1/6

KONRAD ADENAUER STIFTUNG

# Segurança Cibernética e Interesse Nacional durante Período de Campanha

# Cybersecurity and National Interest during Campaign Period

CEBRI BRAZILIAN CENTER FOR INTERNATIONAL RELATIONS

União Europeia

COLEÇÃO DE POLICY PAPERS
THE POLICY PAPERS COLLECTION

XVFORTE

A Conferência de Segurança Internacional do Forte de Copacabana é um projeto euro-brasileiro organizado em conjunto pela Fundação Konrad Adenauer (KAS) e pelo Centro Brasileiro de Relações Internacionais (CEBRI), com apoio da Delegação da União Europeia no Brasil. A conferência é concebida como um fórum de diálogo entre a América do Sul e a Europa. Seu objetivo é reunir especialistas do setor governamental, acadêmico e privado para discutir assuntos atuais no âmbito de segurança que sejam de interesse comum aos parceiros dos dois lados do Atlântico. Desde seu início em 2003, a conferência se transformou, de uma reunião relativamente pequena, no maior fórum de segurança da América Latina. Na sua 15ª edição, a conferência de 2018 tem como tema 'Gestão de crises internacionais'. A conferência é aberta ao público e os participantes são incentivados a participar ativamente das discussões. Esta coleção de Policy Papers reflete os temas centrais do evento e pretende identificar desafios, bem como fazer recomendações políticas para o futuro. As edições anteriores da publicação sobre Segurança Internacional da Conferência do Forte de Copacabana podem ser acessadas na página oficial da KAS Brasil (www.kas.de/brazil).

The Forte de Copacabana International Security Conference is a joint Euro-Brazilian project organised by the Konrad Adenauer Foundation (KAS) in partnership with the Brazilian Center for International Relations (CEBRI) and supported by the Delegation of the European Union to Brazil. The conference is conceived as a forum for dialogue between South America and Europe. It aims to bring together experts from a wide range of government, academic and private-sector backgrounds to discuss current security-related issues which are of interest to the partners on both sides of the Atlantic. Since its inception in 2003, the conference has emerged from a relatively small gathering to Latin America's largest security forum to date. The topic of the 15th edition of the conference is 'International crisis management'. The conference is open to the public and the audience is encouraged to actively engage in discussions. This collection of Policy Papers reflects the major themes of the event and intends to identify challenges as well as make policy recommendations for the future. Previous volumes of the Forte de Copacabana International Security Conference publication can be accessed on the KAS-Brazil Office website (www.kas.de/brazil).

**www.kas.de/brasil**

Editor Editor
**Dr. Jan Woischnik**

Coordenação editorial Project Coordination
**Ariane Costa**
**Diogo Winnikes**
**Reinaldo Themoteo**

Composição Composition
**Nilson Brandão / Conteúdo Evolutivo**

Colaboração Editorial Support
**Rafael Radischat**
**Renata Dalaqua**

Projeto Gráfico Design
**Charles Steiman**
**Daniela Knorr**

Impressão Print
**Stamppa**

© 2018, Konrad Adenauer Stiftung e.V.

Fundação Konrad Adenauer
Rua Guilhermina Guinle, 163
Botafogo CEP: 22270-060
Rio de Janeiro, RJ – Brasil
Tel: (+55/21) 2220-5441
Fax: (+55/21) 2220-5448

www.kas.de/brasil
kas.brasil
kasbrasil

Todos os direitos desta edição são reservados à Fundação Konrad Adenauer. Autores podem ser citados indicando a revista como fonte. As opiniões aqui externadas são de exclusiva responsabilidade de seus autores. All rights are reserved to Konrad Adenauer Foundation. Authors may be quoted if the publication name is referred as source. Authors are exclusively responsible for all concepts and information presented in this book.

ISSN 2176-297X

# COLEÇÃO DE POLICY PAPERS
## THE POLICY PAPERS COLLECTION

### 1/6
Segurança Cibernética e Interesse Nacional durante Período de Campanha

Cybersecurity and National Interest during Campaign Period

Tradução e revisão Translation and Revision: Leslie Sasson Cohen

### 2/6
Gestão de Crises Internacionais

International Crisis Management

Tradução e revisão Translation and Revision: Leslie Sasson Cohen

### 3/6
O Desafio da Migração Venezuelana para a Região Perspectiva Colombiana

The Challenge of Venezuelan Migration in the Region A Colombian Perspective

Francesca Ramos Pismataro

Tradução e revisão Translation and Revision: Leslie Sasson Cohen

### 4/6
Fluxos Migratórios e sua Gestão: A Perspectiva Europeia

Migration Flows and their Management: The European Perspective

Tradução e revisão Translation and Revision: Leslie Sasson Cohen

### 5/6
Risco Climático na América do Sul: Agenda de segurança pública interna ou de defesa interestatal?

Climate Risk in South America: A domestic public security agenda or an inter-State defense agenda?

Eduardo Viola

Matías Franchini

Tradução e revisão Translation and Revision: Leslie Sasson Cohen

### 6/6
A Crise da Mudança do Clima e sua Gestão: A Perspectiva Europeia

Climate Change Crisis and its Management: The European Perspective

Janani Vivekananda

Stephan Wolters

Tradução e revisão Translation and Revision: Leslie Sasson Cohen

KONRAD
**ADENAUER**
**STIFTUNG**

A Fundação Konrad Adenauer (KAS) é uma fundação política alemã. Através do nosso escritório central na Alemanha e dos mais de 90 escritórios espalhados pelo mundo, gerenciamos mais de 200 projetos abrangendo mais de 120 países. Tanto na Alemanha quanto no exterior, nossos programas de educação cívica têm como objetivo promover os valores de liberdade, paz e justiça, bem como diálogo e cooperação. Como think tank e agência de consultoria, nós focamos na consolidação da democracia, na unificação da Europa, no fortalecimento das relações transatlânticas, assim como na cooperação internacional e no diálogo. Os nossos projetos, debates e análises visam o desenvolvimento de uma forte base democrática para ação política e cooperação.
No Brasil, nossas atividades concentram-se no diálogo de segurança internacional, educação política, estado de direito, funcionamento de instituições públicas e seus agentes, economia social de mercado, política ambiental e energética assim como as relações entre o Brasil, a União Europeia e a Alemanha.

The Konrad Adenauer Stiftung (KAS) is a German political foundation. From our headquarters in Germany and 90 field offices around the globe, we manage over 200 projects covering over 120 countries. At home as well as abroad, our civic education programmes aim at promoting the values of freedom and liberty, peace and justice, as well as dialogue and cooperation. As a think tank and consulting agency we focus on the consolidation of democracy, the unification of Europe, the strengthening of transatlantic relations, as well as on international cooperation and dialogue. Our projects, debates and analyses aim to develop a strong democratic base for political action and cooperation.
In Brazil our activities concentrate on international security dialogue, political education, the rule of law, the workings of public institutions and their agents, social market economy, environmental and energy policy, as well as the relations between Brazil, the European Union and Germany.

