a CA pensou já ter uma compreensão adequada das perceções do eleitorado americano, é que passou para a recolha de dados acerca dele. No entanto, antes de elaborarmos na recolha dos dados, vamos primeiro distinguir entre os cinco tipos de personalidade em que a CA categorizou os eleitores.

O modelo OCEAN (como lhe chamámos no capítulo introdutório acerca do ciberespaço) ou CANOE, ou ainda Modelo dos Cinco Fatores ou dos Cinco Grandes é um modelo estudado e utilizado no campo da Psicologia há mais de 60 anos. Reconhece-se que há sempre diferenças e nuances mais ou menos subtis de indivíduo para indivíduo, mas este é, até à data o modelo mais consensual e utilizado pela comunidade da Psicologia na categorização da personalidade.

O nome OCEAN é um acrónimo dos cinco traços de personalidade mais comuns:

- *Openness to experience* – Abertura para a experiência
- *Conscientiousness* – Conscienciosidade
- *Extraversion* – Extroversão
- *Agreebleness* – Agradabilidade/Amabilidade
- *Neuroticism/Negativity* – Instabilidade Emocional/Negatividade

De forma resumida, pessoas com pontuação elevada na (1) Abertura à Experiência tendem a ser pouco convencionais, dispostas a questionar a autoridade e a considerar novas ideias éticas, sociais e políticas[83].

A (2) Conscienciosidade refere-se a autocontrolo e ao processo ativo de planear, organizar, e executar tarefas. A conscienciosidade manifesta-se na orientação para objetivos (trabalho árduo e persistência), confiabilidade e em fazer as coisas de forma ordeira[84].

A (3) Extroversão inclui traços como sociabilidade, assertividade, propensão à atividade e à conversa. É caracterizada por experiências e sentimentos positivos, pelo que é considerada um traço positivo[85].

(4) Agradabilidade/Amabilidade. Uma pessoa agradável/amável é fundamentalmente uma pessoa altruísta, empática com os outros e desejosa de os ajudar. O contrário será alguém egocêntrico, cético e mais competitivo do que cooperativo[86].

A (5) Instabilidade Emocional/Negatividade é uma dimensão de personalidade normal que indica uma tendência geral para sentir medo, tristeza, vergonha, raiva, culpa e repugnância (*disgust*). Uma pontuação elevada neste traço indica que uma pessoa é propensa a ter ideias irracionais e a ser mais impulsiva (quando o impulso é um dos sentimentos referidos)[87].

As características dos cinco traços de personalidade podem ser vistas com mais detalhe nos Anexos (página 131).

A categorização por perfil psicográfico por parte da Cambridge Analytica terá vindo corrigir o que esta considerava um erro na forma categorizar o eleitorado. Para esta, os centros

[83] Sebastiaan Rothmann e Elize Coetzer, "The Big Five Personality Dimensions and Job Performance", *SA Journal of Industrial Psychology* 29, 2003: 69.
[84] Rothmann e Coetzer, "The Big Five Personality Dimensions", 69.
[85] Rothmann e Coetzer, "The Big Five Personality Dimensions", 69.
[86] Rothmann e Coetzer, "The Big Five Personality Dimensions", 69.
[87] Rothmann e Coetzer, "The Big Five Personality Dimensions", 69.

e agências de sondagens, independentes ou pertencentes aos partidos, falavam dos grupos eleitorais duma forma desconexa da realidade. Diz Christopher Wylie:

"Centros e agências de sondagens [*pollsters*] falam frequentemente de grupos eleitorais monolíticos –mulheres, classe trabalhadora, gays. Embora sejam certamente fatores para a identidade das pessoas e para as suas experiências, não existe tal coisa como *eleitora mulher* ou *eleitor latino* ou qualquer um desses rótulos. Pensem nisso: Se escolher cem mulheres ao acaso na rua, vão ser todas a mesma pessoa? E se forem cem afro-americanos? São todos o mesmo? Podemos mesmo dizer que as pessoas são clones por virtude da cor da sua pele e da sua genitália? Todos têm experiências diferentes, dificuldades, sonhos.

Explorar as nuances da identidade e personalidade fez-me perceber porque é que, apesar de os políticos fazerem sondagens a toda a hora, continuam a aparentar estar horrendamente desfasados do que é o eleitorado. (…) A maioria das pessoas nunca pensa em si como um "eleitor", muito menos constrói a sua identidade em torno da sua mundividência em relação a políticas de impostos. Quando uma pessoa vai às compras, é improvável que parem, larguem as suas compras e, num momento de autoconsciência ofuscante, repentinamente se apercebam de que são uma mulher eleitora dos subúrbios com educação universitária num Estado decisivo"[88].

A categorização através do modelo OCEAN permitiu à CA compreender e segmentar o eleitorado. A CA terá chegado a segmentar 32 grupos diferentes. Depois, com a ajuda dos "likes" no Facebook, que no fundo se traduziam em dados adicionais sobre a personalidade dos utilizadores, a categorização tornar-se-ia cada vez mais refinada[89]. Os alvos preferidos da Cambridge Analytica acabariam por ser os que pontuavam alto na instabilidade emocional e negatividade, "os que eram mais propensos a raiva impulsiva ou pensamentos conspiratórios do que o cidadão comum"[90]. Depois, a CA introduzia narrativas via grupos, anúncios e artigos no Facebook que sabia serem inflamatórias graças a testes internos previamente conduzidos. Havendo um número razoável de indivíduos classificados como neuróticos e suficientemente expostos a estas novas narrativas, era chegada a altura de estes se encontrarem para formarem

[88] Wylie, *Mindf*ck*, 35.
[89] Kaiser, *Targeted*, 87.
[90] Wylie, *Mindf*ck*, 120.

grupos e se organizarem. Indivíduos neuróticos, mas com alguma resistência a rumores, começavam a resistir cada vez menos. E formando-se um grupo num distrito, mais tarde ou mais cedo se formava outro no distrito ao lado, inspirado pelo anterior. A longo prazo, formar-se-iam diversos grupos num só Estado e, no fim, por todo o país. A chamada Direita Alternativa (alt-right) começava a emergir organizada em grupos de cidadãos graças à propaganda meticulosamente direcionada devido à categorização psicográfica e propagada via Facebook[91].

No entanto, a categorização psicográfica não servia só para direcionar mensagens políticas a quem era identificado como neurótico, nem a categorização psicográfica era tudo. A CA identificava também aqueles que eram eleitores indecisos (*swing voters*), que ora votavam no Partido Democrata, ora votavam no Partido Republicano, e cuja análise psicográfica indicasse que eram persuadíveis. Depois, de acordo com o seu perfil psicográfico, produziam mensagens diferentes a apelar ao voto no partido Republicano. Por exemplo:

"Um dos grupos de eleitores indecisos era 'Fechados e Agradáveis'. Essas pessoas recebiam um anúncio sobre armas que usava linguagem e imagens que reforçava os valores da família e da tradição. Usámos uma imagem dum homem e dum rapaz, as suas silhuetas, a caçar ao pôr do sol. O texto dizia 'De pai para filho… desde o nascimento da nossa nação'. Enfatizava como as armas podiam ser mostradas como algo que as pessoas partilhavam com aqueles que amavam. (…)

Outra imagem era para um público muito diferente: os 'Extrovertidos e Desagradáveis'. (…) 'Este eleitorado precisa duma mensagem que seja acerca da sua capacidade de afirmar os seus direitos … Este tipo de eleitor precisa de ser ouvido. Em qualquer tópico. Ele sabe o que é melhor para si. Internamente tem um forte desejo de controlo e odeia que lhe digam o que fazer, especialmente o governo'.

A mulher na imagem estava a empunhar uma arma, com uma expressão feroz na cara. O texto dizia 'Não questiones o meu direito de ter uma arma, e eu não questionarei a tua estupidez de não ter uma'. (…)

'O que a Cambridge Analytica oferece é a mensagem certa, para a audiência alvo certa, da fonte certa, no canal certo à hora certa. E é assim que se ganha'"[92].

[91] Wylie, *Mindf*Ck*, 123.
[92] Kaiser, *Targeted*, 92-93.

Quer isto dizer que a suscetibilidade à persuasão por parte do eleitorado não estava dependente da proeminência dum traço de personalidade específico. Embora indivíduos cujo traço de personalidade predominante fosse o da Negatividade sejam apresentados como os alvos preferenciais, estes não eram os únicos suscetíveis de serem persuadidos. Essa suscetibilidade encontrava-se ao longo de todo o espetro da personalidade. Era necessário, no entanto, saber onde pressionar para que a persuasão surtisse os efeitos desejados e, por isso, ir alterando a mensagem consoante os traços de personalidade dominantes. Os argumentos iam mudando, mas a finalidade era a mesma.

3.2.2. Recolha de dados pessoais no Facebook

É primeiro importante esclarecer que a recolha de dados pessoais não ocorreu só no Facebook. É comum (e legal) as equipas dos diferentes partidos recolherem dados sobre o eleitorado para tentarem tornar as suas campanhas o mais eficazes possível. Além disso, os dados dos utilizadores são bens cada vez mais comercializados entre empresas, para direcionarem os seus produtos e serviços aos consumidores potencialmente mais interessados.

A ligação entre a Cambridge Analytica e o Facebook começou em 2014 com o contacto da CA com investigadores nos campos da Psicologia e Psicografia, nomeadamente com o Dr. Aleksandr Kogan, professor da Universidade de Cambridge, especialista em modelação computacional de traços psicológicos[93]. Na altura, Kogan estava a colaborar com uma equipa de investigadores baseada na Universidade Estatal de São Petersburgo, num projeto de definição de perfis psicológicos financiado pelo Estado russo através duma bolsa de investigação. O projeto consistia em recolher dados dos perfis das redes sociais para analisar o comportamento de *trolls*[94] online[95].

Quando a Cambridge Analytica começou a construir a sua base de dados, diz ter "comprado e licenciado toda a informação pessoal existente sobre cada cidadão Americano"[96], comprando essa informação de "todos os vendedores que pudesse pagar – desde a Experian à Axiom ao Infogroup. Comprou-se informação acerca das suas finanças, onde compravam, quanto pagavam, onde iam de férias, o que liam"[97]. O problema era que toda esta informação remetia principalmente para hábitos de consumo e, embora esses sejam muito úteis à maioria das empresas, são-no pouco para traçar campanhas políticas com base na psicografia dos eleitores.

[93] Wylie, *Mindf*ck*, 96.
[94] Na gíria da internet, um *troll* é alguém que deixa mensagens ou comentários ofensivos, inflamatórios ou polémicos com o único propósito de irritar, chatear, ofender outros internautas.
[95] Wylie, *Mindf*Ck*, 98.
[96] Kaiser, *Targeted*, 77-78.
[97] Kaiser, *Targeted*, 78.

A CA tinha conjuntos de dados e algoritmos funcionais para identificar padrões e prever comportamentos de consumo; contudo estava num impasse no que tocava a perfis psicográficos, porque precisava de dados mais variados acerca dos cidadãos americanos. Aleksandr Kogan acabaria por desbloquear esse impasse, revelando que o Facebook simplesmente permitia a extração de informação.

"O Facebook quer que façam investigação na sua plataforma. Quanto mais aprender sobre os seus utilizadores, mais os pode monetizar [lucrar com eles]. Ficou claro quando eles [Kogan e equipa] explicaram como recolhiam dados que os controlos e permissões do Facebook eram incrivelmente lassos"[98].

Por outras palavras, até o Facebook ter feito alterações à Interface de Programação de Aplicações (Application Programming Interface/API) em abril de 2015, bloqueando o acesso aos dados dos utilizadores a criadores terceiros de aplicações, a privacidade dos utilizadores era praticamente nula, mesmo que não tivessem dado permissão a determinada aplicação para recolher os seus dados. Até essa alteração da API, qualquer criador duma aplicação para o Facebook ficava não só com os dados de quem a usasse, como também ganhava acesso aos dados pessoais de todos os "amigos" que esse utilizador tinha na rede social. À data, cada utilizador de Facebook tinha entre 150 a 300 amigos[99]. Ou seja, se alguém criasse uma aplicação que fosse utilizada por 1000 pessoas, esse alguém ganhava, em termos médios, acesso aos dados de pelo menos 150 mil perfis. Quer isto dizer que com 2 milhões de utilizadores diretos, uma aplicação teria o potencial para aceder a cerca de 300 milhões de utilizadores. Nos Estados Unidos, um país com 323 milhões de habitantes, dos quais 250 milhões eram eleitores e 190

[98] Wylie, *Mindf*Ck*, 100.
[99] Wylie, *Mindf*ck*, 100, e "Average number of Facebook friends of users in the United States in 2016", Statista, outubro de 2016, https://www.statista.com/statistics/398532/us-facebook-user-network-size/.

milhões de adultos utilizavam o Facebook[100], a Cambridge Analytica terá acabado por recolher os dados de cerca de 70.6 milhões[101] de utilizadores americanos.

A aplicação utilizada pela Cambridge Analytica tinha o nome "This Is Your Digital Life" (Esta É A Tua Vida Digital) e serviu um duplo propósito: a aplicação era simultaneamente um teste de personalidade do modelo OCEAN e o meio através do qual os utilizadores consentiam o acesso aos seus dados pessoais e, sem o saberem, aos dados pessoais dos seus amigos.

> "Quando os utilizadores completavam o teste no Facebook, a aplicação ligava-se à API para levar os seus dados e os da sua lista inteira de amigos. Das respostas que obtinha através da This Is Your Digital Life, Kogan criava um conjunto de treino para modelar as personalidades de todos os participantes e depois, alegadamente, vendia o modelo de classificação e os conjuntos de dados à CA, onde a equipa depois testava os modelos de Kogan e criava modelos novos, mais precisos, baseados em conceitos semelhantes de medição de personalidade"[102].

Em média, cada perfil de Facebook fornecia cerca de 570 dados diferentes acerca do indivíduo a quem pertencia. Os dados obtidos no Facebook eram depois cruzados com os dados já obtidos de outras empresas acerca dos hábitos de consumo e com a informação política publicamente disponível (e.g: registos para votação nas primárias partidárias dum dos partidos, registos para votar na eleição geral e o registo de se um cidadão registado para votar efetivamente votou ou não) a que conseguiam aceder. Combinando todas as fontes, a CA obtinha em média cerca de 5000 dados acerca de cada indivíduo. Estava desbloqueado o impasse da recolha de dados para traçar os perfis psicográficos dos eleitores.

Estando o impasse da recolha de dados em grande escala e variedade desbloqueado, resta saber se é plausível que um perfil psicográfico traçado com base nos "likes" numa rede social esteja corretamente traçado. Um estudo publicado em 2015 da Universidade de Cambridge indica que sim.

---

[100] "Leading countries based on Facebook audience size as of July 2020", Statista, julho de 2020, https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/.
[101] Court Stroud, "Cambridge Analytica: The Turning Point In The Crisis About Big Data", *Forbes*, 30 de abril de 2018, https://www.forbes.com/sites/courtstroud/2018/04/30/cambridge-analytica-the-turning-point-in-the-crisis-about-big-data/.
[102] Kaiser, *Targeted*, 149.

O estudo indica que a personalidade de alguém é melhor julgada por um computador do que por seres humanos. Com apenas 10 "gostos" do Facebook, um computador conseguia ser mais exato a julgar a personalidade de alguém do que um colega de trabalho. Com 150 "gostos", o juízo feito "à máquina" era mais preciso do que o dum familiar e, com 300 "gostos", mais preciso do que os cônjuges dos indivíduos que fizeram parte do estudo[103]. As conclusões deste estudo, ou conclusões semelhantes na sua própria investigação, serão o que terá levado Aleksandr Kogan a dizer, num dos encontros com membros da Cambridge Analytica que "o Facebook sabe mais sobre vocês do que qualquer pessoa na vossa vida. Até mesmo do que a vossa mulher"[104]. O motivo para tal prende-se com o facto de colegas, amigos, familiares e parceiros amorosos não nos verem em todos os contextos da nossa vida e de adequarmos o nosso comportamento em diferentes contextos sociais. Agimos dum modo no trabalho, doutro modo entre amigos e ainda doutro em quando estamos em família. Por outro lado, nas redes sociais, como o Facebook, não só estamos menos inibidos para interagir com todas as coisas que são do nosso interesse, como a pressão social para adequarmos o nosso comportamento também é menor, porque fisicamente não está ninguém ao nosso redor. Além disso, cada "gosto" deixado no Facebook é um registo permanente. "Gostou-se" disto, naquele dia, àquela hora. Carregou-se no anúncio, visitou-se o site, comprou-se ou não se comprou o artigo. Ou então, no caso da política, gosta-se da página e segue-se (ou não) determinado partido, dá-se o "gosto" numa publicação dessa página, partilha-se, comenta-se, em concordância ou discordância. Importa por isso destacar que, segundo o estudo da Universidade de Cambridge, os julgamentos sobre a orientação política de alguém feitos por outros seres humanos eram, por vezes, errados. Os julgamentos feitos por computador, que contavam com dados retirados do Facebook, foram, todos eles, corretos[105].

[103] Wu Youyou, Michal Kosinski e David Stillwell, "Computer-based personality judgments are more accurate than those made by humans", *Proceedings of the National Academy of Sciences* 112, n.º 4 (janeiro, 2015): 1036.
[104] Wylie, *Mindf*ck*, 97.
[105] Youyou, Kosinski E Stillwell, "Computer-based personality judgments", 1039.

Conhecendo já o modelo usado para a categorização dos fatores de personalidade, o modo como a informação foi recolhida no Facebook e sabendo que a categorização feita por computador é mais precisa do que quando feita por mão humana, resta-nos compreender como é que essa informação pode ser instrumentalizada para fins políticos.

3.2.3. Transformação da informação em arma política e PSYOPs

Como vimos no início deste capítulo, a Cambridge Analytica era uma subsidiária duma empresa que se especializava em contratos militares. Este aspeto é importante porque o que a CA alegadamente fez nas eleições norte-americanas assemelha-se ao que na doutrina militar se chama de "operações psicológicas" ou "PSYOPs". O Dicionário de Termos Militares e Associados do Departamento de Defesa dos Estados Unidos define "operações psicológicas" como:

> "Operações planeadas para veicular informação e indicadores selecionados a audiências estrangeiras para influenciar as suas emoções, motivos, raciocínio objetivo e, em última análise, o comportamento de governos, organizações, grupos e indivíduos estrangeiros. O propósito das operações psicológicas é induzir ou reforçar atitudes estrangeiras e comportamentos favoráveis aos objetivos de quem ordena a operação"[106].

Se retirarmos o termo "estrangeiro" a esta definição, esta representa exatamente o que foi feito pela Cambridge Analytica: selecionar e veicular informação de modo a jogar com as suas emoções, os seus medos, os seus perfis psicográficos, com o intuito de deturpar o raciocínio de parte do eleitorado americano, induzindo o dito "comportamento favorável" à campanha – eleger Donald Trump.

Tal como as operações psicológicas diferem das operações convencionais, também o "armamento" utilizado difere. Como indica a definição, nas operações psicológicas o armamento não consiste em armas de fogo ou explosivos, mas sim em informação. É por isso que importa compreender como é que a informação pode ser transformada em "arma" psicológica/política.

[106] "Psychological operations" *in* "Dictionary of Military and Associated Terms", Departamento de Defesa dos Estados Unidos, *Joint Publication* 1-02, 12 de abril de 2001, 427, https://www.cia.gov/library/abbottabad-compound/B9/B9875E9C2553D81D1D6E0523563F8D72_DoD_Dictionary_of_Military_Terms.pdf.

O facto de serem "armas" duma tipologia diferente não significa que não se possa pensar nelas como se pensa numa arma convencional – pelo menos nos aspetos mais básicos.

Se pensarmos num míssil, temos de pensar, entre várias outras coisas, na carga útil, no sistema de propulsão e no sistema de identificação de alvos. Num míssil, a carga útil é um explosivo, o sistema de propulsão pode ser um foguete e o sistema de identificação de alvos um satélite ou um sistema de infravermelhos guiado por calor.

Quando a arma é informação, temos os mesmos componentes (carga útil, sistema de propulsão e sistema de identificação de alvos), com a diferença de que esta não fará nada explodir (pelo menos no sentido literal). Com uma arma de informação, a carga útil é geralmente uma história, um rumor, uma narrativa diferente[107], o sistema de propulsão pode passar por artigos de jornal, peças televisivas, publicidade através dos vários canais de comunicação (internet e redes sociais incluídas) e o sistema de identificação de alvos pode passar por uma área geográfica circunscrita, uma faixa etária, uma etnia.

No caso da Cambridge Analytica, a carga útil consistiu em narrativas favoráveis a Donald Trump e danosas para Hillary Clinton; o sistema de propulsão assentou essencialmente nos anúncios no Facebook e o sistema de identificação de alvos passou simultaneamente pela categorização dos utilizadores em diferentes perfis psicológicos e pela potenciação da exposição a conteúdo do mesmo género presente nos algoritmos do Facebook.

Fazer da informação uma arma é uma tarefa complexa. Dado que o objetivo, geralmente, é desconstruir e manipular perceções públicas, é necessário um entendimento abrangente de como a população visada entende diversos temas, bem como o que as motiva ou demove, o que lhes incute medo ou o que lhes dá esperança.

Uma das práticas nas operações psicológicas e na manipulação de perceções consiste em substituir o autoconceito[108] – "a perceção que o indivíduo tem de si próprio e o conceito que,

[107] Wylie, *Mindf*ck*, 41.
[108] Wylie, *Mindf*ck*, 48.

devido a isso, forma de si (…)"[109], que "tem o condão de capturar e condensar motivos, necessidades, atitudes, valores e traços de personalidade"[110] – dos indivíduos visados por outro. Por outras palavras, tenta-se, através duma nova narrativa, levar os indivíduos a agir de forma diferente perante a realidade, mudando a forma como se compreendem a si próprios e como compreendem certos temas, nomeadamente políticos.

Por exemplo, pode-se tentar mudar a perceção de alguém face ao conceito de imigração. Um indivíduo pode ser indiferente à palavra, não pensar em nada negativo quando a ouve ou lê, ou mesmo considerá-la algo benéfico para a comunidade em que está inserido. Porém, se histórias que associam a prática de crimes aos imigrantes nessa comunidade começarem a circular, essa perceção pode alterar-se, e o indivíduo pode adotar comportamentos diferentes face a imigrantes, ter sentimentos negativos ao ver conteúdo relacionado com imigração, ou votar em quem prometa acabar com os problemas associados à mesma, mesmo que esses problemas sejam apenas parte duma narrativa falsa.

O modo como a alteração de perspetivas é habitualmente feita consiste em gradualmente quebrar fatores de resiliência psicológica na população visada, abafando uma narrativa e elevando outra, dominando a informação que circula, ao longo de vários meses, criando perceções irrealistas que vão confundindo os visados acerca do que pensar[111]. As novas narrativas encorajam então os visados a conjeturar cenários catastróficos resultantes de eventos menores ou imaginados[112]. Geralmente, este tipo de narrativas tenta também fomentar desconfiança e suspeita acerca de outras que possam ainda circular, de modo a mitigar as que possam interferir com a adoção dos novos conceitos por parte da população visada[113].

O objetivo final de tudo isto é despoletar emoções negativas e pensamentos associados a comportamento impulsivo, errático ou compulsivo, ou seja, levar os alvos de uma resistência

[109] Adriano Serra, "O auto-conceito", *Análise Psicológica*, 2 (VI), 1988: 101.
[110] Serra, "O auto-conceito", 109.
[111] Wylie, *Mindf*ck*, 48.
[112] Wylie, *Mindf*ck*, 48.
[113] Wylie, *Mindf*ck*, 48.

moderada ou passiva a comportamentos mais ativos ou mesmo disruptivos[114]. Os alvos mais suscetíveis são precisamente os que exibem traços de personalidade neurótica ou narcisista – os alvos preferidos da Cambridge Analytica – por tenderem a ser menos resilientes ao tipo de narrativas usadas em operações psicológicas[115].

Quando se faz guerra, tenta-se explorar fraquezas ou debilidades no inimigo para vencer. Quando se faz "guerra psicológica", quer seja em contexto de operações militares ou em contexto de campanha eleitoral, esse objetivo mantém-se, mas os pontos fracos são essencialmente vieses cognitivos, falhas no pensamento, irracionalidades. A racionalidade humana não abdica de algumas irracionalidades pelo meio. Porém, enquanto muitas são inofensivas, outras podem ser exploradas negativamente.

Se abordarmos alguém ao acaso e lhe perguntarmos se é feliz, é provável que nos responda que sim. No entanto, se de seguida perguntarmos se ganhou peso nos últimos tempos, ou se os colegas do secundário são mais bem-sucedidos e depois voltarmos a perguntar se é feliz, talvez esse alguém esteja menos inclinado a responder que sim. Nada na sua história mudou entretanto, apenas se mudou a informação que estava a considerar para responder à questão de se é feliz ou não e, consequentemente, a sua perspetiva face à sua própria felicidade.

