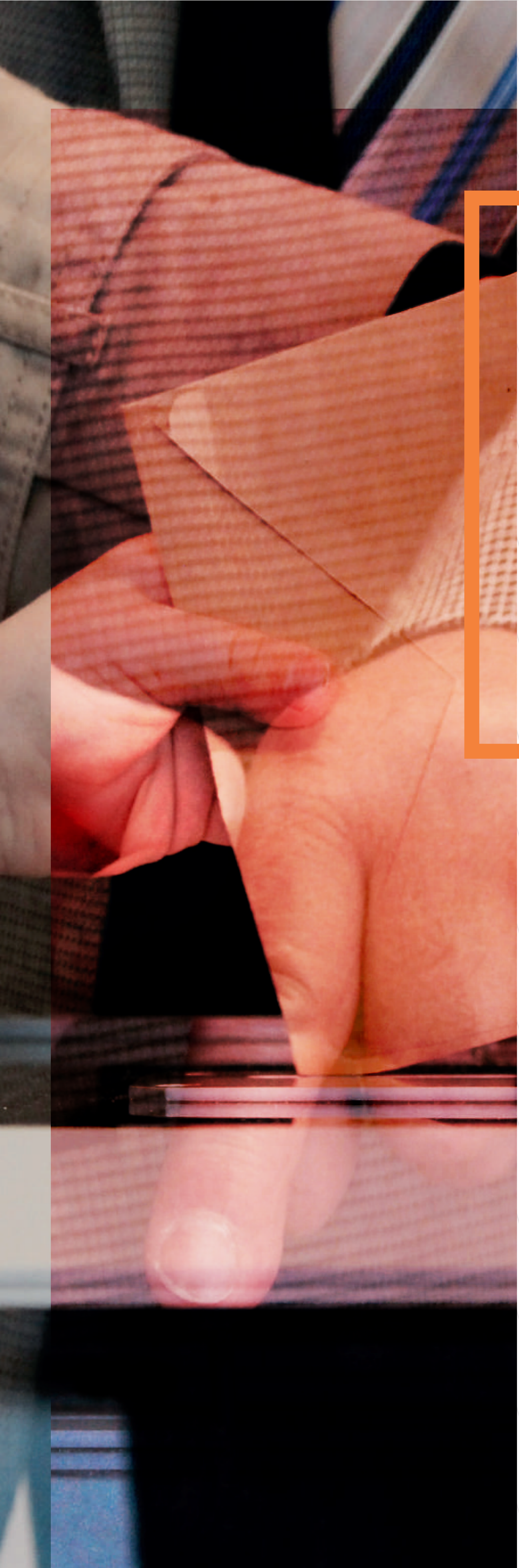
European
Commission



ELECTION INTERFERENCE IN THE DIGITAL AGE

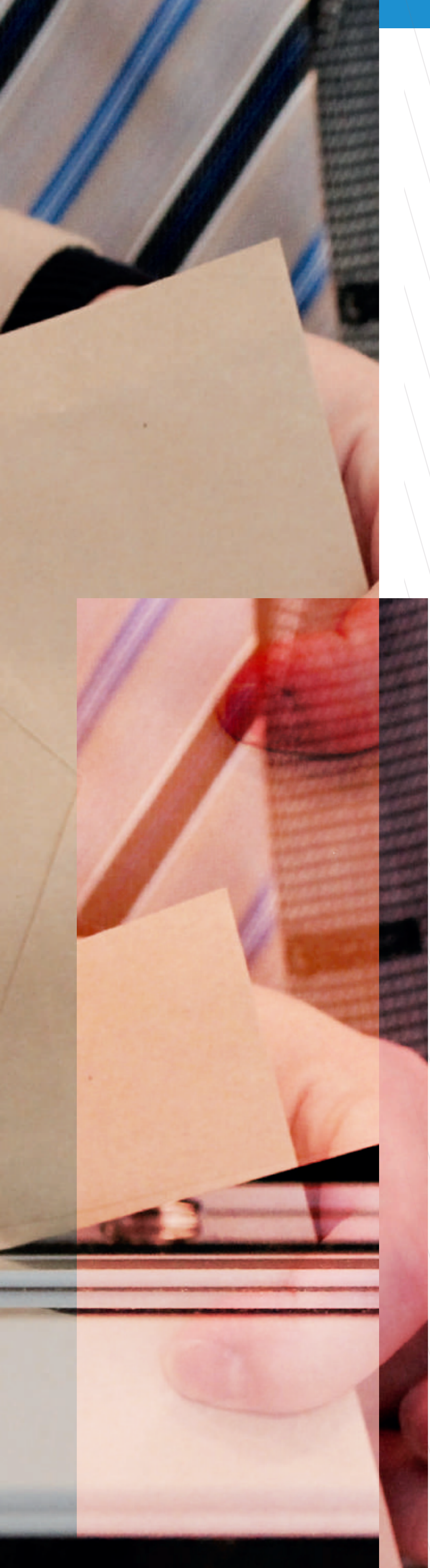
BUILDING RESILIENCE TO CYBER-ENABLED THREATS

A Collection of Think Pieces

from 35 leading practioners and experts

#EUProtects

European **Political Strategy** Centre



ACKNOWLEDGEMENTS

This publication was put together in the context of the **High-Level Conference** on '**Election Interference in the Digital Age: Building Resilience to Cyber-Enabled Threats**' – a two-day event that took place on 15-16 October 2018 under the political patronage of Sir Julian King, European Commissioner for the Security Union, and was organised by the European Political Strategy Centre, the European Commission's in-house think tank, in collaboration with the Security Union Taskforce.

Given the wide array of issues covered throughout the conference, we set out to capture some of our guests' valuable insights in a short collection of essays. Our aim was also to reach beyond the conference's immediate audience and feed into the wider reflection at European level on how to preserve the integrity of electoral systems and democratic processes.

The result is this unique collection of 35 original short essays addressing the different themes of the conference. Many people contributed meaningfully – both intellectually and practically – to the preparation of this publication, as well as to the organisation of the conference itself. We would like to take this opportunity to express our heartfelt gratitude to them.

First and foremost, we would like to thank our contributors. We are tremendously grateful that, amidst their heavy professional, academic and personal commitments, our speakers – as well as some of our participants – generously responded to our request for contributions.

We would also like to thank Silvio Mascagna and David Knight from the Cabinet of Commissioner King, as well as Angelina Gros Tchorbadjiyska, Katarina Cutuk and Christine Erzberger from the Task Force on Security Union.

At the EPSC, we would particularly like to express our gratitude to Ulrik Trolle Smed, Asen Dimitrov, Luis Viegas Cardoso, Cristina Ruiz and Giulia Capitani who steadily carried through the entire process; Ricardo Borges de Castro, Paweł Świeboda, and Agnieszka Skuratowicz who always had purposeful and insightful suggestions. Aura Salla and Jonáš Jančařík, who handled communications, set up our website and orchestrated our online presence; Annick Hilbert, who created our conference design and beautifully laid out this publication; Rachel Smit for her sharp editing; and of course Carmen Tresguerres, who has worked closely with all to ensure that we always strive for more and better, as well as the many other EPSC colleagues who helped turn this conference into reality.

Disclaimer

The views expressed in this EPSC publication are those of the authors and do not necessarily correspond to those of the European Commission.

Photo credit: © Arnaud Jaegers (https://unsplash.com/)

CONTENTS

FOREWORD

Sir Julian King

European Commissioner for the Security Union

Free and open elections are the foundation of our democratic societies. They make Europe what it is – a place where you can speak your mind without fear of being arrested or prosecuted. A place where voters trust that election results reflect open and transparent public debate.

Protecting the integrity of our elections is therefore an absolute priority; for the European Union, for the Member States, and for all European citizens. But the threat to them has been growing in the past couple of years, which have been marked by a series of attempts to manipulate electoral process in at least 18 countries, including in the EU.

The threat can be split into two vectors: attacks that target systems and data to interfere with the electoral process or voting technology, and threats that manipulate voting behaviour. Our work through the Security Union is designed to tackle both.

In terms of the first, although this approach is relatively crude, even the suggestion that it has happened or could happen is corrosive to public trust and confidence.

For the second, we can break it down further into three categories: targeted hacks and leaks to change public opinion; fake news to influence the results; and the use of psychometrically targeted messaging based on mined user data – such as in the Cambridge Analytica case.

How can we counter these threats? We started by reinforcing our cybersecurity to address threats against systems and data by targeting disinformation online to counter behavioural manipulation. We need to ensure our election technology is well protected. We need to deter those who intend to attack us. And we need to make it easier for users see the provenance of content, allowing them to assess its trustworthiness, while also reducing the visibility of disinformation. We are targeting the use of bots – we're for free speech, not artificial speech. We are working with internet platforms to make progress on these issues, and provide more transparency, traceability and accountability online.

We have the first iteration of a code of conduct agreed by platforms – it is a good start but to be effective it needs to go much further, much faster.

And last month we brought forward a package of measures aimed specifically at election security, including a Recommendation to establish election cooperation networks between Member States measures aimed at greater online transparency, measures to increase protection against cybersecurity incidents and strengthening our work to fight disinformation campaigns.

The need for action on this is urgent – doing nothing risks our democratic processes being undermined. That is why it is so important to bring together all the relevant players – from the EU, Member States, and the private sector – to ensure that we form a united front in the battle against those who wish us, and our way of life, harm.

Julian King

Ann Mettler

Head, European Political Strategy Centre

At the onset of the digital revolution, there was significant hope – and indeed an expectation – that digital technologies would be a boon to democracy, freedom and societal engagement.

Yet today – although it is clear that it cannot necessarily be attributed to digital technologies – we note with concern and disquiet that the world has experienced twelve consecutive years of decline in democracy and freedom.[1] At the same time, we are witnessing the rise of what might be dubbed as 'digital authoritarianism'.

Against this backdrop, it is time to better stress-test our assumptions, as well as the emerging technologies that might be put to misuse in an effort to undermine elections and democracies – be it Artificial Intelligence, deep fakes or cyber mercenaries. Given the confluence of potential challenges, we must find the courage to take an honest and unsentimental look at the state of play of election interference driven by cyber threats.

At stake is nothing less than people's trust in our institutions – without which our democracies cannot function. Our adversaries certainly know that, which is precisely why they are using digital tools to disrupt and sow doubt. This is proving not only much more potent than many traditional forms of attack, but also significantly cheaper and more difficult to prove – and ultimately prosecute. That is why I strongly believe that the institutions and processes that underpin our electoral systems deserve to be classified as critical infrastructure.

To achieve this, the EU Directive on security of network and information systems (NIS Directive) is a good place to start. And we should not be afraid to consider extending the approach to other areas, such as for certain parts of social media platforms to ensure that the public and governments receive critical information about attacks on their IT systems or interference through their services.

Nor should we be afraid to consider requesting that platforms better know their customers at a time when foreign or domestic actors so actively polarise our societies under the shelter of anonymity or fake accounts. Would we still see similar levels of hatred, bullying, disinformation and insults if it were otherwise? Is it not time to have an earnest debate about how to restore civility to our public discourse?

Finally, we must seek to bolster the resilience of our societies against interference, by supporting innovative approaches by start-ups, NGOs and volunteers wanting to help protect democracy at this critical moment in time.

And given that the media is the backbone of democracy, preserving the independence and safety of journalists is a must. I shudder to think of a world where our media representatives become mouthpieces for governments, can no longer uncover corruption, or hold public officials to account.

The stakes are high – and they are worth fighting for. Democracy, freedom and liberty must never be taken for granted.

[1] The independent watchdog organisation Freedom House's report for 2018 – entitled 'Democracy in Crisis' – finds that democratic principles such as election integrity and freedom of the press are weakening globally for the 12th consecutive year.

THINK PIECES

EUROPEAN COMMISSIONERS' CORNER

Věra Jourová

European Commissioner for Justice, Consumers and Gender Equality

Securing Free and Fair European Elections

In May 2019, almost 400 million eligible voters will be invited to the ballot boxes across 27 nations, and, in doing so, participate in one of the world's largest democratic exercises.

However, the world in which the 2019 European elections will take place is not the world of 2014. We have uncovered serious threats to the integrity of our electoral processes. Today, if we want Europeans to make their political choices in fair, secure and free elections, we must update our election rules to the digital age.

More precisely, we must take action to curb the risks of manipulation and interference, including by foreign actors. We must counter mass online disinformation campaigns, cyberattacks and other misuses of the online environment.