**União Europeia**

A Delegação da União Europeia (UE) no Brasil é uma das mais de 130 Delegações da UE no mundo. A Delegação da UE no Brasil está focada na promoção das relações políticas e econômicas entre a UE e o Brasil, de acordo com a parceria estratégica EU–Brasil estabelecida em 2007. A UE e o Brasil estabeleceram relações diplomáticas em 1960, criando estreitos laços históricos, culturais, econômicos e políticos. Dentre os tópicos centrais da parceria estratégica entre a UE e o Brasil estão questões econômicas, a cooperação em questões-chaves de política externa e o enfrentamento conjunto de desafios globais em áreas como direitos humanos, mudanças climáticas e a luta contra a pobreza. Mais de 30 diálogos formais no setor político foram iniciados entre a União Europeia e autoridades brasileiras para enfrentar esses desafios. Além disso, a União Europeia e o Brasil são parceiros comerciais importantes e os países da União Europeia recebem mais de 20% da exportação brasileira. A União Europeia também é o maior investidor estrangeiro no Brasil com cerca de 60% do investimento estrangeiro.

The European Union (EU) Delegation to Brazil is one of over 130 EU Delegations around the world. The EU Delegation to Brazil is focused on promoting political and economic relations between the EU and Brazil, in line with the EU–Brazil Strategic Partnership established in 2007. The EU and Brazil established diplomatic relations already in 1960 building on close historical, cultural, economic and political ties. Central topics of the EU–Brazil Strategic Partnership include economic issues, cooperation on key foreign policy issues, and jointly addressing global challenges in areas such as human rights, climate change as well as the fight against poverty. Over 30 formal sector-policy dialogues between the European Union and Brazilian authorities have been initiated to address these challenges. The European Union and Brazil are also important trading partners and the countries of the European Union account for over 20% of Brazil's exports. The European Union is also the largest foreign investor in Brazil with around 60% of the foreign investment originating from the European Union.

CEBRI
BRAZILIAN CENTER FOR
INTERNATIONAL RELATIONS

Independente, apartidário e multidisciplinar, o Centro Brasileiro de Relações Internacionais (CEBRI) é uma instituição sem fins lucrativos, que atua para influenciar positivamente a construção da agenda internacional do país. Fundado há 20 anos por um grupo de empresários, diplomatas e acadêmicos, o CEBRI tem ampla capacidade de articulação, engajando os setores público e privado, a academia e a sociedade civil. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes, e com uma rede de mantenedores constituída por instituições, empresas e indivíduos de múltiplos segmentos.

O CEBRI promove a expansão e aprofundamento do debate sobre a política externa brasileira e a inserção do Brasil no mundo, pautado na formulação de políticas públicas e no fomento de diálogo entre os mais relevantes atores brasileiros e globais. O reconhecimento de sua importância internacional é atestado pelo ranking do Programa de Think Tanks e Sociedade Civil da Universidade da Pensilvânia, que destacou o CEBRI como o segundo melhor think tank do Brasil e o quarto melhor da América Latina.

Independent, nonpartisan and multidisciplinary, the Brazilian Center for International Relations (CEBRI) is a non-profit institution that acts to have a positive influence on the construction of the country's international agenda. Founded 20 years ago by a group of business leaders, diplomats and academics, CEBRI has the ability to engage the public and private sectors, academia and civil society. In addition, it counts on an engaged Board of Trustees formed by prominent figures and on a diverse network of sponsors made up of institutions, companies and individuals from multiple sectors.

CEBRI promotes the expansion and deepening of debates on Brazilian foreign policy and Brazil's international insertion, marked by the formulation of public policies and the promotion of dialogue amongst the most relevant Brazilian and global stakeholders. The recognition of its international importance is evidenced by the University of Pennsylvania's Think Tanks and Civil Societies Program, which ranked CEBRI as Brazil's second best think tank and the fourth best in Latin America.

# Segurança cibernética e interesse nacional durante período de campanha

# Cybersecurity and National Interest during Campaign Period

**1ª Reunião Preparatória para a XV Conferência de Segurança Internacional do Forte de Copacabana em 5 de abril de 2018, no Ministério da Defesa do Brasil**

**1st Preparatory Meeting for the XV Forte de Copacabana Conference on International Security on April 5th, 2018, at the Ministry of Defense of Brazil**

Em 2018, a Conferência de Segurança Internacional do Forte de Copacabana chega a sua 15ª edição. Consolidando-se como o principal foro de debate sobre o tema na América Latina, a Conferência contribui para promover o conhecimento e a troca de experiências entre acadêmicos e *practitioners* das áreas de defesa e segurança internacional.

Como continuidade do importante debate sobre cyber-segurança iniciado na Conferência de 2017, a primeira reunião preparatória para a XV Conferência ocorreu em 05 de abril de 2018, em Brasília, e teve como tema "Segurança cibernética e interesse nacional durante período de campanha". Representantes do governo, do setor privado, da academia e da sociedade civil se reuniram para analisar e debater tal temática, tão importante em ano de eleição presidencial no Brasil. A possibilidade de interferência de robôs e falsos perfis no debate online, propagando *fake news* – justo no momento em que o diálogo precisa ser claro, cristalino e propositivo – também foi levada em consideração na definição das questões para debate.

Além da troca de ideias, a reunião preparatória permitiu a elaboração do presente position paper. Respeitando o princípio de não-atribuição, o paper contém os principais eixos e fundamentos das discussões e, ainda, apresenta recomendações relevantes para aperfeiçoar as práticas e instituições vinculadas à segurança cibernética.

In 2018 the Forte de Copacabana International Security Conference reaches its 15th edition consolidating itself as the main forum for debate on security in Latin America. The Conference contributes to promote the dissemination of knowledge and the exchange of experiences between scholars and practitioners in the areas of defense and international security.

In order to give continuity to the important cybersecurity debate initiated at the 2017 Conference, the first preparatory meeting for the 15th edition took place on April 5th, 2018 in Brasília, and revolved around the theme "Cybersecurity and national interest during campaign period". Representatives from the government, the private sector, the academia and civil society gathered to analyze and discuss this issue, which is so important for Brazil due to this year's presidential elections. The possibility of interference by robots and fake profiles in the online debate, propagating fake news - when the dialogue needs to be clear, transparent and purposeful - has also been taken into account when defining the issues for discussion.

