Elections, when free and fair, are regular and legitimate occasions to vie for power in a democratic country. In order to compete and to be elected, political competitors, usually organized into parties or movements, must follow the democratic principles that rule electoral competitions. There are numerous international regulations that set worldwide standards for democratic elections, which have been adopted by many countries and that constitute the concept of electoral integrity. This refers not only to management of the so-called e-day (election day), but also includes many provisions that must be respected throughout the electoral cycle.

The growing importance of cyberspace in election-related issues has been documented by many observers, including international organizations that focus on democratic governance and electoral issues. These international institutions are increasingly establishing international standards also for conducting elections in cyberspace, in particular regarding electronic voting data management. The so-called e-voting systems must abide by the rules for data management, which at the international level are summarized in the United Nations General Assembly Guidelines for the Regulation of Computerized Data Files that was adopted in 1990. Despite being broad, these guidelines identify some key principles as they assign responsibility for data to those persons who collect it, who become responsible for their accuracy and their transparency; data must lawfully collected, securely stored, and lawfully disseminated. More recently in 2017, the Council of Europe added new principles and recognized that the Electoral Management Bodies (EMB) are those actors that must be held responsible for e-voting standards and for the "availability, reliability, usability and security of the e-voting system." However, although there have been some improvements at the international level in regard to principles for election cybersecurity, these norms have not found an immediate and broad application in the "real"
world. There are other worrisome aspects about cyberspace and how it may affect electoral integrity, which are currently of increasing concern to voters, media, electoral experts, and politicians: big data, voter profiling, hacking voting machines or registries, fake news and disinformation campaigns.

In this analysis I am going to address the main cybersecurity concerns for the upcoming mid-term elections in the United States. The new US National Cyber Strategy stresses that “Securing our democratic processes is of paramount importance to the United States” and it includes electoral institutions among the critical infrastructures that must be protected by recurring to different tools in order to deter possible attacks. In light of the aforementioned considerations, my analysis addresses two main different layers of cyberspace that can affect electoral integrity. The first one refers to the technical dimension, in particular to the electronic voting system (e-voting), a concept that “encompasses a broad range of voting systems that apply electronic elements in one or more steps of the electoral cycle”. There is an ongoing debate about the opportunities and risks of ICT in elections; some countries such as Estonia, introduced e-voting as a standard voting procedure. Others, such as Germany, stopped the use of such technologies, as its Constitutional Court ruled they were unconstitutional in 2009. The second layer of analysis is the informational dimension, which refers to the new media environment and its impact on electoral campaigning and information warfare. On the one hand, the advent of “technology-intensive campaigning” based on big data is re-shaping the means of political advertising and participation; on the other, despite the fact that information warfare have long been a tool in the arsenal of states, what is creating deep concern is the level of directness, the scale of activity and the scope of these operations’ efforts to influence public opinion.

Electronic voting technologies and the new informational capabilities raise multiple concerns, in particular about the security of electronic voting and possible large-scale attacks on the electoral process. Both the technological and the informational dimensions have critical impacts on the so-called digital democracies, where cyberspace is both a functional technology for increasing participation in the polity and a campaign domain where domestic as well as external actors compete for power. Fraud and malpractices are found even in long standing democratic regimes so protecting electoral integrity is imperative to maintaining the trust, legitimacy and accountability of the elected. The 2016 presidential election in the United States brought worldwide attention to cybersecurity and electoral integrity, especially for what concerns foreign interference. In the following paragraphs I will provide an overview of the US cybersecurity electoral environment for the upcoming mid-term elections, first from a technical perspective and secondly from the informational standpoint.

