ISPI DOSSIER 23 May 2019

ELECTIONS AND CYBERSPACE: THE CHALLENGE OF OUR DEMOCRACIES

edited by **Samuele Dominioni**

ISPI

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

DOSSIER
23 May 2019

The upcoming European Parliament elections are just another vote that could be possibly targeted by malicious activities coming from cyberspace, which could have a direct impact on the integrity of the elections themselves. The US presidential vote in 2016 highlighted the possibility of interference by cyber means, due to the widespread use of digital technology to support election campaigns and the electoral process. We are just at the beginning of a radical transformation of the polity and of the way citizens participate in elections. Fake news and digital disinformation, data theft from voter registers and penetration into candidates' digital accounts, hate speech and social platform censorship, echo chambers and social engineering: all of these are new challenges to the electoral processes that have been gaining more and more political relevance and media attention worldwide. Therefore, in order to guarantee the cyber-integrity of elections there are multiple actors and activities to be secured. What are the main threats and how can we deal with them? What is the state of the art for the upcoming European Parliamentary elections? How can (dis)information affect representative democracies?

The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Italian Institute for International Political Studies (ISPI)

Table of Contents

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
23.05.2019

WHY CYBER MATTERS IN ELECTIONS

Samuele Dominioni
ISPI

In the book *Why Elections Fail*[1] Pippa Norris argued that there were multiple factors that could explain the flaws and failures undermining elections. Based on an exclusive dataset, the Perception of Electoral Integrity (PEI), Norris conducted an assessment of different variables that can affect electoral integrity, these are: structural conditions (such as economic factors – richer economies usually have better-quality elections), institutions (such as a proper constitutional division, independence among state institutions and the professionalism of public servants), and international forces (such as globalization and freedom of information flows that have positive impacts on the quality of elections). This book was published in 2015, one year before the 2016 U.S. presidential election, which became a watershed moment for how to consider electoral integrity because, from that moment on, it also began to be dependent on the cybersecurity variable.

As a matter of fact, in the aftermath of the 2016 presidential election several countries and international organizations started to set new norms for conducting elections in cyberspace. For example, the United States National Cyber Strategy[2] includes electoral institutions among the critical infrastructures that must be protected by utilizing different tools to deter possible attacks. The Council of Europe added new principles and recognized that Electoral Management Bodies (EMB) are the actors that must be held responsible for e-voting standards and for the "availability, reliability, usability and security of the e-voting system." The European Union General Protection Data Regulation (GDPR) that went into effect in May 2018 has become particularly important in data management concerning electoral processes and campaigns. However, so far most of the regional and international efforts to regulate elections in cyberspace have taken the form of best practices or guidelines because the field of cybersecurity in elections is still emerging, both in national legislation and in international jurisprudence and standards.[3]

Therefore, it is important to understand how cyber-related risk may affect electoral integrity. As I already argued in a previous analysis[4], there are fundamentally two main dimensions in which cyber threats can impact the integrity of electoral processes: the technical and the information-

al. The first refers to the technical aspects of an election, such as the cybersecurity of the networks, data storage (e.g. electoral registers and other personal records), vote transmission (in the case they are electronically tabulated) and the electronic voting system (a concept that "encompasses a broad range of voting systems that apply electronic elements in one or more steps of the electoral cycle"[5]). Government and electoral management bodies should regularly test the cybersecurity of each passage in order to discover vulnerabilities and patch them (ideally) before the outset of the electoral process. For example,[6] in the Netherlands, despite the fact the voting and ballot-counting process is manual, at the municipality level votes from polling stations are tallied through a software called Ondersteunende Software Verkiezingen (OSV). This software is crucial because it delivers a document with the final calculation of the vote in a municipality. In the run-up to the 2017 elections, the Electoral Council of the Netherlands asked to perform penetration testing in order to discover possible vulnerabilities. As a matter of fact, the test identified a few, which were subsequently patched in time. The European Union NIS Cooperation Group published a Compendium[7] on cybersecurity of election technology to enhance support and information sharing in the run-up to the 2019 parliamentary elections.

The second is the informational dimension, which refers to the new media environment and its impact on electoral campaigning and the information domain. On the one hand, the advent of "technology-intensive campaigning"[8] based on big data is re-shaping the means of political advertising and participation; on the other, despite the fact that information propaganda has long been a tool in the arsenal of political stakeholders, what is creating deep concern[9] is the level of directness, the scale of activity and the scope of these operations' efforts to influence public opinion. Since the case of Cambridge Analytica there have been multiple efforts, both at an international and a local level, to tackle this problem. On the one hand social platforms have become more responsible for the use of their users' data and the spread of fake news or disinformation campaigns. On the other, international organizations are developing guidelines and frameworks to counter these issues (especially during elections), such as the upcoming European parliamentary elections, as explained by Fabio Rugge in his article.[10]

Malicious cyber campaigns or actions, either in the technical or informational dimension, may generate detrimental effects for electoral integrity and, in turn, for the legitimacy of the political institution, for the quality of democracy and for international credibility. Elections, when free and fair, are regular and legitimate occasions to vie for power in a democratic country. Trust, between citizens and political institutions, is at the basis of this process. In the case of malicious actions, both in the real world or in cyberspace, there is the risk of breaking such trust and thus for the political actor to lose legitimacy. As such, the alleged Russian influence in the 2016 presidential elections led some observers[11] to claim that Donald Trump is not a legitimate president. The rise of this kind of resentment, along with the spread of fake news or disinformation campaigns, as explained by Fabiana Zollo[12] and Anna Pellegatta[13] in their articles, can lead to extreme polarization, which may impact the quality of a democracy.[14] Finally, it could be possible that the government that suffered from malicious cyber campaigns or attacks may suffer from loss of international credibility[15] *vis-à-vis* other international partners.

In order to avoid these flaws in the electoral process there are several attempts both at the technical and the political level to find solutions and to guarantee electoral integrity in cyberspace. One of the overhyped responses concerns the adoption of blockchain technology for voting procedures. Yet, as explained by Peter Ryan[16], there are still too many shortcomings that prevent it from being used in general elections. From a political perspective, beyond internal codes of conduct and recommendations (such as those published[17] by the European Union Agency for Network and Information Security - ENISA) to tackle disinformation, there have also been a few but positive examples of electoral assistance programmes regarding tackling fake news and disinformation. As explained by Paul Anderson in his article,[18] this is a particularly important and serious phenomenon in developing countries.