In addition to the exchange of ideas, the preparatory meeting allowed for the preparation of the present position paper. Respecting the principle of non-attribution, the paper contains the main cores and foundations of the debate and also presents relevant recommendations to improve the practices and institutions related to cybersecurity.

Paranoia. No other word can embody so much of the current concerns about cyber attacks, virtual manipulation attempts and the proliferation of what is known as fake news - scattered untruths apparently legitimate in origin and content. Lying is not a novelty in human experience. From Latin come the quotes, according to which, every man is a liar (*omni homo mendax*) and that one lie drags along another lie (*fallacia, alia aliam trudit*).

Notably since 2016 the world has become involved in discussions, research, studies and even accusations between countries on the subject. Russia was accused of influencing the US presidential race that year, and even in 2018 concerns remain that the enemy of the Cold War Era could supposedly interfere in the parliamentary elections scheduled for November. Also in 2016, the information technology environments of the Rio de Janeiro Olympic games were targeted by cybercriminals with over 40 million security alerts issued. In the last presidential elections in Brazil, more than 200 thousand attacks per second tried to overthrow the servers according to official data. A study performed by the Department of Public Policy Analysis (DAPP) of the Getulio Vargas Foundation (FGV)[1] shows that the use of bots (robots) and the propagation of fake news will be inevitable in Brazil's 2018 presidential elections.

The digital ecosystem has transformed the human being's ability to do what he most appreciates - to interact - and has amplified the complexity of ways of relating to one another. Cyber risk advances along with increasing innovation and society's dependence on information technologies. Advances in areas such as the Internet of Things (IOT) and Artificial Intelligence (AI) attract and make cybercrime even more potent. The level of sophistication in the design and execution of attacks includes malicious *malware* (malicious infiltration programs) self-propagating programs aimed at destroying systems, as well as *ransomware* (codes that prevent access to stored data and require ransom to return the connection). In parallel, the advancement of contact and exchange intermediation through digital platforms, applications and social networks to seek information and relationships between individuals and social groups, both increase connectivity effectiveness and bring new opportunities for obscure, illicit and distorted activities.

## Digital Complexity

It is appropriate to size the digital complexity associated with electoral processes in at least three perspectives[3]. The first is related to cybersecurity and actions of influence: one is linked to the integrity of systems that allow elections to be held in connection with electronic ballot boxes and the internet; the other is linked to the legitimate debate and arguments to convince the public opinion. The suspicions about elections that use information technology and are fully computerized, as is the case of Brazil, are usually related to three factors: fear of deviation of votes from one candidate to another, alteration of the proportion of votes given to each candidate and the insertion of procedures that breach the system or generate uncertainty as to the credibility of the process. As for the ability to influence and persuade, the cyber environment has expanded the ways of disseminating information, whether in favor of a healthy debate or by propagating dishonest and unscrupulous information and narratives.

The second dimension, therefore, concerns the deepening of what are legitimate and illegitimate actions of influence, as well as legal and illegal initiatives. Here, legitimacy is directly connected to the motivation of the economic, political and social agents involved. The pursuit of common interest and the greater good, which would be expected at important moments such as the election of candidates who will rule the country, often gives way to masked individual and collective interests. Beyond the ethical debate, which is necessary, and the debate about how perceptions are shaped around what is or isn't legitimate, the cyber environment adds new layers of turbidity. The advancement of technological knowledge rapidly expands the resources available; And the understanding of how they work and the results they produce becomes a challenge to legal practitioners, such as lawyers, judges, prosecutors and to professionals from other fields of knowledge not originally related to technological and scientific production.

In the third dimension, the transnational aspect of cybercrime emerges accompanied by two essential issues: First, how to assign responsibility to actions of interference and attacks on electoral processes. Second, even if the evidence is clear that attacks or interferences have tarnished ongoing proceedings, how long does it take for society and the executive, legislative, and judicial authorities to

Paranoia. Nenhuma outra palavra talvez cristalize tanto as preocupações hoje, no mundo, em torno das invasões cibernéticas, das tentativas de manipulação virtuais e da proliferação das que ficaram conhecidas como *fake news* – inverdades espalhadas com aparente legitimidade de origem e conteúdo. Mentir não é uma novidade na experiência humana. Vêm do latim as citações, segundo as quais, todo homem é mentiroso *(omni homo mendax)* e que uma mentira puxa outra *(fallacia, alia aliam trudit).*

Marcadamente desde 2016, o mundo se envolveu em discussões, pesquisas, estudos e até mesmo acusações abertas entre países com relação ao tema. A Rússia foi acusada de influenciar a disputa presidencial americana daquele ano e mesmo em 2018 remanescem preocupações de que, supostamente, o país inimigo dos tempos da Guerra Fria poderia interferir nas eleições parlamentares previstas para novembro. Ainda em 2016, os ambientes de tecnologia da informação dos Jogos Olímpicos no Rio de Janeiro foram alvo de cibercriminosos, com mais de 40 milhões de alertas de segurança. Nas últimas eleições presidenciais no Brasil, mais de 200 mil ataques por segundo tentaram derrubar os servidores, conforme dados oficiais. Estudo da Diretoria de Análise de Políticas Públicas (DAPP) da Fundação Getúlio Vargas (FGV)[1] mostra que serão inevitáveis nas eleições presidenciais de 2018 a utilização de *robots* (robôs) e a propagação de *fake news*.

O ecossistema digital transformou a capacidade do ser humano em fazer o que mais aprecia – interagir – e amplificou a complexidade das formas de se relacionar.  O risco cibernético avança junto à crescente inovação e dependência da sociedade às tecnologias da informação. Avanços em áreas como a Internet das Coisas (IOT) e Inteligência Artificial (IA) atraem e tornam ainda mais potenciais os cibercrimes. O nível de sofisticação da elaboração e da execução de ataques inclui *malwares* (programa malicioso de infiltração) autro-propagados vocacionados a destruir, bem como os *ransomware* (códigos que impedem acesso a dados armazenados e exigem resgate para devolver a conexão). Em paralelo, o avanço da intermediação de contato e de trocas por meio de plataformas digitais, aplicativos e redes sociais para a busca de informação e relacionamento entre indivíduos e grupo sociais ampliam tanto a eficácia na conectividade quanto trazem novas oportunidades para atividades obscuras, ilícitas e falseadas

## Complexidade Digital

Convém dimensionar a complexidade digital associada a processos eleitorais ao menos em três perspectivas[3]. A primeira é a da segurança cibernética e ações de influência: uma, ligada à integridade dos sistemas que permitem realizar eleições associadas a urnas eletrônicas e internet; a outra, ao jogo legítimo de argumentos para convencimento da opinião pública. As desconfianças quanto a eleições que utilizam tecnologia da informação, caso da brasileira, totalmente informatizada, são em geral ligadas a três fatores: medo do desvio de votos de um candidato a outro, alteração da proporção de votos dados a cada candidato e a inoculação de procedimentos capazes de gerar panes nos sistemas ou gerar incerteza quanto à credibilidade do processo. No que tange à capacidade de influenciar e convencer, o ambiente cibernético ampliou as formas de propagar informações, seja a favor do debate saudável assim como para a propagação de dados e versões desonestas e inescrupulosas.