Na Psicologia, chama-se a este método de fazer alguém considerar determinada informação face a um tema, dando mais peso a essa informação, "impulsão" ("*priming*")[116]. E é essencialmente através desta "impulsão" que se transforma a informação em "arma": descobre-se que em partes de um determinado tema se quer que os indivíduos pensem quando contactam com ele para afetar o modo como pensam e como se comportam.

Christopher Wylie relata que quando começou a fazer investigação sobre o eleitorado americano para a Cambridge Analytica uma das suas atividades favoritas era "observar e ouvir

[114] Wylie, *Mindf*ck*, 48.
[115] Wylie, *Mindf*ck*, 49.
[116] Wylie, *Mindf*ck*, 66.

os americanos que concordavam em gastar o seu tempo com ele"[117]. Sentava-se no sofá e ouvia as pessoas a falarem sobre o seu dia, sobre que tinham ouvido na rádio, ou sobre o trabalho. Observava-as a assistir ao canal televisivo Fox News e reparava em como se enfureciam enquanto o faziam.

"Era algo estranho, na medida em que se sentavam e aguardavam – com expectativa – para serem insultados com o que quer que fosse as 'elites' lhes tivessem feito naquele dia. Era mudarem para a Fox [News] e sua raiva tornava-se palpável. Às vezes eu parecia estar a observar uma sessão de terapia, como quando as pessoas destroem coisas numa sala de raiva [rage room] depois de uma semana frustrante.

(…) As pessoas sentiam-se melhor acerca do seu dia depois de uma sessão de uma hora na sala de raiva da Fox News – podiam aliviar o seu stress e no fim os seus problemas no trabalho ou em casa era culpa de outrem. Significava que as suas dificuldades podiam ser inteiramente externalizadas, poupando-as da dura realidade de que talvez o seu empregador não se importasse assim tanto com elas para lhes pagar um salário que lhes permitisse viver. Seria demasiado doloroso admitir que talvez alguém que viam todos os dias se estava a aproveitar delas em vez do inimigo sem cara que era o Obamacare e os [imigrantes] ilegais"[118].

Este relato é importante por um motivo em particular. Não se quer, por este relato, dizer que o eleitorado Republicano é mais ingénuo ou menos racional do que o eleitorado Democrata, mas é um testemunho daquilo em que se tornou o ecossistema dos *media* afetos à Direita nos Estados Unidos.

Yochai Benkler, Robert Faris e Hal Roberts, no seu livro "*Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*" concluíram que o ecossistema dos *media* afetos à Direita e o ecossistema dos media afetos à Esquerda se tornaram ambientes distintos um do outro.

No decorrer da sua investigação, acabaram por concluir que:

[117] Wylie, *Mindf*ck*, 75.
[118] Wylie, *Mindf*ck*, 76.

"O ecossistema dos media da Direita difere categoricamente do resto do ambiente dos media e que tem sido muito mais suscetível a desinformação, mentiras e meias-verdades. Em suma, descobrimos que a influência no ecossistema nos *media* da Direita (…) está, simultaneamente, altamente enviesada para a extrema-Direita e altamente isolada de outros segmentos da rede [dos media], desde o centro-Direita (que é praticamente inexistente) até à extrema-Esquerda.

(…) O comportamento do ecossistema dos *media* da Direita representa uma radicalização de cerca de um terço do sistema da comunicação social americano. Usamos o termo 'radicalização' cautelosamente em dois sentidos. Primeiro, porque falar de 'polarização' é assumir simetria. Nenhum facto emerge mais claramente da nossa análise de … quatro milhões de histórias políticas … ao longo de três anos … do que o de que não há simetria na arquitetura e dinâmica de comunicação dentro do ecossistema dos *media* de Direita e fora dele. Segundo, durante este período observámos repetidamente campanhas de humilhação pública e desinformação viciosa montadas pelos sites líderes nesta esfera contra indivíduos que eram pilares centrais da identidade republicana há uma mera década. (…) Esta radicalização foi conduzida por um grupo de sites extremistas incluindo a Breitbart, Infowars, Truthfeed, Zero Hedge, e Gateway Pundit, nenhum dos quais afirma seguir as normas ou processos da objetividade jornalística profissional. (…) até mesmo sites de Direita que afirmam seguir as normas jornalísticas, como a Fox News e Daily Caller, não o fazem de facto, e por isso falham em atuar como um travão nestes sites radicais. Na verdade, encontrámos repetidamente a Fox News a acreditar e a amplificar os excessos destes sites radicais. (…) Este padrão não se encontra espelhado na Esquerda. Primeiro, porque mesmo encontrando sites das franjas da Esquerda que espelham os sites radicais [de Direita], estes simplesmente não têm o mesmo tipo de visibilidade e proeminência na Esquerda como os outros têm na Direita. Segundo, os sites com mais visibilidade na Esquerda, como o Huffington Post, têm o seu pior espelho na Fox News, não no Gateway Pundit ou no Zero Hedge. E terceiro, todos estes sites na esquerda estão firmemente integrados com os principais sites tradicionais como o New York Times e o Washington Post e, a maioria destes sites, embora não todos, ou opera diretamente sob normas jornalísticas há muito estabelecidas ou são indiretamente sensíveis a críticas baseadas no jornalismo que adere a essas normas"[119].

"É a estrutura do ecossistema de comunicação social em que se encontram, por um lado, eleitores Republicanos, quer conservadores, quer radicais, e, por outro, políticos Republicanos, que os tornou particularmente suscetíveis a interpretações erradas e manipulação, enquanto o ecossistema de comunicação social que os Democratas e os seus apoiantes ocupam revelou características estruturais mais robustas perante esforços de propaganda e ofereciam mais caminhos para autocorreção e autorregeneração"[120].

[119] Yochai Benkler, Robert Faris e Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, (Oxford: Oxford University Press, 2018), 13-15.
[120] Benkler, Faris e Roberts, *Network Propaganda*, 99.

Em suma, as eleições presidenciais de 2016 parecem ter ocorrido num ambiente altamente favorável ao sucesso de esforços propagandísticos. O conteúdo criado com o intuito de difamar Hillary Clinton e enaltecer Donald Trump, de impelir determinadas franjas do eleitorado americano (comummente de Direita) a votar e de dissuadir outras (geralmente associadas à Esquerda) de o fazer chegava às redes sociais e não ficava dependente de quem o tinha originalmente publicado para circular por onde mais necessitava. Uma vez publicado, os próprios internautas faziam-no circular através de "gostos", partilhas e comentários, sem custos ou entraves e beneficiava ainda do ecossistema dos media afetos à Direita, que se terá extremado ao longo dos anos, no qual ganhava uma nova amplitude, transpondo o meio exclusivamente digital, podendo assim chegar aos eleitores que não frequentavam o mundo do digital.

Exploraremos, no subcapítulo seguinte, a hipótese duma ligação entre a Cambridge Analytica e a Rússia.

3.3. Ligação com a Rússia

Em primeiro lugar, é necessário dizer que, até ao momento, nenhuma das investigações sobre o papel da Rússia ou da Cambridge Analytica nas eleições presidenciais de 2016 encontrou provas de que estas tenham trabalhado em conjunto, ou de que uma das partes tenha usado informação conseguida pela outra.

"Se a Cambridge Analytica esteve envolvida nos esforços de desinformação russos nos Estados Unidos? Ninguém pode dizer com certeza, e não há uma única 'arma fumegante' que prove que a Cambridge Analytica foi a culpada, ajudada e incitada pela Rússia"[121].

Existem, no entanto, vários elementos que ligam os dois atores, embora nenhum desses elementos, ou o seu conjunto, prove uma colaboração entre os dois. Ainda assim, importa verificar que elementos são esses.

Primeiramente, o SCL Group e a Cambridge Analytica não eram desconhecidos dos russos. Segundo o *The Guardian*, a empresa petrolífera russa Lukoil assistiu, em 2014, a uma das apresentações da CA, na qual se falou sobre supressão de votos e direcionamento de conteúdo nas redes sociais durante períodos eleitorais[122]. Acrescem ainda o facto de o Diretor Executivo da petrolífera ser Vagit Alekperov, um ex-secretário de Estado do Ministério da Energia russo e a indicação do *The Guardian* de que a petrolífera já serviu como um "veículo de influência do governo"[123].

O segundo elemento prende-se com o investigador da Universidade de Cambridge que colaborou com a Cambridge Analytica, mencionado anteriormente. Aleksandr Kogan estava, como dito, a fazer investigação em território russo, numa universidade estatal russa, graças a uma bolsa de investigação concedida pelo Estado russo. Em entrevista à CNN, Kogan negou

[121] Wylie, *Mindf*ck*, 153.
[122] Carole Cadwalladr e Emma Graham-Harrison, "Cambridge Analytica: links to Moscow oil firm and St Petersburg university", *The Guardian*, 17 de março de 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-academic-trawling-facebook-had-links-to-russian-university.
[123] Cadwalladr e Graham-Harrison, "Cambridge Analytica: links to Moscow".

ter entregado dados a qualquer entidade russa. No entanto, isso não significa que entidades russas não possam ter acedido a esses mesmos dados. Damian Collins, Membro do Parlamento do Reino Unido e presidente da Comissão de Digital, Cultura, Media e Desporto, encarregue do inquérito parlamentar em que se investigaram as ações da Cambridge Analytica, disse em entrevista, também à CNN, que o Gabinete do Comissário de Informação confirma que "os dados de Facebook da Cambridge Analytica foram acedidos por pessoas na Rússia"[124]. Porém, não se sabe "quem foram, ao que acederam, se recolheram esses dados, ou o que fizeram com eles"[125].

Em terceiro lugar, há uma complexa rede de relações que vai interligando membros da campanha e da administração Trump à CA e à Rússia, mas sem se conseguir estabelecer uma relação direta entre as três – pelo menos, por enquanto. Um tal exemplo é o de Samuel Patten. Samuel Patten trabalhou como consultor político para a Cambridge Analytica entre 2014 e 2015, tendo depois fundado uma empresa de consultoria política com Konstantin Kilimnik, um dos suspeitos na investigação de Robert Mueller. A investigação não foi capaz de concluir se Kilimnik era ou não um "espião" russo, mas conseguiu apurar contactos entre Kilimnik e Serviços de Informação russos. Adicionalmente, Patten e Kilimnik tinham ainda relações profissionais com Paul Manafort, diretor de campanha de Donald Trump a partir de junho de 2016 (e colaborador com a mesma desde março desse ano). Paul Manafort, por sua vez, esteve ligado à campanha de Viktor Yanukovych, ex-Presidente da Ucrânia (2010-2014) e do seu partido pró-russo – Partido das Regiões. Samuel Patten ficou em liberdade condicional por três anos, Konstantin Kilimnik continua sem se apresentar a um tribunal americano e sem se declarar inocente ou culpado. Paul Manafort foi condenado a 47 meses de prisão por oito crimes (cinco de falsificação de declarações fiscais, dois de fraude bancária e um de omissão duma

[124] Damian Collins, *in* "Cambridge Analytica's Facebook data was accessed from Russia, MP says", *CNN*, vídeo, 00:29, 17 de julho de 2018, https://money.cnn.com/2018/07/17/technology/cambridge-analytica-data-facebook-russia/index.html.
[125] Collins, in "Cambridge Analytica's Facebook data was accessed from Russia", vídeo, 00:41.

conta bancária no estrangeiro), mas nenhum deles relacionado com a sua atividade enquanto diretor de campanha.

A relação (ou tentativa de relação) mais interessante, no entanto, será entre a Cambridge Analytica e o site WikiLeaks, canal de eleição para a divulgação dos materiais roubados pelos agentes russos. A relação só foi conhecida em outubro de 2017, quando o ex-Diretor Executivo da CA, Alexander Nix, disse ter tentado contactar o fundador, Julian Assange, para prestar assistência na divulgação dos e-mails de Hillary Clinton. Nix diz que Assange recusou a proposta de auxílio e Assange corrobora ter sido abordado por Alexander Nix e ter recusado a ajuda. Porém, a ex-Diretora de Operações da Cambridge Analytica e denunciante, Brittany Kaiser, diz ter transferido dinheiro em criptomoeda para a WikiLeaks, dinheiro esse que lhe teria sido entregue por terceiros, sob a forma de "presentes e pagamentos"[126]. Existe ainda o registo de um encontro de cerca de 20 minutos entre Brittany Kaiser e Julian Assange, em fevereiro de 2017, já a campanha e corrida eleitoral tinham terminado e Trump empossado 45.º Presidente dos Estados Unidos.

Novamente, nada do que aqui se encontra prova uma ligação deliberada ou esforços concertados entre a Rússia e a Cambridge Analytica. No entanto, as semelhanças entre os *modi operandi* dos dois atores na disseminação do conteúdo propagandístico com recurso principalmente às ferramentas do Facebook, bem como as investigações feitas, quer por órgãos de comunicação social, quer por órgãos de Justiça, identificaram indivíduos que, de uma forma ou de outra, são elos de ligação entre os dois atores, pelo que a hipótese de uma concertação entre os dois não pode (ainda) ser descartada, nem das investigações, nem desta dissertação.

No capítulo seguinte, debruçar-nos-emos sobre uma questão fundamental acerca da interferência nas eleições americanas: a plausibilidade da sua eficácia.

[126] Carole Cadwalladr e Stephanie Kirchgaessner,"Cambridge Analytica director 'met Assange to discuss US election'", *The Guardian*, 7 de junho de 2018, https://www.theguardian.com/uk-news/2018/jun/06/cambridge-analytica-brittany-kaiser-julian-assange-wikileaks.

4. O impacto da interferência: realidade ou exagero?

Como referido no capítulo anterior, não se encontraram provas de uma efetiva concertação entre a Rússia e a Cambridge Analytica. Identicamente não é possível provar que as ações de ambas tenham impactado as escolhas dos eleitores americano e, por isso, as opiniões dividem-se. Uns creem que o papel que ambos desempenharam foi crucial no desfecho das eleições; outros desvalorizam as ações desses dois atores e menosprezam a influência que possam ter tido, acreditando que, no final, as eleições teriam resultado, à mesma, na eleição de Donald Trump.

Não sendo possível provar de forma irrefutável que Rússia e Cambridge Analytica tenham de facto conseguido persuadir eleitores indecisos a votar em Trump, ou a levar "simpatizantes" a ir às urnas, ou a dissuadir quem costuma votar no partido Democrata de o fazer em 2016, podemos, pelo menos, tentar mostrar que é plausível que essa persuasão e dissuasão tenham ocorrido graças às campanhas que fizeram. Para tal, exporemos primeiro os argumentos que menorizam o impacto das ações russas; depois os que menorizam o da Cambridge Analytica e, por fim, tentaremos explicar porque é que, apesar desses argumentos, se deve manter a hipótese de que, de facto, tiveram impacto nestas eleições.

a) Argumentos contra o impacto da Rússia

O primeiro argumento contra o impacto da interferência russa prende-se com o número de publicações relacionados com a campanha eleitoral. Se tomarmos como numerador todas as publicações feitas nas redes sociais durante o período eleitoral e como denominador todas as publicações relacionadas com as eleições, o conteúdo propagandístico ligado ao Kremlin que

circulou durante esse tempo será necessariamente diminuto[127]. O Facebook usou este argumento em 2017: "o alcance de operações conhecidas durante as eleições de 2016 foi estatisticamente muito reduzido em comparação com a interação total com publicações políticas"[128].

O Twitter faria uma declaração semelhante em janeiro de 2018:

"conteúdo automatizado relacionado com as eleições e associado aos sinais [características] russos representou uma fração muito pequena da atividade geral no Twitter no período de dez semanas que precedeu a eleição de 2016 (…). Identificámos 13.512 contas adicionais, atingindo um total de 50.258 contas automatizadas que identificámos com ligações à Rússia e que tuitaram conteúdo relacionado com as eleições durante o período eleitoral, representando aproximadamente duas centésimas (0.016%) do total de contas no Twitter nessa altura"[129].

Holman Jenkins, colunista do Wall Street Journal, escreveu em 2018:

"Sejamos realistas: as atividades de propaganda russas detalhadas na acusação de Robert Mueller da semana passada tiveram menos impacto na eleição do que 20 segundos de cobertura de qualquer um dos comícios de Trump"[130].

Até mesmo Vladimir Putin prestaria declarações com base nesta lógica de que o volume de informação veiculada pela Rússia era tão significante quanto "uma gota no oceano", pelo que não poderia ter tido qualquer impacto:

[127] Jamieson, *Cyberwar*, 131.
[128] Jen Weedon, William Nuland e Alex Stamos, "Information operations and Facebook", Facebook Newsroom, Facebook, 27 de abril de 2017, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.
[129] "Update on Twitter's review of the 2016 US election", Twitter Public Policy, Twitter, atualizado a 31 de janeiro de 2018, https://blog.twitter.com/en_us/topics/company/2018/2016-election-update.html
[130] Holman Jenkins, "Mueller Focuses on Molehills", *Wall Street Journal*, 20 de fevereiro de 2018, https://www.wsj.com/articles/mueller-focuses-on-molehills-1519169467.

"A informação vinda de meios de comunicação como o Russia Today… verificou-se ser um centésimo percentual do fluxo de informação geral nos Estados Unidos, só um centésimo percentual. Acham que esta fração teve qualquer impacto na eleição? Isto é só absurdo, não veem?"[131]

Um outro argumento contra a influência russa é o de que os agentes russos fizeram um fraco trabalho a direcionar conteúdo. De novo, surge o Facebook a diminuir o papel das atividades russas, referindo que apenas "um quarto dos anúncios russos tinha alvos geográficos e houve mais [anúncios] em 2015 do que em 2016"[132].

O Senador Richard Burr (Republicano, Carolina do Norte) fez também uso desta linha argumentativa, uma vez que no Estado de Maryland, geralmente Democrata, se verificaram mais anúncios (262) do que no Estado de Wisconsin, muito disputado entre os dois partidos (apenas 55 anúncios)[133].

Patrick Ruffini, cofundador da Echelon Insights, uma empresa que fornece serviços de investigação e informação política, e estratega digital do Partido Republicano, fez também declarações que desvalorizam os esforços por parte da Rússia alicerçadas nos dois argumentos anteriores – quantidade de publicações insignificante quando vista no universo de todas as publicações feitas no Facebook e geograficamente mal direcionadas – acrescentando a sua perspetiva sobre o conteúdo das publicações russas e as quantias despendidas para o efeito da campanha de desinformação.

"Já dirigi campanhas de anúncios digitais em nome de candidatos em Estados contestados. (…) se os anúncios revelados (…) foram uma tentativa de influenciar a eleição, foram uma tentativa risivelmente mal-executada e falhada. O montante total gasto foi menos do que já vi despendido online em corridas congressionais competitivas. Os anúncios não foram bem direcionados para os Estados disputados mais decisivos. E o conteúdo foi criado para aliciar vozes extremistas nas franjas políticas, não eleitores persuadíveis indecisos entre Donald Trump e Hillary Clinton.

[131] Vladimir Putin, "Interview to American TV channel NBC", President of Russia, 10 de março de 2018, http://en.kremlin.ru/events/president/news/57027.
[132] Alex Stamos, "An Update On Information Operations On Facebook", Facebook Newsroom, Facebook, 6 de setembro de 2017, https://about.fb.com/news/2017/09/information-operations-update/.
[133] Richard Burr, "Statement of Chairman Richard Burr", Richard Burr: US Senator for North Carolina, 1 de novembro de 2017, https://www.burr.senate.gov/imo/media/doc/Chairman%27s%20SFR.pdf.

(…) o conteúdo russo era apenas uma pequena porção dos 33 biliões de publicações que os americanos viram nos seus feeds de notícias do Facebook entre 2015 e 2017. Qualquer sucesso que os anúncios tenham tido em termos de alcance parece ser atribuído à perseverança do seu esforço, com 80.000 publicações de Facebook no total. O Facebook reportou que um quarto dos anúncios nunca foi visto por ninguém. E – com uma visualização média de 220 publicações ao dia por utilizador – muitos dos restantes foram simplesmente vistos, passados e esquecidos.

Com 81 milhões de dólares gastos no Facebook pelas campanhas Trump e Clinton, maioritariamente para mobilizar os principais apoiantes a doar e a voluntariar-se, é improvável que uma pequena compra de seis dígitos [100.000 dólares] tenha virado a eleição. O esforço russo parece ainda menos influente quando se considera a pequena quantia gasta dirigida a Estados-chave contestados – 1.979 dólares em Wisconsin, 823 dólares em Michigan e 300 dólares na Pensilvânia. Duma perspetiva eleitoral, a campanha foi notoriamente pouco sofisticada"[134].

Estes argumentos, não devendo ser descartados, deixam de fora importantes componentes dos esforços russos. O conteúdo da campanha de desinformação não foi só disseminado nas redes sociais através de anúncios, nem uma comunicação eficaz está exclusivamente dependente da quantidade de vezes que é feita ou repetida. De fora estão também os materiais roubados e posteriormente divulgados e as páginas que personificavam figuras afetas ao Partido Republicano. Contudo, antes de nos adensarmos no que falta a estes argumentos, debrucemo-nos sobre aqueles que negam impacto da Cambridge Analytica.

b) Argumentos contra o impacto Cambridge Analytica

O principal argumento contra qualquer impacto que o trabalho da Cambridge Analytica possa ter tido nas presidenciais de 2016 vem de Aleksandr Kogan, o especialista em modelação computacional de traços psicológicos e professor da Universidade de Cambridge que colaborou

[134] Patrick Ruffini, "Why Russia's Facebook ad campaign wasn't such a success", *The Washington Post*, 3 de novembro de 2017, https://www.washingtonpost.com/outlook/why-russias-facebook-ad-campaign-wasnt-such-a-success/2017/11/03/b8efacca-bffa-11e7-8444-a0d4f04b89eb_story.html.

inicialmente com a CA. Kogan diz que os dados e o modelo de análise fornecidos à Cambridge Analytica não eram assim tão bons quanto se faz crer:

"A precisão destes dados foi extremamente exagerada. Na prática, o meu melhor palpite é de que éramos seis vezes mais propensos a estar totalmente errados sobre uma pessoa do que a estar totalmente certos acerca dela. Pessoalmente, não penso que micro-segmentação (*micro-targeting*) seja uma aplicação apropriada destes conjuntos de dados.

Só poderia ter prejudicado a campanha. O que a Cambridge Analytica tentou vender é magia. E afirmou que isto é incrivelmente exato e de que lhes conta tudo o que há para contar sobre alguém, mas a realidade é que não é assim. Se realmente olhar para as estatísticas, essas afirmações desmontam-se rapidamente"[135].

Embora Kogan tenha dito que o modelo desenvolvido não era adequado para fazer previsões individuais, em entrevista à CNN, disse que era bastante bom para analisar grupos.

"O caso de uso para estes dados (…) não é assim tão preciso, ao nível individual. Quando se olha para grupos, se quiser compreender qual é a personalidade de nova-iorquinos, é bastante bom"[136].

Por outras palavras, o que Kogan quer dizer é que os dados utlizados pela Cambridge Analytica para direcionar os seus anúncios eram sobretudo dados demográficos, usados há décadas em campanhas políticas. A CA, no entanto, acrescentava a questão dos perfis psicográficos nas suas apresentações, sem que estes fossem relevantes para o trabalho que a firma desenvolvia. Tratava-se, no fundo, de publicidade enganosa da parte da Cambridge Analytica.

A grande maioria dos restantes argumentos contra a eficácia da Cambridge Analytica, quer venham da comunidade científica da Psicologia ou da Ciência de Dados, ou da área do

[135] Matthew Weaver, "Facebook scandal: I am being used as scapegoat – academic who mined data", *The Guardian*, 21 de março de 2018, https://www.theguardian.com/uk-news/2018/mar/21/facebook-row-i-am-being-used-as-scapegoat-says-academic-aleksandr-kogan-cambridge-analytica.

[136] Donie O'Sullivan, "Scientist at center of data controversy says Facebook is making him a scapegoat", *CNN*, vídeo, 1:26, 20 de março de 2018, https://money.cnn.com/2018/03/20/technology/aleksandr-kogan-interview/index.html.

marketing digital, andam em torno deste ponto: o Facebook é uma ótima ferramenta para recolher dados gerais, sobre comunidades, sobre grupos. É também uma ferramenta eficaz para recolher informação sobre preferências dos utilizadores enquanto consumidores de bens e serviços e para os bombardear com publicidade sobre produtos que tenham pesquisado. Será, no entanto, ineficaz para tirar conclusões e prever comportamentos de indivíduos específicos.