The need to protect the integrity of elections from threats coming from cyberspace is even greater if we look at how

new and challenging ways of political participation are emerging within our democracies. As argued by Michele Sorice,[19] we are witnessing a crisis of institutional representation caused by a growing lack of trust in this system. The solution could be through adopting participatory and deliberative practices in e-democracy tools. Therefore, it is absolutely necessary to assure electoral integrity in cyberspace, even if this would take a long time to be fully developed in terms of principles, policies and guidelines. Nevertheless, as this dossier claims, cyberspace has forcefully entered the electoral arena, becoming one of the most important variables to manage in order to ensure electoral integrity.

1. P. Norris, *Why Elections Fail, New York*, Cambridge University Press, 2015
2. *National Cyber Strategy of the United States of America*, Washington DC, The White House, September 2018.
3. https://aceproject.org/ace-en/focus/heat/literature-review
4. S. Dominioni, *Protecting Electoral Integrity in Cyberspace: The US Midterm Elections in 2018*, ISPI Commentary, 1 November 2018
5. https://aceproject.org/ace-en/focus/e-voting/default
6. *Compendium on Cyber Security of Election Technology*, CG Publication 03/2018, NIS Cooperation Group, July 2018.
7. Ibid.
8. D.G. Lilleker, "Prototype politics: technology-intensive campaigning and the data of democracy", *Journal of Information technology and Politics*, vol. 15, no. 4, 2018.
9. F. Rugge, *'Mind Hacking': Information Warfare in the Cyber Age*, ISPI Commentary, 11 January 2018.
10. F. Rugge, *The EU and Disinformation: A Battle To Be Won Together*, ISPI Commentary, 22 May 2019.
11. T. Schleifer, "John Lewis: Trump is not a 'legitimate' president, CNN Politics, 14 January 2017.
12. F. Zollo, *Polarization in the Online Public Debate*, ISPI Commentary, 22 May 2019.
13. A. Pellegatta, *Divide et Impera: The Art of Disinformation*, ISPI Commentary, 22 May 2019.
14. D. Schraad-Tischler, "The quality of democracy is declining in many industrialized states", Bertelsmann Stiftung, 9 October 2018.
15. S. Herpig and J. Schuetze, *Securing Democracy in Cyberspace*, Stiftung Neue Verantwortung, October 2018.
16. P.Y.A. Ryan, "Are Blockchain Voting Technologies Safe?", ISPI Commentary, 22 May 2019.
17. "Election Cybersecurity: Challenges and Opportunities", The EU Cybersecurity Agency, February 2019.
18. P. Anderson, "Tackling Fake News: The Case of Nigeria", ISPI Commentary, 22 May 2019.
19. M. Sorice, "Between Direct Representation and Participatory Democracy", ISPI Commentary, 22 May 2019.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
23.05.2019

THE EU AND DISINFORMATION: A BATTLE TO BE WON TOGETHER

Fabio Rugge
ISPI

During the March meeting of the European Council there was talk once again of disinformation, the threat it poses (especially when conveyed through social media) and the risk that it could be used to influence the democratic process, both nationally and in the imminent elections for the European Parliament. In other words, just a few weeks after the European Parliament had passed the Cybersecurity Act[1] (a significant step towards greater cybernetic security for Europe's citizens and businesses), threats from the cybersphere returned to the European institutional agenda, telling of a need – unmet, in this case, by any significant decisions – to stay highly alert to what is evidently perceived as a real and present danger. And no wonder: for constant vigilance is, we know, the primary duty of any open democracy.

How serious, then, are these risks? The cybersphere has taken a traditional danger – psychological warfare – and raised it to a new level by making it far more pervasive, firstly because – as anyone who has ever visited a chat room can testify – online behaviour can so easily be anonymous, unfiltered, and unhampered by social conventions in a way which would be unthinkable "in real life". Secondly, the Internet's impact is non-linear: by its nature ("the medium is the message") it fosters distorted news and information; its tendency is to serve up whatever suits and accordingly strengthens pre-existing views of the world (and strengthens preconceptions even more).

This polarizes public opinion and feeds divergent "truths" in public debate, undermining the basis of any opportunity for genuine, informed discussion. For democracy, whose life-blood is the public expression of opinion by citizens who want to participate in political life in a spirit of honest argument, this is a threat to its very existence. Forces outside the Union can exploit these intrinsic vulnerabilities for hostile purposes: to influence public opinion on a particular matter of national interest, for instance, or to delegitimize unfavoured candidates for office, or to stir up popular revolt by orchestrating messages which push people's most sensitive emotional buttons at the moment. This can all be done using totally bogus "news": the technology already exists, for instance, for the near-perfect digital re-shaping of a public person to make it spout whatever messages go down best.

Thirdly, the cybersphere adds another degree of risk by making it possible to profile users according to their opinions (harvested and checked, and/or presumable), so as to maximize the effectiveness of disinformation campaigns. Online propaganda can moreover be automated by using "bots" (special algorithms which get "smarter" and more autonomous every day), or by tweaking or stealing sensitive data from computers compromised by the latest cyberweapons (which may have been bought anonymously on the *Dark Web*), with the aim of subsequently exposing such sensitive data online, more or less selected and/or toned down, at the strategic moment.

In last December's Joint Communication to the Parliament, the Commission and Council of the European Union adopted a "Plan of Action against Disinformation". The Plan identified four main lines of action: improving the capabilities of EU institutions and member states to detect, analyse and expose disinformation; strengthening their coordinated responses to disinformation; putting responsibilities on the operators of digital platforms; and involving individuals, think tanks and universities in the work of preparing a "*common picture*" of any co-ordinated disinformation activities detected on the digital services used by European citizens.

The Plan has already been put into practice: a Rapid Alert System went live on 18 March. In brief, this is a digital platform that will facilitate interaction among all the main stakeholders, both European and national, to exchange information in real time about current disinformation campaigns and coordinate the response to them. In the face of an asymmetric threat like *cyber-enabled information warfare*, teamwork is the most important advantage available to the defence: so the measures taken by the EU are valuable and all the more urgent because the various member states still have no clear strategy or national code of operating procedures to tackle this threat.

