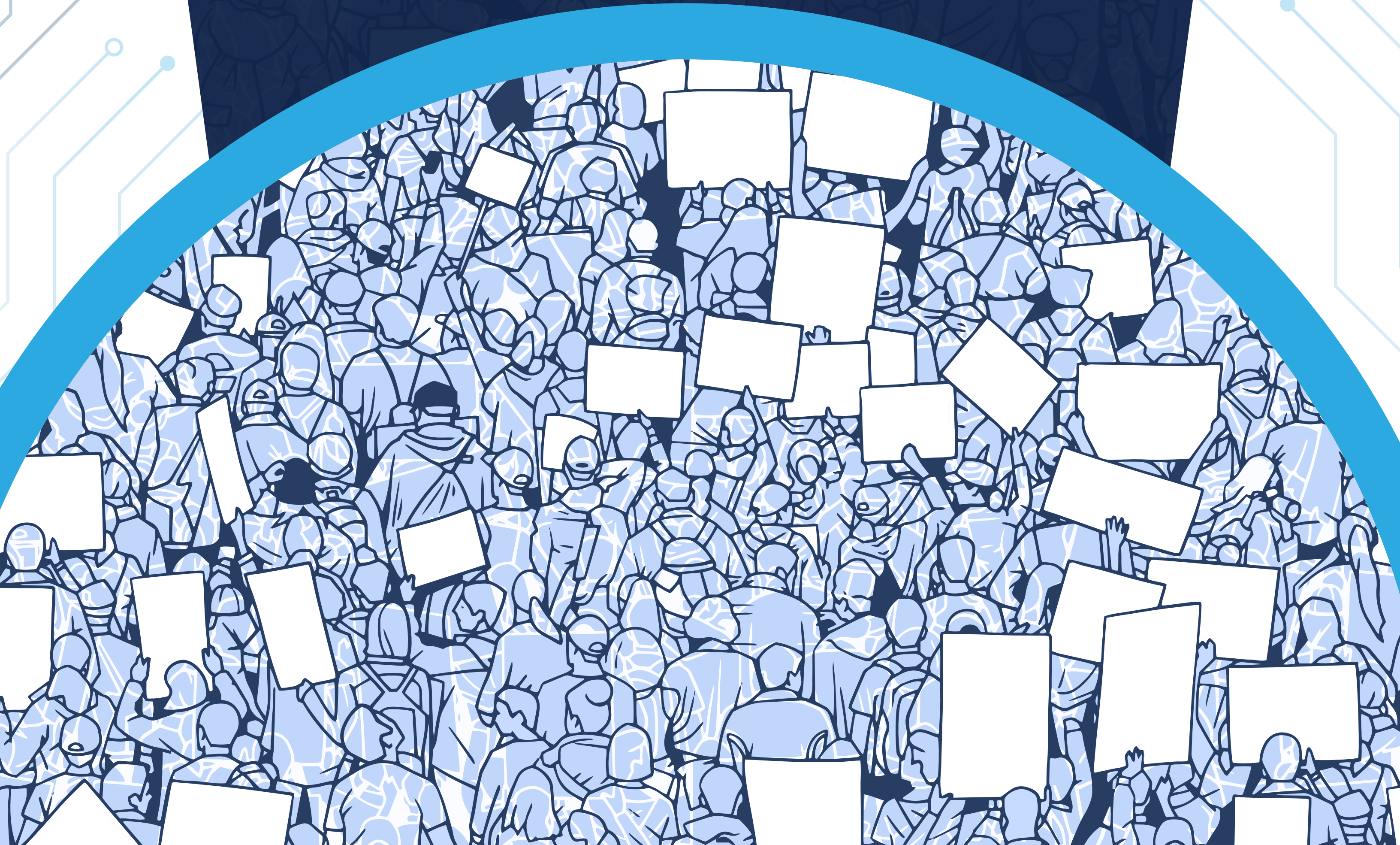