Applying the Data Protection Rules

The Cambridge Analytica scandal showcased the value of our European data protection rules and why they needed strengthening. The 2019 elections will be the first ones to take place under the General Data Protection Regulation (GDPR). Everyone involved in elections – national authorities, political parties and private actors – must be aware and understand the meaning of these rules. In order to help stakeholders to apply these rules, we have developed specific guidance highlighting the data protection obligations that are most relevant to the electoral process. Among others, the GDPR confers stronger enforcement powers to national data protection authorities, to help them address infringements of data protection rules.

Next to this, we have called on Member States to apply appropriate sanctions against data protection infringements that sway or attempt to sway the elections. We are also planning to tighten the rules on European political party funding: parties infringing data protection rules could be fined up to 5% of their annual budget. They would also not be eligible for funding from the general budget of the European Union in the year they are sanctioned.

By addressing data infringements and manipulation directly, we are helping to build the necessary trust in the security and fairness of elections – something that is of benefit to both citizens and political parties.

More Transparency in Online Advertising

As parties increasingly campaign online, the European Commission recommends that all of them, as well as foundations and campaign organisations, do this in a transparent way. Citizens should be able to recognise online adverts that target them in the context of elections and know who is behind them. There should be no hidden or opaque political campaigning in free and fair elections. Rules that apply to offline campaigning – regarding transparency in elections, money spent on political campaigning, silence period before elections etc. – have to apply in the online world as well.

Better Cooperation

Securing free and fair elections across Europe will require tight-knit cooperation among many national authorities and other stakeholders, as well as among the Member States. This is why we encourage each Member State to set up a national election cooperation network of relevant authorities – such as electoral, cybersecurity and data protection authorities – and to appoint a contact point to coordinate at a European level. This will enable authorities to detect potential threats more quickly, to exchange information and best practices, and to ensure a swift and well-coordinated response.

The online world has created unprecedented opportunities for engaging in a political debate and communicating directly with millions of voters. But recent elections and referenda have also shown that it comes with new risks that require specific protection measures.

Mariya Gabriel

European Commissioner for Digital Economy and Society

Stepping Up Our Engagement Against Disinformation

The digital transformation has affected all aspects of our society, from mobility to healthcare to energy distribution. As we have now changed our way of communicating, informing and, sometimes voting, we see the added value that new technological solutions can bring to democratic processes. Thanks to new technologies, more citizens are aware of recent initiatives undertaken by the institutions are in the position to consciously express their preference and contribute to the democratic life. At the same time, new technologies bring increased vulnerabilities. Such vulnerabilities can be exploited by external actors to interfere with the integrity of democratic processes and destabilise democratic governments through disinformation.

Against this background, the European Commission is committed to making sure that all elections remain secure and protected from this type of threat. This is why, last September, we issued a package of measures aimed at securing the next European elections, which will take place on 23-26 May. The principle affirmed through our action is that we will all be more resilient to cyber-enabled threats only if we recognise and prepare for them, in particular by sharing information between relevant parties such as national competent authorities for cybersecurity, data protection, audio-visual services and electoral committees.

However, the improved cyber-resilience of our democratic process will not be enough if we do not make sure that the information reaching citizens is truthful and credible. Hence, last April the Commission launched a strategy for fighting disinformation which aims at guaranteeing better information without disturbing freedom of expression and media freedom, the two fundamental rights which are the foundation of an inclusive and pluralistic public debate. We paid particular attention to involve as many stakeholders as possible in our analysis before deciding which strategy would be the most efficient.

In September, online platforms and the advertising industry agreed on a self-regulatory Code of Practice on Disinformation. The Code includes several commitments that will increase transparency concerning political advertising while contributing to the empowerment of consumers and research community.

A second initiative is the creation of an independent European network of fact-checkers. Their work contributes to making the media landscape more robust. Cooperation between fact-checkers, online platforms and the advertising industry should provide citizens with easier access to more reliable information and, at the same time, make life more difficult for those who want to make money through the spread of disinformation.

Dimitris Avramopoulos
European Commissioner for Migration, Home Affairs and Citizenship

Securing Our Elections, Securing Our Democracies

When the history of the 2019 election is written, it should not be about how external actors tried to influence its outcome.

The essence of the European Union is its defence of democracy and democratic values. In today's rapidly changing world, challenges against our democracy and our values are everywhere. Trust in institutions, international institutions and the very post-war world order is weakening. Populism is on the march. Our citizens' active participation in the democratic process is a fundamental principle, which we are committed to safeguard. Elections are crucial to the functioning of representative democracy and therefore we must ensure that they are fair and free. Our citizens have a right to choose without external interference.

The attacks against electoral infrastructure and campaign information systems are hybrid threats that the Union needs to address. European citizens should be able to vote with a full understanding of the political choices they have and with the security that their vote is properly reflected in the final election results.

Electoral periods have proven to be a particularly strategic and sensitive window of time for cyber-enabled attacks. This included attacks against electoral infrastructures and campaign IT systems, as well as politically motivated mass online disinformation campaigns and cyber-attacks by third countries with the aim to discredit and delegitimise democratic elections.

Malicious actors of different backgrounds can use cyberspace to target elections and election processes in different ways by gaining illegal access to information systems and collecting sensitive information from candidates aiming at influencing the public opinion and/or the election results and disrupting information systems with a distributed-denial-of-service attack to affect campaigns or the coting process.

As we head into a critical election year in Europe, amongst others with the European Parliament elections, and we need to be prepared to counter these cyber threats. In this context, we proposed new measures for securing free and fair European elections that will allow us to better protect our democratic processes from manipulation by third countries or private interests.

We need to build strong cybersecurity for our elections and election processes based on a comprehensive approach that includes resilience, deterrence and a diplomatic response where state actors are involved.

Cooperation and information exchange between all relevant authorities is crucial more than ever now. Experience sharing across Member States on cyber incidents is essential. That is why the Commission recommended the setting up of national elections networks – where national authorities may exchange information capable of affecting the elections but also jointly identifying threats and gaps, sharing findings and expertise, and liaising on the application and enforcement of relevant rules in the online environment.

The national law enforcement authorities will also support and be part of this work, with the support of European agencies such as Europol at European level.

The challenge of defending our democratic institutions is a task that no country and no region can promote alone. The security of our elections affects all of us directly. Let us do our best to ensure safe elections in our European home in 2019. Let the historians of the 2019 elections mark this as a year of fair, free and secure elections in Europe.

Chloe Smith

Minister for the Constitution, United Kingdom

Preserving the Integrity of Electoral Systems and Democratic Processes

There is a reason why Britain is admired around the world for our democracy. Along with our European neighbours, we are part of a community of democracies, extolling its virtues across the globe. We have worked for centuries to build our democracy and protect it from the ever-changing forces that seek to threaten it.

UK voting systems do not lend themselves to direct electronic manipulation. But we are all familiar with the revelations about Cambridge Analytica – the firm that harvested around 87 million Facebook users' profiles to build a system which could influence voters in the 2016 US election. The increase in online disinformation risks stoking a public perception that attempts are being made to undermine the UK's democratic processes.

And while democracy thrives from robust, healthy debate, we are constantly alive to the risks that come when that genuine debate deteriorates into threats and intimidation designed to drive out honest differences. A quick look on Twitter will show you the current, sad state of political debate where rape threats against female members of Parliament are an everyday occurrence.

It is essential that we not just maintain but strengthen public faith in democracy, so we are focussing on concrete steps that ensure we protect voters and the voting system.

Rising levels of intimidation in public life are deterring talented people from standing for election and putting voters off politics. That is why we are consulting on new measures that will protect voters, candidates and campaigners so they can make their choice at the ballot box or stand for public service without fear of being victims of misinformation or abuse.

We are improving the security and integrity of our voting process, bringing us in line with countries around the world such as the Netherlands where voters confirm their identity when they vote.

Currently in the UK you only need to say your name and address to get your ballot paper at the polling station, a test based on a 19th century expectation that people knew their neighbours. Clearly, this process is open to abuse and not fit for purpose in a more modern, populous society.

We are committed to increasing transparency in digital campaigning and we are consulting on proposals for new imprint requirements on electronic campaigning so voters can see who is targeting them.

Voters must have confidence that their vote is theirs, and theirs alone. Not only that, they have to feel that their vote matters, and that their voice is being heard.

We are promoting democracy in schools and to youth groups, and marking the 90th anniversary of women achieving equal voting rights. Our democracy is being made more accessible for people with disabilities and safer for survivors of domestic abuse.

Challenges to our democratic processes are far from new. But our determination to tackle challenges head on makes the UK's democracy fit for the 21st century.

Edvinas Kerza
Vice Minister of National Defence, Lithuania

Lithuania's Example – Preserving the Integrity of Election Processes

2019 is an especially important year for Lithuania, marked with three elections: the Municipal Councils' election in March, as well as the Presidential election and the European Parliament election in May.

Yet, we know that the security of elections and the integrity of democratic processes are being challenged across the Euro-Atlantic community, by a growing number of hostile cyber-activities and disinformation campaigns. We have recently observed a number of attempts by state actors to interfere with other countries' political processes, creating mistrust and confusion, and influencing the voting outcome.

Lithuania too is under constant pressure. Hostile actors are putting effort into falsifying our historical memory and undermining the legitimacy of today's actions. Our cyber-defence teams are fighting cyber-espionage activities and cyber-attacks against government institutions, as well as various public and critical infrastructures, on a daily basis. Our StratComs, media and growing elves community are combating disinformation and fake news day in day out.

To respond to the growing cybersecurity challenges more effectively, Lithuania, in 2018, has consolidated all its cybersecurity institutions and responsibilities under the Ministry of National Defence, bringing government cybersecurity experts under one roof. The unified National Cyber Security Centre (NCSC) has become a national cybersecurity powerhouse and a major asset in the fight against evolving cyber-threats, including in the context of elections. To better prepare for the upcoming elections, the NCSC is working closely with the Central Electoral Commission of the Republic of Lithuania to upgrade security procedures and standards, as well as test the IT systems in place.

Lithuania's experience shows that traditional malicious cyber-activities and cyber-enabled disinformation campaigns today very often go hand in hand. One recent example of this was the mixed disinformation and malware attack against Minister of National Defence which was used to infect ICT devices of politicians and journalists.

Being an important democratic institution, the media has also become a direct target of malicious cyber-activities. Therefore, the Ministry of National Defence recently signed a cooperation agreement with country's main online media portals. The range of cooperation activities includes information sharing, training and support in case of cyber-attacks.

But in the long run, nobody will cope with these issues alone. There is a need to step up cybersecurity cooperation at EU level. Therefore, Lithuania, together with 8 other EU Member States, is working on creating Cyber Rapid Response Teams to provide mutual assistance in the cyber-field in case of major cyber-incidents. Teams could also be used to ensure the cybersecurity of electoral processes by providing targeted support in the preparation phase and during the elections.

Shelley Whiting

Director-General of Global Affairs,
Ministry of Foreign Affairs, Canada

Protecting Democracy: The Role of the G7?

Evidence suggests that foreign actors have undertaken efforts over the past decade to shape public opinion and perceptions around the world with the intent to sow dissent towards democracy as a successful form of governance, to promote political narratives which favour their own autocratic systems, and to challenge democratic and international norms. In this context, foreign interference seeks to establish 'platforms of influence' within all open societies around the globe, mainly targeted at three key spheres: the media, political systems, and the economic and financial sphere. In recent years, we have also heard reports of major western democratic elections and voting processes that have been targets of foreign interference.

We have seen areas that are susceptible to foreign interference include political party funding, political advertising campaigns, and persons in positions of leadership (political, media, and private sector) through bribery, blackmail, and corruption. Interference has also included processes meant to manipulate various social and demographic groups, including diaspora, by using polarising issues, infiltration, coercion and other means. Over the last few years, we have noted the impact of foreign interference has grown, along with its scale, speed, and range, particularly as a result of the powerful combination of the internet, social media platforms, machine learning, and the availability of cheaper and more accessible cyber tools. Tactics have included using the media and online spaces to exploit existing divisive political fractures, target individuals, and manipulate social and demographic groups. The concern is that the intent is to erode citizen confidence in the democratic process, exacerbate divisive political fractures, and sow distrust between governments and civil society.

As the global community becomes more informed of the threat, what can we do as governments and the international community? In Charlevoix, G7 leaders announced the creation of the Rapid Response Mechanism (RRM). This mechanism aims to strengthen G7 coordination to identify and respond to diverse and evolving threats to G7 democracies, including through sharing information and analysis, and identifying opportunities for coordinated response, in a manner that is consistent with universal human rights and fundamental freedoms. We all need to continue to increase our understanding of the threat environment, share information and lessons learned and tactics used, and augment our capacity to anticipate and respond in a coordinated manner that is inclusive of government, society, private sector, and various actors working to protect democracy and the international rules-based system.