Because of these and other strategic considerations, Italy, for its part, has not been slow to actively support these developments and to reiterate whenever possible the need for complementarity between what the European Union is doing and what is being done in NATO. The latter has in fact for some while been paying special attention to hostile disinformation campaigns precisely because they can severely affect decision-making processes and allied solidarity, not least as one definitional component of what is known as "*hybrid warfare*". This has led to a demand for the two organizations to work productively together across the entire range of the potential threat, avoiding harmful duplications and also ensuring consistency in all those areas which may not directly concern disinformation, but which certainly can aggravate it: one thinks of the EU's adoption of the NIS Directive and the GDPR, or the strengthening of intelligence-sharing and the activation of specific military *indicators & warnings*.

Lastly, in the months leading up to the European elections, the Plan of Action requires operators of online platforms to report on what they are doing to stop disinformation campaigns using their systems. Those operators' involvement and their proper discharge of all their responsibilities are essential for practical results, and clearly the EU is in a better position than individual member states to talk to *over the top* operators. In this sense, the prevention of disinformation campaigns is yet another illustration of how the international security situation requires strong actors capable of speaking with a united voice. "Everyone for himself" is in fact an impossible defence when the threat comes over networks which are interlinked by their very nature.

As always, our effective membership of the EU does not replace the "homework" we need to do ourselves; a national effort is needed, especially in terms of education and the raising of awareness,[2] starting with our schools but extending to all occupations and to civil society in general. With correct information and its characteristic critical spirit, Italian public opinion will certainly be capable of responding to needs articulated in Brussels, but it will be our hard put-upon democracies that feel the benefit of the exercise.

1. S. Dominioni, "The EU Cybersecurity Act: When the Going Gets Tough, the Tough Get Going", ISPI Commentary, 18 April 2018.
2. F. Rugge and S. Dominioni, "Cybersecurity in Italia: il nodo della formazione", ISPI Commentary, 7 February 2019.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
23.05.2019

DIVIDE ET IMPERA: THE ART OF DISINFORMATION

Anna Pellegatta
Atlantic Council

With only few days left ahead of the European Union parliamentary elections, the fear of foreign actors trying to influence the democratic voting process has spread rapidly across the continent. On a daily basis, news headlines point fingers at those "bad actors" allegedly responsible for the downfall of the West and at the role that social media plays in the process.

Over the past two years, terms like "disinformation," "misinformation," and "fake news" have become a growing part of the Western lexicon – "fake news" was named "Word of the Year" by Collins Dictionary in 2017; the act of spreading false information unintentionally, referred to as "misinformation" received the same honor from Dictionary.com in 2018. At the same time, Western observers have become increasingly fixated on the use of information as a tool of conflict, especially by Russia. What began as curiosity regarding the hybrid tactics of the Russo-Georgian conflict in 2008 grew from concern in the aftermath of the Russia's 2014 invasion and occupation of Crimea to an obsession following Russia's interference in the 2016 US elections. Now, as Europe faces the worrisome rise of populist and nationalist parties across several of its member countries, these hybrid tactics have begun to feel more like existential threats. In turn, what used to be sober-minded geopolitical analysis is now increasingly tinged with panic.

Every day, news outlets across western countries publish articles aimed at exposing the latest cases of fake news, alerting the public opinion about the risk of being targeted by foreign influence, and blaming social media platforms for facilitating the spread of disinformation. The debate around these issues has been heightened to the point that it now disrupts public discourse, both locally and globally. But isn't this what such "bad actors" look to achieve in the first place?

The so-called "Gerasimov Doctrine," named after the current chief of the General Staff of the Russian Federation, explicitly refers to weaponization of the information sphere as a tactic of modern warfare. To be clear, however, Russia did not invent the practice of manipulating information and targeting specific audiences, and disinformation is not a phenomenon that started in the era of social media.

Political actors have for centuries been undertaking propaganda, biased information used to influence an audience in order to advance their agenda and interests. Disinformation is thus considered a subset of propaganda, which refers specifically to the intention of spreading explicitly false information.

Although disruptive state actors, political parties, or individuals are the ones responsible for purposefully disseminating disinformation, a growing discontent towards social media started to permeate the public debate around Europe, the United States, and the rest of the western world. In particular, in the past few years, media investigations have held social network giants accountable for enabling, instead of preventing and controlling, a number of malicious activities on their platforms. Social media companies were accused, among other things, of allowing "bad actors" to use their platforms to spread disinformation, collecting users' data to create targeted political and commercial campaigns, amplifying hostile narratives, and exploiting so-called "echo chambers" to increase polarization of the public opinion on sensitive political issues. As all these malicious activities combined had a significant impact on the political discourse, and in some alleged cases on electoral results, across all continents – from the United States to the Brexit referendum, from Latin America to South Asia and Europe – the public debate started to identify social media companies themselves as a hazard to democracy.

Denying the role that social media has had in shaping society and the public discourse for the past decade is simply short-sighted, but what do we gain from demonizing it? By design, social media platforms allow communication and information to run in real-time around the globe, making the world's population more interconnected and borderless than ever before, while simultaneously exposing billions of people to the threat of targeted inaccurate or intentionally manipulated information. While more comprehensive regulations of social networks to promote best practices and increase user protection are an absolute necessity, governments, tech giants, media, and civil society have been pointing fingers at each other for too long without developing an adequate response strategy.

When implementing what is known as "chaos doctrine," Russia – but not only – aims to expand its influence sphere in Europe and over the West by undermining democratic institutions on a political, social, and economic level. The strategy is simple: eradicate trust from citizens towards institutions and intensify tensions within a system that has grown unstable. The goal is then achieved, for example, by polarizing public opinion, infiltrating hostile narratives into political debate that deepen discontent and suspicion, and promoting forces from within the system that disrupt unity and cohesion. In other words, the oldest war strategy: "Divide et impera." Thus, by bouncing responsibilities onto one another instead of cohesively working together to protect the interest of their citizens when targeted by malicious influence operations, decisionmakers across all different sectors involuntarily achieve the ultimate goal of those who undermine democratic institutions by nurturing chaos. With time, the same tactics have been learned and applied by domestic political parties and actors, which – either independently or channeling foreign interests – have become the main responsible for the disruption of national political discourses and systems across states.