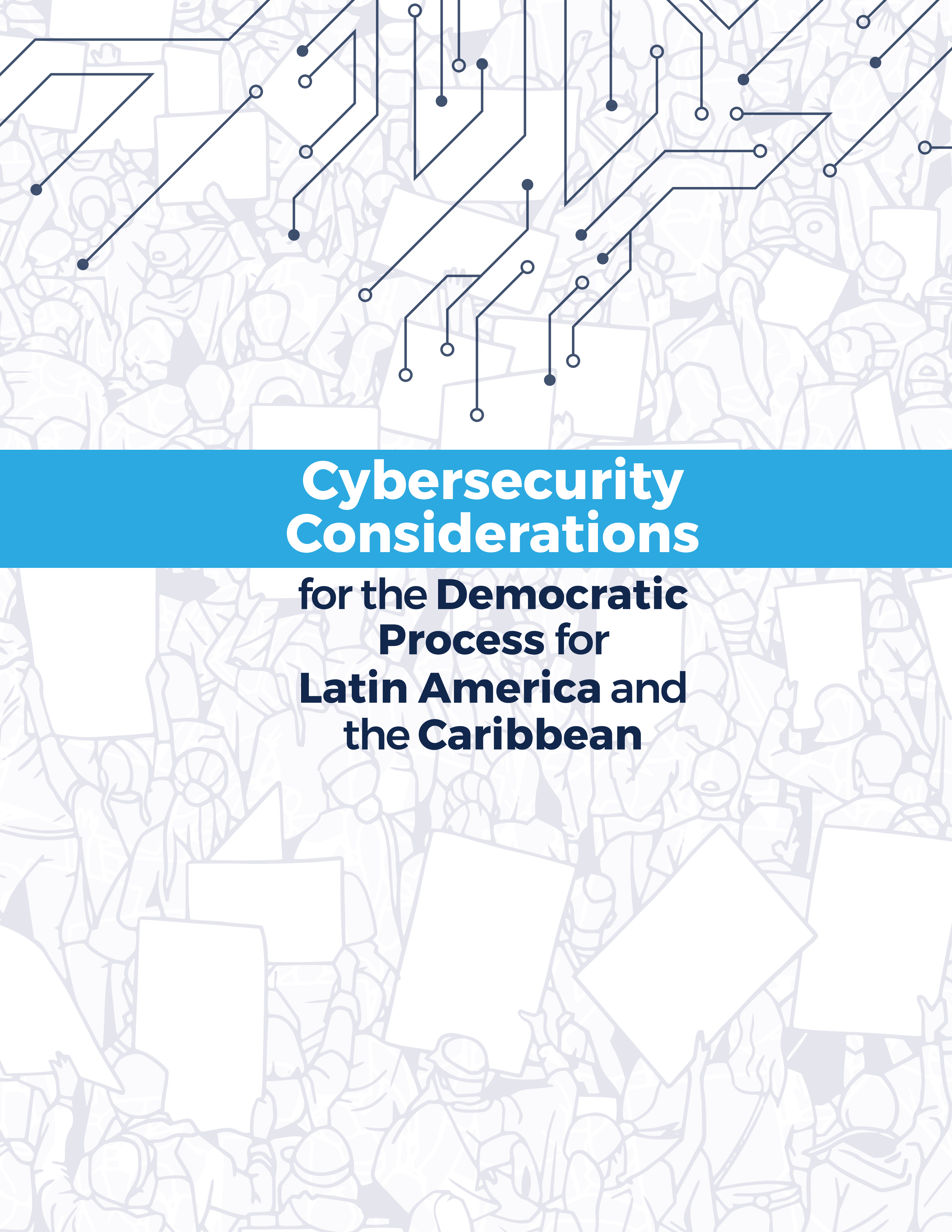
OAS More rights for more people