A segunda dimensão diria respeito ao aprofundamento, então, do que são ações de influência legítimas e ilegítimas, assim como iniciativas legais e ilegais. Aqui, a legitimidade liga-se diretamente à motivação dos agentes econômicos, políticos e sociais envolvidos. A busca do interesse comum e do bem maior, que seria de se esperar em momentos importantes, como a escolha de candidatos que irão governar, muitas vezes perde espaço a interesses mascarados individuais e coletivos. Para além do debate ético, necessário, e sobre como se formam as percepções em torno do que é legítimo ou não, o ambiente cibernético acrescenta novas camadas de turvação. O avanço do conhecimento tecnológico expande rapidamente os recursos disponíveis. E a compreensão sobre como funcionam e os resultados que produzem passam a se tornar desafio aos operadores do Direito, como advogados, juízes, procuradores, outras áreas de saber não originalmente ligadas à produção tecnológica e científica.

Numa terceira dimensão, emerge o aspecto transnacional do cibercrime, acompanhado de duas questões essenciais. Por um lado, como atribuir responsabilidade a ações de interferência e a ataques a processos eleitorais. De outra sorte, ainda que a comprovação de que ataques ou interferências macularam processos em curso torne-se clara, em quanto tempo sociedade e autoridades executivas,

achieve full conviction? Going a little further, what should be done when the process to clarify digitally pernicious and illegal procedures against an election takes longer than the period of the electoral contest, the announcement of the outcome and the start of a new government? In the case of a cyber attack or interference activity turning out to be irrelevant to the outcome of the electoral process, how to deal with the finding in a timely manner? The digital environment causes distortions in the rhythm and movements of reality and its representations.

## The Fake News Explosion

Taking the United State's recent electoral process as an example, in June 2017, six months after the new government's kickoff, the Washington Post[4] reported that in 2016 the CIA had warned the president at the time about suspicions that the Russian government had allegedly ordered actions to interfere in the presidential election. In August 2016, the agency reportedly informed about actions aimed at hacking the Democratic Party's computers and interfering with the presidential election process by spreading rumors, which was denied by Moscow. The US government made the first public statement on the matter only in October 2016 and, according to the newspaper, it took weeks for the issue to be addressed by the public opinion because the government itself feared being accused of manipulating the electoral process, associated with the fact that, at the time, it was believed that the Democratic Party's candidate could win the electoral race.

In Brazil, the role of robots and automated profiles will be a relevant issue this year. Contrary to the issue's rapidly growing discussions in recent years in the United States, the public debate in the South American country has seen a smaller proportion and scale, although it has gained importance as a subject of advanced research by specialists, study centers and has also caught the interest and concern of agents from the government, the private sector and society. Data collected by DAPP/FGV show that the incidence of robots in relevant public events reached nearly a quarter of total interactions. In April 2017, regarding the subject of the general strike scheduled for the end of the month, interaction with robots on social media debates was between 18% and 22%. In the presidential elections of 2014, the level varied between 13% and 19% and for the impeachment of the president in 2015, it varied between 16% and 21% of total interactions.

There are indications that automated profiles already engage significantly in discussions between the main political fields connected to the pre-candidates for the 2018 elections. As an aggravating factor, the phenomenon of fake news is further enhanced by the effectiveness in the use of robots. There is also evidence of external influence on social networks, which raises questions about the risks of foreign interference in this year's presidential race in the country. Ranking among the world's ten largest economies, Brazil supplies other markets with key products and attracts direct investments. At different moments of the socio-political-economic debate in digital channels, the FGV unit analyzed content posted on twitter related to Brazilian issues, based on photographs used by users, locations and origin of the profiles, links associated with other languages, as well as landscapes from other regions of the planet, both in the profile photographs themselves and in different contents. Hence one of the conclusions of the study: only Brazilians will vote, but not only Brazilians will take part in the debate.

Automated accounts allow for dissemination of content and serve as a weapon in the battle of posts and content placement, often within defamation and disinformation strategies. As an adverse effect of misuse, these battles generally reduce reality to a dual and polarized perspective, by dividing society in half and eliminating the development of multiple perspectives, so needed at times of high complexity such as the one Brazil and the World are presently going through. This was seen even during the unfolding debate following the execution of Congresswoman Marielle Franco, councilor in Rio de Janeiro, which was accompanied by the escalation of fake news about her in an attempt to deconstruct her performance and legacy.

However, the degree of polarization in this case was much lower than in other public events and they involved issues of gender, race, ethnicity, besides politics and security. The attacks on the victim's history were strongly rebutted by a wave of denial combatting the fake news. Different fields of society ended up working together replacing facts and information in the perspective closest to reality - the death of the parliamentarian hurt society as a whole and democracy itself. Created with the mission of ensuring that the opportunities and potential benefits provided by technology in the digital age are shared by society, ITS Rio (Rio's Institute of Technology & Society) considers

legislativas e judiciárias alcançariam pleno convencimento a respeito? Indo um pouco adiante. O que fazer quando a clarificação de procedimentos digitalmente perniciosos e ilegais contra uma eleição leva mais tempo do que o período da disputa eleitoral, anúncio do resultado e início de um novo governo? E se a demonstração exitosa de um ataque cibernético ou ação de interferência se mostrar irrelevante ao resultado do processo eleitoral, como lidar no tempo com o achado? O ambiente digital provoca distorções nos tempos e movimentos da realidade e suas representações.

## A Explosão das *Fake News*

Tome-se o exemplo do processo eleitoral recente americano. Em junho de 2017, seis meses após o início do novo governo do país, o jornal *Washington Post*[4] publicou que a CIA havia alertado no ano anterior, ao então presidente, sobre suspeitas de que o governo russo havia supostamente ordenado ações para interferir nas eleições presidenciais. A agência teria informado em agosto sobre ações cujos objetivos seriam *hackear* computadores do Partido Democrata e interferir no processo eleitoral presidencial, por meio da divulgação de boatos, o que foi negado por Moscou. O governo americano fez a primeira manifestação pública sobre o assunto apenas em outubro de 2016 e, segundo o jornal, o tema levou semanas para ser endereçado à opinião pública porque o próprio governo da época receava ser acusado de manipulação do processo eleitoral, associado ao fato de que se acreditava, naquele momento, que a candidata do Partido Democrático seria, talvez, apesar de tudo, a vencedora do pleito.