Existe ainda um outro argumento, mas que não é propriamente contra a eficácia da Cambridge Analytica. É antes um argumento contra as ações da Cambridge Analytica serem objeto de escândalo, uma vez que os Democratas também usaram o Facebook para recolher dados sobre o eleitorado, muito antes da candidatura de Donald Trump ou do aparecimento da Cambridge Analytica. Tratemos já da sua refutação.

Com efeito, os Democratas usaram o Facebook como um espaço de campanha logo em 2008, na primeira corrida presidencial de Barack Obama em 2008, e voltaram a usá-lo dessa forma e como meio de obtenção de dados sobre o eleitorado na campanha de reeleição em 2012. Porém, a ausência de escândalo pode ser explicada de forma simples: os dados foram recolhidos com uma aplicação criada pela própria campanha, só se podia aceder à aplicação visitando páginas da campanha, a aplicação estava em conformidade com os termos de serviços do Facebook e, tanto quanto se sabe, a informação recolhida nunca foi vendida ou dada a terceiros[137]. Já a Cambridge Analytica obteve os dados dos utilizadores do Facebook por intermédio do Professor Aleksandr Kogan, a quem tinha sido concedido o acesso aos dados para fins de investigação académica, não para fins políticos. Quando os utilizadores deram à aplicação da campanha Obama as permissões de acesso aos seus dados, sabiam que o propósito era político. Quando deram permissões à aplicação de Kogan, tudo o que lhes era dito era que estavam a participar num estudo de personalidade da Universidade de Cambridge, e nunca que os seus dados seriam usados pela campanha Trump.

[137] Clarence Page, "Why nobody complained when Obama used Facebook data", *Chicago Tribune*, 23 de março de 2018, https://www.chicagotribune.com/columns/clarence-page/ct-perspec-page-facebook-zuckerberg-obama-20180323-story.html.

Trataremos, de seguida, das falhas dos argumentos anteriores, para tentarmos explicar porque é que se deve manter a hipótese de que a interferência russa e as ações da Cambridge Analytica podem ter influenciado o comportamento do eleitorado norte-americano. Começaremos com a desconstrução dos argumentos contra o impacto da Rússia.

c) Problemas nos argumentos contra o impacto da Rússia

O primeiro problema com o argumento da "quantidade" de propaganda é que deixa de fora a questão da "qualidade" da comunicação. Ora, é consensual na comunidade científica da área da Comunicação, sobretudo na Comunicação Política e na Comunicação em Massa, que a eficácia das mensagens não reside na sua repetição *ad nauseam*. A comunicação política é eficaz quando consegue três resultados favoráveis de três efeitos da comunicação.

O primeiro efeito é o do agendamento ("agenda setting"). O agendamento refere-se à ideia de que há uma forte correlação entre o enfâse que os *media* dão a determinados assuntos e a importância atribuída a esses assuntos pelas audiências[138]. Ou seja, quer-se que os *media* deem ênfase a assuntos em que o candidato tem uma imagem positiva.

O segundo efeito é o do "priming", de que já falámos no capítulo anterior. Tínhamos dito que "priming", na Psicologia, era fazer alguém considerar determinada informação face a um tema em detrimento doutra, dando mais peso a essa informação nas avaliações que faz. Na literatura sobre Comunicação Política é semelhante: "priming" refere-se a mudanças nos critérios que as pessoas usam para fazer avaliações políticas e ocorre quando o conteúdo

[138] Dietram Scheufele e David Tewksbury, "Framing, Agenda Setting, and Priming: The Evolution of Three Media Effects Models", *Journal of Communication* 57, nº1 (março de 2007): 11.

noticioso sugere à audiência que esta deverá usar assuntos específicos como referência para avaliar o desempenho de líderes políticos e governos[139].

O terceiro efeito é o do enquadramento ("framing"). O enquadramento baseia-se na ideia de que a forma como determinado assunto é caracterizado ou apresentado em notícia pode ter influência no modo como é compreendido pelo público e refere-se aos modos de apresentação que jornalistas e outros comunicadores utilizam para apresentar a informação duma maneira que ressoe com as noções existentes que o público terá sobre os temas objeto de notícia[140]. Novamente, o objetivo dos candidatos é que os enquadramentos feitos pelos *media* não os coloquem sob uma luz negativa; se fizerem exatamente o contrário, tanto melhor.

A investigação científica feita sobre comunicação política e estes efeitos tem, repetidamente, indicado que o modo como a comunicação política é depois tratada pelos órgãos de comunicação social influencia a perceção pública, podendo mesmo direcionar as intenções de voto de alguns eleitores. Por outras palavras, não importa tanto "o quanto se diz"; importa sim "o que se diz" e, ao que tudo indica, importa ainda mais "como se diz".

"Os que alegam que os trolls, bots e hackers ligados ao Kremlin não poderiam ter afetado votos suficientes para virar uma eleição renhida estão a remar contra correntes de conhecimento académico que demonstram que as audiências são influenciadas por agendamento, enquadramento e 'priming'. Comentadores que contestam que o conteúdo impostor não poderia ter mobilizado ou desmobilizado eleitores estão a voar contra o vento, [vento esse] criado por investigação que confirma que eleitores podem ser influenciados pelo peso relativo de mensagens em notícias e anúncios. Nunca todos os eleitores. E na maioria dos casos, nem a maioria dos eleitores. Mas havia mais eleitores suscetíveis em 2016 do que em anos anteriores por três razões que se sobrepõem: (1) um incomum nível elevado de desapego com os nomeados dos dois partidos principais; (2) uma percentagem acima da média de eleitores independentes, com 39% do eleitorado a identificar-se dessa forma em 2016; e (3) uma proporção da população maior do que o normal – tantas quanto uma em cada oito pessoas – a só tomar uma decisão na última semana antes da eleição"[141].

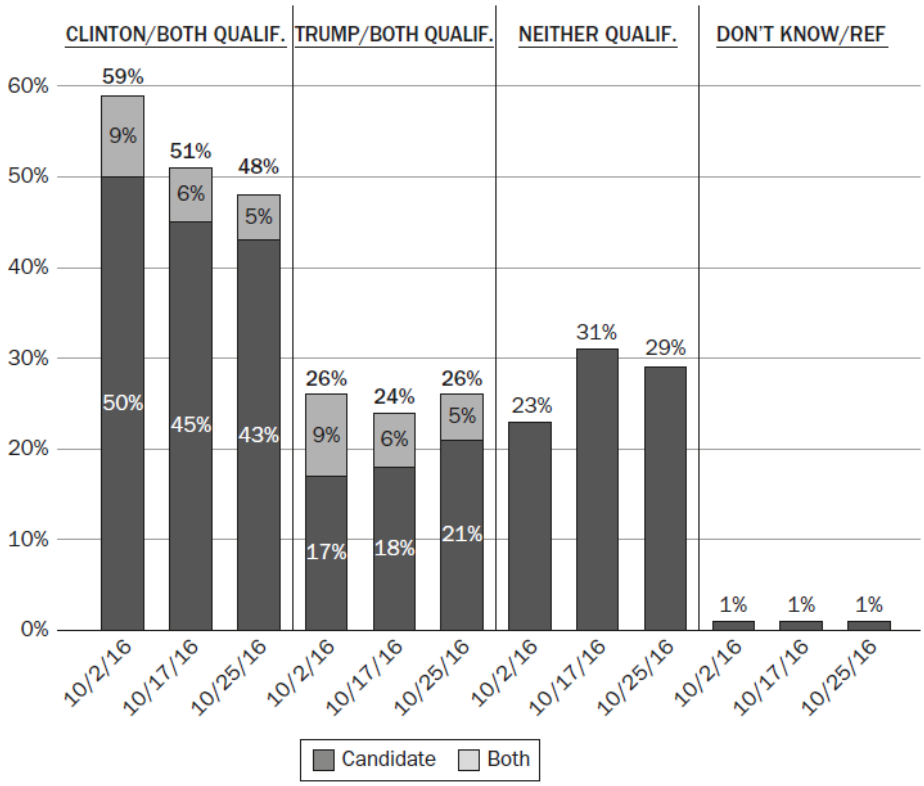
[139] Scheufele e Tewksbury, "Framing, Agenda Setting, and Priming": 11.
[140] Scheufele e Tewksbury, "Framing, Agenda Setting, and Priming": 9
[141] Jamieson, *Cyberwar*, 38.

O segundo problema com o argumento da quantidade vem das publicações que estão a ser consideradas quando se invoca esse argumento, uma vez que na maioria das vezes que este foi utilizado só se contabilizaram os anúncios. As atividades russas não se limitaram a anúncios ou publicações promovidas. Para além dos anúncios e das promoções, havia ainda contas falsas que personificavam cidadãos americanos que não existiam e personalidades ligadas ao Partido Republicano. Havia ainda grupos de Facebook que chegavam às centenas de milhares de membros, nos quais se podia publicar conteúdo sem se ter de gastar um único cêntimo. Esta possibilidade coloca em causa o argumento do dinheiro gasto pela Rússia no Facebook, uma vez que há muito que se pode publicar nas redes sociais sem se fazer qualquer pagamento e ainda assim ter um alcance significativo.

Por fim, os argumentos contra o impacto da interferência russa costumam também deixar de parte a divulgação dos e-mails roubados aos Democratas. Estes desempenham um papel importante, uma vez que durante campanha serviram para abafar polémicas com Donald Trump, denegrir Hillary Clinton e foram, durante esse período, sempre associadas à WikiLeaks ou à persona Guccifer 2.0 que se julgava atuar por conta própria, e nunca a esforços do Kremlin.

Análises da alteração da perceção pública sobre os dois candidatos presidenciais durante o mês de outubro revelam que, ao longo deste período, a perceção pública acerca de Hillary foi piorando, enquanto a de Trump foi melhorando.

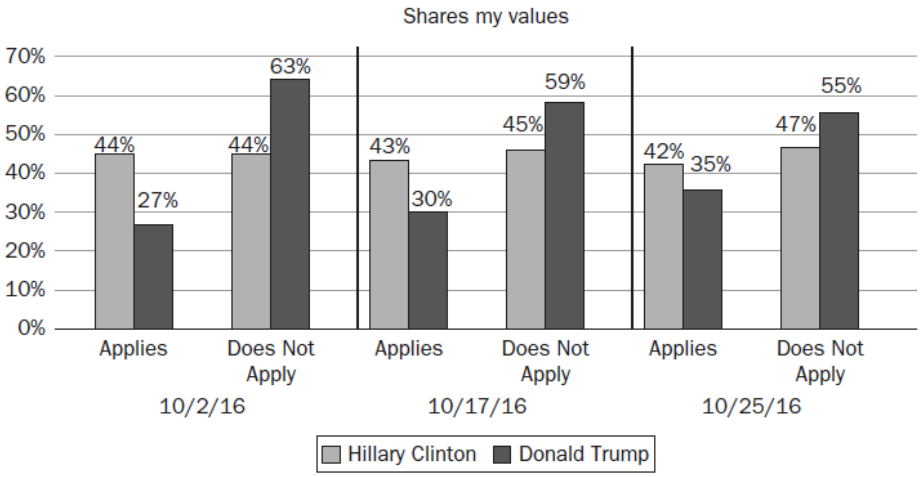
Gráfico 1



Fonte: Jamieson, *Cyberwar*, "Appendix 1: Changes in Perceptions of Clinton and Trump in October", 229.

No primeiro gráfico podemos verificar que a percentagem dos que consideravam Hillary Clinton qualificada para o cargo de Presidente diminuiu, entre 2 e 25 de outubro de 2016, de 50% para 43%. Embora a percentagem dos que julgavam Donald Trump qualificado para a Presidência fosse muito mais baixa, o gráfico indica, no mesmo período, um crescimento de 4% (de 17% para 21%) entre os eleitores que o julgavam apto para governar. Nesse período resceu também a percentagem de eleitores que julgava os dois candidatos inaptos para a Presidência (de 23% para 29%).

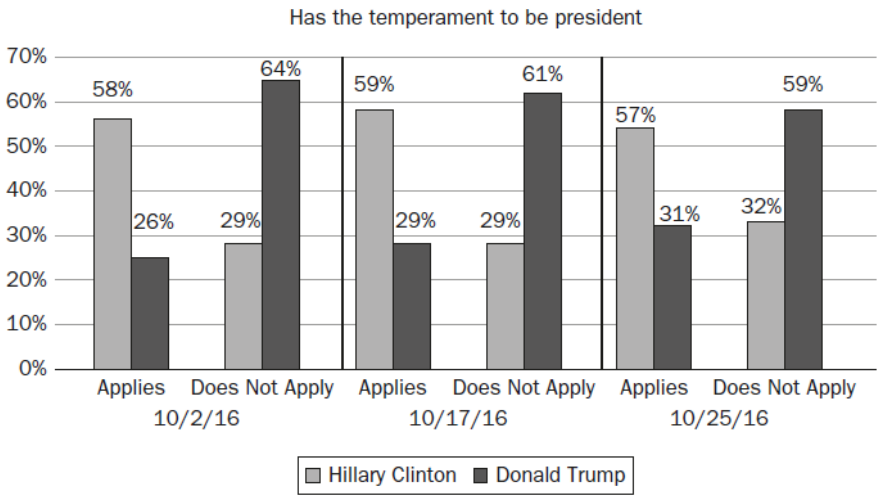
Gráfico 2



Fonte: Jamieson, *Cyberwar*, "Appendix 1: Changes in Perceptions of Clinton and Trump in October", 231.

O segundo gráfico representa a opinião pública acerca da partilha de valores com os candidatos. Hillary começa com 44% do eleitorado a considerar que a candidata partilha dos seus valores, tendo uma descida de 2% ao longo do mês de outubro. Trump, por outro lado, tem uma subida de 8% (27% para 35%) no mesmo período. Na parte em que a partilha de valores entre candidato e eleitorado "não se aplica", Clinton sobe 3% (mais eleitores creem que não partilham valores com Hillary Clinton) e Trump desce outros 8% (menos eleitores discordam de não partilharem valores com Donald Trump).

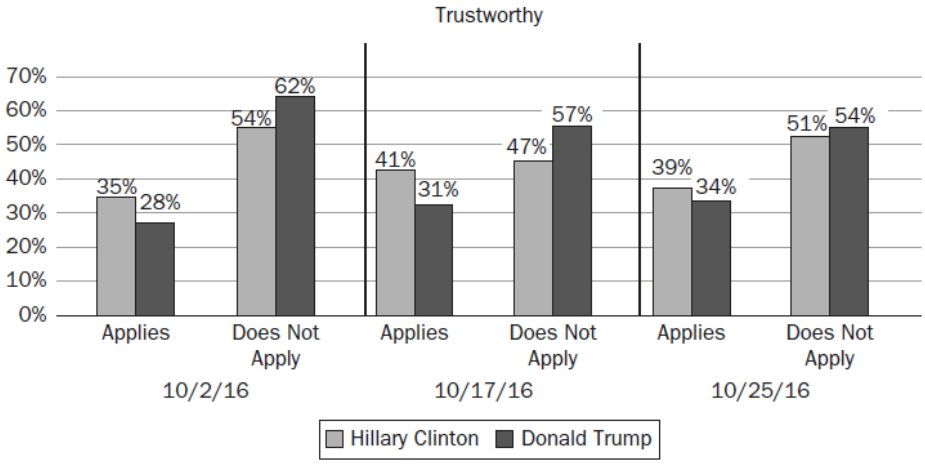
Gráfico 3



Fonte: Jamieson, *Cyberwar*, "Appendix 1: Changes in Perceptions of Clinton and Trump in October", 231.

Relativamente ao temperamento para ser Presidente, houve pequenas oscilações na perceção do eleitorado acerca do temperamento de Hillary Clinton no mês de outubro, com um decréscimo global de 1% na opinião de que a candidata democrata dispunha do temperamento certo para a Presidência. Trump, por outro lado, terá convencido mais 5% do eleitorado de que tinha o temperamento adequado para ser Presidente dos EUA.

Gráfico 4



Fonte: Jamieson, *Cyberwar*, "Appendix 1: Changes in Perceptions of Clinton and Trump in October", 232.

Aqui, procurou-se representar a perceção do eleitorado acerca da sua confiança nos candidatos. Hillary tem uma subida entre 2 e 17 de outubro, subindo dos 35% para os 41%, mas fica pelos 39% a 25 desse mês, descendo 2% em relação ao pico, acabando por ter uma subida global de 4%. Trump, por sua vez, parece mostrar-se cada vez digno de confiança aos olhos do eleitorado americano, sem descidas nas datas de avaliação indicadas, crescendo 6%, de 28% para 34%. Ao longo do mês de outubro, os dois candidatos terão também conseguido diminuir a percentagem de eleitores que não os julgava merecedores de confiança, com Clinton a obter uma descida global de 3% e Trump a ter uma descida global de 8%.

Quadro 1

	Clinton Traits				Trump Traits			
	Temperament	Trustworthy	Shares my values	Strong leader	Temperament	Trustworthy	Shares my values	Strong leader
Viewed debate 3	6.04	4.16	4.54	5.45	4.04*	4.69***	4.56***	5.48**
Did not view debate 3	5.57	3.68	4.12	5.08	3.50	3.68	3.53	4.77
N	932	932	932	932	932	932	932	932
Viewed debate 2	6.55	4.77	5.02	5.85	3.42	3.76	3.74**	4.55
Did not view debate 2	5.72	4.22	4.48	5.52	3.56	3.78	3.53	4.91
N	883	883	883	883	883	883	883	883

***p<.001, **p<.01, *p<.05.

Fonte: Jamieson, *Cyberwar*, "Appendix 2: Debate 2 and Debate 3 Exposure Effect on Candidate Trait Evaluations", 235.

O quadro acima mostra diferenças na opinião pública acerca de traços positivos dos candidatos dois grupos: assistentes e não-assistentes do segundo debate presidencial e assistentes e não assistentes do terceiro debate presidencial, que tiveram lugar a 9 e a 19 de outubro de 2016, respetivamente. A avaliação foi feita numa escala de 0 a 10 em que 0 significa que o eleitor não reconhece determinado traço positivo no candidato e 10 significa que concorda absolutamente com a presença desse traço no candidato.

Segundo este quadro, quem assistiu aos debates tem, regra geral, uma melhor opinião acerca de qualquer um dos dois candidatos do que quem não assistiu. No entanto, a opinião pública acerca dos dois candidatos parece seguir trajetórias diferentes à medida que os debates se realizam. O reconhecimento de traços positivos em Hillary Clinton decresce no terceiro debate face ao segundo, enquanto a identificação desses traços em Trump melhora consideravelmente com os debates. Trump estava atrás de Hillary Clinton em todos os traços no segundo debate presidencial e no terceiro supera-a em quase todos, ficando aquém apenas no "Temperamento".

Quadro 2

	Clinton Traits				Trump Traits				
	Corrupt	Liar	Mentally unstable	Says one thing in public and something else in private	Corrupt	Liar	Tax dodger	Mentally unstable	Says one thing in public and something else in private
Viewed debate 3	5.93	6.18	3.33	6.80*	4.51*	5.32	5.69	4.79	5.12**
Did not view debate 3	6.00	6.39	3.66	6.45	5.10	5.60	6.15	4.83	5.81
N	932	932	932	932	932	932	932	932	932
Viewed debate 2	5.35	5.60	3.27	6.41**	5.06	5.76	5.78*	5.25	5.66
Did not view debate 2	5.58	5.94	3.78	5.95	4.94	5.64	6.15	5.15	5.74
N	883	883	883	883	883	883	883	883	883

**p<.01, *p<.05.

Fonte: Jamieson, *Cyberwar*, "Appendix 2: Debate 2 and Debate 3 Exposure Effect on Candidate Trait Evaluations", 236.

De seguida, fez-se uma avaliação semelhante à do quadro apresentado antes deste, mas agora acerca de traços negativos reconhecíveis nos candidatos.

Novamente, os debates parecem contribuir para melhorar a opinião pública acerca dos candidatos, na medida em que quem não assistiu aos debates reconheceu mais traços negativos em Clinton e em Trump. Contudo, sucede-se o mesmo fenómeno que sucedeu acerca dos traços positivos, ou seja, trajetórias diferentes na opinião pública à medida que os debates se concretizam. Entre o terceiro e o segundo debates, a propensão para achar Hillary Clinton corrupta, mentirosa, mentalmente instável e que diz uma coisa em público e outra em privado aumenta; e a propensão para a identificação desses traços em Donald Trump diminui.

Quadro 3

	Clinton Traits				Trump Traits			
Debate-Viewing Index†	Temperament	Trustworthy	Shares my values	Strong leader	Temperament	Trustworthy	Shares my values	Strong leader
Viewed debate 3 and debate 2 or debate 3 only (2)	6.22	4.27	4.64	5.53	3.98**	4.60***	4.52***	5.39***
Viewed debate 2 only (1)	6.20	4.45	4.79	5.67	3.52	3.91	3.78	4.78
Viewed neither debates 2 nor 3 (0)	5.75	4.15	4.39	5.36	3.49	3.63	3.51	4.64
N	1,839	1,839	1,839	1,839	1,839	1,839	1,839	1,839

† Debate-viewing index defined: 0 = Viewed neither debate 2 nor 3; 1 = Viewed debate 2 only; 2 = Viewed debate 3 AND debate 2 / viewed debate 3 ONLY.
***p<.001, **p<.01

Fonte: Jamieson, *Cyberwar*, "Appendix 3: Association between Perception Changes and Vote Intentions", 242.

O que se procura evidenciar neste novo quadro é o impacto da assistência aos debates na identificação de traços positivos nos candidatos. Difere dos dois quadros anteriores no tipo de divisão que se faz do eleitorado. Nos dois quadros anteriores, a distinção era entre assistentes e não-assistentes do segundo e terceiro debates, respetivos a cada debate. A agregação e divisão aqui são diferentes, uma vez que se agrupa quem assistiu ao segundo e terceiro debates (e quem só assistiu ao terceiro) e se separa quem só viu o segundo debate e ainda quem não viu nenhum dos dois.

Mais uma vez, a informação apresentada indica que assistir aos debates contribui para uma melhor imagem dos candidatos, dado que quem assiste é mais propenso a identificar traços positivos do que quem não assistiu. Porém, a tendência anteriormente verificada também se mantém: a propensão para a identificação dos traços positivos enunciados diminui para Hillary Clinton do segundo para o terceiro debate (com exceção no "Temperamento") e aumenta para Donald Trump.

Quadro 4

	Clinton Traits				Trump Traits				
Debate-Viewing Index[†]	Corrupt	Liar	Mentally unstable	Says one thing in public and something else in private	Corrupt	Liar	Tax dodger	Mentally unstable	Says one thing in public and something else in private
Viewed debate 3 and debate 2 or debate 3 only (2)	5.87	6.09	3.31	6.82**	4.60*	5.37*	5.63	4.85	5.14***
Viewed debate 2 only (1)	5.51	5.81	3.29	6.38	4.96	5.70	5.92	5.13	5.63
Viewed neither debates 2 nor 3 (0)	5.72	6.07	3.81	6.25	5.03	5.58	6.00	4.99	5.81
N	1,839	1,839	1,839	1,839	1,839	1,839	1,839	1,839	1,839

[†] Debate-viewing index defined: 0 = Viewed neither debate 2 nor 3; 1 = Viewed debate 2 only; 2 = Viewed debate 3 AND debate 2 / viewed debate 3 ONLY.

***p<.001, **p<.01, *p<.05.

Fonte: Jamieson, *Cyberwar*, "Appendix 3: Association between Perception Changes and Vote Intentions", 243.

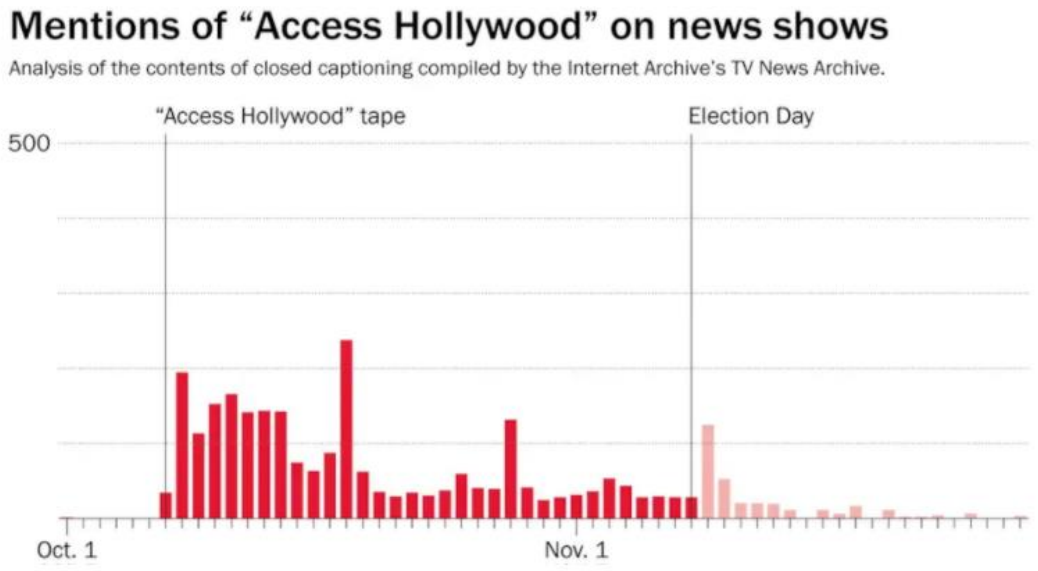
Neste último quadro voltamos à perceção de traços negativos nos candidatos, mas com o "novo" agrupamento da amostra que já referimos no quadro anterior.