E-VOTING IN THE US ELECTIONS

The United States has a longer history than many other nations as regards the adoption of ICT in elections. As concerns the electronic voting system, the first case, which involved scanners for ballot counting, was adopted in 1959 by the Norden Division of United Aircraft. Around the same time, punchcard voting technology was invented and was first used in the US for the 1964 presidential primaries in two counties in the state of Georgia. Punchcard voting systems were rapidly adopted in many states as election officials argued that this system was cheaper and more cost-effective than other systems. Yet punchcard voting systems proved to have many flaws far before the 2000 presidential elections when the Supreme Court ruled on
equipped with a button or a touchscreen displaying the ballot and the voter just has to press on his/her favourite party/candidate, whereas optical scanners are used to read and count marked ballot papers. The choice of which electronic voting systems to adopt is remanded to states’ jurisdictions, which often decide to use more than one system because of county variations. Currently, for the mid-term elections, 41 states and the District of Columbia will use optical or digital scanners to count paper ballots. Direct Recording Electronic machines are still used in some 30 states, 12 of which do not

the re-count of punchcard ballots in Florida. The resultant scandal contributed to decreasing the public’s trust in this voting technology. Two years later, in order to improve electoral integrity in the US, Congress passed the Help America Vote Act (HAVA), which among other provisions called for replacement of the punchcard voting system with the Direct Recording Electronic (DRE) voting machine or optical-scan voting system. In the aftermath of the 2000 election, many people viewed these technological developments as potential aids to solving the problems that had occurred in Florida. DRE machines are equipped with a button or a touchscreen displaying the ballot and the voter just has to press on his/her favourite party/candidate, whereas optical scanners are used to read and count marked ballot papers. The choice of which electronic voting systems to adopt is remanded to states’ jurisdictions, which often decide to use more than one system because of county variations. Currently, for the mid-term elections, 41 states and the District of Columbia will use optical or digital scanners to count paper ballots. Direct Recording Electronic machines are still used in some 30 states, 12 of which do not
provide a voter-verified paper audit trail (VVPAT), which is useful to detect possible malfunctioning or electoral frauds. The absence of such a provision is contrary to the recommendation given by the Office for Democratic Institutions and Human Rights of the Organization for Security and Cooperation in Europe (OSCE/ODIHR).

In order to respect democratic voting principles, e-voting machines, like other systems (such as the traditional paper ballot) must guarantee some prerequisites such as secrecy of vote, freedom to vote and the non-alteration/modification of the vote; in addition, there is the issue of public trust in these technologies. Are the current e-voting systems in the US secure? And if so, are they perceived as such?

In the aftermath of the 2016 election, in order to improve the security of e-voting technology the US government took some provisions aimed at reducing cyber-risks. In January 2017, election infrastructure was designated as part of national critical infrastructure, which would increase the efforts, at both the state and federal levels, to improve coordination and information exchange against cyber-threats. Following this recognition, in October 2017 the Sector Specific Agency (SSA) was created to manage the infrastructure. Subsequently, in January 2018 the US Congress approved an act – the Consolidated Appropriations Act – that allocated $380 million for improving election management (including enhancing cybersecurity) to states. According to international observers, despite the fact that this was a long-awaited act (since 2010) to support HAVA, it came too late, as in some cases states must undertake feasibility studies, which may take a long time, and thus be unable to use these funds before the upcoming elections. Numerous voices have raised concerns about the current state of cybersecurity for election technology in the US. In June 2017, 100 election experts from across the United States wrote an open letter to Congress expressing their deep concern that many jurisdictions were "inadequately prepared to deal with rising cybersecurity risks." In May 2018 The Washington Post published an article showing some of the results of a survey conducted among 100 cybersecurity experts about the US election system: almost all of them said that it was vulnerable. On 28 September 2018, the NYT published an article pointing out that "there are roughly 350,000 voting machines in use in the country today, all of which fall into one of two categories: optical-scan machines or direct-recording electronic machines. Each of them suffers from significant security problems."