No Brasil, a atuação de robôs e os perfis automatizados serão questões relevantes este ano. Diferente da aceleração deste debate nos últimos anos nos Estados Unidos, o debate público no país sul americano tem menores proporção e escala, embora também ganhe corpo, como tema de pesquisas avançadas de especialistas, centros de estudos e já desperte o interesse e a preocupação de agentes governamentais, privados e da sociedade. Dados levantados pela DAPP/FGV mostram que a incidência de robôs em eventos públicos de relevância alcançou patamar de quase um quarto do total das interações. Em abril de 2017, a interação com robôs nos debates nas mídias sociais foi entre 18% a 22% sobre o tema da greve geral prevista para o fim do mês. Nas eleições presidenciais de 2014, o patamar variou entre 13% e 19% das interações totais e no *impeachment* da presidência da República de 2015, representou ordem entre 16% e 21% do total.

As indicações são, ainda, de que perfis automatizados já engajam de forma significativa as discussões entre os principais campos políticos ligados aos pré-candidatos para as eleições de 2018. Como agravante, o fenômeno das *fake news* é ainda mais potencializado pela eficácia na utilização de robôs. Há também indícios de influência externa nas redes sociais, o que levanta reflexões, guardadas as devidas proporções, sobre os riscos de interferência estrangeira na corrida presidencial deste ano no país. Uma das dez maiores economias do mundo, o Brasil abastece outros mercados com produtos-chave e atrai interesse em investimentos diretos. Em diferentes momentos do debate sociopolítico-econômico nos canais digitais, foram analisados pela unidade da FGV conteúdos postados no *twitter* ligados a questões brasileiras, fotografias usadas por usuários, localizações da origem dos perfis, links associados a outros idiomas, além de cenários de outras regiões do planeta, tanto nas próprias fotografias de perfis como em diferentes conteúdos. Daí vem uma das conclusões do estudo: apenas brasileiros votarão, mas não somente brasileiros debaterão.

Contas automatizadas permitem massificação de postagens. Servem como arma na batalha de postagens e veiculações de conteúdos, muitas vezes dentro de estratégias de difamação e desinformação. Como efeito adverso do mau uso, as batalhas, em geral, reduzem a realidade à perspectiva dual e à polarização, como que seccionando a sociedade ao meio e eliminando o desenvolvimento de perspectivas múltiplas, necessárias em momentos de alta complexidade como o atual, no Brasil e no mundo. Assim foi que até mesmo os desdobramentos da execução da parlamentar Marielle Franco, vereadora no Rio de Janeiro, foram acompanhados pela escalada de *fake news* a seu respeito, como tentativa de desconstruir sua atuação e legado.

O grau de polarização foi bem menor do em que outros eventos públicos. Envolviam questões de gênero, raça, etnia, além da política e de segurança. Os ataques à história da vítima fortemente rebatidos por uma onda de desmentidos contra as *fake news*. Campos diferentes da sociedade acabaram trabalhando em conjunto. Recolocar fatos e dados na perspectiva mais próxima da realidade – a morte da parlamentar feriu a sociedade e a própria democracia. Criado com a missão de assegurar que as oportunidades fornecidas pela

that digital education is perhaps one of the most powerful alternatives against the spread of untruthful, distorted or out-of-context content as if they were true.

## Combating Cybercrime

The common view is that to combat fake news and other forms of cybercrime it is imperative that companies in the field of technology, governments, the market and civil society[5] work together. From this perspective, ITS Rio indicates that digital education tends to be one of the most powerful tools for this effort, because it enables users to develop skills and progressively become able to identify false and illegitimate content and denounce it. In this sense, ITS Rio launched a pilot platform, integrated to Twitter that helps users identify if a certain profile is in fact a robot. The platform is called PegaBot (*CatchaBot*) and is currently in its testing phase. However, it is a fact that the spread of fake news is not restricted to robots: fake news is 70% more likely to be retweeted by people than true information[6].

In the eye of the storm, digital platforms have been seeking to respond to the demands for greater integrity of the information that circulates in them. This is the case for Google and Facebook, whose president, Mark Zuckerberg, testified before the US Congress in April this year, addressing the issue of how they would work to improve the security of people's information and safeguard elections around the world[7]. Largest global network, with more than 2 billion monthly users, Facebook still owns Facebook Messenger, Whatsapp and Instagram. Concerns about the power of the company's digital channels, the handling of user data for political purposes and in particular the case involving Cambridge Analytica resulted in the convening of the digital entrepreneur. The allegations were that the UK-based political consultancy collected information from tens of millions of people using the Facebook channel and disregarding company rules.

At the same time, those concerns are reaching Brazil. Experts analyze the topic and focus especially on Whatsapp. Columnists from two of Brazil's leading newspapers have raised the issue over whether the encrypted messaging network will become the main black box of the 2018 presidential election as a fake news[8] disseminating vehicle and they seek to anticipate the application's next move in order to oppose false news in the election year. Whatsapp has 120 million users in Brazil and has become an extremely effective channel for the propagation of information through groups. This is precisely what feeds the fears about its ability to spread misinformation when misused. In general terms, the fight against fake news would focus on user engagement for the dissemination of legitimate information, detection of uncommon massive streams of information, and greater proximity to the electoral justice and public agencies[9].

Last December the Brazilian Superior Electoral Court (TSE) established the Consultative Council on Internet and Elections, with the goal of proposing actions to contain the propagation of fake news and robots in the elections. The court recognizes the advancement of fake news, including news regarding its own activities and the ability to maintain the integrity of electoral disputes through electronic ballot boxes. Among the reasons that led to the automation of Brazil's electoral process are slowness in the vote count and unintentional and premeditated errors. Brazil's election process is considered the most computerized in the world. According to the official statement, frauds in the system are unfeasible due to numerous and different security barriers and systems to identify traces. The topic, however, generates debate in society and represents a field of propagation of narratives that can often go from alarmism to the attempt to undermine the credibility of the process. To a large extent, public ballot-screening tests - with results that are made public - become an important tool for transparency.

These tests began in 2009. The fourth edition occurred in the last week of November 2017. During the test, three flaws were identified in one of the ballot boxes. The test was carried out by researchers and professionals qualified in cryptography, development of secure software and reverse engineering. An official technical report, made public and accessible on the Internet, considered the edition to be the one that contributed the most to the improvement of the ballot boxes software set[10]. The report also concluded that the expert's findings would generate essential corrections and improvements so that the software will be at an even higher level of security and robustness for the 2018 elections. In a press interview, managers from the TSE indicated that there is no possibility that the system failed in previous elections because they are related to updates, that the RDV (Digital Voting Register) was not changed and that voters and votes were not identified[11].

tecnologia na era digital e potenciais benefícios sejam compartilhados pela sociedade, o ITS Rio (Instituto de Tecnologia & Sociedade do Rio) avalia que a educação digital seja, talvez, uma das alternativas mais potentes contra a propagação de conteúdos inverídicos, distorcidos ou fora de contexto como se reais fossem.