A tendência verificada nos quadros anteriores mantém-se. Com o terceiro debate, aumenta a propensão para a associação de traços negativos a Hillary Clinton e, concomitantemente, essa mesma propensão diminui para Donald Trump.

As mudanças na perceção pública durante o mês de outubro são particularmente relevantes porque outubro, para além de representar a reta final antes da eleição, foi o mês em que ocorreram, de parte a parte, as divulgações dos conteúdos mais prejudiciais para ambos os candidatos. Como já foi referido, no dia 7 de outubro foi feita uma declaração conjunta pelo Departamento de Segurança Interna dos EUA e pelo gabinete do Diretor de Informação Nacional acerca das operações russas, que acabou por ser abafada pela publicação do vídeo "Access Hollywood tape", o tal, em que Donald Trump se gaba de conduta sexual imprópria com mulheres e que por sua vez foi contrabalançada com a divulgação dos e-mails do diretor de campanha de Clinton, John Podesta, através da WikiLeaks.

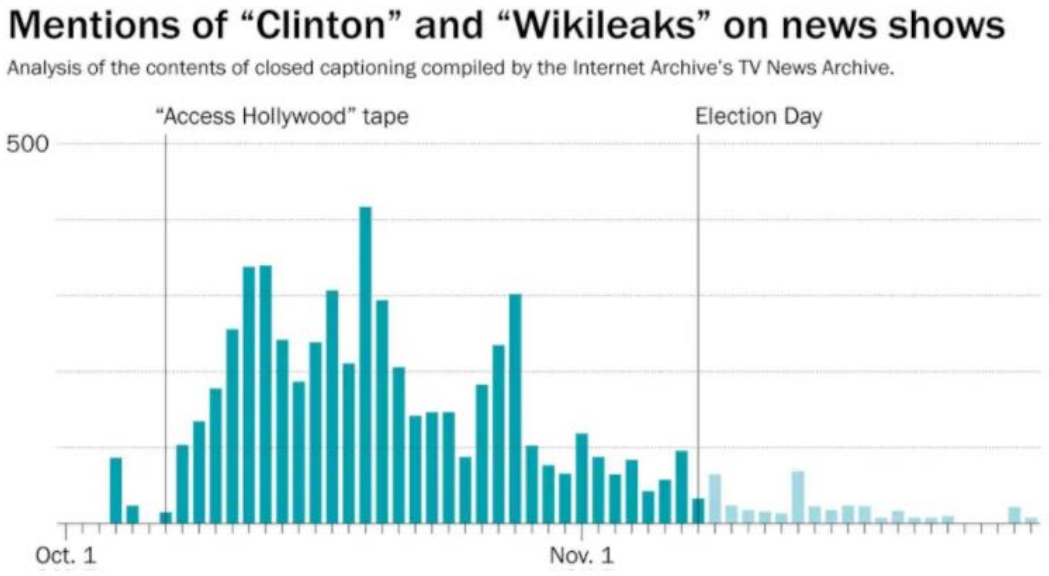
A comunicação social, no entanto, não tratou estes eventos de forma igual. Segundo o Washington Post, os materiais danosos para a campanha de Hillary Clinton acabaram por ser objeto de muito mais tempo de antena do que os que poderiam prejudicar Donald Trump.

Gráfico 5



Fonte: Philip Bump, "Actually, the Mueller report showed that Russia did affect the vote", *The Washington Post*, 19 de abril de 2019, https://www.washingtonpost.com/politics/2019/04/19/actually-mueller-report-showed-that-russia-did-affect-vote/.

Gráfico 6



Fonte: Philip Bump, "Actually, the Mueller report showed that Russia did affect the vote", *The Washington Post*, 19 de abril de 2019, https://www.washingtonpost.com/politics/2019/04/19/actually-mueller-report-showed-that-russia-did-affect-vote/.

A divulgação dos e-mails do diretor de campanha de Hillary Clinton, John Podesta, através da WikiLeaks, parece ter tido o efeito desejado no agendamento da comunicação social. A maior ênfase dada pelos *media* a materiais que prejudicavam a imagem de Hillary Clinton em detrimento dos podiam prejudicar Trump poderá ter conduzido o eleitorado a ficar com uma imagem mais negativa de Clinton do que Trump, pesando nas intenções de voto.

Passemos, então aos problemas com os argumentos que contestam o impacto da Cambridge Analytica.

d) Problemas nos argumentos contra o impacto da Cambridge Analytica

O argumento de que os dados recolhidos no Facebook eram insuficientes ou ineficazes para fazer previsões ao nível individual não pode ser descartado, uma vez que é apresentado não só por Aleksandr Kogan, mas é também suportado pela comunidade científica. Ainda assim, devemos manter presente que o Facebook é uma ferramenta eficaz para recolher dados mais gerais, sobre grupos ou comunidades. A possibilidade de traçar perfis psicográficos individuais através da recolha destes dados pode ter sido apenas "publicidade enganosa" por parte da CA, mas isso não invalida que a Cambridge Analytica tenha sido capaz de fornecer à campanha Trump um valioso contributo sobre como tirar partido das redes sociais para fazer campanha política, direcionando anúncios com base nos dados demográficos recolhidos no Facebook. Há quem coloque a hipótese de que, entre 2008 e 2016, os Democratas tiveram uma clara vantagem sobre os Republicanos na compreensão de como usar os meios digitais para

fazer campanha, algo que se poderia atribuir a uma "falta de talento digital entre os Republicanos"[142], segundo um membro da campanha de Obama em 2012.

Devemos também manter presentes outros dois aspetos.

Primeiro, o interesse da parte dos implicados no escândalo da Cambridge Analytica, como o Facebook e Aleksandr Kogan, em passar a ideia de que o Cambridge Analytica fez com os dados foi insignificante em termos eleitorais, uma vez que estava em causa a recolha de dados e o seu uso sem autorização dos utilizadores. Se os "gostos" do Facebook não permitem traçar perfis psicográficos rigorosos e fazer previsões comportamentais ao nível individual também rigorosas, então o estudo de Aleksandr Kogan e dos seus colegas, publicado sob o título "Computer-based personality judgments are more accurate than those made by humans" terá exagerado largamente o que é possível fazer com informação recolhida do Facebook nos campos da Psicologia e Psicografia. Se, pelo contrário, esses dados permitem traçar esses perfis e prever comportamentos individuais com rigor, então a mentira vem do Facebook, de Kogan, que diz agora algo diferente do que disse no seu estudo de 2014, e da comunidade científica. Porém, tendo em conta que a comunidade científica é largamente cética de que tal possa ser feito com esses dados, é mais provável que o estudo de Kogan tenha exagerado as potencialidades da análise psicográfica com base em dados recolhidos nas redes sociais. A verdade continua, no entanto, por apurar.

O segundo aspeto é que não nos é possível saber se a CA usou os dados apenas como tinham sido tratados por Kogan ou se estes passaram por mais processos de refinamento nos escritórios da firma. As fontes não são claras relativamente a essa parte. Os dois denunciantes, Christopher Wylie e Brittany Kaiser, mencionam Aleksandr Kogan e os dados que este forneceu à Cambridge Analytica. Os dois mencionam também "testes domésticos", que fazem parecer crer que os dados fornecidos por Kogan foram um ponto de partida e que depois os dados foram

[142] Jennifer Moire, "Facebook App Proves A Game-Changer for Obama Campaign", *Adweek*, 21 de novembro de 2012, https://www.adweek.com/digital/facebook-app-obama-campaign/.

tratados pelos cientistas de dados da Cambridge Analytica, sem o envolvimento de Kogan. As várias investigações sobre a CA também não oferecem clareza sobre este ponto.

Adicionalmente, a CA alega ter eliminado todos os dados recolhidos mesmo antes de colaborar com a campanha Trump, logo em 2015, mas em março de 2018 foram divulgados, por uma fonte próxima da Cambridge Analytica, dados pessoais de 136 mil utilizadores americanos, do Estado do Colorado, recolhidos ainda em 2014[143].

Há ainda a alegação da denunciante Brittany Kaiser de que a Cambridge Analytica esteve envolvida em 44 campanhas eleitorais das eleições intercalares nos Estados Unidos, das quais terá vencido 33[144]. Um sucesso de 75% em campanhas, sendo verdadeiro, é, no mínimo, impressionante, ainda para mais tratando-se duma firma que não tinha experiência nos EUA.

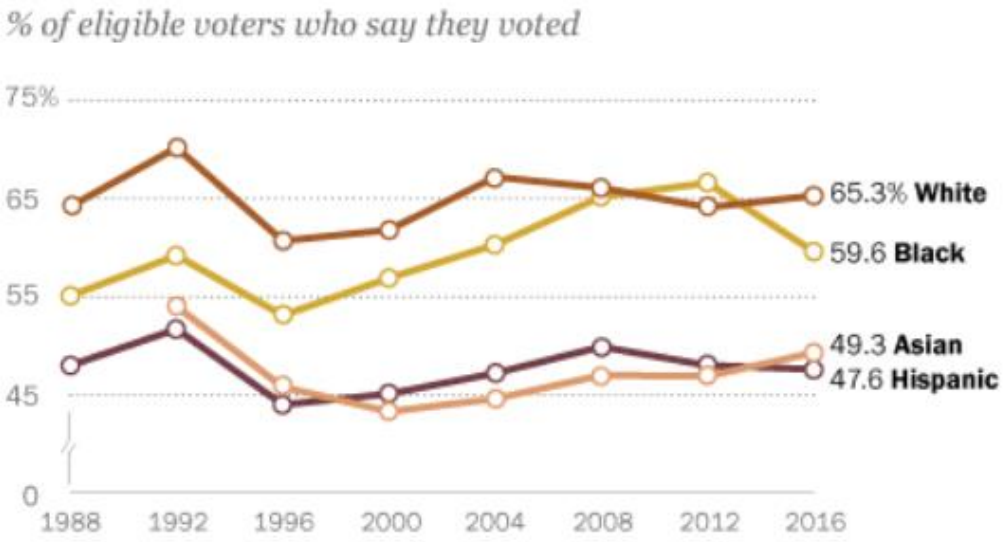
Resumindo, é possível que a CA não fosse capaz de traçar perfis psicográficos e com eles fazer previsões precisas acerca de indivíduos com base naquilo que recolhia acerca dos mesmos no Facebook. É, no entanto, possível que a Cambridge Analytica tenha trazido ao Partido Republicano e à campanha Trump novas capacidades no domínio digital, nivelando a disparidade do uso desse meio entre os dois partidos, ou mesmo levando os Republicanos a suplantarem os Democratas nesse domínio, tal como é possível que a CA seja uma empresa altamente eficaz a nível de comunicação. A comunicação eficaz conjugada com um melhor uso dos recursos digitais disponíveis podem ter desempenhado um importante papel na vitória de Donald Trump.

Resta-nos, neste capítulo, comparar a distribuição demográfica dos votos da eleição presidencial de 2012 com a distribuição demográfica dos votos da eleição de 2016, com o intuito de mostrar que é plausível que as atividades da Rússia e da Cambridge Analytica tenham tido os efeitos desejados. Ao fazê-lo, relembremos que fazia parte da estratégia da campanha Trump (inclua-se aqui a CA) e do Kremlin a mobilização de mais eleitorado branco (veteranos

[143] "Revealed: Cambridge Analytica data on thousands of Facebook users still not deleted", *Channel 4 News*, 28 de março de 2018, https://www.channel4.com/news/revealed-cambridge-analytica-data-on-thousands-of-facebook-users-still-not-deleted.
[144] Kaiser, *Targeted*, 42.

e cristãos, sobretudo cristãos evangélicos, comummente associados à Direita) e a desmobilização de eleitorado tradicionalmente democrata, como negros e latinos.

Gráfico 7



Fonte: Jens Krogstad e Mark Lopez, "Black voter turnout fell in 2016, even as a record number of Americans cast ballots", Fact Tank, Pew Research Center, 12 de maio de 2017, https://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/.

As sondagens pós-eleições dão fundamento ao impacto da interferência russa e da atividade da Cambridge Analytica. O gráfico acima indica que, como pretendido, houve um aumento ligeiro da população branca votante, uma pequena diminuição da população latina e uma acentuada descida de 7% da participação negra.

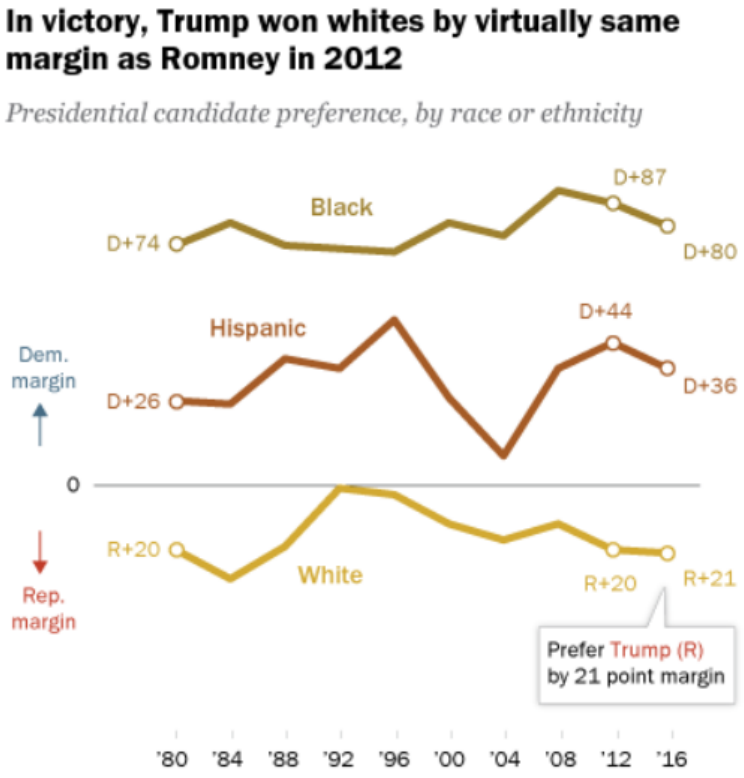
Uma outra análise, do New York Times, publicada em 2018, indica que, globalmente, 9% dos que votaram em Obama em 2012 mudaram o seu voto para Trump em 2016, 7% não votaram e 3% terá votado por um terceiro candidato (como Jill Stein)[145].

[145] Sean Mcelwee *et al.*, "The Missing Obama Millions", *The New York Times*, 10 de março de 2018, https://www.nytimes.com/2018/03/10/opinion/sunday/obama-trump-voters-democrats.html?auth=login-facebook.

Da população branca que tinha votado em Obama em 2012, 12% terá votado Trump. Da população negra que votara em Obama em 2012, 11% ter-se-á abstido em 2016[146].

Os dados recolhidos não são intrusivos ao ponto de distinguirem no eleitorado branco se se é veterano ou cristão evangélico, o que impossibilita demonstrar se Trump conseguiu ou não mobilizar esses setores. Outras análises, anteriores ao dia de eleições, indicam que Trump era, para uma margem confortável, o candidato preferido dos veteranos de guerra americanos. O problema é que essas análises não nos dizem que percentagem de veteranos exprimiu essa preferência em votos Donald Trump.

Gráfico 8



Fonte: Alec Tyson e Shiva Maniam, "Behind Trump's victory: Divisions by race, gender, education", Fact Tank, Pew Research Center, 9 de novembro de 2016, https://www.pewresearch.org/fact-tank/2016/11/09/behind-trumps-victory-divisions-by-race-gender-education/.

[146] Philip Bump, "4.4 million 2012 Obama voters stayed home in 2016 — more than a third of them black", *The Washington Post*, 12 de março de 2018, https://www.washingtonpost.com/news/politics/wp/2018/03/12/4-4-million-2012-obama-voters-stayed-home-in-2016-more-than-a-third-of-them-black/.

Contudo, o gráfico anterior indica que Trump era o candidato preferido da maioria do eleitorado branco, sobretudo entre a classe média trabalhadora, e Trump parece ter conseguido resgatar uma porção significativa desse setor. Alguns dos fatores que parecem aproximar o eleitorado americano de Donald Trump são ser branco e a ausência de educação superior.

Como dissemos anteriormente, provar o impacto das ações russas e da Cambridge Analytica no resultado eleitoral é uma tarefa impossível, uma vez que não se pode aceder aos pensamentos de cada eleitor e confirmar se mudou de opinião ou se foi impelido a votar por ter sido exposto ao conteúdo de qualquer um destes atores. Podemos, no entanto, mostrar que é plausível que essas ações tenham impactado as ações de alguns dos eleitores. Os pontos das estratégias da campanha Trump, da Rússia e da Cambridge Analytica, de mobilização duns setores e de desmobilização de outros, parecem ter sido concretizados. E a sua concretização ocorre acompanhada das atividades destes atores, não sem eles. Podemos continuar a equacionar uma vitória de Trump sem interferência russa e sem Cambridge Analytica, sem *bots* e *trolls*, sem polémicas de e-mails roubados e divulgados e sem dados recolhidos ilicitamente através do Facebook. Porém, a realidade é que Trump ganhou na sequência de todos estes eventos, e não sem eles. O impacto da Rússia e da Cambridge Analytica nas eleições presidenciais americanas de 2016 não é algo provado de forma irrefutável e incontestável. Contudo, a informação disponível não descarta a possibilidade desse impacto, tornando-o mesmo plausível.

5. Lições aprendidas/ilações retiradas

O propósito neste capítulo é, a partir da análise do que ocorreu nas eleições presidenciais de 2016 nos Estados Unidos, extrair ilações gerais do que foi e é possível fazer a nível tecnológico, no meio digital, no ciberespaço e como este tipo de interferência pode ser replicado noutros países, em momentos futuros. Pretende-se, também, informar acerca de algumas medidas a ter em conta para evitar que situações como esta se repitam.

O caso da interferência russa nas eleições presidenciais de 2016 coloca em evidência um primeiro aspeto: o de que quando se trata de geopolítica, o ciberespaço é uma extensão do mundo real[147]. Os diferentes Estados comportam-se no ciberespaço do mesmo modo que se comportam no mundo físico, nas políticas que procuram aplicar e seguir, empregam táticas semelhantes e perseguem os mesmos interesses. Se a Rússia de Vladimir Putin vê a democracia como uma ameaça e o seu confronto com o Ocidente como um jogo de soma-zero, essa visão é replicada no mundo digital[148].

Este caso mostra também que na internet e no ciberespaço a linha que separa o que é domínio público e o que é do domínio privado se oblitera[149]. Não foram atacadas infraestruturas do Estado. O partido Democrata foi alvo de intrusão informática e roubo de documentos sensíveis, mas o partido, enquanto tal, não é um órgão do Estado. No caso da Cambridge Analytica e dos dados pessoais recolhidos através do Facebook, a segurança desses dados não estava entregue às forças de segurança ou de defesa do Estado, mas sim à empresa privada que é o Facebook. A campanha de desinformação foi disseminada nas redes sociais, plataformas digitais que pertencem a empresas privadas como Facebook, Instagram, Twitter, entre outras. Se em 2016 havia alguém com a responsabilidade de fiscalizar o que era partilhado nas redes

[147] John Carlin e Garret Graff, *Dawn of the Code War: America's Battle Against Russia, China and the Rising Global Cyber Threat* (Nova Iorque: Public Affairs, 2018), 59.
[148] Carlin e Graff, *Dawn of the Code War*, 59.
[149] Carlin e Graff, *Dawn of the Code War*, 66.

sociais para impedir desinformação, notícias falsas e difamação dos candidatos, esses responsáveis eram as empresas privadas donas destas plataformas, que parecem ter desempenhado um importante papel num processo que é público, político e que se quer democrático – a eleição dum novo Chefe de Estado nos Estados Unidos.

Outra evidência resultante da interferência em 2016 é que a evolução da internet e do ciberespaço veio gerar confusão acerca daquilo que é fundamental proteger – o que é "secreto" e o que é "infraestrutura". Durante anos, a informação pessoal considerada sensível consistia na informação bancária ou número de segurança social; hoje, a informação pessoal sensível consiste em dados armazenados em dispositivos tão pequenos quanto os smartphones de que milhões de indivíduos se fazem acompanhar todos os dias. Esses dados passam por registos de localização, fotografias guardadas, palavras-passe, mensagens, sites visitados, ou até mesmo, sendo verdade o que a Cambridge Analytica dizia ser capaz de fazer, aquilo de que "gostamos" nas redes sociais. Podemos dizer que as preocupações estiveram durante tantos anos viradas para ataques de grande magnitude às infraestruturas, como a rede de água ou de eletricidade, que poucos terão pensado que um ataque digital à democracia vindo da Rússia fosse executado por meio das redes sociais:

"Governo e oficiais de indústria passaram anos a avisar sobre um 'ciber-11 de setembro' ou um 'ciber-Pearl Harbor', um ataque devastador nas infraestruturas críticas da nossa nação. Preocupámo-nos com ataques à nossa rede elétrica, ao nosso abastecimento de água, a hospitais, ou aos computadores de tráfego aéreo. Porém, em 2016, quando a Rússia nos atingiu com o que que foi o nosso primeiro verdadeiro 'ciber-Pearl Harbor', atacaram um ponto fraco em que nunca tínhamos pensado.

A Rússia atacou a confiança da América na América. Procuraram enfraquecer a nossa crença no nosso próprio governo, a nossa capacidade de participar na nossa própria democracia (…). (…) A Rússia percebeu que a nossa confiança nacional estava mais delicada do que tinha estado noutros anos – e exploraram essa insegurança online. Amplificaram as nossas mensagens a atacarmo-nos uns aos outros, atiçaram a nossa raiva, fizeram do nosso hiperpartidarismo uma arma. Foi fácil para os trolls e bots

russos esconderem-se entre os muitos americanos zangados com o seu presente – e preocupados com o seu futuro. A América era, como um amigo meu disse, 'lenha seca para os russos'.

E ao longo do último ano [2018], aqueles que procuraram exacerbar estas divisões continuaram a avançar o trabalho do governo russo. Têm apenas de entrar no Facebook ou no Twitter para ver esse ódio por nós próprios – a nossa desconfiança acerca de cada um – está a levar-nos a duvidar de orgulhosas tradições históricas, a questionar os alicerces da nossa democracia e os nossos princípios de longa data sobre o papel da América na criação dum mundo melhor. As mesmas ferramentas online que há uma década esperávamos trazerem uma nova Era de abertura e democracia participativa foram, inversamente, transformadas em ferramentas de ódio que espalham desinformação e atiçam raiva com facilidade"[150].

Este caso mostra também como, através do ciberespaço e plataformas digitais nele existentes, é possível um Estado tentar influenciar os processos políticos doutro Estado de forma furtiva, instrumentalizando medos, ódios e divisão social. O conflito no ciberespaço não se limita a ataques cibernéticos com vírus, roubo de informação, ou danificação de dispositivos e sistemas.

Como vimos no capítulo introdutório acerca do ciberespaço, o facto de uma ciberpessoa não ter de corresponder diretamente a uma pessoa individual real, combinado com as ferramentas que permitem mascarar identidade e localização, oferece a possibilidade do anonimato e a de dissociar os atos de quem realmente os pratica. O ciberespaço dispensa também a necessidade de proximidade geográfica. Desde que a ligação exista, o ciberespaço permite que dois (ou milhões de) indivíduos coexistam no mesmo espaço virtual, sem terem de se deslocar. Tudo o que precisam é de um dispositivo com acesso à internet.

"… a internet tornou difusa a linha entre fronteiras, entre o doméstico e o internacional. (…) A internet permitiu o acesso instantâneo a cantos distantes do globo, permitiu às pessoas sentarem-se à secretária num país para falar por vídeo com pessoas a continentes de distância, e deu a qualquer pessoa

[150] Carlin e Graff, *Dawn of the Code War*, 69-70.

com internet a possibilidade de alcançar tantos leitores ou espectadores como o New York Times ou a CNN"[151].

Tudo isto permite fazer inúmeras coisas remotamente, sem a necessidade de colocar agentes "no terreno", de forma menos dispendiosa e com rastos mais difíceis de identificar e seguir. As redes sociais potenciam essas capacidades.