Cybersecurity Considerations for the Democratic Process for Latin America and the Caribbean





Cybersecurity Considerations

for the Democratic Process for Latin America and the Caribbean

Prepared and published by the Cybersecurity Program of the Inter-American Committee against Terroism (cybersecurity@oas.org).

The contents expressed in this document are presented exclusively for informational purposes and do not represent the official opinion or position of the Organization of American States, its General Secretariat or its Member States.

This Publication has been made possible thanks to the financial support of the UKFCO.

We welcome your interest in this Guide. The UK Government is keen to better understand the impact of the projects that it funds and whether they have achieved the desired outcomes. Your feedback on how you have used this guide and whether it helped improved cybersecurity incident response would be valuable information we can use to help design future projects.

Please contact the Foreign and Commonwealth Office at CyberCapacity.Building@fco.gov.uk to share your feedback.

Cybersecurity Considerations

for the **Democratic Process** for **Latin America** and the **Caribbean**

Credits

Luis Almagro
Secretary General
Organization of American States

Farah Diva Urrutia
Secretary for Multidimensional Security
Organization of American States

Francisco Guerrero Aguirre
Secretary for Strengthening Democracy

OAS Technical Team
Gerardo de Icaza
Alison August-Treppel
Brenda Santamaría
Cristobal Fernandez
Yerutí Mendez
Alex Bravo
Belisario Contreras
Kerry-Ann Barrett
Rolando Ramírez

Consulting Team
Lara Pace
David Marcos

This guide was developed by the Cybersecurity Program of the Inter-American Committee against Terrorism of the Secretariat of Multidimensional Security, with the collaborative support and input by the Secretariat for the Strengthening of Democracy and review and input of the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights

Table of Contents

Table of Contents

Foreword

In an age where technology meets everyday life, the very fabric of a stable digital society requires the protection of the networks and devices that support democratic processes. Even countries that use limited technology in the conduct of their elections face cyber-risks to electoral integrity; this topic requires serious consideration even in those limited circumstances. One of the most visible democratic processes is the electoral cycle. Until recently, the debate on cybersecurity and the electoral cycle was mostly about electronic voting and transmission of preliminary results: countries with paper-based electoral processes considered themselves largely free of the risk of cyberattack. However, the technologies used in elections potentially changes with each electoral cycle, and so do adversaries and their tools.

At the most basic level, the use of technology in elections involves voter, party, and candidate registration as well as websites of Electoral Management Bodies (EMBs). The connection of these systems to the Internet makes them more vulnerable to cybersecurity attacks. If not secured properly, they become easy targets and are used as a tool to question the validity of parts of the electoral process or even the election itself in some cases. Ensuring the confidence of the citizenry is critical to maintaining public trust in the process and integral for any election results to be accepted. The Organization of American States (OAS) and the Commonwealth, as two regional bodies, recognize the need to ensure that its member states are aware of the threat their democracies face in this digital environment, and that these states consider what actions may be required for their strategic plans and responses.

The Organization of American States (OAS) as the world's oldest regional organization, dates back to the First International Conference of American States, held in Washington, D.C., from October 1889 to April 1890. Established in 1948, through the Charter of the OAS, the OAS was established in order to achieve among its member states—as stipulated in Article 1 of the Charter—"an order of peace and justice, to promote their solidarity, to strengthen their collaboration, and to defend their sovereignty, their territorial integrity, and their independence." Bringing together all 35 independent states of the Americas, the OAS uses a four-pronged approach to effectively implement its essential purposes, based on its main pillars: democracy, human rights, security, and development. The Commonwealth itself is a diverse community of 53 nations that work together to promote prosperity, democracy, and peace. Building, supporting, and strengthening legal systems in their member countries includes the promotion of regular elections and strengthening the capacities of election bodies, institutions, and processes. The Commonwealth places a high priority on being a community of peaceful and democratic countries and ensuring that shared fundamental political values – including a commitment to human capacity rights, the rule of law, and civilian government – are actively protected and promoted.

This document, developed by the OAS with support from the Foreign and Commonwealth Office, UK, seeks to raise awareness of the issues surrounding technology and democracy and to encourage global dialogue on the topic. The first section sets the context by exploring how the distribution of information via the Internet impacts the democratic process. Building on that theme, we then consider the results of a survey distributed across the OAS member states as it relates to cyberthreats on democratic supporting systems. The paper concludes with suggestions and recommendations on how to facilitate the discourse and positive practices in local, regional, and national areas.

There will be many factors around which democracy would need to navigate and the advent of COVID-19 as a global pandemic made this even more evident. Democracies have had to adapt to these changing circumstances and rely on technological solutions to support essential processes such as elections. This deeper integration of technology, now more than ever, calls for the need to strengthen cybersecurity measures to engender a continued trust and confidence in democratic processes.

Purpose

This document is intended to raise awareness among OAS member states on the processes surrounding and sustaining our democracies. More specifically, it is intended to focus attention on the cybersecurity implications that may affect the processes that support democracy and, in particular, the electoral processes. Even if the actual democratic processes are viewed as technology-free, it is of utmost importance to consider cybersecurity in the broader context of the democratic landscape.

According to the Inter-American Democratic Charter (IDC), 'essential elements of representative democracy include, inter alia, respect for human rights and fundamental freedoms, access to and the exercise of power in accordance with the rule of law, the holding of periodic, free, and fair elections based on secret balloting and universal suffrage as an expression of the sovereignty of the people, the pluralistic system of political parties and organizations, and the separation of powers and independence of the branches of government.' (GA/OAS 2001)

Taking this definition (of the IDC) into account, this document is intended to cover some aspects of cybersecurity measures that guarantee human rights and fundamental freedoms and the holding of periodic, free, and fair elections. Awareness-raising among the citizens, political parties, and candidates about the probable devastating effects of cyberattacks will contribute to the mitigation of the possible consequences of cyberattacks against political parties and their campaigns. The need for a cybersecurity framework for elections has only recently become a highly debated topic. The issue of addressing cyber threats that specifically affect elections is not only being discussed among information technology security officers and professionals, but also among decision-makers and the public-at-large. Therefore, there is a need to not only educate the public on how cyber incidents may affect democratic processes as a whole, but also to develop tools that can be useful to politicians, citizens, and the media and to better protect electoral institutions against cyberattacks.