## Combate a cibercrimes

A visão é a de que para o combate às *fake news* e outras formas de crimes cibernéticos é imperativo que empresas de tecnologia, governos, mercado e sociedade civil[5] atuem em conjunto. Ainda nesta perspectiva, o instituto indica que a educação digital tende a ser uma das alternativas mais potentes nessa empreitada, de forma a que usuários desenvolvam capacidades e se habilitem progressivamente a identificar conteúdos falsos e ilegítimos e a denunciar. Nesse sentido, o ITS Rio lançou uma plataforma-piloto, integrada ao Twitter, para facilitar a identificação, por parte do usuário, se determinado perfil em rede social é um robô. A plataforma chama-se PegaBot e está em fase de testes. Fato é que a difusão de notícias falsas não se restringe aos robôs: notícias falsas tem 70% de mais chances em serem *retweetadas* por pessoas do que informações verdadeiras[6].

Sob fogo cerrado, plataformas digitais vêm procurando responder às exigências de maior integridade das informações que nelas circulam. São os casos do Google e do Facebook, cujo presidente, Mark Zuckerberg, prestou depoimento ao Congresso americano em abril deste ano, endereçando como estariam trabalhando para melhorar a forma como protegem as informações das pessoas e salvaguardando as eleições em todo o mundo[7]. Maior rede global, com mais de 2 bilhões de usuários mensais, o Facebook é dono ainda do Facebook Messenger e das redes Whatsapp e Instagram. Preocupações com o poder dos canais digitais da companhia, a utilização dos dados dos usuários para fins políticos e, em particular, o caso envolvendo a Cambridge Analytica resultaram na convocação do empresário. As acusações foram de que a consultoria política, sediada no Reino Unido, levantou informações de dezenas de milhões de pessoas usando o canal Facebook e desrespeitando regras da empresa.

De forma simultânea, as preocupações chegam ao Brasil. Especialistas se debruçam sobre o assunto e lançam olhar especialmente sobre o Whatsapp. Colunistas de dois dos principais jornais brasileiros levantaram a discussão a respeito de a rede de mensagens criptografadas se tornar a principal caixa preta das eleições presidenciais de 2018 como veículo de fake news[8] e procuram antecipar os próximos movimentos do aplicativo, que tem 120 milhões de usuários no Brasil, para se contrapor às notícias falsas no ano eleitoral. O aplicativo virou canal extraordinariamente eficaz para a propagação de informações por meio de grupos, o que precisamente alimenta os temores a respeito da capacidade de difundir desinformação, também, quando mal utilizado. O combate se daria, em linhas gerais, em torno do engajamento dos usuários para a difusão de informações legítimas, detecção de correntes surpreendentemente massivas de informação e maior proximidade com relação à Justiça eleitoral e órgãos públicos[9].

O próprio Tribunal Superior Eleitoral (TSE) brasileiro instituiu em dezembro do ano passado o Conselho Consultivo sobre Internet e Eleições, com o objetivo de propor ações para conter a propagação de *fake news* e de robôs nas eleições. O tribunal reconhece o avanço das fake news, inclusive a respeito de sua atividade e da capacidade de as urnas eletrônicas manterem a integridade das disputas eleitorais. Lentidão no processo de apuração, falhas não intencionais e as premeditadas foram alguns dos motivos para a automatização do processo brasileiro, considerado a maior eleição informatizada do mundo. A fraude no sistema é considerada inviável, conforme o posicionamento oficial, em decorrência de inúmeras e diversificadas barreiras de segurança e da identificação de rastros. O tema, no entanto, gera debates na sociedade e representa terreno de propagação de versões que alcançam, muitas vezes, matizes que podem ir do alarmismo à tentativa de prejudicar a credibilidade do processo. Em grande medida, os testes públicos de segurança das urnas – com resultados públicos – acabam se tornando instrumento importante de transparência.

Os testes começaram em 2009. A quarta edição ocorreu na última semana de novembro de 2017. Três falhas em uma das urnas foram identificadas no teste, que contou com a participação de pesquisadores, profissionais qualificados em criptografia e desenvolvimento de software seguro e engenharia reversa. Por meio de relatório técnico oficial, tornado público e acessível na internet, a edição foi considerada a que trouxe o maior número de contribuições para o aperfeiçoamento do conjunto de softwares do Ecossistema da Urna[10]. Concluiu, ainda, que os achados encontrados pelos especialistas gerarão correções e melhorias fundamentais

The list of initiatives which is part of the basic criteria of corporate players in the cyber field is: transparency - as much as possible, identification of crimes, efficient interaction with public agencies - as well as with society - and heavy investments in security mechanisms. In order to secure its assets and its customers, Microsoft develops initiatives such as the Digital Crimes Unit (DCU)[12], made up of groups of lawyers, researchers, data scientists, engineers and analysts to combat global malware. The unit's command and control center monitors and analyzes the DNA of digital threats, conducts forensic research, and develops ways to combat cybercrime in court. In each continent, the company has Transparency Centers to meet the public sector's security needs, a kind of permanent transparency data show on privacy criteria, operational and legal models of security. Around one billion dollars is invested annually by Microsoft to ensure cybersecurity.

## Considerations and Propositions

The propositions that emerge from the First Preparatory Meeting for the XV Forte de Copacabana Conference on International Security for combating cyber attacks and the spread of fake news involve a number of initiatives, some of which overlap and complement each other, as summarized by the following aspects and assertions:

- Establishment of a cyber defense center to monitor false information but also, and mainly, to implement actions to deconstruct the fabrication by the Electoral Court on issues related to the Elections process. The truth must be reestablished in the media and channels where the false information was found.

- The development of information technologies must be done including the search for safe solutions throughout their life cycles.

- Restricting or limiting access to information has had a relatively lower impact than ensuring that the internal, public or private infrastructure is updated with the most advanced protection devices available.

- There is no point in restricting the use of the cloud if the infrastructure itself does not ensure the security of basic operations, such as the safe delivery of e-mails.

- The discussion on actions to inhibit fake news should encompass making more information available and not less.

- Prior censorship and the removal of content without a court order should be avoided, based on constitutional principles such as the protection of individual freedoms.

- Although necessary in some cases, the adoption of civil protection and criminal law provisions should be the last resort. Criminal classification does not seem to be enough to contain cybercrime and the propagation of fake news.