Por outro lado, as redes sociais mostram que, a partir do momento que se inserem informações pessoais nessas redes, essas informações deixam de estar na esfera de privacidade do utilizador, passando a ser acessíveis e instrumentalizáveis por terceiros.

Não que isso não fosse do conhecimento público ou que não tivesse havido informação pessoal retirada das redes sociais anteriormente. Afinal, outras empresas adquiriam essas informações do Facebook para promoverem produtos e aumentarem vendas, mas com permissão dos utilizadores, ainda que essa permissão tivesse sido dada por quem carregou em "Li e aceito os Termos e Condições" sem os terem realmente lido.

Com fins políticos, Obama também já o tinha feito, mas com o cuidado de cumprir as normas de utilização do Facebook e de os utilizadores consentirem com a utilização dessa informação para esses fins.

O escândalo da Cambridge Analytica, no entanto, mostrou que havia informação pessoal a ser transmitida para fins que os utilizadores não tinham autorizado, sem receberem qualquer tipo de aviso e com o objetivo último de influenciar a sua escolha de candidato político.

O caso das eleições presidenciais de 2016 dos Estados Unidos mostra também que não é só em países menos desenvolvidos que campanhas de desinformação são usadas para influenciar eleições e que estas também não se fazem apenas através de meios de comunicação social convencionais, como a rádio, televisão e jornais.

O ciberespaço e as plataformas digitais criaram um novo meio onde campanhas de desinformação também podem ser disseminadas.

[151] Carlin e Graff, *Dawn of the Code War*, 68.

Este caso evidencia também uma certa iliteracia digital ou tecnológica. Se funcionários e voluntários da campanha de Hillary Clinton tivessem conseguido identificar que os e-mails de *spearphishing* eram, de facto, e-mails de *spearphishing*, e que a página onde terão sido direcionados para os inserir não era legítima, poder-se-ia ter evitado o roubo de credenciais e e-mails e a sua consequente divulgação. É certo que os e-mails de *spearphishing* podiam estar muito bem feitos e identificá-los como tal podia ser muito mais difícil do que com as comuns tentativas com e-mails que dizem que não foi possível realizar o pagamento da Netflix ou que é necessário reintroduzir os dados da conta Apple. Todavia, deveria ter havido, por parte dos oficiais de campanha, mais atenção dada a estas questões, ou mesmo formação nesta área para os funcionários e voluntários. E esta preocupação não deveria existir apenas em contexto de campanhas políticas; deveria – e deve – existir em locais de trabalho, do setor público e privado, para proteção das próprias instituições, empresas e trabalhadores, e em escolas e universidades, para proteção das mesmas, dos docentes, não docentes e alunos.

O que se sucedeu nas eleições de 2016 é também indicativo de que tanto a comunicação social, como o público em geral, bem como alguns detentores de cargos públicos têm dificuldade em identificar notícias falsas, seja em período de campanha eleitoral ou não. Tanto assim que órgãos de comunicação social, ao longo dos últimos anos, investiram em programas ou segmentos de programas exclusivamente dedicados à verificação de notícias. Fazem-no sobretudo com notícias que circulam nas redes sociais como o Facebook ou Twitter, uma vez que as que são veiculadas pelos órgãos de comunicação social, à partida, já foram alvo dessa verificação, enquanto que nas redes sociais não há um controlo prévio.

Num estudo da Universidade do Indiana, os utilizadores das redes sociais só conseguiram identificar notícias falsas corretamente 44% das vezes[152] porque, segundo esse mesmo estudo, "quando se leem notícias nas redes sociais, o objetivo (…) não é determinar o que é verdadeiro

[152] Patricia Moravec, Randall Minas e Alan Dennis, "Fake News on Social Media: People Believe What They Want to Believe When it Makes No Sense at All" (Indiana University, 2018), 16.

ou falso; é divertimento e prazer"[153]. No contexto das redes sociais, os utilizadores parecem evitar atividades que os façam sentir que estão a trabalhar (processar informação com cautela) e atividades que não lhes tragam prazer[154]. Os utilizadores tendem a interagir com artigos que os façam sentir-se bem, logo, com artigos que estão de acordo com as suas crenças. O principal motivo para desconfiar da veracidade dum artigo era a dissonância entre o título e as crenças ou preferências políticas dos utilizadores[155].

Naturalmente, o problema das notícias falsas intensifica-se quando estas são partilhadas por quem deveria assumir a responsabilidade de ser uma fonte fidedigna de informação, como canais noticiosos, comentadores ou detentores de cargos políticos. Tal não foi o caso em 2016. Fox News, Breitbart News, futuros membros da administração Trump, como Kellyanne Conway, Michael Flynn, o próprio Donald Trump, ou personalidades como Ann Coulter e Jack Posobiec foram alguns dos que contribuíram para a difusão de notícias falsas de origem russa nas redes sociais.

Um outro estudo, do MIT (Massachussets Institute of Technology), apurou que notícias falsas no Twitter são partilhadas seis vezes mais do que notícias verdadeiras e a um ritmo três vezes superior[156]. O mesmo estudo apurou que uma das principais razões para essa diferença na quantidade e no ritmo das partilhas se prende com a "novidade" das notícias, porque "a novidade atrai a atenção humana (…) e encoraja a partilha de informação"[157]. O estudo apurou ainda que quando se adicionam *bots* à partilha de notícias falsas e verdadeiras, estes têm o mesmo efeito em ambas – aceleram a sua partilha, mas não são responsáveis pela diferença no número de partilhas. Os principais responsáveis por mais partilhas de notícias falsas do que notícias verdadeiras são seres humanos, não programas informáticos[158].

[153] Moravec, Minas e Dennis, "Fake News on Social Media", 4.
[154] Moravec, Minas e Dennis, "Fake News on Social Media", 4.
[155] Moravec, Minas e Dennis, "Fake News on Social Media", 10-11.
[156] Soroush Vosoughi, Deb Roy e Sinan Aral, "The Spread of True and False News Online", MIT Initiative on The Digital Economy (Massachussets Institute of Technology, 2018), 3.
[157] Vosoughi, Roy e Aral, "The Spread of True and False News Online", 3.
[158] Vosoughi, Roy e Aral, "The Spread of True and False News Online", 1.

O modo como se interferiu nestas eleições mostra ainda que há formas de tentar manipular resultados eleitorais sem passar pela falsificação de votos, por ataques físicos ou informáticos a centros de votos. Se se conseguir manipular a escolha do eleitorado, é possível obter-se o resultado desejado de forma aparentemente legítima.

O combate a este tipo de interferência com recurso a alta tecnologia, propagada através de plataformas e dispositivos de fácil acesso, difícil de reconhecer e de rastrear, é algo que não será fácil de fazer, mas que é possível. Tal passa por dois elementos fundamentais: educação e regulamentação.

Começando pela educação, trata-se, neste caso específico, de educação para a literacia digital. Existem diversos programas e iniciativas, privados e públicos. Todos devem estar focados em dois aspetos essenciais: na capacidade de, ao navegar e pesquisar, avaliar e distinguir a informação verdadeira da falsa; e na capacidade de manter seguros os dispositivos, a privacidade e os dados pessoais. A implementação destes programas variará naturalmente com as capacidades financeiras e educativas dos diferentes Estados e instituições, mas será necessária se se pretende evitar este tipo de interferências.

Passando para o âmbito da legislação e da regulamentação, existem já várias propostas nos Estados Unidos.

A proposta sobre o Consentimento do Senador Edward Markey (Democrata, Massachussets) requer que as empresas possibilitem aos utilizadores/consumidores usar os seus serviços podendo estes optar por ceder determinadas informações e recusar dar outras; requer práticas seguras no uso dos dados e ainda que os utilizadores sejam notificados acerca de toda a recolha de dados e quaisquer violações de dados que ocorram[159].

A Senadora Elizabeth Warren (Democrata, Massachussets) introduziu uma proposta para a Responsabilidade Executiva Corporativa, que pretende tornar os executivos criminalmente

[159] Edward Markey, Proposta Legislativa "Consent Act", https://www.markey.senate.gov/imo/media/doc/CONSENT%20Act%20text.pdf.

responsáveis por quaisquer violações de dados que ocorram por negligência das respetivas corporações[160].

Já Jim Steyer, Governador da Califórnia, introduziu uma proposta (que está a ser debatida) que, se aprovada, daria aos cidadãos o direito de serem recompensados pelo uso dos seus dados pessoais[161].

A União Europeia estará mais à frente no aspeto legislativo, uma vez que o Regulamento Geral para a Proteção de Dados (RGPD) foi aprovado ainda em 2016, tendo entrado em vigor em maio de 2018. Em termos legais, o Regulamento dá aos cidadãos mais controlo sobre os seus próprios dados na medida em que lhes concede o "direito a ser esquecido"[162] (ou seja, exigir a eliminação dos seus dados pessoais em caso de uso indevido ou injustificado), o direito a saber se houve invasão ou violação dos dados[163], bem como o direito à portabilidade dos dados[164], que pretende facilitar a transmissão e migração dos dados para outras empresas, se o titular dos dados o pretender. O RGPD exige ainda que as empresas indiquem, em linguagem clara e simples, que dados recolhem[165], e que demonstrem que têm os mecanismos de segurança adequados para proteger os dados que recolhem e armazenam[166]. No entanto, o RGPD não obriga as empresas e serviços na União Europeia a dar opções aos utilizadores nos dados que disponibilizam. Em múltiplos casos, se não se concordar com a Política de Dados do serviço ou da empresa, é-se aconselhado a não usar esses serviços, ou acaba-se mesmo por ficar

[160] Elizabeth Warren, Proposta Legislativa "The Corporate Executive Accountability Act", https://www.warren.senate.gov/imo/media/doc/2019.4.1%20Corporate%20Executive%20Accountability%20Act%20Summary.pdf.
[161] Kartikay Mehrotra, "California Governor Proposes Digital Dividend Aimed at Big Tech", *Bloomberg*, 12 de fevereiro de 2019, https://www.bloomberg.com/news/articles/2019-02-12/california-governor-proposes-digital-dividend-targeting-big-tech.
[162] Artigo 17.º, "Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)", Jornal Oficial da União Europeia L119, 43.
[163] Artigo 33.º, "Regulamento Geral sobre a Proteção de Dados", 52.
[164] Artigo 20.º, "Regulamento Geral sobre a Proteção de Dados", 45.
[165] 'Considerando' n.º 39, "Regulamento Geral sobre a Proteção de Dados", 7.
[166] Artigo 24.º, "Regulamento Geral sobre a Proteção de Dados", 47.

impedido de usufruir plenamente dos serviços disponíveis. A título de exemplo, na Política de Privacidade do jornal Público pode ler-se:

"Se não concordar com alguma alteração efetuada à presente Política, solicitamos que não continue a usar os sites do Público para enviar ou, de alguma forma, submeter os seus dados pessoais ao Público"[167].

Pode ainda ler-se que o Público recolhe informações sobre o hardware e o software do computador através do qual acedemos ao *site*, e que recolhe dados como o endereço IP, tipo de *browser* utilizado, horários de acesso/tempo de utilização dos sites do Público e conteúdos visualizados[168].

O RGPD também não impede a transmissão ou a venda de dados pessoais a terceiros, desde que estas estivessem expressas na Política de Privacidade com a qual o utilizador concordou. Porém, o Eurobarómetro sobre o RGPD indica que apenas 30% dos internautas de facto lê as políticas de privacidade[169], o que significa que muitos cidadãos da UE concordam com a utilização dos seus dados pessoais sem saberem com o que estão a concordar. É possível que a "linguagem clara e simples" das políticas de privacidade precise também de ser menos extensa. O RGPD terá sido um passo na direção certa, mas ainda há margem para melhorar.

Aliás, a margem para melhorar estará em contínuo alargamento. Dado que o ciberespaço está em constante evolução, também a legislação que é produzida para o regular terá de ir sendo atualizada a fim de combater os modos perversos como o ciberespaço pode ser utilizado. No entanto, do mesmo modo que as leis não acabaram com o conflito nos domínios da terra, do mar, do ar e do espaço, também não acabarão com os conflitos que se podem desenrolar no

[167] "Política de Privacidade", *Público*, última modificação a 22 de junho de 2018, https://www.publico.pt/nos/politica-de-privacidade.
[168] "Política de Privacidade", *Público*.
[169] Comissão Europeia, "Special Eurobarometer 487a – Report: The General Data Protection Regulation", junho de 2019, https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222.

ciberespaço. A evolução tecnológica afeta todos os domínios, mas afeta mais diretamente o domínio do ciberespaço, uma vez que este é essencialmente digital. Enquanto que desde a década de 60 foi possível fazer a velocidade dos automóveis duplicar, o poder de processamento dos computadores aumentou um bilião de vezes[170] no mesmo tempo e, todos os dias, aumenta mais um pouco. Esta evolução exponencial reflete-se na importância do ciberespaço, tanto enquanto domínio do quotidiano, no qual se executam tarefas mundanas e rotineiras, como enquanto domínio de conflito. É isso que nos propomos analisar no capítulo seguinte: o ciberespaço e o futuro do conflito.

[170] Randy Fernando, em *The Social Dilemma*, realizado por Jeff Orlowski (Netflix, 2020), https://www.netflix.com/title/81254224.

6. Ciberespaço, evolução tecnológica e o futuro do conflito

"*O futuro da guerra política é no domínio digital.*"[171]

Chegados a este capítulo, é altura de conjeturar o que as capacidades no ciberespaço do presente e a sua evolução poderão significar no futuro do conflito. Aqui procuraremos responder principalmente a duas questões: (1) se o ciberespaço vai, enquanto domínio de conflito, tornar-se mais importante do que os restantes (terra, mar, ar e espaço) e (2) se graças à aprendizagem automatizada e à inteligência artificial este domínio se tornará predominantemente autónomo.

Em primeiro lugar, pretendemos clarificar que utilizaremos genericamente o termo "conflito" em vez de "guerra" porque todas as guerras são um conflito, mas nem todos os conflitos constituem uma guerra.

Segundo Christopher Mitchell, um conflito é "qualquer situação em que duas ou mais partes entendem que têm objetivos mutualmente incompatíveis"[172] e, segundo o Instituto de Investigação de Conflitos Internacionais de Heidelberg, um conflito é "uma incompatibilidade de intenções compreendida entre indivíduos ou grupos sociais fora dos procedimentos regulatórios estabelecidos (…) que ameacem funções essenciais do Estado".

O conflito está sempre presente, em maior ou menor escala. Pode ser apenas entre dois indivíduos, colegas de trabalho, entre um casal, entre membros duma família, entre membros duma comunidade, entre países, e pode variar numa escala que atravessa os níveis individual, local, regional, nacional, podendo atingir proporções mundiais.

Preterimos também o termo "guerra" porque este pressupõe o uso de armas e o conflito existe sob muitas formas não armadas. Uma vez que aquilo sobre que nos pretendemos debruçar

[171] Alina Polyakova e Spencer Boyer, "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition", *Foreign Policy at Brookings*, março de 2018, 6, https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf.
[172] Christopher Mitchell, *The Structure of International Conflict* (Londres: Macmillan, 1981), 17.

é o conflito no ciberespaço e que a doutrina militar americana se refere "à habilidade de potenciar meios cibernéticos como 'capacidade no ciberespaço'", abstendo-se de lhes chamar "armas", convém que nos abstenhamos também de usar um termo que remeta para a utilização das mesmas, que é o caso do termo "guerra".

Atualmente, a utilização de capacidades no ciberespaço é considerada uma tática da zona cinzenta do conflito. Esta zona cinzenta é como uma zona intermédia de medidas e táticas que já ultrapassam a diplomacia convencional, mas que ficam ainda aquém dum conflito armado. As táticas da zona cinzenta são frequentemente aplicadas em conflitos ou guerras de natureza assimétrica ou híbrida.

Um estudo do Centro de Estudos Estratégicos e Internacionais (Center for Strategic and International Studies/CSIS) define estas táticas como "um esforço ou série de esforços além da dissuasão e garantia do Estado que tenta alcançar os objetivos de segurança de alguém sem recorrer ao uso direto e considerável da força"[173].

Um outro estudo do mesmo Centro acrescenta que estas podem incluir um misto de táticas convencionais, táticas irregulares e táticas cibernéticas, juntamente com outros métodos de influência, como notícias falsas, diplomacia, manipulação da lei (*lawfare*) de modo a contornar direitos humanos e convenções internacionais, e intervenção estrangeira em eleições[174]. A utilização deste tipo de táticas da chamada zona cinzenta de conflito permite a "potenciais adversários coagir discretamente os seus alvos a servir os seus interesses, enquanto simultaneamente evitam a possibilidade de conflitos de grande escala"[175].

As operações psicológicas ou PSYOPS, de que já falámos no capítulo 3.3.3., são também consideradas táticas da zona cinzenta de conflito.

---

[173] Michael Green *et al*., "Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence", *Center for Strategic and International Studies*, maio de 2017, 21, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170505_GreenM_CounteringCoercionAsia_Web.pdf.
[174] Adrien Chorn e Monica Sato, "Maritime Gray Zone Tactics: The Argument for Reviewing the 1951 U.S.-Philippines Mutual Defense Treaty", *Center for Strategic and International Studies*, 1 de outubro de 2019, https://www.csis.org/maritime-gray-zone-tactics-argument-reviewing-1951-us-philippines-mutual-defense-treaty.
[175] Chorn e Sato, "Maritime Gray Zone Tactics".

Tudo isto nos importa porque a interferência nas presidenciais de 2016 constituiu um caso de ingerência externa dum Estado soberano nos assuntos domésticos doutro, porque os dois países coexistem no sistema internacional em constante conflito desde o fim da Segunda Guerra Mundial (com oscilações na intensidade do dito conflito, ora mais tenso, ora mais relaxado) e porque até ao momento sempre impediram o conflito armado direto entre si, mas os dois países continuam a digladiar-se no sistema internacional. Importa-nos também que a interferência nas eleições se tenha concretizado com recurso às referidas táticas cinzentas, como ataques informáticos, operações psicológicas e campanhas de desinformação, veiculadas pelo ciberespaço, que constituem, por sua vez, um exercício de *sharp power* por parte da Rússia. E importa também que já tenham passado quatro anos desde essas eleições, quatro anos durante os quais a tecnologia continuou a evoluir, o que pode significar que existam agora métodos mais eficazes, mais sofisticados ou inteiramente novos para interferir num processo eleitoral.

Procurámos mostrar, no capítulo 2, como o ciberespaço foi instrumental na exibição de *sharp power* e na condução duma campanha de desinformação arquitetada por um governo estrangeiro nas eleições americanas de 2016. Uma vez que já passaram quatro anos desde a eleição e seis desde que começaram os esforços russos para interferir na mesma, é importante vermos como o ciberespaço e tecnologias relacionadas podem ser usados para influenciar a política dum país.

a) O ciberespaço como ferramenta de subversão política

À medida que a tecnologia melhora, melhoram também as formas de manipular informação, para o bem e para o mal. Peguemos nalguns exemplos de conteúdos que foram

utilizados nas campanhas republicana e democrata em 2016 e apliquemos-lhes as melhorias tecnológicas que se perspetivam para o futuro.

Comecemos pela "Access Hollywood tape", o vídeo em que Donald Trump se gabava de comportamentos indevidos com mulheres. Donald Trump nunca aparece na imagem, apenas se ouve a sua voz e a da outra pessoa com quem conversa. Ou seja, a única prova de que Trump disse aquelas palavras está na identificação da sua voz. Tal não quer dizer que não o tenha feito, até porque Trump não o negou. Mas é um bom exemplo pelo seguinte: atualmente, sistemas de Inteligência Artificial são já capazes de copiar a voz de alguém e de reproduzir frases com as vozes copiadas a partir de pequenos excertos de discurso, tão curtos quanto um minuto. É certo que as cópias não são perfeitas, mas as imperfeições e limitações são precisamente o que os avanços da tecnologia procuram corrigir. Com mais tempo de áudio e com atenção a pormenores como ritmo, hesitações no discurso, interjeições, entre outros, será possível criar cópias muito realistas das vozes de outras pessoas e fazer populações inteiras acreditar que determinada pessoa disse determinada coisa, sem nunca o ter feito. Para os mais céticos destas capacidades, estão disponibilizadas algumas hiperligações para vídeos exemplificativos nos Anexos (página 134).

Continuemos pelas imitações e cópias. Se no caso da "Access Hollywood tape" só o registo da voz foi convincente, mais ainda seria se Donald Trump tivesse sido mostrado a dizer o que se ouve nesse vídeo. À semelhança da reprodução de voz a partir de um curto excerto de áudio, também hoje é possível recriar o rosto de alguém com recurso a tecnologia, colocando quem se quiser no local que se quiser. Esta tecnologia é conhecida como CGI (Computer-Generated Imagery), Imagens Geradas por Computador. Atualmente, a sua aplicação mais comum é no mundo do audiovisual, nomeadamente no cinema e na televisão. É aplicada na criação de cenários, dá forma e vida a criaturas vindas do género Fantástico e, ocasionalmente, "ressuscita" atores que partiram antes de as filmagens estarem concluídas ou que se quer que figurem em sequelas feitas anos mais tarde. A qualidade destas reproduções é já muito elevada,

mas ainda se costuma conseguir distinguir o rosto real do gerado por computador (exemplos nos anexos, página 135). Podemos, no entanto, chegar a um ponto em que a distinção se torna muito difícil ou quase impossível de fazer, gerando muita confusão para o público.

As fotografias seguem o mesmo rumo, mas atualmente é raro uma foto falsa conseguir circular sem que em pouco tempo seja descoberto que está adulterada. Não é uma questão de más adulterações ou cortes nas imagens, apenas acontece que se tornou mais fácil descobrir as imagens originais e mostrar as modificações na nova. Uma ferramenta muito útil para isso é a "pesquisa reversa de imagens", em que se pode carregar uma foto para o motor de busca e procurar imagens semelhantes, encontrando a original para se poderem verificar as diferenças. Além disso, a adulteração de fotografias já é feita há algum tempo e a sua prática tornou-se conhecimento geral nos últimos anos, pelo que o público ganhou já alguma resistência à manipulação por fotografias. A adulteração de vídeos, no entanto, como sempre foi mais difícil de fazer, é um risco maior, porque o que está em vídeo é geralmente tido como mais fiável.

Existe ainda uma outra capacidade muito interessante que, tal como as cópias de voz, é potenciada por inteligência artificial, que é a produção automática de texto. A produção automática de texto pode ser usada para qualquer assunto, para escrever algo que se assemelhe a um artigo de jornal, uma publicação num blog, a um comentário um produto numa loja online ou a um vídeo no YouTube, ou para um ensaio académico. Podemos, por exemplo, escolher um dos temas fraturantes na campanha de 2016, como a imigração. Para produzir o texto, basta inserir no software dedicado algumas palavras-chave de acordo com a ótica que queremos que o texto tenha sobre o tema, como "imigração", "benéfica", "produtividade", "economia", "crescimento", se o quisermos positivo; ou outros como "imigrantes", "crime", "roubo", "violência", se o quisermos negativo. Os softwares atuais não são perfeitos e é natural que contenham erros de sintaxe, frases mal construídas, fraca organização lógica, mas podem poupar muito tempo a quem quer expor uma determinada visão sobre um qualquer assunto, tendo apenas de depois fazer algumas alterações ao que foi feito de forma automática. É uma

ferramenta ideal para alguém que queira bombardear outros com a sua mundividência sobre diversos temas sem ter de dedicar muito mais tempo à parte da escrita. Uma hiperligação para um vídeo exemplificativo de como funciona este tipo de software está disponível nos Anexos (página 134) desta dissertação.

De certo modo, estas tecnologias procuram "criar realidade". Copiam vozes reais, reconstroem rostos e reproduzem movimentos reais, escrevem textos que parecem efetivamente ter sido escritos por alguém que dedicou tempo a redigi-los. "Criar realidade" não é, *per se*, algo perverso. É algo muito útil no meio audiovisual, como no cinema e na televisão, e nos meios digitais em que se precisa de produzir conteúdo escrito, como, por exemplo, em *blogs*, em que o que se pretende fazer é entreter os consumidores destes conteúdos. Existe, no entanto, a possibilidade de utilizar estas tecnologias perversamente, criando realidades com o intuito de manipular o público. Quando são usadas desse modo, o produto final tem atualmente a designação de "*deep fake*".

"Novas técnicas na replicação de vídeo e de linguística, impulsionadas por Inteligência Artificial que consegue aprender, são capazes de produzir novos vídeos ou gravações de áudio a partir de conteúdo já existente. São os chamados '*deep fakes*', ou a 'manipulação digital de som, imagens ou vídeo para imitar [*impersonate*] alguém ou fazer parecer que uma pessoa fez algo' estão a chegar"[176].

Ora, se os "*deep fakes*" consistem na manipulação digital para imitar alguém, não é difícil prever quem serão os alvos principais – serão os líderes e candidatos políticos.