There are multiple reasons that underpin this assessment. The first one concerns the fact that the possible magnitude of threats from state-sponsored cyberattacks is too big for state-level defense. As reported in the article, according to one of the experts – Dave Aitel, former National Security Agency (NSA) security scientist – “Protecting systems from cyber-threats from national states can really only be done on a national level. It's insane to have state-level control of these systems.” Indeed, elections and their management (including cybersecurity) are administered at the state level and often duties are delegated to some 10,500 jurisdictions. At the state or county level there are two main problems that can hamper a proper cybersecurity policy: lack of human resources and lack of funding. There is no federal body to oversee the electoral process and the Election Assistance Commission (EAC), which is a national advisory body, provides only guidance for what concerns the testing of e-voting machines. This leads to the second main problem regarding e-voting machines: lack of mandatory federal security standards for them. Indeed, the EAC has a national voting system certification program but states are not required to use certified election systems, therefore the process of testing and getting the federal certification is completely optional. To date few US jurisdictions have fully
adopted these standards as obligatory. Yet even if the jurisdiction has the willingness, the funds and the staff to conduct e-voting testing, it is based on 2005 standards or, even worse, in some cases on 2002 standards. The Election Assistance Commission is constantly updating new standards, the latest introduced in 2015 but not yet adopted by any test, and is currently working on new set of standards but it will take another two years before any machines will be tested and certified as compliant with them.

Hacking experts from the Voting Village, a section of DEFCON, one of the world’s largest hacker conventions held annually in Las Vegas, published a report about their hacking the e-voting machines currently adopted by US jurisdictions. The findings are shocking:

- A voting tabulator that is currently used in 23 states is vulnerable to remote hacking via a network attack […] hacking just one of these machines could enable an attacker to flip the Electoral College and determine the outcome of a presidential election.
- A second critical vulnerability in the same machine was disclosed to the vendor a decade ago, yet that machine, which was used in 2016, still contains the flaw.
Another machine used in 18 states could be hacked in only two minutes, while it takes the average voter six minutes to vote.

Ackers had the ability to wirelessly reprogram, via mobile phone, a type of electronic card used by millions of Americans to activate the voting terminal to cast their ballots.

Election systems, like other critical infrastructure – such as nuclear plants - are supposed to be air-gapped, meaning that they are disconnected from the Internet and from other machines that might be connected to the Internet. Nevertheless, room remains for hacking. For example, hackers at DEFCON 2017 took only five seconds to plug in a USB or a fake voter card to the machine and thus infect it. Or, on election nights, many polling places around the country transmit voting results to their county election offices via modems embedded in or connected to their voting machines. Moreover, there is always the possibility of the human factor, which is the weakest one when it comes to cybersecurity. As acknowledged by Richard DeMillo, a Georgia Tech computer scientist, it may be possible for devices such as thumb drives to be used to transfer data from air-gapped machines to computers with Internet connection. The vulnerabilities of current e-voting machines are well known and there is a lively debate in e-voting states about the opportuneness of returning to paper-based voting. Georgia, for example, which is one of the five totally paperless voting states, is exploring the idea of replacing its e-voting system with paper ballots by 2020.

Another issue of concern comes from voter registration databases, which are managed by each state. Following the 2016 elections the Department of Homeland Security (DHS) published a joint statement urging upgrading voter registration systems against possible cyberattacks and offered several services to state and local election officials to assist in their cybersecurity. Nevertheless, a study published in September 2017 by Harvard researchers affirms that it could be very easy for hackers to manipulate voter data “armed with personal information obtained through legitimate or illegitimate sources, hackers could learn enough to impersonate voters and change key information using the online registration systems.” Voter data could also be stolen and sold on the dark web, as researchers at Anomali Labs and Intel 471 demonstrated with the discovery, a few weeks before the mid-term elections, of a large quantity of voter databases for sale (19 states and at least 23 million records), including valuable personally identifiable information and voter history.

Despite the numerous sources of concern regarding the technological dimension of the upcoming mid-term elections, which could eventually undermine the integrity of the process, US citizens seem to be confident about the security of voting procedures. In particular, regarding election hacking, voters have become somewhat more confident that election officials are taking the steps necessary to fend off cyberattacks. As demonstrated in figure 2, 27.5% of the interviewed answered “very confident” and 34.8% responded “somewhat confident” to the question “How confident are you that election officials in your county or town will take adequate measures to guard against voting being interfered with this November, due to computer hacking?” The result, compared with those collected few months ago, is quite important.