- The digital ecosystem is changing. In this context, applications and social networks play a prominent role. This means that we rely (largely) on digital intermediaries, such as these platforms, to mediate our communication.

- The months leading up to the elections should have more open and public debates on fake news.

- Promoting awareness and greater education about the use and manipulation of social networks is fundamental for both the ordinary user and the legislator.

- The preservation of "rights-based approaches" as our experience with the Civil Code are important precedents in perpetuating our national reflection on how to preserve democracy in electoral times.

- In addition to reflecting on the ultimate objectives to deal with misinformation (e.g., establishment of new laws), political propaganda and fake news, it is imperative to focus on processes.

- When dealing with the electronic ballot test applied a few months ago, we refer to sustainability, resilience, and system integrity. When dealing with digital platforms, we refer to greater transparency about algorithms used, which influence the way and ability to access and exchange information.

- When addressing the issue of security, it emerges in different aspects: the security of a healthy, public, open, transparent political debate; the safety of users; national security against external interference, and, specifically here, the improvement of governance mechanisms of cybersecurity in Brazil.

- Many tragedies have been produced throughout history revolving around the theme of national interest. In a democracy, it is

para que o conjunto esteja em um patamar ainda mais elevado de segurança e robustez para as Eleições 2018, conforme o texto original do relatório técnico. Em entrevista à imprensa, gestores do TSE indicaram que não existe a possibilidade de o sistema ter falhado em eleições anteriores, porque associadas a atualizações, e que o RDV (Registro Digital do Voto) não foi alterado, assim como não foram identificados o eleitor e a opção de voto[11].

A lista de iniciativas que faz parte de critérios básicos de *players* corporativos no campo cibernético é: transparência tanto maior quanto possível, identificação de crimes, interação eficiente com órgãos públicos - bem como com a sociedade - e pesados investimentos em mecanismos de segurança. Com vistas a garantir seus ativos e de seus clientes, a Microsoft desenvolve iniciativas como a Unidade de Crimes Digitais (DCU, no inglês para Digital Crimes Unit)[12], formado por grupos de advogados, investigadores, cientistas de dados, engenheiros e analistas, voltados ao combate de *malwares* globais. O centro de comando e controle da unidade monitora e analisa o DNA das ameaças digitais, desenvolve investigação forense e desenvolve formas de combate a crimes cibernéticos, junto à justiça. Em cada continente, a companhia dispõe de Centros de Transparência, para atender necessidades de segurança do setor público, uma espécie de *datashow* permanente de transparência sobre critérios de privacidade, modelos operacionais e jurídicos de segurança. Ao redor de US$ 1 bilhão são investidos ao ano pela Microsoft para garantia da segurança cibernética.

## Reflexão e Proposições

As proposições que emergem da 1ª Reunião Preparatória para a XV Conferência de Segurança Internacional do Forte de Copacabana sobre o combate aos *cyber attacks* e à propagação das *fake news* envolvem um conjunto de iniciativas, algumas das quais se sobrepõem e se complementam, conforme o resumo dos seguintes aspectos e assertivas:

- Estruturação de um centro cibernético de defesa, incluindo o monitoramento de versões falsas mas também, e principalmente, ações de desconstrução da mentira por parte da Justiça Eleitoral sobre questões ligadas ao processo das Eleições.. A verdade deve ser restabelecida nos meios e canais onde as informações falsas foram encontradas.

- O desenvolvimento de tecnologias da informação deve nascer já incluindo a busca por soluções seguras, ao longo de seus ciclos de vida.

- Restringir ou limitar o acesso à informação tem impacto relativamente menor do que assegurar que a infraestrutura interna, pública ou privada, esteja atualizada, com os mais avançados dispositivos de proteção disponíveis.

- Pouco adianta restringir a utilização da nuvem se a própria infraestrutura não assegura a garantia para operações básicas, como o recebimento seguro de e-mails.

- A discussão sobre as ações para inibição de *fake news* deve passar por mais informação e não por menos informações disponíveis.

- A remoção de conteúdo sem ordem judicial e a censura prévia devem ser evitadas, tomando por base princípios constitucionais, como a proteção de liberdades individuais.

- Ainda que, em alguns casos, seja necessário adotar tutela cível e também dispositivos do Direito Penal, este deve ser o último recurso. A tipificação penal não parece ser suficiente para conter as ações de crime cibernético e propagação de notícias falsas.

- O ecossistema digital está se transformando. Nesse contexto, aplicativos e redes sociais tomam papel de destaque. Isso significa que dependemos (em grande parte) de intermediários digitais, tal como essas plataformas, para mediar nossa comunicação.

- Os meses que precedem as eleições devem vir acompanhados, de forma mais intensa, de debates públicos e abertos sobre notícias falsas.

- Promover conscientização e maior educação a respeito do uso e manipulação de redes sociais é fundamental tanto para o usuário comum como para o legislador.

- A preservação de "rights-based approaches" como a experiência que tivemos com o Marco Civil são importantes precedentes na perpetuação de nossa reflexão nacional sobre como preservar a democracia em tempos eleitorais.

- Para além da reflexão sobre os objetivos finais para se lidar com desinformação (ex: estabelecimento de novas leis), propaganda política e notícias falsas, o enfoque sobre os

expected that different perceptions of interests (the population's broader interests) find in the *agora* a middle ground that enables establishing long-term political agendas for society.

- International cooperation is essential and necessary to address the issue of cybersecurity and the dialogue between countries and institutions needs to be encouraged.

In addition to a certain level of anguish over the advancement of cybercrime and fake news among experts in the face of the problem, it seems to be a consensus that the quest for solutions will be more successful if four dimensions move in the same direction: individual, collective, international and one referring to technological platforms. The nature of the interconnected world and the different areas of knowledge involved in these phenomena also lead us to believe that it will be inevitable to coordinate efforts here in Brazil, as well as in the rest of the world, between government, private agents, academia, professional communities capable of adding value and between each one of us, citizens. Threats will occur simultaneously, with extreme speed and changeable form, making it increasingly difficult to differentiate real situations from those manipulated in a virtual environment. Worry, concern, surprise, fear and mistrust form a fraction of the lexicon of this complexity. Overcoming this will depend on commitment, effort and resilience in face of the challenge.