So far, the measures implemented by governments and civil society organizations to counter the impact of information operations promoted by malicious actors have been only partially adequate and still too limited, especially given the caliber and the continuously changing nature of the threat. In fact, while social media platforms have centralized all sources of information – once diversified across television, press, radio, etc. –, the development of new technologies has concurrently made the production and viral spread of disinformation way easier and faster than it is to counter it. The fast-changing nature of such malicious tactics made, for example, a mere activity of fact-checking simply ineffective, while restrictive measures taken by social media companies on the content shared on their platform upon quality analysis still incur in the risk of being mistaken for censorship.

In order to limit the disruptive impact of manipulated information targeting different audiences, therefore, governments, tech companies, media, and civil society need to collaborate to foster digital resilience across popula-

tions around the globe to make them less vulnerable to disinformation, influence operations, and manipulation. Promoting digital resilience means providing citizens with the adequate tools to navigate the digital space that allow them to move from being passive consumers of massive volumes of information online to activating quality filters during such consumption, applying critical thinking, selecting truthful sources and information, and, consequently, making informed decisions in their day-to-day life. While keeping working to build policies that regulate and protect the information environment by malicious actors, both domestic and foreign, governments, tech companies, and civil society need to promote coordinated digital information literacy programs to educate global citizens on how to defend themselves from hostile influence operations. Fostering digital resilience, therefore, is the only sustainable approach to fight bad actors and it means building a world population resistant to the infiltration of disinformation, misinformation, and other similar disruptive forces.

Although information operations aimed at creating division within western democracies gained significant traction at first by infiltrating a system that was unprepared to respond, citizens around the world are becoming increasingly skeptical and are starting to react. Building digital resilience might take some time, and it might be a more complex process than debunking false information case by case, but, if built across borders with joint efforts by governments, civil society, and tech companies, it will undoubtedly represent a more sustainable and a stronger measure to eventually make disinformation and influence operations ineffective.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
23.05.2019

POLARIZATION IN THE ONLINE PUBLIC DEBATE

Fabiana Zollo
Ca' Foscari University of Venice

Over the years the internet has been celebrated for sharing information, disseminating knowledge, promoting freedom and debate, thus contributing to the enthusiastic rethoric of the so-called collective intelligence, a new form of intelligence that emerges from the collaboration and collective efforts of single individuals.[1] Indeed, a hyperconnected environment such as the internet greatly facilitates communications among people, bringing down both temporal and spatial barriers. The small-world theory tested by Milgram in the 1960s (Milgram 1967) – resulting in the famous *six degrees of separation*[2] – was recently verified by researchers at Facebook, who found out the same number to be reduced to 3.57, meaning that each person is now connected to every other person by an average of three and a half other people.[3] This is an example of how the advent of new technologies, and social networks in particular, has revolutionized the way we communicate and share information, at the same time allowing everyone to produce contents and share their opinion. As of the fourth quarter of 2018, Facebook had 2.32 billion monthly active users, generating 2.46M posts and 1.8M likes every minute.[4] Social media have rapidly established as the main information source for many of their users, who prefer to access news through social media, search engines, or news aggregators, rather than going directly to a news website. Over the years, traditional media such as print, radio, and television have been joined by a heterogenous mass of alternative news sources, where information is no longer mediated. However, despite the increasing quantity of contents, quality may be poor, due to issues of content monetization and the persisting reduction of investments in the news production and distribution.[5] Moreover, smartphone reach for news is significant, and might affect the way we consume information and the time that we devote to its processing. Such a context has contributed to the loss of reputation and trust for traditional media, encouraging people to rely on alternative information sources, not always qualified.

It is since 2013 that the World Economic Forum (WEF) has been placing the global risk of massive digital misinformation at the core of technological and geopolitical risks such as the rising religious fanaticism, cyber-attacks and terrorism.[6] On the Internet, a huge amount of information

competes for our attention, which is instead limited, and it is often difficult to apply our abilities to analyze, reflect and draw conclusions. Instead, our cognitive biases – i.e. shortcuts, heuristics that we use to simplify the reality and (re)act rapidly – emerge forcefully. As human beings, we need such biases to interpret the reality. Unfortunately, while these cognitive mechanisms are often fundamental to our survival, they might also act as mental traps and mislead us. Among them, a fundamental role in information consumption and diffusion is played by confirmation bias, which is the human tendency to look for information that is already coherent to one's system of beliefs. Indeed, despite the availability of a huge, virtually infinite variety of information, online users tend to fragment into bubbles – the so-called echo chambers.[7] Users in a same community share a common narrative and, immersed in echo chambers, select information coherent to their worldview, even when false,[8] ignoring information dissenting from their beliefs. Users from different and contrasting communities rarely interact and, when that happens, the debate degenerates, especially for longer discussions.[9] Response to debunking attempts is not that dissimilar, and results in the well-known backfire effect. [10] Correction is perceived as a further attempt to manipulate information, thus reinforcing users' original positions.[11] Such aspects are especially important in a media pluralism perspective. Indeed, it is widely assumed that citizens and democracy benefit from a greater quantity of information available in the information system.[12] However, due to users confinement into echo chambers, information pluralism on social media does not appear to produce the positive effects generally connected with citizens' exposure to different points of view.[13]

It is possible to quantify the turnover of Facebook news sources by measuring the heterogeneity of users' activity. We may observe that, for increasing levels of activity (number of likes) and *lifetime* (the temporal distance between the first and last interaction of a user on the platform), users interact with increasingly fewer new sources.[14] While users with very low lifetime and activity levels interact with about 100 pages in a year, 30 in a month, and ten in a week, the same values are far lower for more active and long-lived users, who interact with about ten pages in a year, and less than four monthly and weekly. News consumption on Facebook is therefore dominated by selective exposure, showing a natural tendency of users to confine their activity on a limited set of pages, focusing their attention on certain topics (and claims), thus contributing to the formation of a high-polarized community structure. Such dynamics appear to be independent of the topic, and also applies to online political debates.[15] In this regard, looking at users' behavior on Facebook pages engaged in the debate around Brexit,[16] we observe the spontaneous emergence of two well-separate communities (echo chambers), where connections among pages are a natural result of users' interaction on them. Users are divided into two main distinct groups, confine their attention on a specific narrative and seem to ignore the other. Similar patterns may be found around the Italian Constitutional Referendum's debate, where the emergence of five main communities of news pages in Facebook, and four in Twitter[17] is observed. Also in this case, users are strongly polarized and tend to confine their attention on a specific cluster (community) of pages.