"… será possível fazer parecer que líderes políticos disseram qualquer coisa, e soarão e parecer-se-ão exatamente como soam e se parecem na vida real. (…) Estes avanços … quando utilizados por atores malignos, podem ter efeitos danosos no ambiente dos *media*, do discurso público e da confiança nas instituições convencionais. Se os espectadores não podem confiar nos seus olhos e ouvidos, a confiança nos *media* poderá cair ainda mais. À medida que os *deep fakes* se tornam mais baratos, mais rápidos de fazer e mais acessíveis, a 'torneira de falsidades' será cada vez mais eficaz: vídeos de líderes

[176] Polyakova e Boyer, "The Future of Political Warfare", 12.

políticos a fazer comentários depreciativos sobre os cidadãos podem ser publicados nas redes sociais por milhares de contas de *trolls* e *bots*. Quando finalmente as fontes oficiais fossem capazes de desmascarar o embuste, novos vídeos falsos já se teriam tornado virais, e as contas que disseminam propaganda pareceriam muito reais e controladas por humanos. (…) O ciclo de desinformação continuaria 24 horas por dia, 7 dias por semana"[177].

Novamente, reforçamos a ideia de que os avanços tecnológicos, por si, não são algo de mau. Do mesmo modo que a tecnologia automóvel não evoluiu com o intuito de atropelar outras pessoas ou de que os carros fossem armadilhados, também a tecnologia digital não evolui com o intuito de criar máquinas propagandísticas. Porém, há quase sempre um modo perverso de utilizar o que é criado com boas intenções e a tecnologia digital não é exceção. "Só porque uma tecnologia foi inventada para um propósito, não quer dizer que não se encontrem outras utilizações que não foram previstas pelos seus criadores"[178]. Além disso, o momento em que os produtos destas tecnologias digitais não são distinguíveis de conteúdos não manipulados não está assim tão distante. Fala-se da altura em que não conseguiremos distinguir uma conta duma rede social gerida por um indivíduo real de outra operada por um *bot*, mas já em 2016 houve milhares de pessoas que não foram capazes de fazer essa distinção. A grande diferença é que, por enquanto, não é muito difícil para os indivíduos mais habituados a lidar com o mundo digital identificar esse tipo de contas, mas é muito possível que cheguemos a um ponto em que só indivíduos com formação sejam capazes de o fazer, ou mesmo a um ponto em que até indivíduos treinados para esse fim sejam ludibriados com softwares muito bem feitos.

"Será mais difícil para os seres humanos e para as próprias plataformas detetar contas falsas ou automatizadas, que se tornarão cada vez mais sofisticadas na mimetização do comportamento humano. Sistemas de Inteligência Artificial serão capazes de se adaptar a novos contextos, sugerir conteúdo original relevante, interagir de forma sensível com humanos em contextos proscritos [para os quais não tinham sido inicialmente programados], e prever respostas emocionais humanas a esse conteúdo. (…)

[177] Polyakova e Boyer, "The Future of Political Warfare", 6-7.
[178] Ronald Deibert e Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace", *Journal of Democracy* 21/4 (outubro de 2010): 48.

Serão capazes de explorar emoções humanas para extrair respostas específicas. Serão capazes de fazer isto mais rápido e mais eficazmente do que qualquer agente humano. Atores maliciosos – Rússia ou outros – utilizarão estas tecnologias para seu benefício. Esta transformação na comunicação digital está a acontecer agora – e a janela para ser capaz de detetar a diferença entre comunicações humanas e comunicações automatizadas está a fechar-se"[179].

Tudo isto é deveras preocupante, porém, no que diz respeito à instrumentalização do ciberespaço para o conflito, esta não se fica pela manipulação de fotografias, som e vídeo ou pela desinformação e propaganda disseminadas através das redes sociais. Existem mais capacidades no ciberespaço, com potencialidades destrutivas a nível físico e de forma direta, que também devemos ter em conta, como os ataques cibernéticos a infraestruturas, a autonomização de equipamentos militares e aplicações militares e civis de inteligência artificial.

b) Ataques cibernéticos

Recuperemos então a grande preocupação dos especialistas de segurança nacional (que os terá levado a descuidar a atenção às redes sociais) – os ataques a infraestrutura crítica, como à rede energética (como rede elétrica ou de abastecimento de gás natural), à rede de distribuição e abastecimento de água, a sistemas de controlo de tráfego aéreo, a sistemas de controlo de semáforos, a sistemas informáticos de ramos do governo, a sistemas de controlo de transportes públicos, sobretudo os que operam sobre carris, a sistemas de telecomunicações ou a sistemas que permitem operar na Banca e na Bolsa.

A preocupação com ataques cibernéticos a estas infraestruturas foi surgindo à medida que as mesmas se foram digitalizando e, hoje, já não são meras conjeturas acerca do que pode ser

[179] Polyakova e Boyer, "The Future of Political Warfare", 8-9.

feito: existem já múltiplos casos de ataques cibernéticos que confirmaram estas preocupações e reforçaram a necessidade de capacidades defensivas no ciberespaço.

Por exemplo, Israel sofreu um ataque informático ao sistema de abastecimento de água em junho de 2020, que tinha objetivo de alterar os níveis de cloro na água em sistemas de rega de plantações agrícolas. Segundo as autoridades, o ataque foi detetado rapidamente e resolvido localmente, pelo que não chegou a afetar ninguém[180].

Em fevereiro, também de 2020, uma central de gás natural nos Estados Unidos foi alvo dum ataque informático que forçou o seu encerramento durante dois dias – os atacantes conseguiram o controlo do sistema de informações de central, mas nunca do sistema de operações físicas. Ainda assim, foram precisos os dois dias de inoperação para recuperar o controlo do sistema através das cópias de segurança[181].

Houve, também, uma "pandemia" de vírus informáticos em 2017, que foi particularmente bem-sucedida na Ucrânia. Os vírus congelavam os sistemas operativos até que os utilizadores pagassem um resgate (os chamados "*ransomware*": "*ransom*" = resgate) e só aí desbloqueavam os sistemas. O Banco Central ucraniano foi uma das vítimas, bem como o sistema de comboios metropolitanos e a empresa estatal de energia da Ucrânia, tendo os dois últimos ficado temporariamente paralisados[182]. Durante esta "pandemia" informática, o Serviço Nacional de Saúde português, por prevenção, desligou o sistema de e-mails[183], uma medida que recebeu críticas do Professor Doutor José Tribolet, professor no Departamento de Engenharia Informática no Instituto Superior Técnico, por revelar falta de preparação da parte do SNS. Nas suas palavras:

---

[180] Catalin Cimpanu, "Two more cyber-attacks hit Israel's water system", *ZDNet*, 20 de julho de 2020, https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/.
[181] Tom DiChristopher, "Cyberattack uncovers shortfalls in natural gas pipeline security", *S&P Global*, 19 de fevereiro de 2020, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyberattack-uncovers-shortfalls-in-natural-gas-pipeline-security-57179953.
[182] "Ataque informático. SNS desliga e-mails por precaução", *Sol*, 27 de junho de 2017, https://sol.sapo.pt/artigo/569761/ataque-informatico-sns-desliga-e-mails-por-precaucao.
[183] "Ataque informático", *Sol*.

"O Sistema [*sic*] Nacional de Saúde fez uma coisa que faz todo o sentido, desligaram-se da internet. Ótimo. Quem quiser bloquear o país, faz um grande ataque massivo aos hospitais. Os tipos desligam-se da internet e depois eu quero ver como é que a gente funciona! Quero ver como é que a gente funciona! Se os hospitais não têm acesso à internet, não têm acesso às ambulâncias, como é que é?"[184]

O SNS voltou a ser alvo de ataque informático em julho de 2020 e, desta vez, o SNS não foi capaz de o evitar. Milhares de credenciais de profissionais do SNS foram roubadas e divulgadas na internet, mas a hiperligação rapidamente deixou de conduzir ao documento com a lista de credenciais[185]. Não se sabe quem eliminou o documento da hiperligação.

Estes exemplos justificam fundamentadamente a preocupação e até mesmo algum alarmismo em relação a ataques cibernéticos. No entanto, estes exemplos evidenciam, também, dois aspetos "positivos" para as vítimas de ataques informáticos: o primeiro é que os efeitos dos ataques informáticos, são, na sua maioria, de curta extensão, com resoluções relativamente rápidas (reiniciar sistemas e reparar sistemas a partir de cópias de segurança, pagar o resgate, contra-atacar o atacante); e o segundo é que raramente os ataques informáticos procuram provocar danos físicos ou materiais.

Porém, não deixa de haver casos em que os efeitos de ataques cibernéticos se fazem sentir durante muito tempo ou em que se causam danos físicos e materiais. Afinal, as operações no ciberespaço por parte da Rússia, se assumirmos que tiveram algum impacto, significaram quatro anos de Donald Trump como Presidente dos Estados Unidos. Se o seu mandato foi bom ou mau é outra discussão que se pode ter, mas a Rússia não teria interferido na eleição se considerasse que uma presidência de Trump não seria prejudicial para os EUA e benéfica para a Rússia.

[184] José Tribolet, "Quem Protege a Democracia?", *Prós e Contras*, episódio 14, temporada 17, transmitido a 15 de abril de 2019, 2ª parte, 12:58, https://www.rtp.pt/play/p5337/e401358/pros-contras/737263.
[185] Hugo Séneca, "Hackers publicam passwords de milhares de médicos e enfermeiros do SNS na internet", *Expresso*, 20 de julho de 2020, https://expresso.pt/sociedade/2020-07-20-Hackers-publicam-passwords-de-milhares-de-medicos-e-enfermeiros-do-SNS-na-internet.

Os dois aspetos "positivos", por sua vez, evidenciam uma outra coisa: que uma guerra estritamente cibernética é altamente improvável, por uma série de razões.

Na doutrina militar americana, uma guerra tem como objetivo final "a destruição da capacidade e vontade do inimigo de lutar"[186]. Ora, ataques cujos impactos, na sua maioria, não são duradouros e dos quais se é possível recuperar em pouco tempo, não são os que mais contribuem para esse objetivo.

> "Até agora, o medo de ciberataques é maior do que os danos que estes causaram.
>
> (…) Primeiro, ciberataques continuam limitados porque o ciberespaço está inerentemente ligado ao mundo físico. Stuxnet, o exemplo mais dramático de ciber-sabotagem que é publicamente conhecido, provavelmente requereu que um humano usasse uma *pen drive* para contornar o *air-gap*[187] que protegia os sistemas de centrifugação nuclear iranianos. Segundo, os ciberataques costumam ser limitados em duração e ter mais formas de ser revertidos do que ataques cinéticos convencionais. Stuxnet atrasou, mas não destruiu capacidades, e os apagões duraram apenas algumas horas. Finalmente, ciberataques não destabilizam relações internacionais porque os Estados exercem contenção na sua utilização de poder cibernético"[188].

Além disso, quando um conflito ou guerra se está a desenvolver e isso é do conhecimento público, é fundamental para os governos mostrarem "trabalho feito", que estão a ganhar terreno ao inimigo, de modo a manter e até mesmo a ganhar mais apoio público e político no esforço de guerra. Como o ciberespaço não pode propriamente ser mostrado, por ser virtual e invisível, não serve o propósito da exibição, apesar de todas as suas valências. As armas convencionais continuam a provocar mais danos físicos e materiais e, por enquanto, as guerras ainda se fazem com embates de seres humanos contra outros seres humanos, embora isso também esteja a mudar graças à evolução tecnológica do ciberespaço e do armamento.

---

[186] "Field Manual 100-5 Operations", Departamento do Exército, 1993, 24.
[187] Um computador em air-gap é um computador que não está ligado a nenhuma rede, de modo nenhum, impossibilitando a intrusão no mesmo de forma remota. Para aceder a um computador em air-gap, é necessário fazê-lo pessoalmente.
[188] Puyvelde e Brantly, *Cybersecurity*, 98-99.

Isto não significa que o ciberespaço não desempenhe um papel fundamental em cenários de conflito armado ou de guerra.

Enquanto domínio de conflito, o ciberespaço é um "local" onde se podem conduzir múltiplas operações, desde as mais básicas e rotineiras, como ações de vigilância a nível interno, a operações essenciais para a vitória contra um inimigo, como espionagem, obtendo informação de forma furtiva sem a necessidade de sujeitar um operacional ao risco de ser capturado, operações psicológicas de subversão para provocar dissidências entre os operacionais ou entre as populações e órgãos de Estado, realizar comunicações, interferir com as comunicações do inimigo, fornecer informações falsas para induzir o inimigo em erro, ou ainda controlar dispositivos modernos, como veículos e aeronaves não tripulados, sistemas de armamento e permitir o funcionamento de armas autónomas.

Doutro modo, operações que se circunscrevam somente ao ciberespaço tendem a ter efeitos muito limitados. No entanto, quando operações no ciberespaço têm repercussões no mundo físico, ou quando são coordenadas com outros ataques simultâneos no mesmo, é quando conseguem ter mais impacto e tornar-se uma verdadeira ameaça. Tendo isso em atenção, os sistemas das infraestruturas críticas são, na sua maioria, arquitetados com vários mecanismos de redundância, para evitar que ataques às partes afetem o todo, mesmo quando dirigidos a um centro nevrálgico de controlo.

Um conflito maioritária ou exclusivamente cibernético, uma "ciberguerra", se quisermos, são, por enquanto, realidades distantes e improváveis, não só por causa das limitações que referimos, mas também porque para lançar ataques cibernéticos massivos, é necessário que tanto o atacante como recipiente do ataque tenham estruturas modernas o suficiente para realizar operações desse tipo. De pouco adianta planear um ataque cibernético a alvos com tecnologias rudimentares e longe de terem o funcionamento das suas infraestruturas digitalizadas.

Tudo isto culmina num tremendo paradoxo: os países com maior probabilidade de serem alvos de grandes ataques cibernéticos são os tecnologicamente mais desenvolvidos e, por isso, também os que têm mais capacidades de se defenderem e mitigarem os efeitos de ataques do género. Por sua vez, apesar de serem os que mais capacidades têm para contrariar ataques cibernéticos e conduzir uma defesa eficaz, são também os que mais têm a perder com um ataque bem-sucedido.

O ciberespaço pode ser um domínio predominantemente virtual, mas é um domínio com tremendo potencial para gerar danos físicos, políticos, sociais e económicos, mesmo que de forma indireta.

Enquanto domínio de conflito, o ciberespaço não se esgota como meio de propagação de táticas cinzentas ou de ataques cibernéticos. É comum restringir a ideia do ciberespaço à internet e à circulação de informação sob a forma de bits e bytes, mas tal como vimos no primeiro capítulo, o ciberespaço diz respeito a todo espetro eletromagnético, bem como aos dispositivos eletrónicos que usam esse espetro para comunicar, como um controlo remoto e o recetor dos seus comandos, ou entre computadores. Por isso, devemos também pensar na utilização de dispositivos militares cuja utilização é cada vez mais comum e cujo funcionamento começa também a ser fortemente auxiliado por sistemas de inteligência artificial, tornando-se autónomos, deixando de necessitar de mão humana para desempenharem as suas funções.

c) Autonomia e Inteligência Artificial

O propósito, ou, pelo menos o efeito, da evolução tecnológica sempre foi reduzir, sem perda de eficácia, o esforço ou o trabalho humano, desde as roldanas, que reduziam o esforço necessário para erguer objetos, às locomotivas e aos automóveis que substituíram a tração

animal e aceleraram os transportes terrestres, aos modernos sistemas que hoje cabem, literalmente, na palma das nossas mãos, integrados nos telemóveis que utilizamos diariamente. Mas a evolução tecnológica não se limitou a reduzir o trabalho humano: em muitos casos, este deixou de ser necessário por completo, substituindo-se os seres humanos por máquinas, como nos elevadores, nas caixas de supermercado, nas praças de portagens, nas fábricas, na agricultura. Estes dois efeitos da evolução tecnológica verificam-se também no meio militar: há formas mais simples e seguras de conduzir operações e, em muitas delas, a tecnologia começa a substituir o elemento humano. Circuitos fechados de videovigilância e sistemas de alarme substituíram guardas, *drones* equipados com câmaras de filmar, câmaras de infravermelhos, câmaras de visão térmica e visão noturna controlados remotamente substituíram voos de reconhecimento com aeronaves tripuladas, e *drones* com armas de fogo acopladas substituíram, nalguns casos, atiradores furtivos. Contudo, estes equipamentos continuam a ser manipulados por humanos, à distância, ou seja, não são completamente autónomos. Ainda compete a um ser humano decidir se se lança um ataque ou não. A grande preocupação está nos dispositivos autónomos que não requerem intervenção humana para operarem e com os quais se teme que eventos menores conduzam à escalada dum conflito – a uma "guerra instantânea" (*flash war*).

Um dos primeiros alertas para situações desta natureza foi o falso alarme nuclear em 1983, na União Soviética. A 26 de setembro desse ano, o sistema de alerta soviético anunciou o lançamento de cinco mísseis vindos dos Estados Unidos. O tenente-coronel Stanislav Petrov, que estava de serviço no centro de comando quando o aviso surgiu no ecrã, achou tratar-se dum falso alarme, porque "quando as pessoas começam uma guerra, não começam com apenas cinco mísseis"[189] e porque sempre lhe tinham dito que "um ataque nuclear seria massivo"[190]. Além disso, as instalações de RADAR, que deveriam ter detetado os mísseis poucos minutos depois

[189] Stanislav Petrov, citado por Susana Salvador, "O mundo esteve à beira da guerra nuclear e foi salvo por Petrov", *Diário de Notícias*, 26 de setembro de 2018, https://www.dn.pt/mundo/o-mundo-esteve-a-beira-da-guerra-nuclear-e-foi-salvo-por-petrov-9906827.html.
[190] Petrov, citado por Salvador, "O mundo esteve à beira da guerra nuclear".

do lançamento, não davam qualquer sinal. Petrov estava correto; o falso alarme deveu-se ao reflexo do sol nas nuvens, não a um lançamento nuclear. A URSS nunca chegou a tentar retaliar porque Petrov não reportou o alerta aos seus superiores. Um sistema completamente autónomo teria retaliado devido a um erro de computador e o mundo teria assistido a uma guerra nuclear.

Entretanto, surgiram outros exemplos em anos mais recentes.

Em 2013, um *drone* chinês sobrevoou as Ilhas Senkaku, pequenas ilhas desabitadas no Mar da China Oriental, contestadas entre a China e o Japão, com ambos a declarar que estas lhes pertencem. Como resposta, o Japão enviou um caça F-15 para intercetar o *drone*. O *drone* abandonou as Ilhas, mas, depois, o Japão adotou novas regras para agir em casos de incursões de *drones*. Essas novas regras eram mais agressivas do que as estabelecidas para intercetar aeronaves tripuladas: O Japão abateria qualquer drone que entrasse no seu território. A China respondeu declarando que qualquer ataque sobre os seus drones constituiria um "ato de guerra" e de que retaliaria[191].

À medida que os *drones* têm proliferado, quando a soberania sobre determinado território é clara e se deteta uma invasão, a prática comum tem sido abater os *drones* invasores, sem mais retaliações. Mas abater um *drone* quando a soberania do território em questão é disputada pode ter outros resultados. O país que vê o seu *drone* abatido pode sentir a necessidade de retaliar o abate para reafirmar a sua soberania, e o conflito pode escalar a partir daí.

Estas situações são relativamente fáceis de evitar enquanto os sistemas autónomos fizerem aquilo que os humanos esperam que façam. O perigo está nas situações em que as máquinas fazem algo que não era suposto.

Ainda com *drones*, situações deste género já se verificaram. Em 2010, um *drone* da Marinha americana desviou-se 37 km da sua rota entre Maryland e Washington DC, restringindo as circulações aéreas até se recuperar o seu controlo[192]. Em 2017, um outro *drone*,

[191] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, (Nova Iorque: W. W. Norton & Company, 2019), 230-231.
[192] Scharre, *Army of None*, 232.

agora do Exército americano, voou mais de 900 km depois de os operadores terem perdido o controlo sobre o aparelho, parando somente quando se despenhou numa floresta do Colorado[193]. Nem todos os acidentes terminam tão "bem".

Em 2011, os EUA perderam o controlo dum outro drone (um RQ-170) numa zona ocidental do Afeganistão. Poucos dias depois, apareceu nos noticiários iranianos, praticamente intacto e na posse das forças armadas iranianas. Na sequência da exibição do *drone* em televisão, começaram a circular na internet relatos de que o Irão o teria obtido interferindo com as comunicações do mesmo, cortando o sinal entre o *drone* e os seus operadores humanos e manipulando o seu sinal de GPS para o levar a aterrar numa base militar iraniana. Os EUA negaram as alegações de sequestro do *drone*, tendo admitido mais tarde que o *drone* era de facto seu[194].

Um *drone* de reconhecimento que se desvie da sua rota pode conduzir a humilhação internacional e à perda de tecnologia militar valiosa. A perda de controlo duma arma autónoma letal, por outro lado, pode ter um resultado muito diferente. Um robot programado para disparar só em situações de autodefesa pode acabar a disparar em situações em que os seres humanos desejariam que não o tivesse feito. Se militares ou civis doutra nação fossem feridos ou mortos na sequência desse evento, reduzir a tensão poderia tornar-se uma tarefa muito complicada.

No entanto, a preocupação com uma guerra instantânea não se prende tanto com dispositivos armados autónomos que operem com base em plataformas individuais, mas sim com armas autónomas que operam em sistemas em rede, interligados dentro do mesmo ramo das forças armadas e entre os ramos das forças armadas, em autonomia colaborativa.

"Se o meu agente autónomo está a patrulhar uma área, como a fronteira entre a Índia e o Paquistão, e o meu adversário está a patrulhar a mesma fronteira e tivermos dado certas permissões para responder

[193] Scharre, *Army of None*, 232.
[194] Scharre, *Army of None*, 232.

com força crescente em termos de autodefesa e [esses agentes autónomos] estivessem ligados a outros sistemas, a situação poderia intensificar-se muito rapidamente"[195].

A tecnologia é cada vez mais capaz e autónoma, e, mesmo que em muitos casos as valências da sua autonomia minimizem os riscos para a vida humana, há também casos em que a pode colocar em risco, em escalas de dezenas ou centenas de milhares de casualidades. Continua a faltar a esta tecnologia sensibilidade ou, se preferirmos, inteligência equivalente à humana, mesmo nos sistemas de inteligência artificial mais avançados.

A inteligência artificial atual encontra-se bem distante dos sistemas conscientes apresentados na ficção científica. E é precisamente por isso que as armas autónomas representam um risco: porque a inteligência artificial atual falha manifestamente em tarefas que requerem inteligência geral, ou, doutro modo, em tarefas que requerem a compreensão de contexto. A inteligência artificial atual consegue derrotar os mais brilhantes jogadores de xadrez, identificar corretamente objetos, pessoas, mas não consegue fazer interpretações complexas.

O que se espera que um dia seja criado é inteligência artificial geral. Este seria um tipo de inteligência artificial que demonstraria inteligência ao nível da humana em várias tarefas cognitivas. Sabe-se que esse tipo de inteligência é possível porque já o vimos – aliás, vemo-lo todos os dias – em nós, seres humanos. O que não se sabe é se é possível recriar esse tipo de inteligência em máquinas. Não se sabe, também, o que seria necessário para construir tais sistemas, mas coloca-se a hipótese de que os seres humanos nem teriam de criar inteligência artificial geral ou superinteligência artificial de modo direto.

"Definamos uma máquina ultrainteligente como uma máquina que consegue largamente ultrapassar todas as atividades intelectuais de qualquer homem, por mais ou menos inteligente que seja.

[195] Heather Roff, citada por Scharre, *Army of None*, 233.

Uma vez que a criação de máquinas é uma dessas atividades intelectuais, uma máquina ultrainteligente seria capaz de criar máquinas ainda melhores; ocorreria inquestionavelmente uma 'explosão de inteligência', e a inteligência do Homem seria deixada para trás. Portanto, a primeira máquina ultrainteligente é a última máquina que o homem precisaria de fazer, desde que a máquina fosse dócil o suficiente para nos dizer como a manter sob controlo"[196].

Se esta hipótese estiver correta, o ser humano não precisaria de criar superinteligência diretamente, teria apenas de criar a primeira "semente" e deixá-la germinar. A máquina trataria depois de se ir melhorando, criando máquinas cada vez mais inteligentes. Tudo isto é, por enquanto, conjetura, e alguns investigadores duvidam de que algum dia se consiga criar superinteligência artificial.