Recently, there have been alleged hacking incidents during Latin American elections[1], from defacing campaign websites, breaking into other parties' databases for espionage, and using malicious software. However, the existence of political polarization and some recent economic instability sets the stage for more sophisticated attacks. Digital technologies and the Internet have provided additional means for conducting an election, such as Internet voting or moving parts of the electoral process online, such as online voter registration. Therefore, beyond social media manipulation or modern-day propaganda, an electoral process can become vulnerable as institutions adopt new technologies.

This document presents several topics for consideration that highlight the potential challenges and impacts of technology on the democratic process. It is not an authoritative, step-by-step guide for the implementation of cybersecurity measures, nor is it an in-depth report on current trends and threats against the technology used within the democratic process, though some specific recommendations are offered. It is important to shift the mindset of the region from thinking of a democratic process as a linear event (whether it be a referendum for a specific purpose or an electoral cycle). Instead, the democratic process should be addressed continuously within a cyclical mindset and through a cyclical approach. The challenge of identifying good technology practices for a region as diverse as the OAS is significant, particularly given the dynamic nature of cybersecurity threats. With this complexity in mind, this document focuses more on how technology can be managed to control its impact on the democratic process in the context of the various commonalities across the diverse region of the Americas and the Caribbean. Starting a dialogue across all stakeholders in the region is necessary in order to increase their understanding of the threat technology brings to the democratic process. We must expand and heighten their knowledge to mitigate one of the most pressing challenges of our time.

When it comes to cybersecurity, we have seen several publications that address the complexity before us. This document brings to the discussion some alternative ideas that bind together democracy, cybersecurity, and information. By addressing the challenge head-on, and reinforcing freedoms of expression, we hope that the political will in the region may increase to address this new reality.

Introduction

The Organization of American States (OAS) serves as a political forum for the Americas, where the independent countries of North, Central, and South America and the Caribbean come together to advance their shared goals and work out their differences. Political dialogue is important within each of the four pillars of the OAS—democracy, human rights, security, and development. Such dialogue led to the development of the Inter-American Democratic Charter, a blueprint for what democracy should look like in the region developed by the OAS and its member states.

In accordance with the Inter-American Democratic Charter, (adopted by the General Assembly at its special session held in Lima, Peru, on September 11, 2001), (GA/OAS 2001):

> ***[Article 1]*** *"The peoples of the Americas have a right to democracy and their governments have an obligation to promote and defend it."*
>
> *"Democracy is essential for the social, political, and economic development of the peoples of the Americas."*
>
> **Further,**
> ***[Article 7]*** *"Democracy is indispensable for the effective exercise of fundamental freedoms and Human rights in their universality, indivisibility and interdependence, embodied in the respective constitutions of states and in Inter-American and international Human rights instruments."*
>
> **Also,**
> ***[Article 2]*** *"The effective exercise of representative democracy is the basis for the rule of law and of the constitutional regimes of the member states of the Organization of American States. Representative democracy is strengthened and deepened by permanent, ethical, and responsible participation of the citizenry within a legal framework conforming to the respective constitutional order."*

In this regard, the OAS promotes a democratic culture and continues to carry out programs and activities designed to promote democratic principles and practices to strengthen a democratic culture in the Hemisphere, bearing in mind that democracy is a way-of-life based on liberty and enhancement of economic, social, and cultural conditions for the people of the Americas.

The OAS continues to work more specifically on democratic issues from various angles and to build on its long history in the deployment of Electoral Observation Missions (EOMs). Since 1962, the OAS has deployed over 275 OAS/EOMs in 28 member states[2]. As part of its process of systematizing and standardizing Electoral Observation Missions (OAS/EOMs), the OAS Department for Electoral Cooperation and Observation (DECO) of the Secretariat for Strengthening Democracy (SSD) develops various tools and methodologies to support member states in the institution-wide strengthening of their electoral systems and processes[3]. One particularly relevant document from the General Secretariat of the OAS is "Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions" (GS/OAS 2010). This document is used by observers in the field when examining the use of technologies. It covers aspects that should generally be considered in the observation of any elections in which technology is a factor.