Empirical evidences suggest that the increasing segregation of users in echo chambers plays a pivotal role in (mis)information spreading on social media. To contrast misinformation, and encourage effective communication, smoothing polarization is thus essential. To this end, users' behavior and their interactions with information may be used to determine in advance the targets for hoaxes and fake news in the short term[18]. A timely identification of potential misinformation targets may allow for the design of tailored counter-narratives and appropriate communication strategies. In this direction, within the EU H2020 project QUEST[19], we are now working to analyze, design, test, and evaluate different strategies to improve science communication on social media, with special attention to delicate and polarizing topics that need to be addressed with care, such as climate change or vaccines[20]. It is finally crucial to promote a culture of openness and to emphasize the importance of critical think, together with a better awareness of both digital tools and humans limits (and biases).

P. Levy and R. Bononno, *Collective Intelligence: Mankind's Emerging World in Cyberspace*, Helix Books, Paperback, 10 December 1999.
2. According to the theory, six is the number of intermediaries necessary to connect any two individuals in the world.
3. S. Bhagat, M. Burke, C. Diuk, I.Onur Filiz, and S. Edunov, *Three and a half degrees of separation*, Facebook Research, 4 February 2016.
4. Statista 2019.
5. AGCOM, 2018. News vs. Fake in the Information System. Interim Report Sector Inquiry "Online platforms and the news system".
6. L. Howell, "Digital Wildfires in a Hyperconnected World", World Economic Forum, 2013.
7. M. Moore and *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple*, Oxford University Press, 2018.
8. A. Bessi et al., *Science vs Conspiracy: Collective Narratives in the Age of Misinformation*, 2015.
9. https://login.medscape.com/login/sso/getlogin?urlCache=aHR0cHM6Ly9yZWZlcmVuY2UubWVkc2NhcGUuY29tL21lZGxpbmUvYWJzdHJhY3QvMjY0MjI0NzM=&ac=401
10. B. Nyhan, "When Corrections Fail: The Persistence of Political Misperceptions", *Political Behavior*, vol. 32, no. 2, June 2010, pp. 303-330.
11. F. Zollo et al., "Debunking in a world of tribes", *Plos One*, 24 July 2017.
12. A. Pratt and D. Stromberg, *The Political Economy of Mass Media*, 26 November 2013.
13. AGCOM (2018).
14. https://login.medscape.com/login/sso/getlogin?urlCache=aHR0cHM6Ly9yZWZlcmVuY2UubWVkc2NhcGUuY29tL21lZGxpbmUvYWJzdHJhY3QvMjgyNjUwODI=&ac=401
15. L. Adamic and N. Glance, *The Political Blogosphere and the 2004 U.S. Election: Divided They Blog*, 4 March 2015.
16. "Mapping social dynamics on Facebook: The Brexit debate", *Social Networks*, ol. 50, July 2017, pp. 6-16.
17. A.L. Schmidt et al., "Anatomy of news consumption on Facebook", *PNAS*, 21 March 2017.
18. M. Del Vicario et al., *Polarization and Fake News: Early Warning of Potential Misinformation Targets*, ACM Transactions on the Web, vol. 13, no. 2, March 2019.

19. EU H2020 Project QUEST: https://questproject.eu.
20. A.L. Schmidt, "Polarization of the vaccination debate on Facebook", *Vaccine*, vol. 36, no. 25, 14 June 2018, pp. 3606-3612.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
23.05.2019

TACKLING FAKE NEWS: THE CASE OF NIGERIA

Paul Anderson
Eropean Centre for Electoral Support

At a recent launch of a new TV station in the capital, Abuja, the Minister of Information, Lai Mohammed, said that as well as damaging Nigeria's reputation broad, fake news was destroying the media industry and sowing national disunity. This is a favourite theme of the Minister. Last year he described fake news as a "time bomb" waiting to explode. Misinformation and hate speech, he said, "threaten the peace, unity, security and corporate existence of Nigerians".

A scan of the long list of fake news items to emerge in the past months (a period during which elections for President, National and State Assemblies and Governors were held) shows just how far things have gone in the country.

PRESIDENT BUHARI: I'M REAL

One example is the well-documented video report touting a conspiracy that President Muhammadu Buhari, who in his first term suffered illness and long absences, had in fact died and been replaced by a Sudanese double. It was viewed half a million times and prompted the President, standing for a second term, to make a public denial while on a visit to Poland. "This is the real me," he insisted.

Welcome to election season Nigerian style. Such stories are legion. As Lolade Nwanze, a journalist and digital specialist at the Guardian Nigeria newspaper, says, fake news "has been on steroids". For example, a claim that Mr Buhari's main opponent for the presidency, Atiku Abubakar, was being supported by the LGBT community was designed to damage his support in the religious and socially conservative north.

ASSUMED GUILTY UNTIL PROVEN INNOCENT

Neither side is innocent. It's well known, according to Fredrick Nwabufo, a political analyst, that the two big parties ran media operations to disseminate misinformation and fake news during the elections. President Buhari's Special Adviser on Social Media posted a video on Twitter which showed his supporters at a big rally when in reality the images were from a religious gathering the year before. She

also posted a photo of a major road construction, citing it as an example of the President's public works. The public works were in Rwanda. She issued an apology, saying: "My big mistake, apologies to all, friends and wailers alike. It won't happen again."

Months later, it did. A tweet came out accusing Mr Abubakar of sharing food and money during his campaigning. It came with a photo of food packs with money attached and a caption saying: "Keep them in poverty, then give them handouts. Atiku in Sokoto yesterday." The hurly-burly of political campaigning? Or evidence of how fake news has become engrained in Nigeria's political culture? Many think the latter, and that it has to stop. The Twitter claims against Atiku Abubakar were investigated by a coalition of journalists, brought together by the International Centre for Investigative Reporting, that comprises 16 leading Nigerian media houses as well as Agence France Presse (AFP). They discovered the image was from an earlier charity event.[1]

FACT CHECKERS UNITED

The journalists' initiative is called CrossCheck Nigeria[2] and is one of several fact-checking organisations dedicated to exposing fake news and preserving the reputation and credibility of well-researched and honest journalism. Another is FactCheck Nigeria.[3] CrossCheck says its method is simple: to identify claims and posts it thinks are fake, investigate them, then publish the real version.