CYBERSECURITY IN ELECTIONS: A LOOK AT THE LANDSCAPE

Liisa Past

Next Generation Leader at the McCain Institute for International Leadership and former Chief Research Officer at the Cyber Security Branch of the Estonian Information System Authority

Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses

Attempts to influence democratic processes have long been part of adversarial strategy seeking to sow doubt and distrust in rule-of-law-based societies. Cyber-enabled attacks against elections aim to compromise the confidentiality, availability and integrity of the systems and data involved. As such, they are often integrated with information and influence operations that mostly target public discussions.

While the 'processes of elections themselves – the registering of voters and candidates, the gathering and counting of votes, and the communication of the election results – are by no means impervious to attack',[2] 'it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyberattack or intrusion'.[3] Therefore, the possible attack surface is likely to include a wide selection of auxiliary targets, including the candidates and parties as well as their staffers and volunteers, media or other solutions used to display and publish results, election technology vendors, the local election officials and other systems that elections partially rely on, such as voter rolls, population or property registries as well as connections between these systems.

Thus, a comprehensive, whole-of-government approach is called for. As an example of a comprehensive approach, the *Compendium on Cybersecurity of Election Technology*, published under the auspices of the Cooperation Group of the Network and Information Security (NIS) Directive, reviews the complete lifecycle of elections. It offers comprehensive, practical and actionable guidance on bolstering cybersecurity for election organisers and cybersecurity agencies alike, based on the contributions of around two dozen EU Member States and a number of European institutions.

In addition to the systems controlled and owned by election management bodies, the compendium also reviews how government actors can advise owners of auxiliary systems that have been the most common target of cyberattacks in connection to elections. In the context of the elections to the European Parliament it is important that these principles are followed through, including the last mile of communication of election results. The transfer from capitals to Brussels has to be particularly carefully considered as it lacks a common security approach and, unlike national elections, has not been live tested in this new security environment where elections are considered a legitimate target of politically-motivated cyberattacks.

In addition to the comprehensive approach as laid out in the compendium, the EU and Member States need to consider:[4]

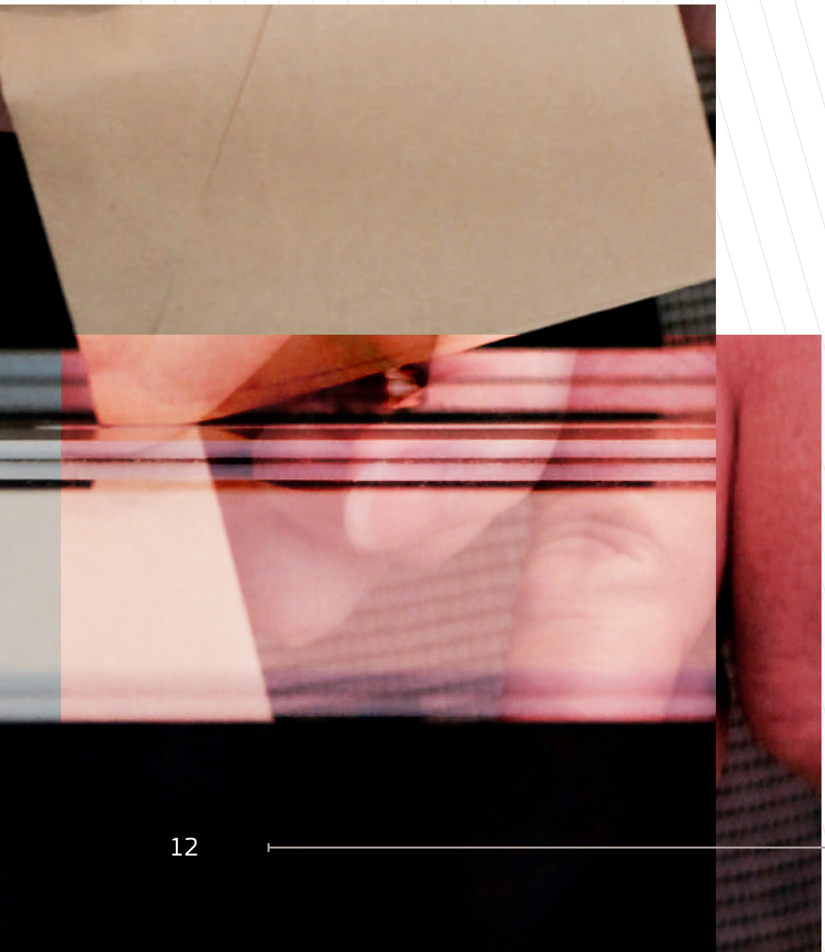
- Designating elections as critical national infrastructure or essential services: This would extended the mandated standards and extra protections to them automatically. While there are a number of successful examples of protecting elections as critical infrastructure, many fear the approach to be too inflexible or to set an unrealistically high standard given current capabilities.

- While elections are necessarily a national business and the variations in national electoral systems serve partially as a safeguard against widescale compromises, Europe can further use its potential arising from cooperation. In particular, further threat intelligence sharing, and sharing of tools and techniques is called for. As a first step, the Compendium on Cybersecurity of Election Technology can be updated as needed. Building on that, however, those tasked with cybersecurity would greatly benefit from operational cooperation as the adversarial tactics are likely to be similar.
- Attribution and increased public discussion of cyberattacks is key as it can lead to increased deterrence. Attribution is the essential first step in taking legal and diplomatic countermeasures, be it prosecutorial action or sanctions. While there has not yet been collective international response per se to cyberattacks on elections, the coordination efforts so far are promising and coordinated responses have been taken. The EU Cyber Diplomacy Toolbox allows for Common Foreign and Security Policy (CFSP) measures in response to aggression in cyber space and could be used in the case of election meddling.

[2] Cooperation Group of the Network and Information Security Directive (2018). Compendium on Cyber Security of Election Technology, CG Publication 03/2018, Brussels. Available at: https://www.ria.ee/public/Cyber_security_of_Election_Technology.pdf.

[3] Department Of Homeland Security; Office of the Director of National Intelligence, 2016

[4] Past, L. (2017). All Elections are Hackable: Scalable Lessons from Secure I-Voting and Global Election Hacks. European Cybersecurity Journal, 3(3), 34–47, https://www.ria.ee/public/RIA/ECJ_Volume3.Issue3_Extract_PAST.PDF.



CYBER ELECTION STRESS TEST: ARE WE PREPARED FOR THE WORST?

Laura Rosenberger

Senior Fellow and Director of the Alliance for Securing Democracy, German Marshall Fund of the United States

A National Security Issue – Not a Partisan One

Europe is no stranger to Russian government efforts to interfere in and undermine democracy. These operations employ a range of tools, including information operations, cyberattacks, malign financial influence, strategic economic coercion, and subversion of civil society. Russian-linked efforts to interfere in Macedonia's recent referendum on the name agreement with Greece were just one recent example of how these tools are used together. Moscow exploits these relatively low-cost methods to attempt to gain relative power by weakening others, including NATO and the EU.

Despite Russia's aggressive use of these tactics across its periphery, the export of these tools to Western Europe and the United States took many by surprise, particularly their use to target elections. While elections provide a particularly ripe opportunity for malign actors to undermine democratic institutions, election interference is one part of ongoing efforts aimed at undermining faith in government, deepening divisions, and in some cases, fomenting violence. Russia is not the only authoritarian power using these tools – the Chinese government has also begun to use social media to manipulate public discussion outside its borders, and has funded information operations and directly supported politicians to influence political debate abroad, including in parts of Europe. Several companies also recently took action against Iranian information operations online. While using similar tools, the strategies employed by different authoritarian actors for their interference efforts will likely differ based on their long-term goals, and these operations are therefore likely to have differences in how they manifest.

Countering foreign interference requires robust action from governments, the private sector, and civil society, and it is critical that any countermeasures are not only consistent with, but also help strengthen, democracy. Transparency and exposure of such foreign interference operations is critical to reducing their effectiveness and deterring them. Many of these issues fall in the seams between bureaucracies – within individual governments, between the EU and NATO, and between the public and private sectors – and it is critical that we develop structures both within and between governments, and with the private sector, to ensure a unified and integrated approach to the whole problem.

In the United States, a robust response has been hindered by partisanship around the issue. It is critical that decisions about whether to expose and respond to foreign interference be removed from a political context and understood as a national security issue.

Governments also need to send deterrent warnings to foreign actors about the consequences of interference. Together with tech companies, they need to close off vulnerabilities that are being exploited, while protecting citizens' ability to engage freely and robustly in speech. We need to harden our electoral infrastructure against cyberattacks, and both the press and candidates should pledge to handle leaked material appropriately. We also need to identify threats in new technology before they are exploited. And it is essential that democracies work together to share information about threats and collaborate on responses. Finally, civil society needs to play a robust role in both exposing interference and in building societal resilience. Foreign interference operations work because they exploit real vulnerabilities; strengthening ourselves at home will be critical to a strong defence.

Mikael Tofvesson

Head of Global Monitoring and Analysis,
Swedish Civil Contingencies Agency

Swedish Election 2018 – A Preliminary Assessment

As a part of Sweden's preparations to protect the Swedish election, the Swedish Civil Contingencies Agency (MSB) investigated influence activities targeting elections in other countries and conducted a vulnerability study regarding the Swedish election process and organisation.

Election interference is only a part of a long-term influence campaign aiming at weakening a future government and its ability to act internationally. The aggressor is using a whole of society approach to interfere with the election. To be able to understand the impact of an influence campaign, you have to identify the vulnerable areas that are under attack. Looking at other elections and comparing the methods of the attacks, MSB assessed that four areas, relevant to Sweden, were targeted:

- The election process and its integrity
- The will and ability of the population to vote
- The political preferences
- The trustworthiness of the political leadership

Influence campaigns against elections were effective when:

- There was a lack of awareness about the threat and the vulnerabilities to the threats in a society.
- There was a weak or non-existing cooperation between the political decisions makers, agencies and authorities conducting the election and among the agencies protecting the country against foreign influence.

As a response to the threat and the identified vulnerabilities in the Swedish election, MSB implemented a wide range of activities and supported other organisations in their work to conduct and safeguard the election. MSB developed and implemented capabilities in four areas:

- Identifying information influence activities by monitoring vulnerable areas in our society and threat actor's activities.
- Coordination/Cooperation between the authorities and agencies conducting and protecting the election.
- Information sharing among all relevant stakeholders.
- Awareness about our own vulnerabilities and the threat with a whole of society approach.

Eva Maydell
*Member of the European Parliament,
European People's Party*

Democracy and Elections under Attack: Competing with Trolls, Terrorists, Populists and Advertisers

When we talk about elections, we tend to think about them in two extremes – a rather technical exercise or a purely political thing. Experts know well that organising elections is one of the most complex operations. If you can imagine, one election in a single country entails at least several thousand teams that need to be recruited, trained and assessed on their performance. It means organising logistical support and equipment at several thousand locations. On the other hand, we politicians need this process done in a manner that maintains the highest possible integrity because elections are the most visible, democratic and fair instrument for any society to make public choices. In order to work properly, the election machine needs to have the trust of those involved – both candidates and voters – otherwise, it cannot deliver its main product: a choice that is accepted by everyone.

Yet, two main elements of our democracy and electoral processes are today under severe attack:

The first is common sense in our public conversation and communication. Call it fake news, disinformation, or whatever else: we have lost the sense of what is true and what is false. The problem was well formulated – 'more information, but less informed'. There is no silver bullet to solve that. We have already started working with the big online platforms to make the Internet a better and more reliable place for information and facts. We have already started preparing the next generation for this new phenomenon 'more information, but less informed' with targeted subjects in school. But for us politicians during elections, it is more difficult. We are competing for the attention of our citizens with Russian trolls, terrorist organisations, political populists, and advertisers. The only way to win is to offer our citizens a logical narrative, based on principles and facts, filled with brave but conceivable ideas for the future.

The second element that is under a serious attack in our democracies – as the 2016 US elections showed – is our election infrastructure. The threats designed to undermine the electoral process integrity can be fatal. It is obvious that we should re-conceptualise the use of technology in the process so that the voting rolls, the act of voting, tabulation and final results are more secured to external influence.

We should also reform our election administration with significant focus on resilience to cyber-attacks. Many US states have already implemented a series of stress tests to their election infrastructure and staff. The EU should follow. What the European Parliament could do is, in cooperation with the Organisation for Security and Cooperation in Europe, the Venice Commission of the Council of Europe, to work for new standards for election security.