Countries in the western hemisphere are experiencing the longest period of uninterrupted democracy in the history of the region (save for a few exceptions). In that context, the media must consider the role it plays in the social environment and the conditions within which candidates compete. The media is an increasingly influential component of an electoral process and an associated level of influence on democracy. In that regard, staying abreast of current issues such as cybersecurity threats and the implications of these on democracy is critical. In the wake of an attack, the media could report on events without reference to the correct terminology or report inaccurately, the impact that some cyber incidents may have on the overall results of democratic processes.

This document, therefore, speaks to some core themes around information, the media, and the democratic process under the following chapters: ***the Power of Misinformation in the Digital Era; Cybersecurity Challenges in the Democratic Process - Latin American and the Caribbean; Global Efforts In Cybersecurity and Democracy; The Democratic Process: Institutional Infrastructure and the Cybersecurity Considerations; Community Engagement in Democratic Processes; and Facilitating the Dialogue and Considering Next Steps - Recommendations.***

Reflection:
The power of information in the digital era

The access and distribution of information has played an essential role in the establishment—as well as the consolidation—of many democracies worldwide. The availability of information influences democracy. We must consider the past, present, and future influence of information as we continue to adapt our democratic institutions and processes in preparation of an era shaped by information technology. We must be prepared to respond to new threats as well as new opportunities for democracy as a whole.

Context

Information has existed since time began, but perhaps it was referred to or identified by a different name. The art of storytelling formed the basis of thousands of years of shared history. The act of sharing and imparting knowledge on future generations has defined the various cultures we share across our people worldwide.

This historical sharing of knowledge and forming of our cultures through spoken word began to take shape in its written form on clay tablets around 3200 BC. Much later, Guttenberg allowed for mass production of print (which is perhaps where we begin to think of this exchange of ideas or knowledge-sharing as information or, more to the point, information exchange). (Nelson 1998)

Information and its modalities require some form of definition, as there are various ideas of what is meant by the term information, especially within a cyber context. For the current dialogue, we consider information to be a form of messaging such as an image, video, or written word, as well as the spoken word, all of which inform or shape public debate and opinion. This definition offers the most useful and broadest idea of information, and so is most useful in the context of this paper. A more technical definition of the term 'information' (specifically, packets of technical information distributed across a network) may be more appropriate for a cybersecurity discussion and audience, but that does not suit the wide scope we see information having on the democratic landscape.

> *"Information is increasingly seen as a common good, the protection of which falls onto all citizens concerned with the quality of public debate." (Vilmer 2018)*

If one were to look back at the last 100 years in history, it would not be too difficult to draw out specific cases where information has played a vital role in the various administrations of the day. We could also draw out examples where information – publicly accessible information – has even contributed to the Western perception of significant wars, which taint our shared history[4]. Similarly, we could draw on specific examples where information has simply created world leaders and retained their power. The common theme in these varied examples is the overwhelming power of information. Whether within the context of a home, the workplace, or even public office, the ability to control a narrative within these contexts offers total control over those same contexts.

At an international level, there is much discussion of what constitutes 'hard power' or 'soft power,' but perhaps we have reached a point in our societies where we can begin to talk about 'real power.' Real power is the ability to control a narrative, irrelevant of the context in which one is operating. Information and its distribution allow a narrative to be told and established and re-enforced through re-distribution. It is at this point where security and safety measures need to be considered – within their very contexts – at the distribution level and the scalability of the distribution process.

There are discussions within the Inter-American System[5] on the balance between the need of the State to execute its function of the provision of public safety and that of the human rights guarantees of a citizen. In this regard, any restrictions "must be interpreted in strict adherence to the just demands of a democratic society, which take into account the balancing of different interests at stake and the necessity of preserving the object and purpose of the American Convention."[6]

Walking that fine line

One of the more powerful actions the Internet has made possible is the ability to distribute content at a large scale, with great ease, and at significantly lower costs than traditional avenues of content distribution such as print and broadcast media (radio and television), gallery spaces, the cinema, and so on. The Internet also has enabled the sharing of content at incredible speeds. Internet access allows every stratum of society to share information equally (in most cases), and it is this ability, associated with the freedom to express opinions, that has generated volumes and volumes of content on a daily basis, of varying degrees of interest and accuracy. This freedom of expression remains a universal human right that must be upheld at all times, conscious that there is a need to avoid any punishment of opinions unless same is 'backed up by actual, truthful, objective and strong proof that the person was not simply issuing an opinion (even if that opinion was hard, unfair or disturbing), but that the person had the clear intention of committing a crime and the actual, real and effective possibility of achieving this objective. Acting otherwise would mean admitting the possibility of punishing opinions, and all the States would be authorized to suppress any kind of thought or expression critical of the authorities that, like anarchism and opinions radically opposed to the established order, question the existence of current institutions. In a democracy, the legitimacy and strength of institutions are strengthened by the force of the public debate over their operation, not by its suppression'[7].