WORLD WAR 3?

However, in Nigeria fake news has an arguably more invidious and dangerous purpose: to stoke rivalries and hostilities between different ethnic nationalities, pitting the country's mainly Muslim north against the predominantly Christian south. This aspect was highlighted in early 2019, when the BBC organised a symposium on fake news, attracting some of the best thinkers on the issue in Nigeria. Among them was the Nigerian Nobel Prize laureate Wole Soyinka, who described the threat thus: "I've said this before that fake news may cause World War 3 and that fake news will be started by a Nigerian." Witness the forcing of the country's nationalities "into ethno-tribal cocoons," he argues.

WHAT'S TO BE DONE?

On World Press Freedom Day, an annual UNESCO event, many media professionals in Nigeria said the authorities had failed to respond to the dangers of fake news by providing better protection for journalists reporting from often difficult terrain.

It is also important for government communication to be faster and more pro-active. Pro-activity is an opportunity to establish the facts in any given controversy, as well as to build credibility and trustworthiness. ECES[4] has been particularly active in this sphere, supporting INEC with its strategic communications and its future capacity to monitor traditional and social media, collecting quantitive and qualitative data over long periods of time.

Others have called for a public campaign on social media literacy to help people question more effectively what they read, a point noted by Professor Lai Oso of School of Media, Lagos State University: "Not many people are able to make a distinction between the real media and social media, and this has posed a serious challenge to the country at large."

Especially during election season. Combatting fake news presents election assistance organisations with particular challenges. Political parties of all persuasions have been identified as among the culprits. In Nigeria and Kenya for example, in the face of fierce competition for elective offices at all levels, the parties' use of fake news to undermine opponents is unlikely to diminish.

However, there are approaches explored by some election assistance providers such as ECES, IFES, the Centre for Democracy and Development and BBC Media Action, that can tackle the rise from a number of different angles:

- Public awareness through different media engagements, building people's capacity in spotting and call-

ing out fake news, disinformation and misinformation.
- Supporting the increasing number of fact-checkers, especially around the time of General Elections.
- Establishing traditional and social media monitoring operations to build hard data-based records of incidents and profile perpetrators.
- Pro-active engagement with social media companies like Facebook to design and introduce more effective and fast-acting systems to police fake news.
- The symbiotic relationship of fake news and hate speech is well documented. Avenues are open to election assistance providers, like ECES, with the EU and its implementing partners, to support advocates of legislative measures to combat both.
- Supporting capacity of those engaged in building counter-narratives to fake news, particularly where it affects trust in institutions that still retain some degree of public trust (such as INEC).
- Quantitative and qualitative, data-based media monitoring, of the type provided by ECES in Madagascar, and soon Nigeria, can support this by providing statistics and insights into trends.
- The Nigeria-based Centre for Democracy and Development (CDD) also suggests active support for the traditional media to reinforce their credibility and as a means of reducing the space in which fake news thrives

"A MODIFIED SYSTEM OF PROPAGANDA MORPHING INTO FALSEHOOD"

Mr Ralph Akinfeleye, Professor of Mass Communication and multimedia consultant to the Centre of Excellence Radio, Television, said those involved in spreading fake news and hate speech are information traffickers. "We saw how this affected the election processes. Fake news is a modified system of propaganda, which has metamorphosed into falsehood. Its credibility cannot last."

But its omni-presence can, and will. Social platforms like Facebook and Twitter have been turning summersaults to tackle fake news, the more so after the rise and demise of Cambridge Analytica. Facebook says it is continuously monitoring and taking action against fake accounts and is investing heavily in people and technology to prevent abuse. Twitter says it has been working closely with the INEC to make reporting problem accounts, and switching them down, easier.

WHATSBREWING?

As for WhatsApp, which is widely used in Africa, it is particularly difficult to establish the source of fake news because of the platform's end-to-end encryption. CNN says an 8-year-old report about weapons being smuggled into Nigeria, filmed in the lead-up to the 2011 elections, was shared recently on WhatsApp as if it was current news related to the 2019 elections. The 2011 elections were among the most violent in the country's history.

To what extent fake news influenced the result of the election is not clear. President Buhari was re-elected by a clear margin of victory, almost 4 million votes. Is that gap, or part of it, the result of public opinion having been steered in his favour through misinformation and fake news? It impossible to quantify, but it seems improbable. But who's to say fake news can't be disseminated deeper and wider, and more convincingly, with new technologies such as 5G and Artificial Intelligence, and through new delivery methods such as more personalised smart devises replacing smart phones and the provision of detailed information, whatever the source, on voice command?

It is clear the strategy for dealing with fake news needs to be multi-pronged and to evolve around new technologies and new levels of public awareness. Because elections are at the heart of democracy, election assistance needs to play a central role.

It is also clear that the fight against fake news needs to involve communities of fact checkers, not just inspired journalist cooperatives. Part media organisations, part government, part community grassroots activity. It's a national scourge in Nigeria and it needs national solutions, from individuals and communities up, and from government and institutions down, and no time is more vulnerable than election time.

1. https://twitter.com/GuardianNigeria/status/1070060988085489664
2. P. Arnold, "CrossCheck Nigeria launches to fight information disorder", *First Draft*, 28 November 2018.
3. http://www.factchecknigeria.com/
4. The European Centre for Electoral Support, ECES, has been active in supporting efforts to detect and counter fake news in the Independent National Electoral Commission, INEC.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
23.05.2019

ARE BLOCKCHAIN VOTING TECHNOLOGIES SAFE?

Peter Y.A. Ryan
University of Luxembourg

At the height of the blockchain frenzy, many evangelists were proclaiming that blockchains would provide solutions to most of humanities problems, and in particular that they would enable secure, online voting. Much of the initial frenzy has died down now, and few blockchain "solutions" have actually emerged. Regarding voting, a few blockchain based schemes have been proposed and some even been trialled. Whether any of these are secure in a meaningful sense is very doubtful, despite grandiose claims by their advocates.