Having in mind the importance of elections, there is no surprise that those who want to see our societies divided and dysfunctional concentrate their activity on them. It is already clear: today foreign interference aims not only to support a single candidate in a single race, but also to ruin the basic mechanism that our societies use to make decisions. With no credible elections that are seen by the citizens as open and fair, our societies will end up divided, perplexed, in deep confrontation.

Elizabeth Carolan
Founder, Transparent Referendum Initiative

What Happens Online: Boosting Awareness and Accountability

Ireland's 2018 referendum shows that when specific digital threats to democracy are known, concrete action can be taken to expose and limit its effects. Building long-term resilience to digital threats will rely on identifying threats early – ideally before they manifest during live contests. The European Commission can help enable this by mandating that tech companies be more open about the tools and technology they are developing, and more responsive when things go wrong.

The issues with digital political advertising – targeted content on social media, sometimes misleading, that is difficult to scrutinise and trace and can be purchased anywhere in the world – have been highlighted as significant factors in retrospective analysis of electoral campaigns in the UK, US and other countries.

Knowing this, and that Ireland was about to hold a referendum on abortion, my civil society project - the Transparent Referendum Initiative – built an open database of referendum-related Facebook ads which journalists could fact-check and source trace. We highlighted behaviour online that otherwise would have gone unscrutinised, and that would not have been allowed offline.

For example Ireland's electoral law says political posters must have labels stating who has paid, so groups behind them can be identified and asked about their claims. But online, hundreds of the ads we found were placed by unregistered or untraceable groups, some containing disinformation. Likewise Irish law bans overseas donations to campaigners, but during this referendum we found overseas groups purchasing Facebook ads directly targeting Irish voters.

Pressure from these revelations prompted Facebook and Google to limit advertising during the campaign. Additionally, our Government has since committed to updating our electoral laws, and has added the issue to our national risk assessment.

This specific issue is slowly being addressed as tech firms are starting to fix their political ad policies and products, and governments debate new rules. This has been slow, as companies in particular can be blind to the unintended consequences of the technology they build.

But new issues are emerging all the time – for example the spread of disinformation on closed messaging networks seen recently in India – and will continue to emerge as connectivity, algorithms and data holdings develop at exponential rates.

Building resilience to these threats will take efforts by a range of actors; governments will need to strengthen the independent institutions that oversee our democracies so they can respond more quickly. Civil society and the media will need to be prepared to be at the forefront of investigating risks and bringing problems to public attention.

But tech companies will also need to make major changes, to become more open and responsive; to start sharing information on tools and technology so risks can be identified early; and to be available to and responsive to those concerns emerging in different countries. The European Commission should explore ways to ensure that these companies take these steps, and are held accountable if they fail to do so.

Vaidas Saldžiūnas
Defence Editor and Media Expert on Disinformation, DELFI

Viktoras Daukšas
Director, Demaskuok.lt initiative

How to Spot Disinformation within 2 Minutes in Real Time?

Disinformation agents already skilfully employ a large spectrum of measures ranging from historical sentiments to the most advanced IT solutions. And it is important to acknowledge that the intentional spreading of false information in order to deceive and to undermine trust in existing models of governance will not slow down and will become even more advanced and more creative.

Countermeasures often prove too slow and too fragmented, and they still rely on an outdated '2G' approach, where the first G stands for Google search (manual monitoring) and the second G for Gut feeling (no data-driven evidence).

What is more, most public institutions come across allegations of attempting to become 'Ministries of truth' if they get into debunking.

The problem is complex, and it requires complex solutions – involving both technology and cooperation between multiple parties.

Against this backdrop, the Lithuanian-born initiative Demaskuok! (Debunk! in English) seeks to provide a speedy, independent, transparent and fair solution, with maximum outreach.

An analytical tool capable of spotting and identifying disinformation within 2 minutes in real time, it brings together the seven largest media outlets in Lithuania (online, TV, radio) – representing 90% of national audience coverage; the three StratCom units of the Lithuanian Ministry of Defence, Ministry of Foreign Affairs, and armed forces; volunteers comprising Lithuania's community of 'elves', journalists, as well as researchers); and an experienced team of IT geeks.

The platform, which is funded by Google Digital Innovation Fund and DELFI – the biggest media outlet in the Baltics – has been developed in 18 months and, over the last 7 months, it has been tested by 2 full-time journalists and 30 elves. In the near future, 20 more journalists will be trained to use the platform. The tool analyses 10,000 articles in Lithuanian and Russian languages per day, but that is definitely not the limit.

The platform also provides automated user-friendly solutions for repetitive and manually-performed tasks, thus saving journalists significant amounts of time for investigation and writing. The current record track is a full debunking process – from spotting disinformation to release of an article – implemented just in two hours.

Seeking to raise awareness and get the EU and media organisations trained up ahead of next year's various crucial elections, the team of Demaskuok! is now seeking partnerships to make the platform operational cross-language, cross-country.

Jennifer Kavanagh

Associate Director, RAND Corporation,
and Co-author of the report 'Truth Decay'

Truth Decay: A Tale of Decreasing Trust in Institutions

At RAND, we are studying Truth Decay—the diminishing role that facts, data, and analysis appear to play in our political and civil discourse and the policymaking process. We define Truth Decay as comprising four trends: an increasing disagreement about objective facts and data, blurring of the line between fact and opinion, an increasing relative volume of opinion compared to fact, and decreasing trust in institutions that used to be looked to as sources of factual information. While our work thus far has focused on the United States, Truth Decay is a global phenomenon and these trends exist in Europe as well.

The example of vaccine scepticism is one example of this phenomenon. Despite an overwhelming amount of evidence in support of both the safety and the efficacy of vaccines, an increasing number of people in the United States and Europe are sceptical of their safety and refuse to vaccinate their children or themselves. This scepticism is fuelled by disinformation, fabricated research, and misinformed opinion sold as facts. As trust declines in institutions like the government, people do not know where to turn for factual information. Declining vaccination rates have consequences, however, including rising numbers of cases of diseases like measles, that were disappearing.

Our research suggests that these trends are driven by a confluence of at least four factors, including cognitive biases (the ways we process information), changes in the information system (e.g., the rise of social media, the diversification of media outlets, the role of filters and algorithms), increasing demands on the education system that challenge the ability of schools to provide students and adults with the skills they need to navigate this more complex information system, and polarisation – political, economic, and demographic divisions within society.

RAND is concerned about the phenomenon because of its consequences for American democracy and democracies elsewhere, including in Europe. Without a common set of shared facts and objective benchmarks, policymakers struggle to debate policy options and reach compromise on key policy issues. Furthermore, a failure to attend to objective data has contributed to some of the United States' greatest policy failures – the Great Depression, for example, was made worse by a failure to attend to macroeconomic fundamentals.

Before we can move to solutions and responses, however, we need to look back, to understand the historical roots of the phenomenon. Our research on US historical experience suggests that while Truth Decay is new in some ways, it also has historical analogues – the 1890s, the 1920s-1930s, and the late 1960s-1970s. In each of these periods we see significant and rapid changes in the way information is disseminated and consumed, leading to a blurring of the line between fact and opinion and a surge in the dissemination and spread of false and misleading information. Yellow Journalism in the 1890s, for example, and the spread of radio journalism in the 1920s and 1930s are both instances when new technologies empowered those seeking to spread exaggerated and misleading information or to promote their own ideologies and beliefs, often at the expense of fact. What we see today is similar in many ways, but occurs on a larger scale – the changes that have occurred in the scale and scope of information flow in the past 15 years are phenomenal. In addition, we see declining trust in key institutions like the government and the media in each of these three periods (but especially the 1960s-1970s). Polarisation is also relevant in our historical analogues. In the 1960s-1970s, that polarisation was political and social, with many competing ideas about the future of the country should look like. In the 1920s-1930s, economic inequality was the great axis of polarisation. Once again though, the polarisation that we observe today has been supercharged. Now, polarisation along political, economic, and social lines reinforce each other, making it a more powerful dividing force. What we do not see in our historical analogues, however, is the increasing disagreement in objective facts and data—this may be the defining characteristic of today's manifestation of Truth Decay.

While these three examples come from American history, it is likely that there are comparable analogues in European history as well. Because historical examples can provide insights to guide our response to today's Truth Decay, in Europe and the United States, mining these examples for lessons should be a focus of future research.

What can we do in the near term to address the challenges posed by Truth Decay, disinformation, and declining trust in key institutions? Because of the complexity of the challenge, many solutions will be required. However, central among these will need to be a change in the way information is disseminated and shared. Investigative journalism has played a significant role in each of the prior periods in bringing Truth Decay-like phenomena to an end, and so it is likely to be important now. However, we need alternative models for the news industry that support investigative journalism in a more sustainable way. One option would be to incentivise the development of philanthropically-funded news organisations, like ProPublica in the United States, which have the sole mission of pursuing high quality investigative journalism. Without profit as a driving force, such a model may be able to encourage an increase in both the quality and quantity of investigative journalism available for news consumers.

A second key step would be to require transparency about funding sources for news content and advertising. Social media companies are already taking steps to prevent foreign-funded political advertising, and to provide information on funding for all political content on their platforms. However, it is not clear that this goes far enough. Transparency about the funders behind all advertising and news content (where it is not obvious) should be a requirement not only on social media platforms, but also digital, print, and television outlets. Disinformation does not only operate in the political sphere and may have serious implications on issues including health and climate change. Transparency about funding sources can provide consumers with more information and the ability to understand and interpret bias.

These are just two of many possible ways to improve how information is provided. Just as important, however, there will also need to be changes in the way that citizens are equipped with the competencies and tools to distinguish fact from opinion, sound information from misleading information, reliable sources from lower-quality sources. At RAND, we're committed to identifying the best strategy on both sides of this challenge.

Elizabeth Denham

Information Commissioner, United Kingdom

Democracy Disrupted? The Use of Data Analytics in Modern Political Campaigns

Free and fair elections are the cornerstone of any democracy. But rapid developments in technology, opaque online political advertising, and our increasing reliance on social media challenge these principles. The public is increasingly concerned about echo chambers, misinformation and big data politics.

My recent investigation into the use of data analytics in political campaigns aimed to 'draw back the curtain' on the use of personal data in modern political campaigns. The use of online platforms over the last decade has inevitably led to data-driven political campaigns as political parties seek to take advantage of sophisticated marketing techniques to engage with voters.

This brings a number of advantages. Social media provides unprecedented opportunities to engage hard-to-reach groups in the democratic process through issues of particular importance to them. But if left unchecked these new techniques leave voters on the back foot and in the dark about how their personal data is being used to micro-target them with political messages. Voters can't challenge a view if they don't know its provenance.

The catalyst for the Information Commissioner's Office investigation were the links between Cambridge Analytica, Aggregate IQ and allegations that data obtained from tens of millions of million Facebook users may have been misused in the UK EU membership referendum and used to target voters during the 2016 US Presidential Election. Facebook is used by millions of people each day to keep in touch with family and friends. The fact that information shared on the platform could then be used to micro-target them for political purposes without their knowledge or consent has caused deep public concern. My office has signalled its intention to fine Facebook for two breaches of data protection law. We have also progressed civil and criminal enforcement action against a number of parties, including Cambridge Analytica, and data brokers.

But as a data protection authority my long-term goal is to maintain public trust and confidence in how data is used, including in the democratic process. To that end, we have issued a policy report[5] containing recommendations for political parties, online platforms, data companies.

These recommendations are aimed at the UK Government and Parliament but the issues are equally relevant to other jurisdictions. We are at a crossroads; citizens need greater control about how their data is used, genuine transparency about the use of data analytics, and robust enforcement of their rights. Without an informed debate our deeply-held democratic principles will be permanently undermined.

[5] https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

Thomas Myrup Kristensen

Managing Director EU Affairs and Northern Europe, Facebook

Preventing Election Interference on Facebook

When you build services that connect billions of people around the world, you'll see all the good humanity can do. You'll also see people trying to abuse those services in every way possible. This is especially true when it comes to elections.

Free and fair elections are the heart of every democracy. Since the 2016 US elections, we have focused on improving our defences and making it much harder for anyone to interfere in elections.

Key to our election security efforts is finding and removing fake accounts. We have learned a great deal in the past two years and have made significant investments to eliminate bad actors from the platform who try to interfere with election outcomes through coordinated acts of misinformation, spreading of inauthentic ads, spam and cyber-attacks. With advances in Artificial Intelligence, we now block millions of fake accounts every day as they are being created. Where posts are flagged as potentially false, we pass them to independent fact-checkers to review and demote posts rated as false in our news feed, which reduces future traffic and visibility by 80 percent.

Over the past year, we started proactively looking for potentially harmful election-related content, such as pages registered to foreign entities that post divisive content to sow mistrust and drive people apart. When we find them, our security team manually reviews the accounts to see whether they violate our policies. If they do, we quickly remove them. There is no place for this behaviour on Facebook.