Meanwhile there are stakeholders, such as think tanks and other observers, that call for enhancing the security of voting technologies. The recommendations to the US administration are disparate and include: developing mandatory guidelines for the electoral process, from election equipment vendors to polling stations or e-voting machines and guidelines for election equipment vendors; allocating...
more funding for state and local governments; introducing a voter-verified paper audit trail where this is not already in use. Nevertheless, many other interlocutors contacted by the OSCE/ODHIR Need Assessment Mission expressed their confidence in the level of cyber-preparedness at all levels of the US government.37

TECHNOLOGY-INTENSIVE CAMPAIGNS AND DISINFORMATION THREATS

By reading the French philosopher Jacques Derrida, Anthony Whitem – the author of Democracy in the Digital Age – claims, “new technologies are more than just more efficient techniques or means to perform a certain function or task. Rather, they are effecting profound transformations in the public sphere, changes that alter the dimensions of public space as well as the very structure of the res publica.” The informational dimension can be split into at least two sub-dimensions. The first one refers to exploitation of the impressive amount of data available for political purposes. The second regards so-called information warfare, which allows malicious actors to spread disinformation to alter voters’ preferences. The two sub-dimensions are not disconnected and may mutually reinforce the negative effects on electoral integrity. Indeed, according to international organizations concerned with democratic elections, both data-driven electoral campaigning and disinformation during electoral campaigns may reduce trust in the electoral process, thus eventually harming democratic institutions.

With the advent of so-called “data science” the way of doing political campaigning changed abruptly. The degree of pervasiveness and rapidity of political debate, propaganda and communication has never been so high. According to some scholars that are looking at it from an historical perspective, we are currently in the 4th phase of running campaigns in terms of style and dynamics. This phase is characterized by the strong mediatisation of political campaigning, which is occurring in a hybrid communication environment (in which media are deeply integrated into different spheres of society) and by technological developments enabling a heavy use of data. The advent of technological developments had four important implications for conducting political campaigns: the first is the possibility of rapid interaction in terms of communication between politicians and citizens; this leads to the second implication, which refers to the emotional and personal sides of political campaigns. Thanks to widespread connectivity there is more and more line-blurring between the public and personal lives of voters. In order to keep citizens engaged in politics – and this is the third element – participation must be easily accessible and political messages must reach those who are not yet involved by means of ad hoc campaigns. Thus, and this is the fourth implication, data are extremely important for efficient and effective campaign design. The first technology-intensive campaign was Obama’s 2012 presidential campaign, which recurred to electioneering through big data and computational analytics. The use of electioneering got worldwide attention in early 2018 when a former Cambridge Analytica employee, Christopher Wylie, revealed how social media were involved in user profiling for political campaign purposes. Following that scandal, social media have battened down the hatches, promising much more control over their users’ data, and Cambridge Analytica shut down in May 2018.

Data are at the basis of any type of information and disinformation campaign. Disinformation can be defined as “false information or intentionally misleading facts communicated with the intent to deceive”, and fake news is part of it. How data are reshaping and changing democracy is
still a question of academic debate, nevertheless the advent of so-called technology-intensive campaigning took the aspect of information insecurity to a new level of threat. Digital disinformation has become so pervasive in online social media that it has been listed by the World Economic Forum as one of the main threats to human society. Indeed, cyberspace enhances the opportunities for malicious actors to spread manipulated content online in order to “deceive, distract, and misinform public opinion, trash[ing] the debate with diverging truths, which eventually disorient and corroborate a sense of doubt among the public, or shape the opinion of a specific target audience on a certain issue.”

As a result, the White House’s latest National Cyber-Security Strategy, released in September 2018, includes countering malign cyber influence and information operations as priority actions: “The United States will use all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation.” In the same month, President Trump signed an executive order “on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election”, which underlines that “[i]n recent years, the proliferation of digital devices and Internet-based communications has created significant vulnerabilities and magnified the scope and intensity of the threat of foreign interference.”

The reinforced US position against external actors’ cyber propaganda and disinformation followed the 2016 presidential election, when according to US intelligence services Russian hackers penetrated emails to and from Hillary Clinton and the National Democratic Committee and spread their content through WikiLeaks. The effect, beyond demonstrating the cybersecurity vulnerabilities of their accounts, contributed to widening the internal rifts dividing Clinton and Bernie Sanders supporters. Some commentators suggested that “Donald Trump would not have been elected president were it not for the influence of fake news.”