So, let's examine that claim that blockchains can enable secure voting, either remote or in-person, or at least help. At first glance this seems quite plausible: many so-called "end-to-end verifiable" voting schemes have invoked the notion of a "Secure Public Bulletin Board", in effect an append-only public ledger. In most cases, it was never explained how such an entity would actually be implemented, it was simply assumed that such a magical beast could somehow be invoked. So here at least it seems that blockchains can help, and indeed they can, up to a point. But we have to be careful: blockchains, or more generally distributed ledger technologies (DLT), come in many flavours, permissioned vs permission-less, private vs public, decentralised vs distributed. So, if we are to advocate the use of a DLT we have to be clear what flavour we have in mind.

So, could Bitcoin style, fully decentralised blockchains be used for voting? The answer seems to be: probably not. Leaving aside issues of latency, i.e. the time for transactions to be confirmed-currently about 10 minutes for Bitcoin, it seems quite dangerous to leave the acceptance of rejection of submitted ballots to an unknown, unaccountable pool of miners from around the globe. We already know about the 51% attack and indeed other forms of attack requiring smaller percentages of the mining pool.

So, it would seem wiser for voting to opt for a distributed but not fully decentralised solution, in which a selected set of trustees collaborate to maintain the ledger. Such entities would be chosen to be (widely) trusted but independent, for example the political parties, pro-democracy organisation like the League of Women Voters in the US etc. But now we are into more traditional forms of Byzantine consensus.

It is worth noting at this point that the Bitcoin style blockchains did not come out the blue. Many of the ingredients were already know to and used by cryptographers and dependability folk: Crypto hashes, hash chains, consensus algorithms etc. Nakamoto brought these together in a novel way to achieve a novel form of consensus, under certain assumptions, in which anyone can in principle participate as a miner. This is certainly interesting, and has spurred a lot of fascinating research, but as argued above, seems inappropriate for voting. At first glance, Nakamoto consensus seems democratic, in that anyone can contribute. In reality though it is only entities able afford the specialised mining hardware who can participate effectively.

So, DLTs can contribute to one aspect of challenge of securing voting systems, can they help with others aspects? For this we need to identify what are the real challenges and what are the unsolved (or only partly solved) problems. I will not detail all the challenges, just focus on the principle one: how to ensure verifiability while at the same time preventing coercion or vote–buying? This is particularly challenging in the remote, internet context, where we cannot enforce the isolation of the voter at the time of casting, and we may have active attackers interacting with the voter before, during and after the voting period, demanding that the voter give up credentials, passwords, and to follow detailed instructions on how exactly to cast the ballot.

The transparency required for verifiability is clearly in conflict with the secrecy requirements, and this tension is typically resolved by use of "modern" cryptography, public key crypto, zero-knowledge proofs, homomorphic cryptography etc. Typically votes are encrypted before being posted to the public ledger and it is essential that the voter be able to confirm to their own satisfaction that this encryption is performed correctly. However, we must take great care in how we do this: any proof provided to the voter must not be transferable to a coercer or vote-buyer. Furthermore, we don't want to have to trust the software on the encrypting device so we typically allow the voter to "audit" the encryption in some form of cut-and-choose procedure to detect a corrupted encryption device or app.

But even this is not enough: a voter might perform such an audit and claim that the vote revealed when the encryption is opened up does not agree with the vote they input. Now we have to decide if the voter is telling the truth as to what vote they input, and it really was the device cheating, or they are lying, or possibly just mistaken, in which case the device may be perfectly honest. This is often referred to as "dispute resolution" and designing a system that provides this while avoiding any coercion threats is a challenge that researchers have been bashing their heads against for about three decades. Reasonable solutions exist for the in-person case, but to date none are known for the remote case.

And we must add to these requirements that whatever design and interface we come up with must be supremely simple to use and understand, the system must be usable by people with a wide spectrum of ability, who might only use it once every few years. Put all of these requirements together and we have arguably the greatest challenge facing security engineers. It is quite possible, even probable, that no solution exists that will fully meet all of these requirements, at least for the remote context.

So, to return to our question: can DLTs help solve this challenge. As far as I can see there is nothing that DLTs can bring to the table that help with the coercion threat, and based on discussions with other researchers in this field, this is the generally held view of people who have devoted time and effort to this challenge.

So, we are left with the key, high-level question: should we be attempting internet voting at all? As so often, the answer depends on the context. For critical, binding elections, the answer is, for the time being at any rate, a resounding "No!". We have no technology at present capable of securing internet voting, in the sense of making it verifiable, coercion resistant and usable. Solutions do exist that can provide two of these requirements, but achieving all three simultaneously remains out of reach.

Of course, there are plenty of elections for which the stakes are much lower, where the motivation and resources of

potential attackers will be much lower, hence much milder threat scenarios. For such elections, satisfactory solutions do exist and indeed are used, just as a cash-box is enough to secure the takings at a lemonade stand. For high-stake elections, of the US president or a referendum on membership of the European Union to take a couple of random examples, we do not have locks that can withstand state actors, or even in some cases script-kiddies.

Research and development on securing elections continues and progress is being made. In terms of deployment, we should move cautiously from low-stake elections towards higher stake. In this, DLTs do have role to play, at least helping to implement the notion of a secure bulletin board, and perhaps also the maintenance of an electoral role, but for the other challenges thrown up be secure voting we need different tools and ideas, many yet to be invented.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
23.05.2019

BETWEEN DIRECT REPRESENTATION AND PARTICIPATORY DEMOCRACY

Michele Sorice
LUISS University

The concept of political representation is traditionally connected to two reference poles: from one side the electoral dimension, from the other side the practices of participation. This linkage, however, is a relatively recent conceptual constraint and was not present in the development of the "electoral method" in the rising American nation: James Madison,[1] for example, described democracy as a troubled system, destined to a quick and violent death. The same terms "democracy" and "participation" were used with suspicion.