We're not working alone. After 2016, it became clear that everyone — governments, tech companies and independent experts — needs to do a better job of sharing the signals and information they have. Bad actors don't restrict themselves to one service, so we shouldn't approach the problem in silos, either. That's why we're working more closely with other technology companies on the cybersecurity threats we all face, and we've worked with law enforcement and other appropriate bodies to take down accounts.

We work with institutions, like we have with the European Commission for the EU Code of Practice on Disinformation, to tackle online misinformation. We also work with independent academics and experts, for example through the recently-established Elections Research Commission, to learn from their expertise and provide us with independent assessments of the broader role that Facebook plays in elections.

We've made a lot of progress, as our work during the French, German, and Italian elections has shown. The investments we continue to make in people and technology will help us improve even further with every upcoming election, like the European elections. But we face sophisticated, well-funded adversaries who are getting smarter too. It's an arms race, and it will take the combined forces of private and public sectors to protect democracy from outside interference.

DEEP FAKES: THE NEXT STAGE OF DISINFORMATION AND ‘ELECTIONS 3.0’

Károly Zsolnai-Fehér

Doctoral Researcher, Institute of Visual Computing and Human-Centered Technology, Technical University of Vienna

Towards a Democratisation of Artificial Intelligence

Transforming audio and video information has become easier than ever: through the recent ascendancy of neural network-based learning algorithms, researchers have been able to solve scientific problems that were deemed unfathomable until just a few years ago. This remarkable research progress left no branch of science untouched: self-driving cars, diagnosing eye conditions, cancer detection, and many more practical applications have surfaced recently, many of which will no doubt enhance our lives in the near future.

As is frequently the case with rapid technological progress, ethical and legal considerations are lagging behind. Today, we not only have to be vigilant about the potential misuse of these powerful methods, but have to make sure that we are also equipped to deal with such cases. This is far from trivial: for instance, it generally requires more effort to detect a piece of audio footage that has been tampered with than creating the forgery itself. It is also important to consider that such a detector network can potentially help an adversary to craft even more convincing forgeries, which makes the development of practical solutions even more challenging.

To address this, we have to endeavour to inform as many people about the existence of these techniques as possible, and make Artificial Intelligence research more open and accessible. This would lead to the democratisation of Artificial Intelligence where not only a few powerful and well-funded ivory towers, but every citizen and research institute is equally equipped to gain access to these techniques.

As many of these techniques are already in use, the urgency of these challenges grows rapidly over time – tackling these issues will require ample discussions and a renewed commitment to empower Artificial Intelligence research within Europe.

IS SEEING BELIEVING? HOW TO PRESERVE TRUST IN ELECTIONS IN THE DIGITAL AGE?

Ricken Patel
Founder and Chief Executive Officer, Avaaz

A GDPR for Democracy to Combat a Digital Blitzkrieg on Europe

The Wright brothers invented the first planes to connect people. But within years, hundreds of thousands of fighters were produced for combat, not transportation.

The full power of this new technology was not felt until the invention of 'Blitzkrieg'[6] – an innovative 'method of warfare whereby an attacking force, spearheaded by a dense concentration of armoured infantry formations with close air support, breaks through the opponent's line of defence by short, fast, powerful attacks and then dislocates the defenders, using speed and surprise to encircle them with the help of air superiority'.[7]

The deployment of new technology and innovative asymmetric tactics was catastrophic. Have we learned this lesson of history?

Today the greatest existential threat facing the EU is a disinformation Blitzkrieg. This is a method of information warfare in which attacking trolls and fake accounts, spearheaded by a dense concentration of weaponised bots that manipulate social media virality algorithms, break into Europe's democratic and electoral processes, and continue their short, fast, and powerful attacks through spreading disinformation and distrust until they dislocate those defending basic European values and democracy.

Russia's government, right-wing extremists like Steve Bannon, and other malicious actors are prepared for battle, yet Member States and the European Union institutions are far from ready to face this existential threat.

Think this is an exaggeration? Let's not forget how people felt about Trump and Brexit. The good news is that the solution to this problem is at our fingertips.

The first step is to follow France's successful resistance during last year's elections: Build a large and well-resourced cyber team to work side by side with independent (Europe Wide) election committees, media, and law enforcement bodies to track and disrupt disinformation attacks rapidly and effectively.

This step is far more likely to succeed if implemented hand in hand with installing defences for democracy on the battlefield itself — the large social media platforms. Both the European Commission and EU governments have the historic responsibility to regulate these platforms, putting in place a GDPR for democracy, before it is too late.

The Avaaz team has fought disinformation for years, and after many months of research and deliberation with experts, social media executives and lawmakers worldwide, has defined 5 key objectives that regulations must achieve to safeguard the democratic process from disinformation.

Avaaz has campaigned against Internet censorship for a decade. These 5 reforms, overwhelmingly supported by our 18 million EU members, protect freedom of speech as well as democracy:

- Ban ALL fake or imposter accounts deployed for political influence
- Correct ALL false content - warn citizens each and every time they're targeted
- Fund Independent Fact Checkers
- Clearly label ALL paid political content
- Independent quarterly audits of large platforms to ensure transparency and cooperation in fighting disinformation

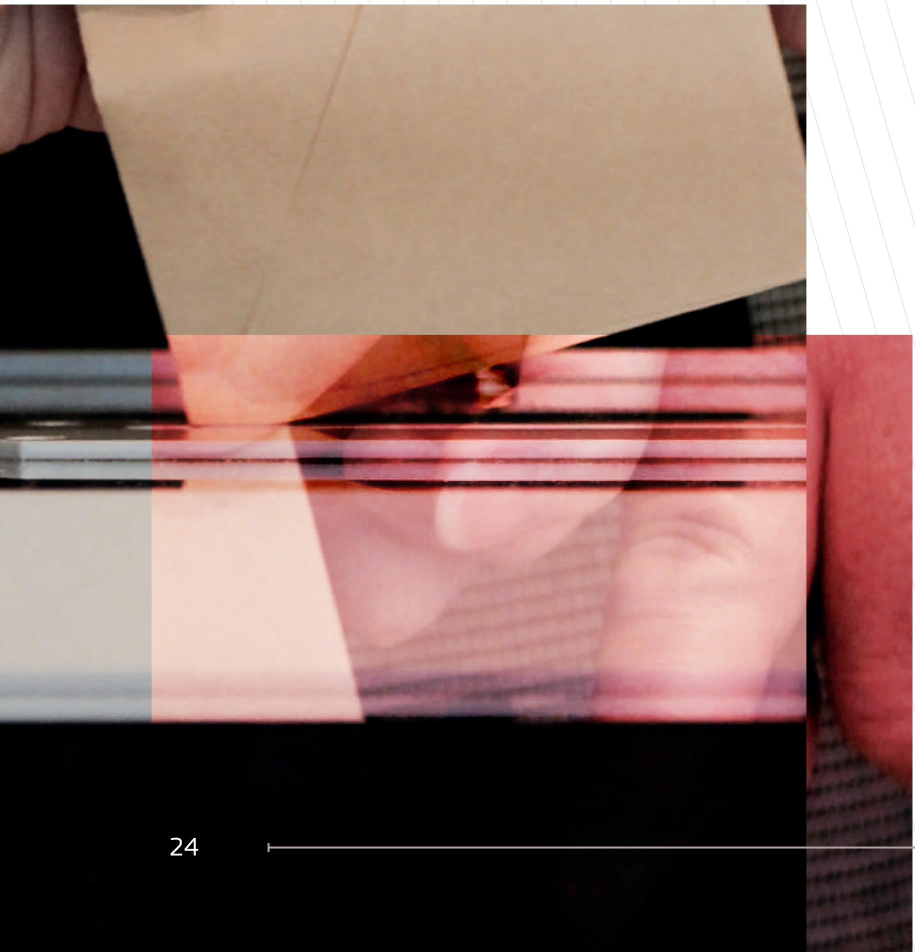
Matched with the French model of cyber-defence, we believe these reforms will severely cripple current disinformation techniques, though constant innovation will also be necessary.

European citizens want their elections to be fair and safe. They want their voices to be heard. The people at this conference can deliver that goal.

Let's not let them down.

[6] David Sanger, Chief Washington correspondent for the New York Times, in his new book 'The Perfect Weapon' provides a detailed account of the invention of airpower, its use in the Blitzkrieg, and how that innovation resembles where the world is today as pertains cyber warfare.

[7] Most common definition from Wikipedia: https://en.wikipedia.org/wiki/Blitzkrieg#CITEREFGlantz2010



Steven Brill
Co-Founder and Co-Chief Executive Officer,
NewsGuard Technologies, Inc.

Give Readers the Power of Transparency

The great innovations of Silicon Valley were initially celebrated as forces only for good; more people could access more information more easily than ever before. But, as it is now clear, these miracles of technology have a dark side: the easy spread of false information, misinformation and disinformation.

Democracies can only function if their citizens have the information they need to participate in civic affairs. Purveyors of false information know this, which is why they target the citizens of the world's democracies. False information can spread quickly, crowding out reliable information, if citizens have no help in determining which is which.

Governments, international organisations and private companies are now working to counter the problem. The European Union Code of Practice on Disinformation, signed in September, 2018, calls on digital platforms to facilitate 'the assessment of content through indicators of the trustworthiness of content sources'. Journalists can play a critical role in solving this problem of journalism. At NewsGuard, journalists arm readers with unbiased information about the reliability of those feeding them the news. NewsGuard, which launched first in the US in August and intends to launch in Europe in 2019, is creating 'Nutrition Labels' write-ups, summarised with a 'green' or 'red' icon, for all the news and information websites responsible for 98% of all online engagement in each country.

The Nutrition Labels demonstrate what, ironically, may now be a counterintuitive idea: sometimes human intelligence is better than the artificial kind. The Nutrition Labels are produced by humans – journalists – who read every site laboriously and provide information about the its background, its financing and its adherence to nine universally agreed basic journalistic standards. Before NewsGuard writes anything negative about a site, its analysts call for comment. Algorithms don't call for comment.

And unlike how algorithms currently operate, NewsGuard is transparent about its decisions and who is making them, and transparently corrects mistakes or changes its ratings if the sites change. Algorithms maintain that if they were transparent, sites would 'game' the system. We *want* sites to game our system – by adhering to our completely transparent nine criteria, and getting better at providing reliable journalism.

The national governments of EU Member States could take more steps to support news literacy through educational institutions and libraries. Librarians across the US are installing NewsGuard on the thousands of computers at their facilities. This is in advance of the platforms, search engines, and browsers themselves licensing the ratings and Nutrition Labels so that they will be ubiquitous – and so that these technology companies can begin to address a problem that they inadvertently but undeniably created.

The human approach to rating and reviewing news websites – rather than trying to review or fact-check individual articles after they have been published – scales well. This kind of large-scale global effort does, however, require the kind of investment more typical for companies such as NewsGuard rather than for NGOs that rely on annual donations or grants. NewsGuard does not presume to tell anyone what to read and does not block anything. Rather, NewsGuard arms people with the information, via the Nutrition Labels, to make their own choices. The digital platforms can choose to use NewsGuard or other providers of this kind of information that the platforms understand need to come from journalists, not technology companies. The two alternatives being most discussed today seem far less desirable: having governments decide on 'good' or 'bad' content or leaving it to the tech companies to jigger and re-jigger black-box algorithms that will never get it right and that will never be accountable.

Stefan Heumann

Director, Stiftung Neue Verantwortung

Why Social Media Platforms Should Be Treated as Critical Infrastructures

In order to function properly, democracies depend on open deliberations and fact-based discussions. As our public discourses have increasingly moved online, social media platforms have become critical infrastructures for our democracy. Citizens and politicians use these platforms to share information, to engage in discussions and to inform themselves. If these platforms do not function properly our democracy suffers. And if these platforms are used to spread disinformation, manipulate our discourses, and undermine our ability to engage in fact-based conversations, our democracy is being directly attacked.

How can we better protect our democracy against disinformation on social media? This is a difficult and complex problem. There are no easy solutions or silver bullets. Governments have only very limited information about how social media platforms work and how they might be exploited to spread disinformation. After all, social media platforms are operated and owned by private companies. Currently private companies make and enforce rules on their platforms and respond to the disinformation problem as they see fit without much government oversight or scrutiny. This is not a new problem. In order to facilitate information sharing and coordinate effective responses to threats in the IT-sector, governments have introduced the concept of critical infrastructure. Applying this concept to social media platforms can help us solve an important piece of the disinformation problem.

