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 Strategy² 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 analysis⁴, there are fundamentally two main dimensions in which cyber threats can impact the integrity of electoral processes: the technical and the information-
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”). 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, 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 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” 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 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.

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 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 and Anna Pellegatta in their articles, can lead to extreme polarization, which may impact the quality of a democracy. Finally, it could be possible that the government that suffered from malicious cyber campaigns or attacks may suffer from loss of international credibility, as explained by Fabio Rugge in his article.

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, 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 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, 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, 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.

4. S. Dominioni, Protecting Electoral Integrity in Cyberspace: The US Midterm Elections in 2018, ISPI Commentary, 1 November 2018
7. Ibid.