The so-called "crisis of democracy" (which perhaps could be more accurately understood as a crisis of institutional representation) arises precisely within the short-circuit between the delegitimization of representative institutions (the intermediary bodies) and the individuals' perception of the loss of that power that the mass parties seemed to guarantee in the past. The lack of trust in political and representative institutions generates three possible areas of response from citizens: a) social apathy, which manifests itself as a disinterest in politics, often accompanied by strongly anti-political feelings; b) the request for more specific control over representative institutions – this request is expressed in what Pierre Rosanvallon[2] defines counter-democracy and evolves into a sort of systemic distrust (the "sanctioning democracy", as Nadia Urbinati[3] has defined it), often finding in the appeal for direct democracy a presumed solution for a stronger citizen participation; c) the request for new forms of participation, ranging from active citizenship to the use of digital platforms for democratic participation, from the most advanced application of open government[4] to the many different experiences of democratic innovations[5] (collaborative governance, public debate, participatory budgets, territorial co-management, etc.). In this area, the emphasis on active citizenship and participatory democracy is usually very strong.

The rhetoric on direct democracy is often accompanied by the emergence of what has been called "direct representation"; as Stephen Coleman and Jay Blumler[6] stated, "indirect representation is characterised by an apparently inevitable fracture between the representing centre and the represented outer layer". In this fracture, some forms of direct representation are developed along two paths, not

necessarily antithetical: a) on the one hand the use of the internet (from clicktivism to specifically designed online participatory platforms); b) on the other hand, the emerging forms of hyper-representation, where the subjects become representatives of themselves or, more frequently, accept a leader claiming himself/herself for the representative (the hyper-representative).[7]

The request for a more diffused use of direct democracy can be also framed in the development of another trend of post-representative politics:[8] namely the depoliticisation, that can be defined as a sort of reduction of politics to the only dimension of policy, accompanied by the shifting from "government" to "governance". In other terms, depoliticisation – in the words of Fawcett, Flinders, Hay and Wood[9] – is a "bridging concept operating at the nexus between micro-trends (the disengagement of individual citizens), meso-level institutional mechanisms and reforms (modes of governance), and macro-level ideologies and dominant growth models".

At this point, we are at a crucial crossroads. Democracy seems to have entered a post-representative phase and the recourse to direct democracy fits perfectly in this phase, accentuating both the tendency to depoliticisation and the affirmation of "direct representation". At the same time, however, the popular demand for greater decision-making power is evident and it cannot be left to the demagogy of the neo-populist parties. It is not surprising that an ideological element of the neo-populist parties resides precisely in the attempt to delegitimise representation in the name of the practice of direct democracy, which is however based upon the principle of aggregation (who has one more vote wins) and it is meaningfully opposed to the logic of participatory and/or deliberative democracy. It is no coincidence that Stefano Rodotà[10] warned about the risks of plebiscitarism inscribed in the digital referendums or, more generally, in some forms of online direct democracy.

In everyday language – and also due to simplification operated by some journalists and politicians – there is a tendency to overlap the concept of direct democracy with those of deliberative and participatory democracy. These are actually three different concepts, even with different cultural backgrounds. Direct democracy previews that people can vote on different topics, having usually a binary choice; the policy making process is distinct from that of decision making. An example of direct democracy is the referendum, an institution which is also present in many liberal democracies (both in consultative and abrogative forms). On the opposite, the distinctive dimension of deliberative democracy lies in the idea that there are not necessarily predefined preferences but that they can be transformed in the course of interaction. In other words, deliberative democracy is based upon the shared formation of opinions and preferences. Finally, participatory democracy involves a series of social practices, continuous over time, aimed at improving representation in the logic of strengthening the quality of responsiveness. The practices and theories of participatory democracy are addressed to the formation of active city communities,[11] also improving commitment and politicization of the participants. In short, deliberative and participatory democracies are not alternatives to representative ones, but can enrich them.

The merging of participatory democracy and deliberative procedures can play an important role in increasing inclusiveness, improving the quality of democracy[12] and facilitating a not intermittent citizens' participation. In this perspective, digital platforms[13] for democratic participation can be elements of improvement of the participation quality and could also strengthen the legitimacy of representative democracy, if they don't just offer the possibility of voting. As shown by various international experiences,[14] the use of e-voting, for example, didn't determine the growth of people's participation and caused many doubts[15] about its reliability.

The issue is not just about technology, even if the platforms' architecture plays a role in the policy/decision making procedures; the peculiar dimension, in fact, lies in the adoption or not of participatory and deliberative practices in the e-democracy tools. A deliberative/participatory e-democracy can be the right way to reshape representative democracy and avoid the risks of plebiscitary approaches, that instead structurally belongs to direct democracy.

1. https://world.wallstreetenglish.com/v2/student/dashboar
2. P. Rosanvallon and A. Goldhammer, *Counter-Democracy Politics in an Age of Distrust*, Cambridge, 2008.
3. N. Urbinati (ed.), *Democrazie in transizione*, Milano, Fondazione Giangiacomo Feltrinelli, 2016.
4. E. De Blasio and D. Selva, *Why Choose Open Government? Motivations for the Adoption of Open Government Policies in Four European Countries*, Policy and Internet, 2016
5. https://participedia.net/
6. S. Coleman and J.G. Blumler, *The Internet and Democratic Citizenship. Theory, Practice and Policy*, Cambridge University Press, 2009.
7. E. De Blasio and M. Sorice, "Populism Among Technology, E-Deocracy and the Depolitisation Process", *Revista Internacional de Sociologia RIS*, vol. 76, no. 4, October-December 2018,
8. J. Keane, "Tibet: or, How to Ruin Democracy", *The Conversation*, 29 March 2013.
9. P. Fawcett, M.Flinders, C. Hay, and M. Wood, *Anti-Politics, Depoliticization, and Governance*, Oxford Scholarship Online, 2017.
10. S. Rodotà, *Iperdemocrazia*, Roma, Editori Laterza, 2013.
11. U. Allegretti, "Democrazia partecipativa: un contributo alla democratizzazione della democrazia", in U. Allegretti (ed.), *Democrazia partecipativa: esperienze e prospettive in Italia e in Europa*, Firenze, Firenze University Press, 2010.
12. L. Diamond and L. Morlino, "Assessing the Quality of Democracy", *Journal of Democracy*, Johns Hopkins University Press, 2005.
13. http://opendemocracy.it/e-democracy/democratic-tools/
14. "E-voting experiments end in Norway amid security fears", *BBC News*, 27 June 2014.
15. D. Springallet al., *Security Analysis of the Estonian Internet Voting System*, Scottsdale, Arizona, 2014.