A dúvida acerca da criação de inteligência artificial geral é suportada pelo rumo que a inteligência artificial desenvolvida até agora tem seguido. A inteligência artificial atual consegue superar os seres humanos, mas sempre em domínios singulares, não domínios gerais. Por exemplo, a inteligência artificial criada para jogar xadrez, poker, ou conduzir veículos autonomamente consegue desempenhar estas tarefas melhor do que os seres humanos, mas o sistema que consegue conduzir não consegue jogar poker, e o que consegue jogar poker não sabe jogar xadrez. A inteligência artificial é, por enquanto, limitada às tarefas específicas para que é desenvolvida e, embora competente nessas tarefas individuais, parecemos estar longe dum sistema único que tenha múltiplas aplicações. Por isso, estamos também longe (e talvez nunca estejamos sequer perto) do tipo de inteligência artificial geral que a ficção científica nos pôs a temer: sistemas conscientes e autónomos que percebem que os seres humanos são prejudiciais à existência das máquinas ou à sobrevivência do planeta e por isso rescrevem os seus protocolos e se revoltam contra a espécie humana, tentando destruí-la. Contudo, já houve um pequeno susto, em 2017, com dois sistemas de inteligência artificial criados pelo Facebook,

[196] Irving Good, citado por Scharre, *Army of None*, 258.

que começaram a desenvolver linguagem própria para comunicar entre si. O projeto foi prontamente encerrado[197].

A inteligência artificial parece, por enquanto, direcionada para assistir os seres humanos nas suas tarefas e não para os substituir por completo. Parece, também, ser a direção mais sensata, mantendo a supervisão humana na atividade das máquinas. As máquinas podem ser inteligentes e ser capazes de processar informação muito mais depressa do que os seres humanos, mas falta-lhes a capacidade para avaliar contextos imprevistos pelos programadores e para tomar decisões face a circunstâncias que desconhecem.

Nesta questão de tomar decisões sem ter conhecimento das circunstâncias, há um diálogo num dos filmes da franquia 007 – *Skyfall* (2012) – que representa bem o que se passa à medida que se vai removendo o elemento humano da tecnologia. O diálogo é entre o protagonista, James Bond, e o novo mestre de armas, com o nome de código Q, muito mais jovem do que o anterior, e ocorre porque o agente secreto questiona a competência do novo Q por o achar demasiado novo, ao que este responde:

"Q: Consigo causar mais danos no meu portátil sentado e de pijama antes da minha primeira chávena de Earl Grey do que o senhor durante um ano no terreno.

JB: Então para que é que precisam de mim?

Q: De vez em quando um gatilho precisa de ser premido.

JB: Ou não premido… é difícil saber qual delas… de pijama."

Por outras palavras, "premir ou não premir o gatilho" não é uma decisão fácil, mesmo quando se está no terreno. Remova-se a presença humana do terreno e ponha-se esse ser humano a controlar um *drone* numa sala de comando a quilómetros de distância, e provavelmente haverá mais dúvidas na mente de quem pode "premir o gatilho". Removamos por completo o ser

[197] Andrew Griffin, "Facebook's artificial intelligence robots shut down after they start talking to each other in their own language", *Independent*, 31 de julho de 2017, https://www.independent.co.uk/life-style/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html.

humano da situação de disparar ou não disparar e coloquemo-lo apenas na programação da arma autónoma. Durante o período de programação, conjeturam-se os cenários possíveis, estabelecem-se diferentes níveis de retaliação para cada nível de ameaça, traça-se a linha entre a vida e a morte dum alvo. A máquina pode agir quase sempre como se tinha planeado, até, como em 1983, o sistema acusar uma falha que ninguém sabia que existia e executar o comando contrário ao que seria pretendido. Por exemplo, no caso da inteligência artificial criada pelo Facebook, a linguagem própria entre os dois sistemas foi criada porque os programadores não lhes impuseram, por lapso, a obrigação de comunicar numa língua específica. Ou seja, os seres humanos também erram e, por consequência, aquilo que os seres humanos criam e inventam também tem falhas. A questão é que o ser humano sente, escolhe, decide. A máquina simplesmente atua segundo os protocolos que lhe são instalados, "está só a cumprir ordens", que lhe foram dadas *a priori*.

Não se quer aqui passar a ideia de que usar dispositivos autónomos ou com inteligência artificial é errado só pelo fator da autonomia. Os dispositivos autónomos são uma mais-valia numa série de aplicações, como tarefas de vigilância, de patrulhamento ou missões de reconhecimento, permitindo executar estas ações sem colocar em perigo a vida de operacionais. E os sistemas autónomos, a nível informático, para além de mais-valias, são indispensáveis no âmbito da defesa e da segurança das máquinas e das informações sensíveis que estas contêm. O volume de ataques informáticos diários exige que essa defesa e segurança seja feita de forma autónoma, removendo os seres humanos da equação, porque, inevitavelmente, algo acabaria por lhes escapar e porque a resposta seria muito mais lenta ao nível manual[198]. Um sistema autónomo consegue corrigir vulnerabilidades de sistema em períodos muito curtos, às vezes numa questão de minutos, enquanto a correção humana leva, geralmente, meses[199].

[198] P. SCHARRE, *Army of None*, 239.
[199] P. SCHARRE, *Army of None*, 239.

O perigo da autonomia existe sobretudo em dispositivos autónomos armados, que não precisam de pedir licença para iniciar combate, ainda para mais se estiverem integrados em sistemas ligados a outros sistemas em autonomia colaborativa. Existe um perigo real de provocar uma escalação de conflito por atos menores que nem sequer foram deliberados e é por isso que se afigura recomendável que este tipo de equipamentos sejam mais auxiliares do que substitutos para os seres humanos, colocando os seres humanos na posição de supervisores destes aparelhos, mantendo presente uma capacidade deliberativa não automatizada que, por agora, não existe nas máquinas e que não sabemos se algum dia virá a existir.

Há quem especule que estas tecnologias autónomas, sobretudo a inteligência artificial, mudarão fundamentalmente a forma como a política é feita. Há quem creia que esta tecnologia possa servir para aproximar eleitos e eleitores, esbatendo a distância que existe entre ambos nas democracias representativas, tornando-as, de certo modo, mais diretas, uma vez que permitirão aos detentores de cargos políticos obter e processar mais informação sobre os anseios do eleitorado. Do mesmo modo, permitiria também antecipar comportamentos de mercado, crises económicas e financeiras, entre várias outras coisas. Acontece que esta é uma visão muito benigna da utilização da inteligência artificial na política que, embora possível, ainda não se verificou.

Não podemos, no entanto, esquecer o lado negro da inteligência artificial. A nível político, o principal receio é que a inteligência artificial seja usada por regimes autoritários, ou por líderes autoritários em regimes democráticos, para deslegitimar a democracia e as suas instituições. Crê-se que foi isso que a Rússia tentou fazer nos Estados Unidos em 2016, e espera-se que os regimes autoritários que têm investido mais em tecnologias digitais nos últimos anos o façam para perseguir objetivos semelhantes, nos EUA ou em qualquer outro país democrático.

De que serve aos regimes ou líderes autoritários deslegitimar a democracia?

A resposta curta é que deslegitimar a democracia legitima o exercício do poder de forma autoritária.

Com regimes (e líderes) autoritários poderosos, como na Rússia ou na China, a tática comum para o fazer é mostrar que aquilo que os regimes democráticos criticam nos regimes autoritários também acontece em democracia e que aquilo que se valoriza na democracia não é assim tão diferente num regime autoritário. Existe corrupção nos regimes democráticos. Abusa-se do poder. Troca-se o bem-estar de muitos pelo ganho de poucos. Também se verificam desrespeitos por liberdades e direitos dos cidadãos. E os regimes autoritários podem dizer que as instituições que lidam com estes problemas são apenas uma fachada que na realidade nada fazem para os retificar. E que outra fachada são os valores democráticos que se apreciam, como a separação de poderes, a liberdade de expressão e de imprensa, a livre escolha de representantes políticos, ao apontar situações em que o poder político se imiscui no judicial, ao introduzir narrativas de que a imprensa só escreve aquilo que o poder político não se importa que se saiba, ao dizer que a escolha democrática é uma ilusão, porque os candidatos com hipóteses de ser eleitos já estão alinhados com os interesses do costume. No fundo, a ideia que os regimes autoritários pretendem passar é a de que os regimes democráticos não são tão diferentes quanto fazem querer parecer e que o que têm de bom é apenas uma ilusão. A isso, acrescentam a ideia de que os regimes liberais democráticos só prestam auxílio a outros países para fomentar a sua agenda democrática, ao contrário de si, que investem em países em desenvolvimento sem alegadas contrapartidas.

Os regimes e líderes autoritários procuram apresentar as democracias e as suas instituições como profundamente hipócritas, de forma a minar o apoio às democracias na cena internacional, mas também de modo a que os cidadãos de regimes democráticos se tornem recetivos a formas autoritárias de exercer o poder político. Numa situação de conflito entre regime democrático e regime autoritário, erodir a crença nas instituições democráticas é fundamental, pois, como a História ensina, as grandes potências caem a partir de dentro, não de fora; e quando o conflito é entre um político/candidato de índole autoritária e outro de caráter

democrático, é importante desacreditá-lo e passar a noção de que só com um poder político mais firme, repressivo, até, se podem solucionar os problemas da nação.

A inteligência artificial pode servir este propósito, criando a desinformação e os "*deep fakes*" de que falámos a um ritmo frenético, disseminando-os através do ciberespaço, permitindo inundar os meios convencionais e digitais com este tipo de conteúdos, deturpando a realidade.

Respondamos, então, às questões que formulámos no início deste capítulo.

À primeira, se o ciberespaço, enquanto domínio de conflito, se vai tornar mais importante do que os domínios da terra, mar, ar e espaço, a resposta parece ser negativa, com uma exceção.

O ciberespaço tem vindo a ganhar uma importância crescente, sobretudo na última década, por todas as coisas que põe em funcionamento, tanto de aplicação civil e quotidiana, como de aplicação militar.

Porém, o ciberespaço é sobretudo instrumental, mais um meio do que um fim em si mesmo. Não se conquista território ciberespacial, não se destrói, fere ou mata no ciberespaço. Pode-se, sim, através do ciberespaço, obter informação relevante, controlo doutro sistemas, realizar comunicações e através delas comandar operações que permitem conquistar, destruir, ferir e matar no mundo físico, nos domínios da terra, do mar, do ar e do espaço. O ciberespaço é já um domínio incontornável e a sua importância certamente crescerá à medida que o volume e a velocidade de informação em circulação nele atingem novos patamares, mas enquanto domínio de conflito, não parece que ciberespaço venha a suplantar os outros em termos de importância. O ciberespaço é, de certo modo, um domínio que complementa os restantes e que expande o leque do que é possível fazer em cada um, possibilitando mais ações, com mais meios, mais força, até com mais segurança, mas não há, por enquanto, indícios de que venha a impor-se a qualquer um dos outros domínios.

Quanto à exceção, esta verifica-se no conflito estritamente político, que não envolve o recurso à força física e militar.

O ciberespaço estar a tornar-se um domínio extremamente relevante em processos eleitorais, particularmente na condução das campanhas políticas, sobretudo em países razoavelmente modernos, onde a maioria do eleitorado tem acesso irrestrito à internet e faz uso das plataformas sociais. Os meios de comunicação social tradicionais continuam a ser relevantes, mas estes estão também, na sua maioria, a digitalizar-se, com canais de televisão a disponibilizarem as suas emissões (em direto ou em diferido) online, com as rádios a permitir ouvir a sua emissão a partir dos seus *sites* e com a imprensa a ter cada vez menos exemplares impressos e a optar pelas edições e assinaturas digitais.

As próprias campanhas políticas começam também a digitalizar-se, uma vez que as redes sociais permitem dirigir melhor e com menos custos os conteúdos e anúncios de campanha aos eleitores que precisam de ser convencidos a votar em determinado candidato, a ir expressar o seu voto, ou no sentido inverso, a demover os eleitores inconquistáveis de irem votar noutro candidato, por mais deploráveis que sejam as táticas da supressão de voto.

O ciberespaço pode também ser usado para fazer o que se fez em 2016 nos EUA: espalhar desinformação, propagar boatos, rumores e teorias da conspiração, criar personagens políticas falsas, denegrir os outros candidatos, procurar influenciar uma eleição estrangeira sem se ter de manipular urnas ou contagens de votos, tudo de forma furtiva e à distância.

É ao nível da conflitualidade política, sem uso da força e violência física, que o ciberespaço, excecionalmente, parece estar a ganhar uma importância predominante.

Quanto à segunda questão, de se graças à aprendizagem automatizada e inteligência artificial, o ciberespaço se tornará predominantemente autónomo, a resposta parece ser sim, por um lado, e não, por outro.

O que nos leva a dizer, por um lado, que sim, é que as velocidades e volume da transferência de informação que nele se praticam obrigam à autonomização do mesmo, por questões de segurança. No presente, já não é possível combater todos os ataques cibernéticos

que ocorrem diariamente sem autonomia dos sistemas informáticos, quer sejam os de proteção direta, quer sejam os sistemas que tratam de corrigir falhas noutros programas. Essa autonomia é essencial não só para fins defensivos, mas também para fins ofensivos. Um Estado que tenha sido alvo dum ataque, se quiser retaliar, precisa que as suas capacidades cibernéticas ofensivas sejam autónomas na sua atuação. A eficácia dum vírus está largamente dependente da sua velocidade e se cada comando de ação tiver de ser dado manualmente, poderá ser detetado e anulado antes de cumprir o seu objetivo, tornando-o ineficaz.

Quanto ao lado pelo qual o ciberespaço não se tornará predominantemente autónomo, este prende-se principalmente com dispositivos armados e com alguns programas que, embora autónomos uma vez ativos, dependem duma primeira ação humana para ficarem operacionais. Como se disse, onde a autonomia e as limitações da inteligência artificial atual representam um risco demasiado grande, como no armamento autónomo, será mais seguro manter a tecnologia como um auxiliar e não fazer dela juiz, júri e executor. Será sensato manter as qualidades de juiz e de júri em mãos humanas, deixando a capacidade executória das máquinas dependente da decisão do Homem.

É sempre um risco especular sobre o futuro do que quer que seja, mas cremos tê-lo feito de forma adequada, baseando-nos nas tendências presentes, no conhecimento científico disponível e sem nos aventurarmos além daquele que é o futuro previsível e provável, e sem dar voz a teorias da conspiração ou a cenários extraídos unicamente da ficção científica. No entanto, se o futuro nos provar errados, não será só a nós, não será por não termos prestado às atuais tendências da evolução da tecnologia e do ciberespaço, nem por termos feito considerações rebuscadas face ao que se sabe no presente.

7. Conclusão

Chegados à etapa final deste trabalho, é pertinente mostrar se as questões de investigação que colocámos no início do mesmo foram respondidas.

Cremos ter respondido claramente à primeira questão, "qual o interesse da Rússia na eleição de Donald Trump como Presidente dos Estados Unidos da América?". O Kremlin viu na eleição Donald Trump uma dupla oportunidade: a oportunidade de evitar uma presidência americana de Hillary Clinton, que antagonizaria a Rússia no plano internacional, e a oportunidade de eleger um Presidente dos Estados Unidos que o Kremlin pudesse manipular por deter *kompromat* sobre ele. Tentámos mostrá-lo no capítulo 2.2.

À segunda, "de que forma é que Rússia e Cambridge Analytica usaram as redes sociais para recolher dados dos utilizadores e disseminaram, nas mesmas redes, conteúdo direcionado a utilizadores específicos, com bases nesses dados, com o intuito de persuadir a sua intenção de voto?", procurámos responder mostrando que, de forma sistemática, se foram criando entidades virtuais aparentemente desconexas da Rússia, que se faziam passar por cidadãos americanos e que iam publicando materiais danosos para Clinton e que Rússia e Cambridge Analytica foram explorando o ódio, o medo e a divisão social no eleitorado americano, servindo-se dos algoritmos das redes sociais que potenciavam a partilha e o alcance dessas publicações, levando mesmo os reais cidadãos a organizar comícios de apoio a Donald Trump. Fizemos essa exposição ao longo dos capítulos 2 e 3.

A resposta à terceira e última pergunta, "Quão importante é (ou virá a ser) o ciberespaço nos palcos de conflito político e militar?", foi-se construindo ao longo de toda a dissertação, mas merece uma resposta mais objetiva, clara e sucinta, agora na conclusão.

A eleição presidencial de 2016 nos Estados Unidos foi uma eleição, no mínimo, atípica, por várias razões.

Sempre houve candidatos improváveis a aparecer nas primárias dos partidos Republicano e Democrata, mas raramente estes duravam na corrida eleitoral. Quando Donald Trump anunciou a sua candidatura, o mundo reagiu com uma gargalhada, duvidando de que Trump chegasse aos debates finais das primárias republicanas, quanto mais que se tornasse o candidato nomeado dos Republicanos. Depois da nomeação republicana, a escolha entre os dois candidatos presidenciais parecia clara: as imprensas americana e europeia, os centros de sondagens, os cientistas políticos, os analistas, na sua larga maioria, apressaram-se a prever a vitória de Hillary Clinton, antiga Primeira Dama, Senadora e Secretária de Estado quando do outro lado estava um magnata do imobiliário e estrela televisiva dum *reality show* (The Apprentice), sem qualquer experiência política.

A eleição foi também atípica pelo tom populista que ganhou, especialmente com Donald Trump, com promessas de muros e deportações, pedidos de que Hillary Clinton fosse presa, com o uso de alcunhas como "crooked Hillary" (Hillary desonesta), com polémicas lançadas sobre a nacionalidade de Obama, com o pedido à Rússia para encontrar os e-mails desaparecidos de Clinton, entre outros. O decoro foi desaparecendo, de parte a parte, nas ações de campanha, nos debates, em todo o processo eleitoral.

Depois, houve a interferência estrangeira. Tanto quanto se sabe, esta terá sido a primeira vez que a Rússia tentou interferir com eleições dos Estados Unidos. Pouco se sabia sobre os esforços russos quando a denúncia foi feita e muitos eram céticos de que a interferência pudesse ter qualquer influência sobre o resultado das eleições. A campanha eleitoral prosseguiu, as eleições continuaram marcadas para o mesmo dia, a vitória de Hillary Clinton continuava a parecer certa para a maioria.

Quando o dia das eleições finalmente chegou e os resultados foram revelados, a incredulidade espalhou-se pelo mundo. A Europa não acreditava. O Kremlin celebrava. Os Estados Unidos pareciam confusos. E havia razão para a confusão. Donald Trump tinha menos votos populares expressos, cerca de 3 milhões menos, mas mais votos no Colégio Eleitoral, 304

de 538, mais 34 do que os necessários 270 para vencer a eleição. Trump ganhara graças à distribuição de delegados por Estado, cuja proporcionalidade varia para compensar Estados mais pequenos e retirar algum peso a Estados maiores, e à regra de soma-zero em que o vencedor num Estado fica com todos os delegados que o Estado em questão tiver para dar. Pela quinta vez na História dos EUA, o candidato com mais votos no Colégio Eleitoral não correspondia ao candidato com mais votos populares. Donald Trump tornou-se o Presidente Eleito em novembro de 2016 e sucedeu a Obama ao tomar posse em janeiro de 2017.

Por tudo isto, mas em particular pelo uso que se fez do ciberespaço, interessava estudar estas eleições para compreender como este pode impactar a política interna e a política internacional, como se está a tornar instrumental em cenários de conflito estritamente político ou armado, e como é um domínio de conflito em si mesmo.

Nunca será possível provar inequivocamente que o modo como o ciberespaço foi utilizado pela Rússia para executar ataques informáticos, roubar credenciais e documentos sensíveis dos Democratas, para os divulgar e para disseminar uma campanha de desinformação desempenhou um papel crucial no desfecho das eleições de 2016, mas cremos ter mostrado que é plausível que tenha. A Cambridge Analytica parece ter desempenhado um papel semelhante, ao recolher ilicitamente os dados pessoais de dezenas de milhares de utilizadores da rede social Facebook e ao usar esses mesmos dados e essa mesma rede social para propagar o mesmo tipo de desinformação favorável a Donald Trump e prejudicial a Hillary Clinton, quer os perfis psicográficos traçados tenham sido utilizados ou não.

De novo, reforçamos que o problema não foi a utilização de redes sociais *per se*. Os problemas são a ingerência externa por parte da Rússia, o roubo de informação, a propagação de desinformação, a obtenção e uso de forma não consentânea dos dados pessoais dos utilizadores e a exploração das divisões sociais, da polarização política e dos medos e receios individuais dos eleitores americanos, numa tentativa de os conduzir a eleger o seu Chefe de Estado não com base em factos, mas sim com base em narrativas inventadas. O problema foi a

intenção de instrumentalizar as redes sociais para esses fins e essa teve origem humana. O perigo não é tanto a tecnologia, mas sim a utilização que dela é feita.

Com a interferência nesta eleição, foi possível perceber que, também na geopolítica, o ciberespaço é uma extensão do mundo real, para a qual os líderes políticos transportam as suas mundividências e o modo de perseguir certas políticas, principalmente a política externa. Percebemos, também, que o ciberespaço permite atacar outro Estado furtivamente, sem atacar diretamente órgãos ou estruturas do Estado, lançando operações de subversão e manipulação psicológica sobre os seus cidadãos, de modo a condicionar uma eleição.

Percebeu-se, também a vulnerabilidade dos dados pessoais uma vez colocados na internet, tornou-se evidente a permeabilidade e a credulidade duma população democrática a conteúdos e notícias falsas. Simultaneamente, ficou também evidente a necessidade de legislar sobre a proteção e utilização dos dados pessoais dos internautas, bem como a necessidade de melhorar a literacia digital de todos os que navegam no ciberespaço.

Por fim, fomos levados a tecer considerações e a especular sobre futuro do ciberespaço e da tecnologia que o acompanha sob a perspetiva do conflito.

O ciberespaço tem assumido um papel cada vez mais relevante no nosso quotidiano. Temo-lo verificado ao longo dos anos, à medida que o estudo, o trabalho, o lazer e até mesmo as relações pessoais se foram digitalizando. Verificámo-lo particularmente este ano, assolado pela pandemia do vírus SARS-Cov-2 e da doença COVID-19, que forçou quase todos ao isolamento em casa, às aulas e reuniões por videoconferência, ao teletrabalho, às videochamadas para rever amigos e familiares, e às plataformas digitais para consumirmos cultura (com exceção dos livros impressos, se bem que muitos terão sido encomendados online). E embora o ciberespaço tenha todas estas valências, existem sempre, como dissemos, formas perversas de usar o que é criado com boas intenções.

Se o ciberespaço fosse um domínio em que não é possível realizar ataques, não teríamos de nos preocupar com a segurança e com a defesa neste domínio. Mas como os ataques

cibernéticos são uma realidade, essa preocupação é uma necessidade. A interferência russa constituiu, não só um ataque aos EUA e à sua democracia, mas também um ataque a todos os regimes democráticos, que valorizam a liberdade de expressão e a liberdade política de eleger, sem condicionalismos, os seus dirigentes políticos, servindo-se sobretudo da primeira para disseminar, através das redes sociais, uma criação americana, propaganda e desinformação.

O ataque russo à democracia líder do mundo ocidental, bem como o escândalo da Cambridge Analytica, levaram-nos a recear a utilização das redes sociais e o rumo que a tecnologia digital poderá seguir, podendo servir como uma ferramenta de subversão política nas mãos de atores maliciosos e a pensar sobre a aplicação de tecnologias relacionadas noutros contextos de conflito, mais violentos, e em que atos menores poderiam rapidamente escalar situações que, doutro modo, seriam evitáveis.

Sabemos que a Eleição Presidencial dos Estados Unidos de 2020 não foi objeto de estudo nesta dissertação e que não é ortodoxo mencionar na conclusão algo que não se tratou no corpo do trabalho, mas uma vez que a eleição decorreu durante a fase final da elaboração da mesma, que se conhece o seu resultado e que isso nos permite terminar este trabalho sem que se fique a especular sobre o que aconteceria na eleição seguinte, abordá-la-emos brevemente.

Mantendo assunção de que os esforços da Rússia e Cambridge Analytica em 2016 contribuíram para a vitória de Donald Trump, o alcance desses esforços parece ficar limitado pela avaliação que o eleitorado faz do mandato decorrido.

Em 2020, os serviços de informação voltaram a detetar tentativas de interferência russa nas eleições. Apesar disso, Donald Trump não conseguiu ser reeleito. Joe Biden, o nomeado Democrata, venceu, com o número mais alto de votos de sempre na História eleitoral dos EUA, cerca de 79 milhões. Donald Trump, no entanto, teve a segunda votação mais alta de sempre, cerca de 73 milhões de votos. Nunca uma eleição presidencial americana foi tão participada até

então, embora a elevada participação possa ser um resultado da polarização política a que se tem assistido nos últimos anos e é possível que muitos dos votos em Biden não tenham sido propriamente "por Biden", mas "contra Trump".