The meddling of Russian hackers in the 2016 elections was for many a watershed moment in history as it was a wake-up call to Western democracies regarding Russian behaviour in cyberspace. The following year Special Counsel Robert Mueller indicted the Russian Internet Research Agency and thirteen of its employees for their efforts to influence the 2016 US election using social media while the US Intelligence agencies published a warning regarding the risks of Russian information warfare for the upcoming elections, which would mainly be directed towards polarizing voters through the spread of fake news.

Recently, on 19 October 2018 the Director of National Intelligence published a joint statement affirming that there are “ongoing campaigns by Russia, China and other foreign actors, including Iran, to undermine confidence in democratic institutions and influence public sentiment and government policies.” In the same period the US Cyber Command started targeting individual Russian operatives to deter them from interfering in elections. This is the first (known) overseas cyber operation to protect electoral integrity. The strategy is in line with the “continuous engagement” foreseen by the new US position in cyberspace. On their side, social media platforms have been undergoing “cyber hygiene” practices to reduce the risk of spreading fake news through them. Twitter for example recently released a statement where it disclosed all the suspicious accounts and related content associated with potential information operations that it had found on its service since 2016 to enable independent academic research and investigation. Moreover, in recent months both Facebook and Twitter suspended or cancelled millions of suspect accounts in order to prevent the mushrooming of fake news that might go viral.

As briefly outlined, the threat of foreign interference in the United States elections through propaganda and disinform-
mation features very high on the US political agenda. Yet, since cyberspace is the domain of ambiguity where attribution is almost impossible, it could be interesting, beyond naming and shaming foreign actors, to look at the impact of the so-called fake news on the 2016 US elections. This is still a highly debated issue. There are scholars\(^5\)\(^6\) claiming that the impact of fake news on electoral results was exaggerated, whereas others found a strong correlation between aggregate voting patterns and the average daily fraction of users visiting websites serving up fake news.\(^5\)\(^7\) It is possible that the fake news phenomenon is particularly important for swing voters or those who usually do not vote. However, to my knowledge, what remaining to be assessed is the effect of fake news on voter turnout. It is also important to underline that the problem of foreign propaganda has always existed, and addressing the issue by accusing foreign actors may not be most useful strategy if the same content is produced in-house.\(^5\)\(^8\) Indeed, fake news and the post-truth world has been fuelled by domestic politicians who repeatedly attack journalists and traditional media daily.\(^5\)\(^9\) In this context external actors, such as Russian hackers, may find a fertile environment and they contribute to exacerbating mistrust toward traditional media and disinformation spreading. Despite being highly debated and in the spotlight issues, disinformation campaigns and fake news need further academic inquiries in order to assess their impact on electoral behaviours. For the time being, there have been very few elements regarding possible Russian interference in this upcoming election and even the last OSCE/ODIHR interim report\(^6\)\(^0\) states that there are only concerns about possible online disinformation campaigns.

**CONCLUSION**

The analysis of the current status of the electoral integrity of the upcoming US mid-term elections in terms of cybersecurity shows two main pictures. The first one refers to the technical side of the voting process, which includes several elements of the electoral cycle – in particular, voter registration and voting machines. Here the analysis highlights multiple concerns regarding the protection of these fundamental components of the electoral process. White hat hackers proved to be able to penetrate voting machines even when they are air-gapped. Moreover, the recent discovery of millions of voter records on the dark web poses a serious threat to the protection of sensitive data. So far, the international community has particularly emphasised the importance of guaranteeing the secrecy and the security of stored electoral data. Moreover, many observers are complaining about the lack of funds and human resources that are necessary to better manage the security of voting technologies at the state level. Eventually, and this is one of the most worrying elements, there must be mandatory federal requirements for jurisdictions as well as for producers and vendors of voting technologies, including certification of the supply chain.