IT-systems play a central role in our economy and society. They run our energy systems, organise workplans and treatment in hospitals, and manage our banking operations. All these systems are owned and operated by private companies. But the government takes a strong interest in them. Cyberattacks directed at these IT-infrastructures could have devastating real-world impact such as an extended breakdown of the energy supply or a large scale manipulation of the financial systems. This is why the government has deemed them as critical. This has two important implications. First, operators of critical infrastructures have to share information regarding attacks against their IT-systems with the government. This gives the government the ability to better understand the scale and nature of attacks and craft appropriate responses in collaboration with the private sector. Second, the government can use the knowledge about attack vectors to define and enforce the implementation of higher technical security standards.

So what does it mean to apply the concept of critical IT-infrastructures to social media platforms? First, information-sharing: since social media platforms are critical infrastructures for our democracy, the government needs to be informed about any attempts to manipulate public discourses or spread disinformation. This will help government officials to better understand the scale and nature of the threat and to evaluate whether the companies’ responses to the attacks are effective and sufficient. Second, based on this deeper understanding the government can make and enforce appropriate regulations to better protect social media platforms against such abuses. This is not a quick fix but a long-term approach. Given that this problem won’t be quickly solved, long-term thinking is exactly what we need. And given what is at stake we have little choice to recognise and treat social media platforms for what they are: critical infrastructures of our democracy.

PLAYING TO WIN: INNOVATIVE APPROACHES TO COMBATING DISINFORMATION

Ruurd Oosterwoud

Founder, DROG

The Bad News Manifesto

Last May two Dutch fourteen-year-olds perfectly spread a fake story about an upcoming heat wave that attracted 800,000 unique visitors in just one week. And we made them do it, during class, with their teacher's encouragement. It shows we need to accept that disinformation is an easy and powerful instrument. It perfectly exploits our human weaknesses and is successfully dividing societies. It is the first choice of weapon for demagogues and authoritarian regimes. And it wields great power to involve and mobilise the public, more so than journalism or politics.

This may look like we're heaping praise onto your worst nightmare, but if we want to solve what people often refer to as 'the problem' of disinformation, we should not be afraid of it; we should embrace it. Because after all, fear and distrust are the nuclear engine of disinformation. In order to achieve this we need to adhere to the following rules:

1. Facts are obsolete in the first line of defence against disinformation. As much as we want the truth to be about objective facts, the reality is that the acceptance of truth is a social construct. And emotions are more effective than facts.

2. The greatest victims cause the greatest problems. Disinformation can only be effective if it is amplified by true believers. Factors like distrust of authority, the feeling of loss of control, or even the feeling of belonging make people active amplifiers of disinformation and at the same time extremely hard to reach.

3. The Internet has never been a sacred place, and we should not want to clean it entirely. Trying to defend ourselves from encountering disinformation by blocking it will not increase the resilience of society and will only further convince true believers of the righteousness of their path.

4. We need to create our own playing field. Accept that disinformation has a high entertainment value and use those same techniques to make something else, something harmless that will meet the demand.

That is why, at Bad News, we let people experience the process of disinformation first hand. Developed in collaboration with researchers at the University of Cambridge, the aim of our individual approach is to create triggers in people's minds so that they can recognize manipulation when they encounter it. We want them to feel confident about their ability and learn to embrace the problem in order to diminish societal anxiety.

Barend Mons

Professor of BioSemantics and Founder,
FAIR Data Initiative, Leiden University

What Role for Machines in Helping Us to Effectively Detect False or Divisive Information?

A prerequisite for machines and algorithms to effectively analyse data and information is that, wherever possible, the representation of that information is in machine-readable format 'at the source' – in other words, in FAIR format (Findable, Accessible, Interoperable and Reusable for machines and people).[8] Although text and data mining techniques have improved significantly over the past few decades, text and images are not meant for machines but for people to consume. Consequently, the first hurdle for machines to help us is that we mainly communicate in the form of text, audio and images. Assuming that the computer will be able to 'detect' aberrant information, we first need to accept that mistakes will be introduced when recovering machine-readable and -actionable information from text, audio and images, and check for those errors first. Once simple mining errors are ruled out, and we have a 'suspicious assertion, or another piece of information, there are many ways in which the machine can assist us. Governments, large businesses and many other actors should be prepared to invest in making legacy data FAIR and stimulating FAIR formats wherever possible, especially for 'formal communication'.

How could this ever work?

In essence, machine readable 'knowledge graphs' are composed of 'atomic meaningful assertions' of the type subject-predicate-object (triples), connected in a logical graph structure. These graphs can be used by machines as a 'reference background' of commonly agreed knowledge and there are many ways in which 'tensions', phase transitions and 'inconsistencies' introduced to these knowledge graphs by new information can be automatically detected.

Obviously, a machine will, at first glance, only detect something that 'does not fit' well in consensus knowledge representation. This could be 'fake news' or on the other hand a new (correct) major insight that violates earlier conceptual models. But at least such 'anomalies' in the graph can be detected by machines and suggested for review by human experts.

Interestingly, the most 'dangerous' misleading information will likely be deliberately 'very close to the truth' and therefore the provenance of each piece of information is critical, invoking the trustworthiness of the source. A most important point is that future graphs should be made 'dynamic' to enable near real time alerts. Early versions of such 'Dynagraphs' are being explored. Information should be detected by 'visiting information sources on site' using an *Internet for machines approach* (www.go-fair.org*)*

[8] https://www.nature.com/articles/sdata201618

A DEMOCRATIC RESPONSIBILITY: WILL BUSINESSES HELP SECURE ELECTIONS?

Cristina Frutos López
Head of European Operations, Elections, Indra

A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats

The elections world is experiencing what I would call a real 'Tsunami' in which hybrid threats have managed to challenge the resilience of our democratic processes. From disinformation campaigns that have a direct impact on voters' engagement, to cyber-attacks targeting vote counting and election reporting systems – these are new grounds for the electoral bodies responsible for delivering accurate and secure elections.

In this context, technology may be perceived as a vulnerability and some countries have chosen to put it aside and revert election administration to the old 'pen and paper' times. Last year, France dropped electronic voting for citizens abroad over fears of cyber-attacks, and The Netherlands banned the count data transmission software as it presented vulnerabilities that could be exploited by hackers.

At Indra we believe that there are other ways to protect our electoral systems. Our customers are electoral organisations from all over the world requiring advanced technology solutions to support their elections processes – from voter registration to vote count and reporting of results. For a few years now, in addition to cyber-attacks (mainly DDoS[9] attacks and hacking attempts to critical infrastructure), we are observing more sophisticated threats such as disinformation campaigns designed to cause voter confusion or to damage the reputation of an institution itself – a highway to undermine the entire democratic process. These campaigns have a direct link to discouraging voters from finishing their journey to the ballot box.

Indra is now investing many resources in research and development on new work streams to provide solutions to our elections customers. Our experience tells us that this new threat environment cannot be addressed from the protection perspective only. It requires a strategic approach in which monitoring and analysis of open data sources, understanding of motivations and therefore anticipating potential attacks are key to provide guidance to electoral organisations in their prevention and reaction plans. And this approach needs to be tailored on a case-by-case basis.

The design of these strategic models require a pool of expertise, technology and insightful analysis. They must be nurtured by advanced tools and combined with expertise and understanding of the elections ecosystem and communication strategies. A multi-disciplinary skills approach is difficult for electoral organisations to pull together in-house. Our responsibility as industry actors is to fill in that gap and provide the strategic vision on elections interference to support electoral organisations in the anticipation and counter-measurement of potential attacks.

We are grateful for the opportunity given to us by the European Political Strategy Centre to share our experiences. Especially now when so much is at stake.

[9] Distributed Denial of Service

Guido Caldarelli

Professor in Theoretical Physics, Sapienza University of Rome

A European Observatory for Social Media Content

Fake news, alternative facts, post-truth era, circular reporting, echo chambers, have nowadays become very popular in journals and TV news. The number of headlines that pop-up each day on fake news and the challenges of today's media environment show how timely this issue is and how pressing it is to come with a systematic, empirical and theoretical approach to deal with the issue of how (mis)information spreads on social media.

Therefore, studying the mechanisms that shape social media and their impact on society will allow to respond to the key challenges posed by the increasingly broad and diverse community of stakeholders interested in this topic. These include researchers, policymakers, regulators, journalists, media companies (traditional and new), industry, civil society organisations and citizens.

Starting from an evaluation of the state of the art of current and ongoing literature and research on this topic (and keeping in mind that, today, no single solution satisfactorily addresses the issues implied by the rapid diffusion of content on social media), it is necessary to build a pilot European Observatory that can gather and analyse content from different social media. This would make it possible, to a certain extent, to identify, select and differentiate true from false content, to learn how this content is produced and distributed, and how citizen's react to it (which narratives are more trusted, why, by whom...).

The Observatory should also provide tools to visualise and analyse the dynamics of news spreading; experiment algorithms for defining an online reputation for news producers; use human behaviour and null models to test the possibility to forecast outcomes, and compare with evidence in data.

Micro-targeting should also be investigated in its current practices, with a view to, on the one hand, showing how personality and behaviours can be predicted on the basis of online data and, on the other hand, raising users' awareness about the existence of these practices.

The issue is particularly sensitive, since we do not want to create a 'Ministry of truth'. We should push for an ecosystem of different fact checkers that can help the debunking procedure. We should rapidly prepare a list of questions to target (i.e. one or more app to check if the twitter user is a bot or not) and ask practitioners and scientists to develop the instruments necessary.

Interesting further readings include: http://arxiv.org/abs/1603.01511; http://cnets.indiana.edu/blog/2016/12/21/hoaxy/; https://politoscope.org/2018/09/publication-inaugurale-politoscope.

PARTICIPANTS’ CORNER

Michael Chertoff

Former US Homeland Security Secretary;
Co-Chair, Transatlantic Commission on Election Integrity

Eileen Donahoe

Executive Director, Global Digital Policy Incubator, Stanford University; Member, Transatlantic Commission on Election Integrity

Deepfake Threat on the Horizon

As we look ahead to future elections, there will be a far more dangerous tool in the election interference toolkit: deepfakes, which are Artificial Intelligence-based human-image synthesis techniques, that combine and superimpose existing images and video onto source video.

Deepfake technology will enable malign actors anywhere to create video of virtually anyone, doing and saying whatever they want them to. Deepfakes are becoming less prohibitively costly to produce just as they become more convincing. This technology will soon be available not only to malign states, but to malign individual actors.

Imagine what could happen to public trust and civic discourse around elections as this technology spreads. Put bluntly, deepfakes could transform not just election interference, but politics and geopolitics as we know it.

So what can be done to prepare ourselves for the next wave of election interference via deepfakes?

First off, Artificial Intelligence-based detection of deepfakes must be turned against malign actors, so that deepfakes can be quickly identified and stopped before they spread. Artificial Intelligence can now be utilised to sniff-out imperfections in manipulated video invisible to the human eye, through watermarking algorithms and metadata built into authentic video. Development of this detection technology must be job number one.

Private sector platforms should embrace this detection challenge as a shared public interest priority. They should turn their R&D fire onto this urgent threat, before it shows up and spirals out of control on their own platforms. The key here will be to focus on detecting manipulation of source video (not evaluation of political content).

But perhaps most importantly, civic education about the threat of deepfakes must be seen as an essential element of democratic defence against this new generation of disinformation. Governments, civil society and private industry should team up in a massive public education campaign to inoculate the public – before deepfakes spread virally, dramatically impact public opinion, or change an election outcome.

In this vein, we believe strongly that deepfake technology itself, must be utilised to educate the public and showcase the power of this technology. This is why the Transatlantic Commission on Election Integrity is enlisting the help of technologists in building a Deepfakes Civic Education Platform. Our goal is to help citizens become discerning consumers of video and audio material, especially around elections.

The bottom line is that without greater public awareness of the danger, deepfake technology has the potential to cause electoral chaos and geopolitical instability. Democratic governments need to get ahead of this threat by engaging the public in the defence of democracy. Building citizen resilience to deepfake disinformation must become a shared public interest priority.

Richard Barrett

Member of the Venice Commission for Democracy through Law, Council of Europe

The Importance of Upholding Our Core Values in a Digital Age

The core values of fundamental rights and electoral or political rights, as enshrined in international law and national constitutions, have to be respected whatever the changes in the environment.

These are the freedoms of expression and opinion, freedom of association, and, in the area of political rights, the right to equity in the electoral contest and equal value in the ballot.

While it is an oft quoted tenet of constitutional rights in the US that 'freedom of expression is the lifeblood of democracy', when this is applied in the electoral sphere the expressions of individual citizens are more sacrosanct and immune from restriction that the expressions in political campaigning. All our legal systems now have campaign funding rules and limits and transparency obligations. In the individual sphere it may be that the expression deserves protection irrespective of content, but that does not apply to a campaign.