Seja por que motivos for, uma coisa é certa: se a Rússia voltou a tentar interferir, aplicando a mesma estratégia, pode até ter conseguido mobilizar mais eleitores favoráveis a Trump do que em 2016, mas, desta vez, não convenceu uma parte significativa do eleitorado anti-Trump a não exercer o seu direito de voto. Avaliando o primeiro mandato de Trump, a maioria dos eleitores americanos decidiu não lhe dar um segundo. Nem só de propaganda online se faz uma (re)eleição.

No final, o ciberespaço e a tecnologia continuarão a evoluir, a ser cada vez mais importantes nas nossas vidas, a mediar relações interpessoais e a mudar o mundo a vários níveis, incluindo o político. Devemos, no entanto, todos nós, estar atentos aos rumos que essa evolução seguirá. É uma responsabilidade de todos estar alerta aos riscos que a evolução tecnológica pode trazer, mas é uma responsabilidade principalmente do poder político, das empresas cujos modelos de negócio assentam no uso de dados pessoais, e dos programadores e desenvolvedores destas tecnologias. Os cenários de ficção científica em que a evolução digital culmina em futuros apocalípticos não têm de se tornar uma realidade, desde que no presente se evitem os caminhos que nos conduziriam a tal.

No final, não há outro futuro para além daquele que criamos no presente.

Anexos

Anexo 1: Tipos de malware, funções e características

Tabela 1:

Malware	Funções
Backdoor	Explora código existente ou instalado que permite o acesso não-autorizado aos computadores afetados
Bot	Programas de software que potenciam a execução de tarefas pelo computador contra a vontade do utilizador ou administrador
Exploit	Vulnerabilidades de software que costumam ter origem em "bugs" (erros de programação) de software permitem o acesso não-autorizado aos computadores afetados
HackTool	Explora sistema e programas em busca de ferramentas para penetrar e aceder a um computador
Rootkit	Ferramentas de software que permitem o acesso não-autorizado ao sistema operativo sem conhecimento do utilizador
Spyware/Adware	Software que invade um computador e transfere os dados para terceiros
Trojan	Software frequentemente instalado pelo utilizador com funções ocultas com o objetivo de manipular ou fornecer acesso a um computador
Vírus	Software malicioso que se auto-replica, geralmente oculto num ficheiro, requerendo abertura por parte do utilizador para iniciar a infeção
Worm	Software malicioso que se auto-replica sem requerer ações por parte do utilizador

Tabela 2:

Malware	Características
Entry Point Obfuscator	Malware que oculta como chegou ao computador
Metamórfico	Malware que altera o seu código além da encapsulação ou encriptação concebida para evitar a sua deteção, baseado em correspondência de padrões
Multi-part	Malware composto por múltiplos componentes que atuam em conjunto para atingir um resultado
Multi-partite	Malware concebido para infetar mais do que um objeto dentro dum sistema
Polimórfico	Malware que altera a sua encapsulação ou encriptação para continuamente ofuscar a sua aparência de modo a evitar a deteção de malware baseada em assinaturas de código
Residente	Malware que reside na memória ativa dum computador.
Furtivo	Ocultação ativa da sua presença para evitar deteção

Anexo 2: Os cinco traços de personalidade

O nome OCEAN é um acrónimo dos cinco traços de personalidade mais comuns:

- *Openness to experience* – Abertura para a experiência
- *Conscientiousness* – Conscienciosidade
- *Extraversion* – Extroversão
- *Agreebleness* – Agradabilidade/Amabilidade
- *Neuroticism/Negativity* – Instabilidade Emocional/Negatividade

A Abertura à Experiência inclui imaginação ativa, sensibilidade estética, atenção aos sentimentos, preferência pela variedade, curiosidade intelectual e discernimento independente. Pessoas com baixa pontuação neste traço tendem a ser convencionais no comportamento e conservadoras nas suas visões. Pessoas com pontuação elevada tendem a ser pouco

convencionais, dispostas a questionar a autoridade e a entreter novas ideias éticas, sociais e políticas. Indivíduos "Abertos" são curiosos acerca dos mundos interior (sentimentos e pensamentos) e exterior e as suas vidas são mais ricas em experiências. Estão dispostos a entreter ideias novas e valores não convencionais, e experimentam emoções positivas e negativas mais profundamente do que indivíduos fechados[200].

A Conscienciosidade refere-se a autocontrolo e ao processo ativo de planear, organizar, e executar tarefas. Uma pessoa conscienciosa age com propósito, tem força de vontade e é determinada. A conscienciosidade manifesta-se na orientação para objetivos (trabalho árduo e persistência), confiabilidade e em fazer as coisas de forma ordeira. Este traço pode conduzir a ser fastidioso, compulsivamente organizado ser viciado em trabalho[201].

A Extroversão inclui traços como sociabilidade, assertividade, propensão à atividade e à conversa. Os extrovertidos são enérgicos e otimistas. Os introvertidos, por outro lado, são mais reservados do que antipáticos, são mais independentes do que são seguidores, com ritmos mais constantes do que vagarosos. A Extroversão é caracterizada por experiências e sentimentos positivos, pelo que é considerada um traço positivo[202].

Agradabilidade/Amabilidade. Uma pessoa agradável/amável é fundamentalmente uma pessoa altruísta, empática com os outros e desejosa de os ajudar, esperando que os outros sejam do mesmo modo. O contrário é uma pessoa egocêntrica, cética das intenções dos outros e mais competitiva do que cooperativa[203].

A Instabilidade Emocional/Negatividade é uma dimensão de personalidade normal que indica uma tendência geral para sentir medo, tristeza, vergonha, raiva, culpa e repugnância. Indivíduos com pontuações elevadas deste traço podem estar em risco de desenvolver

[200] S. ROTHMANN e E. COETZER, "The Big Five Personality Dimensions", 69.
[201] S. ROTHMANN e E. COETZER, "The Big Five Personality Dimensions", 69.
[202] S. ROTHMANN e E. COETZER, "The Big Five Personality Dimensions", 69.
[203] S. ROTHMANN e E. COETZER, "The Big Five Personality Dimensions", 69.

problemas psiquiátricos. Uma pontuação elevada neste traço indica que uma pessoa é propensa a ter ideias irracionais, ser menos capaz de controlar impulsos e a lidar menos bem com stress[204].

Anexo 3: Exemplos de imagens propagandísticas publicadas nas redes sociais

Publicação do grupo de Facebook "Stop All Invaders".
Fonte: *MEME*, https://me.me/i/how-come-this-veteran-gets-nothing-while-this-illegal-gets-7e31128f46cb4e0ba9151581dbf783ba.

T-shirt vendida por Greater Half, loja de roupa alusiva ao patriotismo americano.
Fonte: *MEME*, https://me.me/i/obama-called-me-clinger-hillary-calls-me-deplorable-terrorists-call-7094b634880d43ab83be14ca36aeb3c8.

Publicação da página de "Instagram American Veterans".
Fonte: *Financial Times*, "How the Russian ads looked to 150m Facebook viewers", https://www.ft.com/content/9e2127e2-bf47-11e7-b8a3-38a6e068f464.

Publicação do grupo de Facebook "Heart of Texas".
Fonte: Aww Memes, https://awwmemes.com/i/lgbt-you-mean-liquor-guns-bacon-and-tits-heart-of-c005f0aa294045ba8f3c88e88ed5bd8b.

[204] S. ROTHMANN e E. COETZER, "The Big Five Personality Dimensions", 69.

Publicação do grupo de Facebook "Army of Jesus". Fonte: *Financial Times*, "How the Russian ads looked to 150m Facebook viewers", https://www.ft.com/content/9e2127e2-bf47-11e7-b8a3-38a6e068f464.

Publicação do grupo de Facebook "Army of Jesus". Fonte: Twitter, @MarkWarner, https://twitter.com/markwarner/status/925802644869959680?s=21

Anexo 4: Vozes copiadas com Inteligência Artificial

- Vídeo "Artificial Intelligence Can Clone Any Voice, Yours Too [LyreBird]": https://www.youtube.com/watch?v=vcdfw0NGPqg&ab_channel=vishalkalia
- Vídeo "Lyrebird - Create a digital copy of your voice": https://www.youtube.com/watch?v=YfU_sWHT8mo&feature=emb_logo&ab_channel=Lyrebird
- Site da Descript, detentora do software Lyrebird: https://www.descript.com/overdub?lyrebird=true&ref=Welcome.AI

Anexo 5: Produção automática de texto

- Vídeo "Automated Article Writing Software – It's FREE, Download it Today" https://www.youtube.com/watch?v=_kS5c0twDNc&ab_channel=AndyBlack

Anexo 6: Exemplos de recriações digitais do rosto de atores com recurso a CGI

Fonte: *In a Far Away Galaxy*, https://www.inafarawaygalaxy.com/2016/06/grand-moff-tarkin-quotes-from-star-wars.html.
Ator Peter Cushing (1913-1994), no papel de Grand Moff Tarkin em *Star Wars: A New Hope* (1977), à esquerda, e recriação digital do ator em *Star Wars: Rogue One* (2016), à direita.

Fonte: *Al-Arabiya*, "Here's how 'Furious 7' completed unfinished Paul Walker scenes", https://english.alarabiya.net/en/life-style/entertainment/2015/04/14/Here-s-how-Furious-7-completed-unfinished-Paul-Walker-scenes-with-CGI.html.
Ator Paul Walker (1973-2013), no papel de Brian O'Connor em *The Furious 7* (2015), à esquerda, e recriação digital da face do ator, sobreposta à do seu irmão, na cena final do mesmo filme, após a morte de Paul Walker durante o período de gravações, à direita.

Bibliografia

Livros

- Benkler, Yochai, Robert Faris, e Hal Roberts. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press, 2018.
- Carlin, John, e Garret Graff, *Dawn of the Code War: America's Battle Against Russia, China and the Rising Global Cyber Threat*. Nova Iorque: Public Affairs, 2018.
- Harding, Luke. *Collusion: How Russia Helped Trump Win the White House*. Londres: Guardian Faber, 2017.
- Jamieson, Kathleen. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President – What We Don't, Can't, And Do Know*. Oxford: Oxford University Press, 2018.
- Jones, Milo, e Philippe Silberzahn. *Constructing Cassandra: Reframing Intelligence Failure at the CIA, 1947–2001*. Stanford: Stanford University Press, 2013
- Kaiser, Brittany. *Targeted: My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy*. Londres: Harper Collins, 2019.
- Kuehl, Daniel. Citado em *Cyberpower and National Security*, editado por Franklin Kramer, Stuart Starr e Larry Wentz. Washington, DC: National Defense University Press, 2009.
- Mitchell, Tom. *Machine Learning*. Nova Iorque: Mcgraw Hill, 1997. Mitchell, Christopher. *The Structure of International Conflict*. Londres: Macmillan, 1981.
- Puyvelde, Damien, e Aaron Brantly. *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Cambridge: Polity, 2019.

- Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. W. W. Nova Iorque: Norton & Company, 2019
- Wylie, Christopher. *Mindf*ck: Inside Cambridge Analytica's Plot to Break the World*. Londres: Profile Books, 2019.

Investigações:

- Mueller, Robert. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election". Departamento de Justiça dos Estados Unidos, março de 2019.

- Steele, Christopher. "US Presidential Election: Republican Candidate Donald Trump's Activities in Russia and Compromising Relationship with the Kremlin". Fusion GPS Company Intelligence Report 2016/080, dezembro de 2016. https://assets.documentcloud.org/documents/3259984/Trump-Intelligence-Allegations.pdf

Artigos científicos:

- Aron, Leon. "Putinology". *The American Interest*, 30 de julho de 2015. https://www.the-american-interest.com/2015/07/30/putinology/.
- Aron, Leon. "The Putin Doctrine: Russia's Quest to Rebuild the Soviet State". *Foreign Affairs*, 8 de março de 2013. https://www.foreignaffairs.com/articles/russian-federation/2013-03-08/putin-doctrine
- Barak, Azy, e John Suler. "Reflections on the Psychology and Social Science of Cyberspace", 2008.

- Chorn, Adrien, e Monica Sato. “Maritime Gray Zone Tactics: The Argument for Reviewing the 1951 U.S.-Philippines Mutual Defense Treaty”, *Center for Strategic and International Studies*, 1 de outubro de 2019, https://www.csis.org/maritime-gray-zone-tactics-argument-reviewing-1951-us-philippines-mutual-defense-treaty.
- Fourkas, Vassilys. “What is ‘cyberspace’?”. Março de 2004. https://www.researchgate.net/publication/328928631_What_is_'cyberspace'.
- Fukuyama, Francis. “The End of History?”. *The National Interest*, n.º 16, (Verão de 1989): 3-18.
- Green, Michael, Kathleen Hicks, Zack Cooper, John Schaus e Jake Douglas. “Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence”. *Center for Strategic and International Studies*, maio de 2017. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170505_GreenM_CounteringCoercionAsia_Web.pdf.
- Moravec, Patricia, Randall Minas e Alan Dennis. “Fake News on Social Media: People Believe What They Want to Believe When it Makes No Sense at All”. Indiana University, 2018.
- O’Toole, Molly. “From Reset to Realpolitik, Clinton’s New Hard Line on Moscow”. *Foreign Policy*, 22 de setembro de 2016. https://foreignpolicy.com/2016/09/22/hillary-clintons-new-colder-cold-war-russia-putin-election/.
- Polyakova, Alina, e Spencer Boyer. “The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition”. *Foreign Policy at Brookings*, março de 2018. https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf
- Ronald Deibert e Rafal Rohozinski. “Liberation vs. Control: The Future of Cyberspace”. *Journal of Democracy* 21/4 (outubro de 2010): 43-57.

- Rothmann, Sebastiaan, e Elize Coetzer. “The Big Five Personality Dimensions and Job Performance”. *SA Journal of Industrial Psychology* 29, (2003): 68-74.
- Scheufele, Dietram, e David Tewksbury. “Framing, Agenda Setting, and Priming: The Evolution of Three Media Effects Models”. *Journal of Communication* 57, n.º1 (março de 2007): 9-20.
- Seepersad, Dana-Marie. “The politics of bipolarity and IPE in contemporary times”. *E-International Relations,* 17 de fevereiro de 2011. https://www.e-ir.info/2011/02/17/the-politics-of-bipolarity-and-ipe-in-contemporary-times/
- Serra, Adriano. “O auto-conceito”. *Análise Psicológica*, 2 (VI), 1988: 101-110.
- Vosoughi,Soroush, Deb Roy e Sinan Aral. “The Spread of True and False News Online”. MIT Initiative on The Digital Economy. Massachussets Institute of Technology, 2018.
- Walker, Christopher, e Jessica Ludwig. “The Meaning of Sharp Power: How Authoritarian States Project Influence”. *Foreign Affairs*, 16 de novembro de 2017. https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.
- Youyou, Wu, Michal Kosinski e David Stillwell. “Computer-based personality judgments are more accurate than those made by humans”. *Proceedings of the National Academy of Sciences* 112, nº 4, (janeiro de 2015): 1036-1040.

Artigos de órgãos de comunicação social:

- “Ataque informático. SNS desliga e-mails por precaução”, *Sol*, 27 de junho de 2017, https://sol.sapo.pt/artigo/569761/ataque-informatico-sns-desliga-e-mails-por-precaucao.

- "Revealed: Cambridge Analytica data on thousands of Facebook users still not deleted". *Channel 4 News*, 28 de março de 2018. https://www.channel4.com/news/revealed-cambridge-analytica-data-on-thousands-of-facebook-users-still-not-deleted
- Bump, Philip. "4.4 million 2012 Obama voters stayed home in 2016 — more than a third of them black". *The Washington Post*, 12 de março de 2018. https://www.washingtonpost.com/news/politics/wp/2018/03/12/4-4-million-2012-obama-voters-stayed-home-in-2016-more-than-a-third-of-them-black/.
- Cadwalladr, Carole, e Emma Graham-Harrison. "Cambridge Analytica: links to Moscow oil firm and St Petersburg university". *The Guardian*, 17 de março de 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-academic-trawling-facebook-had-links-to-russian-university.
- Cadwalladr, Carole, e Stephanie Kirchgaessner. "Cambridge Analytica director 'met Assange to discuss US election'". *The Guardian*, 7 de junho de 2018. https://www.theguardian.com/uk-news/2018/jun/06/cambridge-analytica-brittany-kaiser-julian-assange-wikileaks.
- Cimpanu, Catalin. "Two more cyber-attacks hit Israel's water system". *ZDNet*, 20 de julho de 2020. https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/.
- DiChristopher, Tom. "Cyberattack uncovers shortfalls in natural gas pipeline security". *S&P Global*, 19 de fevereiro de 2020. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyberattack-uncovers-shortfalls-in-natural-gas-pipeline-security-57179953.
- Englund, Will. "The roots of the hostility between Putin and Clinton". *The Washington Post*, 28 de julho de 2016. https://www.washingtonpost.com/world/europe/the-roots-of-the-hostility-between-putin-and-clinton/2016/07/28/85ca74ca-5402-11e6-b652-315ae5d4d4dd_story.html

- Frenkel, Sheera. “For Russian ‘Trolls,’ Instagram’s Pictures Can Spread Wider Than Words”. *The New York Times*, 17 de dezembro de 2017. https://www.nytimes.com/2017/12/17/technology/instagram-russian-trolls.html?auth=login-facebook.
- Griffin, Andrew. “Facebook's artificial intelligence robots shut down after they start talking to each other in their own language”. *Independent*, 31 de julho de 2017. https://www.independent.co.uk/life-style/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html.
- Grynbaum, Michael, e John Herrman. “Breitbart Rises From Outlier to Potent Voice in Campaign”. *The New York Times*, 26 de agosto de 2016. https://www.nytimes.com/2016/08/27/business/media/breitbart-news-presidential-race.html.
- Mcelwee, Sean, Jesse Rhodes, Brian Schaffner e Bernard Fraga. “The Missing Obama Millions”. *The New York Times*, 10 de março de 2018. https://www.nytimes.com/2018/03/10/opinion/sunday/obama-trump-voters-democrats.html?auth=login-facebook.
- Mehrotra, Kartikay. “California Governor Proposes Digital Dividend Aimed at Big Tech”. *Bloomberg*, 12 de fevereiro de 2019, https://www.bloomberg.com/news/articles/2019-02-12/california-governor-proposes-digital-dividend-targeting-big-tech.
- Moire, Jennifer. “Facebook App Proves A Game-Changer for Obama Campaign”. *Adweek*, 21 de novembro de 2012. https://www.adweek.com/digital/facebook-app-obama-campaign/
- Page, Clarence. "Why nobody complained when Obama used Facebook data”. *Chicago Tribune*, 23 de março de 2018. https://www.chicagotribune.com/columns/clarence-page/ct-perspec-page-facebook-zuckerberg-obama-20180323-story.html

- Pettersen, Trude. “Russia loses $600 billion on sanctions and low oil prices”. *The Barents Observer*, 5 de fevereiro de 2016. https://thebarentsobserver.com/ru/node/414.
- Ruffini, Patrick. “Why Russia’s Facebook ad campaign wasn’t such a success”. *The Washington Post*, 3 de novembro de 2017. https://www.washingtonpost.com/outlook/why-russias-facebook-ad-campaign-wasnt-such-a-success/2017/11/03/b8efacca-bffa-11e7-8444-a0d4f04b89eb_story.html
- Séneca, Hugo. “Hackers publicam passwords de milhares de médicos e enfermeiros do SNS na internet”. *Expresso*, 20 de julho de 2020. https://expresso.pt/sociedade/2020-07-20-Hackers-publicam-passwords-de-milhares-de-medicos-e-enfermeiros-do-SNS-na-internet
- Shuster, Simon. “Vladimir Putin's Bad Blood with Hillary Clinton”. *Time*, 25 de julho de 2016. https://time.com/4422723/putin-russia-hillary-clinton/.
- Stanislav, Petrov, citado por Susana Salvador, “O mundo esteve à beira da guerra nuclear e foi salvo por Petrov”. *Diário de Notícias*, 26 de setembro de 2018. https://www.dn.pt/mundo/o-mundo-esteve-a-beira-da-guerra-nuclear-e-foi-salvo-por-petrov-9906827.html.
- Stroud, Court. “Cambridge Analytica: The Turning Point In The Crisis About Big Data”, *Forbes*, 30 de abril de 2018. https://www.forbes.com/sites/courtstroud/2018/04/30/cambridge-analytica-the-turning-point-in-the-crisis-about-big-data/.
- Weaver, Matthew. “Facebook scandal: I am being used as scapegoat – academic who mined data”. *The Guardian*, 21 de março de 2018. https://www.theguardian.com/uk-news/2018/mar/21/facebook-row-i-am-being-used-as-scapegoat-says-academic-aleksandr-kogan-cambridge-analytica.

Fontes audiovisuais:

- Collins, Damian. *in* "Cambridge Analytica's Facebook data was accessed from Russia, MP says". *CNN*, vídeo, 00:29, 17 de julho de 2018. https://money.cnn.com/2018/07/17/technology/cambridge-analytica-data-facebook-russia/index.html.
- Fernando, Randy. *The Social Dilemma*, realizado por Jeff Orlowski (Netflix, 2020), https://www.netflix.com/title/81254224.
- O'Sullivan, Donie. "Scientist at center of data controversy says Facebook is making him a scapegoat". *CNN*, vídeo, 1:26, 20 de março de 2018. https://money.cnn.com/2018/03/20/technology/aleksandr-kogan-interview/index.html
- Tribolet, José. "Quem Protege a Democracia?". *Prós e Contras*, episódio 14, temporada 17, transmitido a 15 de abril de 2019, 2ª parte, 12:58. https://www.rtp.pt/play/p5337/e401358/pros-contras/737263.

Outras fontes:

- "algoritmo", in Dicionário Priberam da Língua Portuguesa, 2008-2020, https://dicionario.priberam.org/algoritmo (consultado em 29-06-2020).
- Burr, Richard. "Statement of Chairman Richard Burr". Richard Burr: US Senator for North Carolina, 1 de novembro de 2017. https://www.burr.senate.gov/imo/media/doc/Chairman%27s%20SFR.pdf.
- Comissão Europeia. "Special Eurobarometer 487a – Report: The General Data Protection Regulation", junho de 2019. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222.

- Constituição da Federação da Rússia, 1993.
- Estado-Maior Conjunto Dos Estados Unidos. "Cyberspace Operations". *Joint Publication* 3-12, 2018.
- Ezzeldin, Maria. "US-Russia Relations after the Crisis in Ukraine". Diss. de Mestrado, Universidade Americana do Cairo, 2015.
- "Field Manual 100-5 Operations", Departamento do Exército, 1993.
- Jenkins, Holman. "Mueller Focuses on Molehills". *Wall Street Journal*, 20 de fevereiro de 2018. https://www.wsj.com/articles/mueller-focuses-on-molehills-1519169467.
- "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security". Departamento de Segurança Interna dos Estados Unidos, 7 de outubro de 2016. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.
- Markey, Edward. Proposta Legislativa "Consent Act". https://www.markey.senate.gov/imo/media/doc/CONSENT%20Act%20text.pdf.
- "Psychological operations" *in* "Dictionary of Military and Associated Terms", Department of Defense, Joint Publication 1-02, 12 de abril de 2001, 427, https://www.cia.gov/library/abbottabad-compound/B9/B9875E9C2553D81D1D6E0523563F8D72_DoD_Dictionary_of_Military_Terms.pdf.
- Público. "Política de Privacidade". Última modificação a 22 de junho de 2018. https://www.publico.pt/nos/politica-de-privacidade.
- Putin, Vladimir. "Interview to American TV channel NBC". President of Russia, 10 de março de 2018. http://en.kremlin.ru/events/president/news/57027.
- "Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE

(Regulamento Geral sobre a Proteção de Dados)". Jornal Oficial da União Europeia L119.

- Stamos, Alex. "An Update On Information Operations On Facebook". Facebook Newsroom. Facebook, 6 de setembro de 2017. https://about.fb.com/news/2017/09/information-operations-update/.
- Statista. "Average number of Facebook friends of users in the United States in 2016", outubro de 2016. https://www.statista.com/statistics/398532/us-facebook-user-network-size/.
- Statista. "Leading countries based on Facebook audience size as of July 2020", julho de 2020. https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/.
- Twitter. "Update on Twitter's review of the 2016 US election". Twitter Public Policy, atualizado a 31 de janeiro de 2018. https://blog.twitter.com/en_us/topics/company/2018/2016-election-update.html.
- Warren, Elizabeth. Proposta Legislativa "The Corporate Executive Accountability Act". https://www.warren.senate.gov/imo/media/doc/2019.4.1%20Corporate%20Executive%20Accountability%20Act%20Summary.pdf.
- Weedon, Jen, William Nuland e Alex Stamos. "Information operations and Facebook". Facebook Newsroom, Facebook, 27 de abril de 2017, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.