Any expression can have an immeasurable reach through distribution channels on the Internet. If we were to compare distribution of a single message on the Internet to the distribution of that same message through traditional town hall meetings, we could imagine agreement being reached at a scale only limited to the reach of the message when distributed on the Internet, as opposed to the finite reach generated by the town hall meeting.

The Cyber Security Connection

In previous sections of this paper, we have addressed some of the more straightforward arguments regarding the relationship between information and the Internet. There is an implied assumption up until this point that the information distributed across the Internet is positive, factual, true, accurate, and in pursuit of the common good.

Considering the issues more broadly, however, we may find information to be the opposite of the description above, i.e., negative, non-factual, untrue, dishonest, and in pursuit of political gain and power. What steps could be taken to prevent this unhelpful narrative from being established and rooted across a society?

The challenge is incredibly difficult, given the principles of freedom of expression as enshrined in the Universal Declaration of Human Rights, Article 19, and the human right to have access to the Internet and equally to reliable and factual information. (UN 2016)

> ***[Article 19]*** *"Everyone has the right to freedom of opinion and expression; this right includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontier."*

It is not necessarily the technicalities of cybersecurity that make this challenge a cybersecurity challenge; it is the Internet's ability to virally spread information at rates we have never experienced before that makes the entire subject of information a cybersecurity consideration. To this end, the OAS has recommended states to "[c]arry out positive education, training, and awareness actions on the phenomenon of misinformation"[8].

Misinformation, Disinformation[9], Fake News, Manipulation of information

Publications from national governments describe issues such as fake news, misinformation, disinformation, and any number of other terms that can be used to describe varying forms of the distribution of inaccurate information.[10] All this terminology describing the different types of misinformation is simply one aspect of the problem that needs to be considered when addressing the distribution of information.

> *"We live in a world where there is more and more information, and less and less meaning." (Baudrillard 1983)*

It is through an awareness of the depth and breadth of misinformation, disinformation, and other forms of information manipulation that we can begin to understand how relevant actors can affect the result of their own electoral process. Similarly, through the same tactics and approaches, we can start to understand the emergence of foreign state interference in the very same manner, affecting the result of an electoral process of a foreign country.

State-on-State manipulation is also a consideration and could include traditional cyberattacks on infrastructure. This manipulation could result in the inhibition of the actual conduct of an electoral process, reducing the ballot share and directly affecting a result.

The Scalability Problem

Political messaging has always existed. Whereas crime has always existed, the Internet has exacerbated the market and its access for criminals. It is this scalability which the world is focused on combatting through various national and international initiatives to counter cybercrime. Similarly, propaganda and political messaging have always existed; the Internet has exacerbated its impact and reach. There is no technical solution to the growing scale of cybercrime and its impact on the democratic process. Instead, longer-term strategic solutions must be considered and implemented.

The Economics of a Captive Audience

During an instant where a message, expression, or piece of information is distributed and goes viral, there is an added feature of a captive audience (a mass audience that is distracted by viral content) that is often overlooked. Whereas messages can be shared almost instantly, as with a virtual Town Hall, other information of a more negative nature can be shared just as quickly. The ability to access a captive audience to introduce malware for economic gain into a fast-paced sharing community is essentially dealt with through traditional mechanisms aimed to counter cybercrime, and similarly can be mitigated through tooling available to law enforcement and industry.

The Question About Personal Data

Social media has created a new dimension to the challenges of technology and the democratic process by making available a wealth of publicly accessible information about all members of society. There are several examples of how the exploitation of personal information and personal data points to further economic or political gain. It is important to accept the realities of the current landscape we navigate as citizens and voters in a country, understanding that the information we publish on social media may be used in ways that we do not understand.[11] Beginning to change the mind-set around personal data by increasing the notion of value that individuals attribute to their own data, coupled with a robust data protection regime, may begin to reduce the power and influence of social media companies in the distribution of political information.[12] It is also imperative for large enterprises whose business model is premised on the mass storage of personal data and the trade of that data [13] to shoulder responsibilities (in the short term) in ensuring that the common good or the will-of-the-people is not compromised through manipulation of publicly available data that is held on their platforms and infrastructure.