1 *Robôs, Redes Sociais e Política no Brasil: Análise de interferência de perfis automatizados nas eleições de 2014*, DPPA/FGV

2 *Uma Breve História da Humanidade, Sapiens*, Capítulo 2. Yuval Noah Harari, editora LP&M

3 Paper do Secretário-Executivo da Unasul (Escola Sul-Americana de Defesa), Antonio Jorge Ramalho da Rocha

4 Obama's secret struggle to retaliate against Putin's election interference - Washington Post

5 *Fake news: como proteger a liberdade de expressão e inibir notícias falsas?,* Chiara Spadaccini de Teffé, ITS Rio https://feed.itsrio.org/fake-news-como-proteger-a-liberdade-de-express%C3%A3o-e-inibir-not%C3%ADcias-falsas-8058aedd9f5c

6 *The soread of true and false news online*, Soroush Vosoughi, Deb Roy, and Sinan Aral, MIT Iniciative on the digital economy research brief, http://ide.mit.edu/sites/default/files/publications/2017%20IDE%20Research%20Brief%20False%20News.pdf

7 Transcrição do depoimento do president do Google, Mark Zuckerberg ao Congresso americano, https://www.politico.com/story/2018/04/09/transcript-mark-zuckerberg-testimony-to-congress-on-cambridge-analytica-509978

8 WhatsApp, o berço das 'fake news', Pedro Doria, O Globo, 29.03.2018, https://oglobo.globo.com/economia/whatsapp-berco-das-fake-news-22540542

9 Popular e de difícil controle, WhatsApp mira notícias falsas, Nelson de Sá, Folha de S. Paulo, 13.05.2018, https://www1.folha.uol.com.br/poder/2018/05/popular-e-de-dificil-controle-whatsapp-mira-noticias-falsas.shtml

10 Vulnerabilidades e sugestões de melhorias encontradas no Teste Público de Segurança 2017 sobre o Ecossistema da Urna, Relatório Técnico do TSE, http://www.tse.jus.br/hotsites/teste-publico-seguranca-2017/arquivos/tps2017-relatorio-tecnico.pdf

11 Teste em urnas eletrônicas identifica três falhas; TSE diz que não há riscos em votação, Breno Pires e Rafael Moraes Moura, O Estado de S.Paulo, 01.12.2017, http://politica.estadao.com.br/noticias/geral,teste-em-urnas-eletronicas-identifica-tres-falhas-tse-diz-que-nao-ha-riscos-em-votacao,70002104642

12 DCU Fact Sheet, https://news.microsoft.com/uploads/2018/02/dcuFS_170106.pdf

processos é imprescindível.

- Quando tratamos do teste da urna eletrônica aplicado há alguns meses atrás, nos referimos à sustentabilidade, resiliência e integridade de sistemas. Quando tratamos de plataformas digitais, tratamos sobre maior transparência sobre algoritmos utilizados, que influenciam a forma e capacidade de acessar e trocar informação.

- Quando se aborda o tema da segurança, esta emerge em diferentes aspectos: a segurança de um debate político saudável, público, aberto, transparente; a segurança dos usuários; a segurança nacional contra interferências externas e, aqui, o aprimoramento de mecanismos de governança da segurança cibernética no Brasil.

- Em torno do tema interesse nacional, não foram poucas as tragédias produzidas ao longo da história. Em uma democracia, espera-se que distintas percepções dos interesses (mais amplos da população) encontrem, na ágora, um meio termo que permita estabelecer agendas políticas de longo prazo para a sociedade.

- A cooperação internacional é essencial e necessária para lidar com a questão da segurança cibernética e os diálogos precisam ser estimulados entre países e instituições.

Além de certo nível de angústia frente ao avanço dos crimes cibernéticos e das *fake news* entre os especialistas diante do problema, parece consenso que a busca de soluções será tão bem-sucedida quanto for possível que quatro dimensões se movimentarem na mesma direção: individual, a coletiva, a internacional e a que se refere às plataformas tecnológicas. A natureza do mundo interconectado e das diferentes áreas de conhecimento envolvidas nestes *phenomena* também leva a conceber que será inevitável a coordenação de esforços e empenhos, aqui mesmo, no Brasil, como no resto do mundo, entre governo, agentes privados, academia, justiça, comunidades profissionais capazes de agregar valor, além, naturalmente de cada um de nós, cidadãos. As ameaças não apenas tenderão a ocorrer simultaneamente, com extrema rapidez e forma mutáveis, tornando cada vez mais difícil diferenciar situações reais das manipuladas em ambiente virtual. Preocupação, susto, surpresa, medo, desconfiança formam uma fração do léxico dessa complexidade. Ultrapassar isso dependerá do compromisso, empenho e resiliência diante do desafio.

1 *Robôs, Redes Sociais e Política no Brasil: Análise de interferência de perfis automatizados nas eleições de 2014,* DPPA/FGV

2 Uma Breve História da Humanidade, Sapiens, Capítulo 2. Yuval Noah Harari, editora LP&M

3 Paper do Secretário-Executivo da Unasul (Escola Sul-Americana de Defesa), Antonio Jorge Ramalho da Rocha

4 Obama's secret struggle to retaliate against Putin's election interference - Washington Post

5 *Fake news: como proteger a liberdade de expressão e inibir notícias falsas?*, Chiara Spadaccini de Teffé, ITS Rio https://feed.itsrio.org/fake-news-como-proteger-a-liberdade-de-express%C3%A30-e-inibir-not%C3%ADcias-falsas-8058aedd9f5c

6 *The soread of true and false news online,* Soroush Vosoughi, Deb Roy, and Sinan Aral, MIT Iniciative on the digital economy research brief, http://ide.mit.edu/sites/default/files/publications/2017%20IDE%20Research%20Brief%20False%20News.pdf

7 Transcrição do depoimento do president do Google, Mark Zuckerberg ao Congresso americano, https://www.politico.com/story/2018/04/09/transcript-mark-zuckerberg-testimony-to-congress-on-cambridge-analytica-509978

8 WhatsApp, o berço das 'fake news', Pedro Doria, O Globo, 29.03.2018, https://oglobo.globo.com/economia/whatsapp-berco-das-fake-news-22540542

9 Popular e de difícil controle, WhatsApp mira notícias falsas, Nelson de Sá, Folha de S. Paulo, 13.05.2018, https://www1.folha.uol.com.br/poder/2018/05/popular-e-de-dificil-controle-whatsapp-mira-noticias-falsas.shtml

10 Vulnerabilidades e sugestões de melhorias encontradas no Teste Público de Segurança 2017 sobre o Ecossistema da Urna, Relatório Técnico do TSE, http://www.tse.jus.br/hotsites/teste-publico-seguranca-2017/arquivos/tps2017-relatorio-tecnico.pdf

11 Teste em urnas eletrônicas identifica três falhas; TSE diz que não há riscos em votação, Breno Pires e Rafael Moraes Moura, O Estado de S.Paulo, 01.12.2017, http://politica.estadao.com.br/noticias/geral,teste-em-urnas-eletronicas-identifica-tres-falhas-tse-diz-que-nao-ha-riscos-em-votacao,70002104642

12 DCU Fact Sheet, https://news.microsoft.com/uploads/2018/02/dcuFS_170106.pdf

XVFORTE