On the informational side there are multiple sources of concern too. For what concerns technology-intensive campaigns it seems the main social networks are putting limitations on their third-party data policies, which should reduce voter exploitation and profiling. Yet social networks are just one of the factors involved in this 4th phase of political campaigning. Fake news and disinformation have scored very high in political debate and in public opinion since 2016. On this issue some actions have been undertaken but the general polarisation of public opinion as well as the ongoing attacks on traditional media foster mistrust and radicalisation of the political debate. In such a scenario foreign actors spreading disinformation and fake news find a fertile environment. Yet the effect of fake news and disinformation campaigns has yet to be assessed by academic...
mic research. Notwithstanding the lack of empirical evidence on the impact of foreign actors’ cyber-propaganda, the US government decided to tackle this issue seriously and recently launched the first (known) cyber operation overseas in order to deter possible external influences in the upcoming election.

To conclude, I would underscore that while this analysis found most of the vulnerabilities to be at the technical and thus, domestic, level, which would require urgent actions by the US government, it seems that the government is much more concerned about social media propaganda and foreign influences from the usual suspects. This, after all, reflects the US position regarding cyberspace, which is more and more an arena where national interests naturally collide and thus where international confrontations are mirrored⁶¹.

*Raffaello Stefani contributed to data research

---

2 For what concern transparency it refers to, for example, “access to preliminary voter lists in order to verify details and to challenge registrants who are not eligible, and access to final voter lists is important so these can be used by party agents on Election Day and for voters to know which polling station to go to”, IFES, “Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies”, 2018, https://www.ifes.org/sites/default/files/2018_heat_cybersecurity_in_elections.pdf
4 Council of Europe, CM-Rec (2017), 5 June 2017, Appendix I, sec. VIII.
5 “We will also deter malicious cyber actors by imposing costs on them and their sponsors by leveraging a range of tools, including but not limited to pro-


8 F. Rugge, Mind Hacking: Information Warfare in the Cyber Age, Analysis 319, ISPI, 2018

9 Aceproject: http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b1


12 Optical Scan Paper Ballot Systems: Voters mark their votes by filling in an oval, box, or similar shape on a paper ballot. Later, the paper ballots are scanned either at the polling place or at a central location. Direct Recording Electronic (DRE) Systems: DRE systems employ computers that record votes directly into the computers’ memory. These interfaces may incorporate touchscreens, dials, or mechanical buttons. The voter’s choices are stored by the computer on a cartridge or hard drive. Some DRE systems are also equipped with a printer, which the voter may use to confirm his or her choices before committing them to the computer’s memory. The paper records can be preserved to be tabulated in case of an audit or recount. Ballot Marking Devices and Systems: These systems are designed to help disabled voters who might be unable to vote using other methods. Most devices utilize a touchscreen along with audio or other accessibility features. Rather than recording the vote into the computer’s memory, the ballot is instead marked on paper and later tabulated manually. Additionally, some jurisdictions use paper ballots that are manually counted at the polling place. Other jurisdictions use these paper ballots for absentee or provisional voting (https://ballotpedia.org/Voting_methods_and_equipment_by_state).


14 Defined as: “storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments”. Ibid.

15 Ibid.

16 Ibid.

17 https://www.electiondefense.org/election-integrity-expert-letter/


21 The FEC (Federal Election Commission) oversees and enforces campaign finance law.


23 See https://www.eac.gov/voting/equipment/certified-voting-systems/


26 Ibid.

27 CBS News, Hackers break into voting machines within 2 hours at Defcon, 30 July 2017.


30 Ibid.


33 See https://www.cybersecurityintelligence.com/blog/35-million-2018-us-voter-records-for-sale-3823.html

34 See https://electionupdates.caltech.edu/2018/10/10/americans-are-slightly-more-confident-about-fending-off-computer-hacking-in-the-upcoming-election/


36 OSCE/ODIHR (2018)

37 Ibid


42 A. Rommele and D. von Schneidmesser (2016).

43 Ibid


PROTECTING ELECTORAL INTEGRITY IN CYBERSPACE: THE US MID-TERM ELECTIONS IN 2018

51 Ibid.
52 P. Norris, S. Cameron, and T. Wynter (2018).