Large corporations that are in possession of large banks of data must shoulder responsibility for the data they possess and control the manner in which that data is used. This responsibility goes beyond international legislative requirements, which aim to prevent the misuse of personal information. It also encompasses the moral responsibility of these companies to ensure that not only is the data protected from a purely technical security perspective, within the confines and mandates of the rule of law, but also, that individuals are educated about the use – and potential misuse – of their personal data.

Companies that do not have large banks of data about the public still have data about their employees that must be protected. It is the responsibility of employers to ensure their employees understand the hiring entity's policy on the processing of personal information and how this is maintained (and defended) to all extents possible.

Political Information

> *"Describing ourselves as (also) inforgs, who forage for, produce, cultivate, curate, process, and consume information, inhabiting an environment also made of data and computational processes, means adopting an ecological perspective" (Floridi 2013).*

In his paper, "Marketing as Control of Human Interfaces and Its Political Exploitation," Professor Floridi describes the shift in landscape and the change in the relationship between marketing and politics.

> *"Politics has become a matter of marketing, it is important to understand why this is true."*

It is not that politics has shifted its position. Instead, it is marketing and the ability to access and distribute information that has shifted. The relationship between individuals, the platforms they navigate, and the resource they own or exchange, encompasses two paradigms. The first paradigm is one where the individual is the target of marketing campaigns (i.e., where political marketing is designed to massage the individual ego). The second one is where the process of an exchange of resources is at the center of the relationship (i.e., where a resource is either our economic credit or data or vote).

Educating the Populace

As our information society continues to develop and occupy every aspect of life, there is a dramatic and urgent requirement to empower the general public with the necessary skills to be able to navigate the complex landscape that dominates daily life. The education sector, with the support of academia, has a role here to truly and meaningfully begin to build the knowledge and skills required by the public at large to think critically about information.

The ambition for all stakeholders should be to equip the general public at the earliest of ages with the following skills:

> ***1. Deciphering advertising and marketing messaging (in this case political, but should be broad)***
> Equipping the general public with an ability to understand the veracity of messaging and the context within which the messaging exists is of utmost importance. The threat before us in understanding communication not only in a political context but also within a commercial setting, empowers individuals to think critically and make informed decisions, and build a direct filter on a significant level of information manipulation strategies in play at the moment.

Building a personal filter to information decreases the exacerbation of information manipulation through online means.

2. Sourcing and Identifying investigative journalism

Building an appreciation and understanding of the world of journalism across the globe to combat current trends that see a decrease in the value of independent journalism. Encouraging and empowering the general public to identify and follow media houses that provide a transparent report on political discourse and debate enables valuable dialogue and shapes the political landscape. The varied sourcing of information, identified through a bolstered understanding of deciphering messaging, enables this.

3. Building an understanding of transparency and accountability

The principle of transparency and accountability, together with the respect of fundamental human rights, is at the foundation of good governance. As information manipulation has overwhelmed the current political discourse so interconnected with a world audience, it is critical to remind the public at large of the importance of transparency and accountability.

4. Building an understanding on conflict of interest

Driving an understanding of conflict of interest is also integral to the threat before the world. Without understanding what ethical conduct looks like, the general public is unable to make a judgment on what is correct and what is incorrect. Constant, targeted online communication campaigns for political gain or favor are a growing information manipulation tactic. It is important to encourage critical thinking on the part of the general public in order to mitigate the relentless propaganda that seeks to normalize the tolerance of conflict of interest in public office.

The working Solution

There is no straightforward answer to the challenges the world is currently facing across all political systems and spectrum. There is no rulebook or step-by-step guide to combating the distribution of malicious or malign targeted information campaigns. Instead, we need to focus our attention on longer-term solutions and begin to sow the seeds to empower our nations to make adequately informed decisions when participating in democratic processes. It is the responsibility of each administration, in collaboration with big data companies or information holders, to ensure and foster reliable information and critical thinking by the public in order to maintain healthy democracies. Nevertheless, there are two key takeaways from this exercise:

1. The fact that there are several publications globally focused on the topic of misinformation and fake news and a number of debates and academic research currently taking place is a testament that people are paying closer attention to what occurs around them. This level of analysis is a great thing for democracy. Our societies are moving in the right direction, heavily focusing on awareness-raising programs to counter the threat.

2. It is important to review and evaluate previous events and interventions, debunking the myth that once an election process is completed, we can park the priority of addressing challenges the democratic process faces for the duration of the term of office. Proper evaluation must take place at this point in order to draw out the lessons learned from each election cycle. We must ensure there is collaboration across the board to develop, build, and sustain awareness and understanding of how data is being used throughout the democratic process to inform appropriate data protection regimes.