All campaign restrictions, even those promoting transparency, must be seen firstly as an interference which must be justified, in European systems, according to a test of necessity and proportionality.

Regulators and election bodies during campaigns are now struggling to apply the existing tests to social media content or foreign material. This is a huge challenge but the principles do not change. The principles are well expressed in the Venice Commission's Code of Good Practice on Electoral Matters from 2002. They include:

- Equality of opportunity for parties and candidates;
- A neutral attitude by state authorities with regard to the election campaign, to coverage by the media, and to public funding of parties and campaigns;
- Equality of opportunity can be proportional rather than strict, and applies in particular to 'radio and television air-time';
- 'In conformity with freedom of expression, legal provision should be made to ensure that there is a minimum access to privately owned audio-visual media, with regard to the election campaign and to advertising, for all participants in elections';
- Campaign funding must be transparent;
- Equality of opportunity can lead to a limitation on political party spending, especially on advertising.

In the new digital world, manipulation of social media during an election campaign can undermine that equality of opportunity.

This undermining of equality of opportunity is one of the threats to democracy in the digital age. On the other side of the coin is the danger that excessive state intervention can undermine the very rights we are trying to protect.

Benedetta Berti

*Head of the Policy Planning Unit,
Office of the Secretary-General, NATO*

How Does Election Interference Affect Security and Stability in Europe and the Transatlantic Community in General?

National elections are first and foremost a domestic matter. But the impact of external interventions and interferences in such local processes transcends the national dimension. Interference can a have a negative ripple effect, questioning the accuracy and validity of the electoral process far beyond the targeted nation. What is more, by targeting a core feature and symbol of the democratic system, these attacks attempt to discredit the value of democracy itself and, along with it, rule-based liberal order as a whole.

While both our countries and institutions, from the European Union to NATO, have proven able to withstand these challenges and are making significant strides in improving their resilience; we simply cannot be complacent to the risks these attacks may pose to our societies' constitutive values and principles.

Indeed, the impact of electoral interference goes beyond the political realm. If successful, these operations can undermine the validity of the democratic process and, just as importantly, they can fuel a public sense of distrust and disillusionment. In turn, sowing doubt in the democratic process can have a serious impact far beyond the political arena: it can fuel polarisation and societal fragmentation, as well as undermine resilience and even stability. In extreme circumstances, severely undermining internal cohesion and stability in a Member State could negatively impact unity and cohesion at the European level, with potential impact on matters of foreign and security policy.

Understanding the complexity and multi-faceted dimension of this threat is hence key to better prevent and respond to future attempts by non-state armed groups or states alike to interfere with domestic election.

Countering these attacks – with their domestic and international impact – requires strengthened international cooperation: democratic countries, in Europe and beyond, have much to gain by sharing information and exchanging best practices on prevention and countering of electoral interference, both in the physical and digital realm. Increased cooperation between NATO and the European Union can positively contribute to tackling these type of threats, first of all by increasing situational and strategic awareness and understanding. What is more, there other concrete ways through which NATO-EU working together can make a difference, including by bolstering concrete cooperation, planning and information sharing on relevant related areas, from countering hybrid threat, to cyber security, to strategic communication.

In addition, at the domestic level, effectively tackling interference in elections requires investing in both a whole-of-government and a whole-of-society response. Much progress has occurred in recent years in this direction: for example, by working with journalists, teachers, civil society activists and social entrepreneurs, among others, to help identify, debunk and counter disinformation and to boost societal resilience. More in general, strong, free and independent media and civil society can play an essential role in countering disinformation; just as promoting transparency and accountability in the political institutions can serve to boost trust and counter attempts to discredit the democratic system. Again, multilateral institutions like the EU can support these efforts by promoting, facilitating and encouraging sharing of information and best practices among Member States.

Yevhen Fedchenko

*Co-founder and Chief Editor, StopFake.org;
Director, Mohyla School of Journalism, National
University of Kyiv-Mohyla Academy, Ukraine*

Building Resilience: Ukraine's Experience with Russia's Information Warfare

Russian television has long been a channel used for influencing Ukrainian public opinion. Its propagandistic capacities were deployed well before the Crimean annexation and the beginning of the war in Eastern Ukraine.

Russia has extended its dominance over the Ukrainian media landscape to include Internet news media, social media and shared entertainment industry. All of these have been gradually weaponised – starting well before 2014.

Russian media – both state-owned and private – has been involved extensively in manufacturing and distributing textual fakes, manipulative titles, visual (photo and video) fakes, false claims, forged documents, hoax experts, fake news sources and witnesses.

With these tools, the Kremlin has created whole narratives discrediting different aspects of life in Ukraine, targeting different audiences: in Russia, Ukraine and globally.

Since its launch in 2014, StopFake.org – the fact-checking platform set up within the Mohyla School of Journalism to verify facts about events in Ukraine and debunk disinformation systematically appearing in Russian mainstream media – has already debunked more than 1,500 fake 'news' stories coming from Russian media.

Thanks to its work, it has been able to evidence that Russian propaganda is a systematic approach of the Russian government and to establish a clear connection between Russia's information warfare and the kinetic war in the East of Ukraine and annexation of Crimea.

Research conducted by StopFake in 2017 revealed that a majority of Ukrainian citizens (58,3% of the respondents) shared the opinion that there is a threat of Russian propaganda in Ukraine. Among the most widely-named sources of Russian propaganda, Ukrainians pointed to Russian TV channels, online media and social networks (45%, 34,5% and 19,8% respectively).

In light of this, Ukraine has started to build up its resilience to disinformation. Different NGOs (including StopFake) have been researching and explaining the scope and impact of disinformation efforts, and educating people about critical ways of media consumption. In response to growing dangers of information warfare, Ukrainian courts regulated the presence of hostile TV broadcasts in Ukraine and Russian social media companies were sanctioned.

The Ukrainian experience of tackling information warfare is one of a unique blend of grass-root initiatives and governmental efforts to protect citizens under conditions of war while at the same time protecting the democratic nature of media ecosystem.

Daniel Fried
*Distinguished Fellow, Future Europe Initiative,
Atlantic Council*

Democratic Defence against Disinformation – The Need for a United Transatlantic Response

The transatlantic community is finally organising itself to defend against a new form of an old challenge. Autocratic and aggressive Russia has adopted 21st century technologies to increase the reach of its propaganda. Officially-sponsored (directly or otherwise) use of bots, trolls, and other techniques to exploit social media platforms and enter the public dialogue and political space of the US and other countries has been going on for years, especially in Europe's East. But the reach of Russian disinformation in the US 2016 election campaign, and Russian use of such techniques in countries of Western Europe, alarmed Americans and others. Many who believed that Russian aggression had nothing to do with them discovered their error. Where Russia has begun, other governments of similar mind will follow.

In an Atlantic Council Report published last February, '*Democratic Defense Against Disinformation*,' Alina Polyakova and I – benefiting from substantial advice from Swedish and other European colleagues – urged that the transatlantic community unite in common purpose to deal with Russian and other sources of foreign disinformation. Our first principle was that transatlantic responses must be consistent with our democratic norms and principles, and that an effective response must include governments, social media companies, and civil society, working together.

The paper's two most ambitious recommendations included the establishment of a transatlantic 'Counter-Disinformation Coalition,' including governments, social media companies, and civil society, to share information about the evolving disinformation threat and develop best practices against it. An early task of this Coalition should be development of a voluntary code of conduct, including governments and social media companies. The paper also recommended greater on-line transparency, including through legislation and regulation; support for civil society groups that seek to expose disinformation campaigns; and support for long-term social resilience through education and training.

Since the report's publication, the EU, some European national governments, and social media companies have advanced their thinking and policies. The transatlantic community appears to be moving from a phase of 'admiring the problem' to seeking practical solutions. Indeed, US, EU and European governments, notwithstanding policy and other differences, have been moving in converging directions, pushing once-reluctant social media companies to greater responsibility for finding solutions and supporting civil society groups dedicated to exposing disinformation.

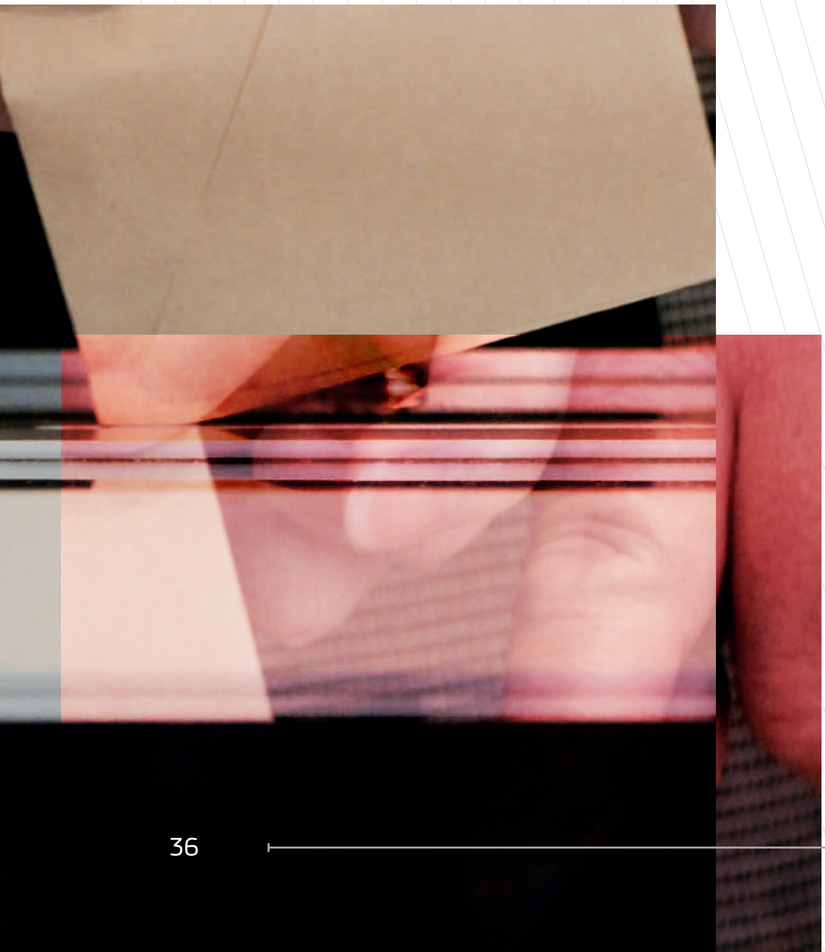
Recent actions include:

- A significant shift in declaratory policy by major social media companies, e.g. Facebook, Google, YouTube, and Mozilla. These companies have moved from denial to public commitments to combat disinformation and have announced policy steps to this end.
- In the United States:
  - The US Congress has pressed social media companies to become more active in combatting information manipulation through repeated hearings.
  - The US State Department's Global Engagement Center received its first funding of $20 million and is using it to fund organisations working to counter disinformation on the frontlines in Europe.
  - The State Department is informally coordinating with the EU and like-minded European governments about common best practices.

  - The Department of Homeland Security (DHS) is leading an interagency effort to counter malign influence, including disinformation, which includes the intelligence agencies, State, and the Department of Defense.
  - Treasury has moved ahead with sanctions related to Russian cyber and election-related interference.
- In Europe:
  - The European Commission has developed recommendations to combat disinformation[10] and EU Council Conclusions of June 28 call for an action plan by December 2018. This process has generated an EU Code of Practice on Disinformation to which major social media companies have signed on.
  - The European Commission's recommendations also include creating of an independent European network of fact-checkers, though funding remains an issue, and a 'multi-stakeholder forum on disinformation'.
  - In France, the National Assembly introduced legislation to counter information manipulation around elections. The law would require a judge to decide in 48 hours whether a piece of false online content constitutes information manipulation and allows the government to suspend (temporarily) and foreign news agency that deliberately disseminates false news.

The basis for a sustained transatlantic campaign to counter disinformation may be developing. Despite other transatlantic differences on some issues, this is an area of common assessment of a problem and common action. Next steps could include whether the EU Code of Practices could be linked to similar US guidelines and what the best institutional vehicle could be for long-term coordination of efforts, bringing together official, business, and civil society lines of effort. Finally, the US and Europe need to maintain sustained political support for counter-disinformation efforts. This effort will take time and an all-of-society approach.

[10] Communication from the Commission: Tackling online disinformation: A European Approach, 26 April. 2018, COM(2018) 236 final



Iskra Kirova
Senior Analyst, Open Society European Policy Institute

Election Interference in the Digital Age: Accountability of the Online Sphere

There are more ways to steal an election today and get away with it than there have ever been. The unregulated nature of the Internet – our new public sphere – has a lot to do with it. To protect the integrity of elections in the digital age, we need to ensure the integrity and accountability of our online sphere.

Over the last few years, we have seen the online sphere mutate from a space for free expression into a tool for disinformation and manipulation of unsuspecting users. It has made it possible for state and non-state actors to work globally to target voters on a massive scale with misleading or outright false information whose source and financing are easily obscured; and to do so through sophisticated psychological profiling techniques to get to people on a personal level – something no other medium can deliver.

Beyond the influence of malicious actors, the ad-driven business model of social media and other platforms such as Facebook or Google, and the need to maximise the time users spend online have privileged sensationalist low-quality information and reinforced 'echo-chambers'. The spread of conspiracy theories or aggravation of personal biases are therefore not merely a secondary effect of today's online discourse. They are built into the algorithms of online media, distorting informed debate, and more than that – polarising, even radicalising, political views with damaging effects on the quality of our democracies.

To address these problems we need a new social media ecosystem.

The online sphere is the locus of activism, political campaigning and social mobilisation today. It should remain an open space for opinion and expression. But policymakers should not be confounded by what is a false dilemma between censorship and freedom of expression. In fact, what regulation should ensure is transparency and a competitive marketplace of ideas.

Attempts to regulate content do not offer real solutions or could be outright dangerous. The initial experience of Germany's NetzDG legislation has shown how, by adapting their vocabulary, offenders can easily remain within the grey zone outside the scope of hate speech rules. 'Fake news' laws belong rather to the arsenal of authoritarian regimes such as in Egypt or Azerbaijan than democratic governments.

But this does not mean that regulation as such is a bad idea. It should focus for starters on significantly increasing transparency around how and why content is curated and delivered to us, and preventing bad actors from manipulating the system. Different platforms raise different problems. For example, Twitter is more vulnerable to activity by bots (automated accounts), crowding out the space and raising the profile of messages that in fact might be far less popular, while on Facebook, Google or YouTube (the latter is owned by Google) the main issue is the algorithm they use to surface content. Improving the health of the online sphere would require some first steps to address current algorithmic use in order to increase access to quality information and open up filter bubbles.

Secondly, more should be done to encourage industry cooperation with experts and civil society, particularly by sharing data so as to enable the expert community to investigate and respond to manipulation and disinformation more effectively, as well as play an active as a watchdog and in policy development.

Long-term, more difficult solutions, that policymakers, industry and civil society need to begin considering in earnest concern the current extraordinary concentration of power over information and the digital market within the hands of a handful of companies and the fundamental business model of the web that relies on tracking and monetising users' data.

If all parties play their part, we could begin to see a more accountable and democratic online public sphere.

Miriam Lexmann

Director, EU Office, International Republican Institute

Why Fact-Checking Will Not Bring Disinformation to an End

Gaps in democratic governance, combined with lasting societal vulnerabilities and social challenges and injustice render European societies particularly susceptible to subversion. Moreover, in an age of live news feeds and oversaturated media markets, citizens are bombarded with information that is often unverified, decontextualised, and touches upon people's emotions caused by various social fissures.

In this regard, the key to addressing the phenomena of disinformation (as well as other forms of subversion) lies in improving our understanding of and ability to address wider vulnerabilities, and to focus not only on the rational but primarily on the emotional.

This requires a holistic approach that shifts away from the perception of disinformation as merely requiring technical solutions, such as fact-checking, and towards a deeper political debate on both the Member-States and European-level, that takes into account the nature and adherence to our values and the desire of EU citizens to keep more decision-making powers in the EU capitals. This would require examining and addressing vulnerabilities in relation to i) the strength and flexibility of our institutions, ii) the social, and political processes and the changing nature of political discourse, and iii) the social conditions and disparities faced by our societies.

As an example of this: research conducted by the International Republican Institute has found that the average citizen of the Visegrad countries is increasingly distrustful, frustrated, confused, and focused on making ends meet personally or for their children. Concurrently, they hold a number of concerns, some genuine, others more apparent than real, including:

- Frustration with the direction of the European Union and the feeling that the EU is pushing people to abandon their traditional values;
- Despite limited knowledge of Russia (to a certain extent, including of human rights abuses), there is belief that Russia is a defender of traditional values (such as family, religion, state sovereignty) that the EU has rescinded on;
- Social-economic vulnerabilities (poverty, social inequality, or and corruption) and the gaps in democratic governance continue to dominate people's concerns and undermine their trust in democratic institutions and liberal democracy *per se*;
- The lack of impartiality among mainstream media pushes people towards fringe media outlets, often promoting pro-Russian narratives. They generally know that *RT* is a mouthpiece to serve someone's interests, but they feel the same way about most of the national or international mainstream media.

Our research continues to highlight that factual disinformation is only part of the problem and so fact-checking does not bring disinformation to end. Disinformative outlets are moving from factual disinformation to emotional disinformation which is harder to recognise and vindicated from law. It is also often echoed by mainstream media as the use of hyperbole increases traffic and generates shares and likes and thus earns money.

These phenomena underline the need for more robust and comprehensive research looking into correlations between social fissures and vulnerabilities to various disinformative narratives and the role that emotions play in this. As they often exploit existing (and all too often genuine) vulnerabilities and concerns, this will require:

- A deeper political debate about the state of European and national governance, including the limits to the competencies of EU institutions and strict adherence to the subsidiarity principle;
- Greater connection between European and national leadership and citizens;

- Rebuilding citizens' trust and paying greater attention to citizens' most pressing concerns, such as corruption, poverty and migration. But also to the increasing tensions between Western and Eastern and Northern and Southern parts of the EU;
- Respect for and safeguarding of ideological diversity in the media space by European leaders and institutions, to address the above-mentioned lack of impartiality of media;
- Funding opportunities for academia and civil society (from the European Commission) to conduct more thorough research and analysis aimed at understanding the various vulnerabilities and tailoring measures with a greater precision.

Michael Meyer-Resende

Executive Director, Democracy Reporting International

A Game of Catching Up

With the advent of the digital space and social media in particular, the public space has fundamentally changed. This transformation is ongoing, with new trends upsetting what seemed to be established patterns (for example, the shift of much communication into chat groups). Actors that spread disinformation are adapting fast to exploit the weaknesses of these new trends. According to the annual disinformation report by the Oxford Internet Institute, disinformation has become a half-a-billion dollar industry.

Among many examples for increasing sophistication and learning of disinformation campaigns, Democracy Reporting International observed how extremist accounts got involved in a Twitter debate on whether Germany's Social Democratic Party should join a grand coalition. Pretending to be supporters of that party, they pushed for a rejection of that coalition, which would have served extremist purposes (failed government negotiations, implying a sense of crisis). The problem was not being against a Grand Coalition. The disinformation aspect lied in pretending to be supporters of the Social-Democratic Party and having its interests in mind.

To catch up with the challenges of democratic discourse in the digital space, several gaps need to be closed:

- *Real-time information gap*: Too often there is a sense that something is wrong with social media in elections, but it takes too long to find out what. More real-time monitoring of discourse on social media and the wider digital world is needed in order to respond in good time. Media reported that Facebook opened a 'war room' to follow developments in real-time ahead of the US mid-term elections. ICT companies should do such real-life monitoring in elections anywhere. Monitoring should also be done by election observers, think tanks, civic tech groups or NGOs.
- The *responsibility gap*: The major ICT companies have woken up to the disinformation threat, but their responses are too little too late. At a minimum they should open an office in every country in which they provide a significant platform for public discourse. Remote operations that chiefly rely on Artificial Intelligence are insufficient to respond to complex social realities. Such low-cost, light approaches betray obligations of corporate social responsibility.
- The *public policy gap*: Media, like The Guardian, have been influential in uncovering online disinformation, but they do not undertake systematic research to recommend policy. Academia is also carrying out research, but results come too late and usually do not include policy recommendations. Think tanks and NGOs tend to be critical of governments' attempts of regulation, but they rarely propose concrete policies that could work better.

Susan Ness

Distinguished Fellow, Annenberg Public Policy Center,
University of Pennsylvania

Wake Up Call

The 2016 presidential election was a wake-up call in the United States. In hindsight, it was the demarcation line between a euphoric but naïve time when online services and platforms were applauded for promoting freedom of expression and democracy around the globe – for offering 24/7 access to information on every imaginable subject, and for presenting a cornucopia of free apps to enhance our daily lives – and a dark time when platforms were vilified for breaching consumer trust, for profiting from disseminating disinformation, and for blithely enabling foreign demagogues to wreak havoc on our political institutions.

Neither the pre-election idyllic vision of Internet technology nor the reviled post-election vision reflects reality. Technology is neutral.

We're awake now.

During the past two years, noteworthy progress has been made toward detecting and countering the systems that enabled foreign powers to conduct cyber warfare by micro-targeting unsuspecting social media users receptive to their deceptive messages. Machine learning has accelerated the ability to identify and remove offending posts, bot accounts, and foreign propaganda. Statistics are published now, summarising the number of accounts, postings, and pages that have been blocked, taken down, or cancelled. Journalism programmes are being retooled to help weed out viral deception. Transparency is emerging in the sponsorship and funding of online political ads. And more citizens – although hardly enough – are becoming aware of their digital surroundings.

Europe has forged ahead, significantly contributing to the body of knowledge on how society builds cyber resiliency. Better tools are needed on both sides of the Atlantic to prepare for the upcoming elections.

Unfettered elections underpin democracy. But democracy is fragile, as so many countries have demonstrated. And there is no democracy without freedom of expression.

A free and open Internet affords access to information about corruption and government atrocities that tyrants do not want their citizens to see. Such regimes may pass laws that label such posts as terrorist or 'fake news' and demand deletion. They justify their actions by citing western government rules.

In our rush to inoculate our citizenry from the impact of cyber-scoundrels, let's make sure that free expression is not sacrificed for expediency. Government pressure may unintentionally incent platforms to block user-posted content instead of evaluating nuance and context – effectively deputising platforms to be government censors.

Multi-stakeholder initiatives – including those created by the Commission – potentially offer greater flexibility to address cyber content issues while protecting free expression. A transatlantic approach may further that outcome.

Denis Teyssou
Head, Agence France-Presse Media Lab R&D

The Force of Falsity

In a lecture given at the University of Bologna in the mid-nineties, entitled 'The force of falsity' and included later in his book 'Serendipities', Italian semiologist Umberto Eco argued that false tales, 'as narratives, seemed plausible, more than everyday or historical reality, which is far more complex and less credible. The (false) stories seemed to explain something that was otherwise hard to understand'.

And he added: 'False tales are, first of all, tales, and tales, like myths, are always persuasive'.

During the CrossCheck operation on the 2017 French presidential election, one of the debunked stories was a viral video of a man presented on social networks as a migrant assaulting nurses in a French hospital.
The video was disgusting, producing emotional repulsion. 'Here is what the media is hiding from you' could be read in the first caption. Later copies tried to launch a campaign against universal medical care.

But that so-called migrant was in fact a Russian citizen in a Novgorod (Russia) hospital, drunk according to the local press and caught one month before by a monitoring camera. The story was reported by several Russian media outlets.

An image similarity search on keyframes was enough to understand that this barbarian act was used out of context to spread an insidious xenophobic campaign, with millions of views on Facebook.

Copies of the same video were used again and again in the following weeks at least in Italy, Spain, Belgium, Turkey, then France again, always as a migrant locally attacking hospital staff members, triggering again several millions views and more debunks.

Although the above example is only reaching the first of the five stages of election meddling proposed by Finnish researcher Mika Aaltola ('using disinformation to amplify suspicions and divisions'), it shows the level of insidious manipulation that circulates with impunity on social networks, fostering racism and extremism.

As French researcher François-Bernard Huyghes rightly pointed out: 'the goal is to make (the voter) political choice appear to be spontaneous: I believe A, therefore I receive a message telling me that candidate Y thinks so as well. According to this model, we have gone from a strategy of mass political persuasion dumped by the media, to targeted soliciting tailored to our deepest wishes.'

In our societies already shaken by economic crisis and mass unemployment, we should not underestimate the force of falsity.

European **Political Strategy** Centre

The European Political Strategy Centre (EPSC) is the European Commission's in-house think tank. It reports directly to President Juncker and operates under his authority.

The mandate of the EPSC includes: **strategic analysis and policy advice**, both short- and long-term, to the President and the College on issues related to the policy priorities of the Juncker Commission (as defined by the President in his political guidelines presented to the European Parliament on July 15 2014); and **outreach** to decision-makers, think tanks and civil society at large.