It is important to empower our societies. We have to continually evaluate the environment in which we are in because it is continuously changing. Establishing strong ties and relationships with social media and Internet service providers is a tool to make this evaluation practical.

Cybersecurity Challenges in the Democratic Process- Latin American and the Caribbean

In the past 20 years, the Internet and Information Communication Technologies (ICTs), among other emerging technologies, have revolutionized different realms of daily living. Digital solutions have continuously been developed to facilitate social interaction and communication, as well as access to information. The applications of these technologies have been limitless, and democratic processes have been no exception. Electoral processes, for example, integrate technology in many of its steps: EMBs use websites to publish voting results and other systems to maintain electoral registries. In many countries, EMBs also use different kinds of technological solutions in order to process and transmit tally sheets more efficiently, transparently, or at faster times (compared to more manual options).

As digital solutions continue to be adopted, their exposure to cybersecurity risks might be unavoidable. The Americas region is a notable target and source of cyberattacks. The Internet Security Threat Report ranked the three largest economies in the region, Brazil, Argentina, and Mexico, as 3rd, 8th, and 10th, respectively, in its global ranking of origin of cyberattacks. (Symantec 2019) Similarly, in a 2017 article published by Kaspersky, it was reported that Internet users in Latin America are victims of over 177,500 malware attacks per hour, which translates to an average of 33 attacks per second taking place in the region. (Kapersky 2017) More recently, according to a report presented by the Internet Addresses Registry for Latin America and Caribbean's Warning, Advice and Reporting Point (LACNIC WARP) during the webinar titled "Cybersecurity Trends in Our Region," it discussed how phishing continues to be the leading cause of cyberthreats in Latin America and the Caribbean, representing over 60% of recorded attacks, while the use of malware (18.9%) and redirect (16.35%) have continued to increase in the past years. (LACNIC 2018) In other words, countries of the region are and will continue to be a target and source of malicious cybersecurity activity.

The growing number of digital solutions used in democratic processes, in addition to the expanding cybersecurity threats in the region, have created a demand to understand the degree of adoption of digital solutions in democratic processes, and their respective cybersecurity challenges within the Americas.

Therefore, the OAS elaborated a survey directed to specific stakeholders involved in the democratic processes of its 34 member states. This survey took into consideration the changing cybersecurity landscape in the region, as well as the technological applications used for electoral processes. The survey analyzed: (1) the degree of digitalization of the electoral process, (2) legislative frameworks, (3) cyber-threats against democratic process, and (4) levels of implementation of cybersecurity measures to protect the electoral process. Using clustered sampling, the OAS identified electoral officials, parliamentarians, national incident response teams, and various government ministries as the appropriate sample set to respond to the survey. Questions were answered on the basis of what each respective stakeholder could answer or disclose. For example, questions directed to EMBs were answered specifically by electoral officials.

The OAS electronically distributed the 28-question survey to the above-mentioned entities, which either participated in the four workshops and one webinar (please refer to Annex II), or to the EMBs which conform part of OAS Secretariat for Strengthening Democracy's mailing list. Responses from 17 countries [14] with profiles predominately comprised of Electoral Officials (85% of responses) and the remaining 15% consisted of Government Ministry Representatives, Parliamentarians, and National Incidence Response Teams.

This sample is not representative of the 34 Member States; it cannot be assumed that the results reflect the institutional views of each stakeholder that is either directly or indirectly involved in electoral processes within each country. Nevertheless, while a more comprehensive study is required to provide a deeper understanding of this topic in the region, it is hoped that the analysis of the data collected through this survey might still shed some light in an effort to understand the cybersecurity challenges in electoral processes in the region.

For the purpose of the analysis, the responses were grouped into two regions: (1) Latin America, and (2) the Caribbean. As the countries of each respective region share similar levels of maturity in cybersecurity capacities, this provided a useful baseline for a comprehensive analysis of the region. The analysis was supplemented through a series of in-depth interviews with regional experts who provided additional information that complemented the survey results.

Taking into account the aforementioned limitations of this study, the survey results revealed that approximately 13 of the 17 of the countries that responded (75% of the respondents) had implemented Voter Registration Databases (proportionally quite balanced among both the Caribbean and Latin America) and Institutional Webpages (with Latin American member states having implemented this tool more frequently).

Compared to their Caribbean counterparts, Latin American countries are more active in the utilization of Institutional Webpages, Election Reporting Systems, Social Media, and Vote Tally Systems. Voting machines and Internet Voting are not widely-used solutions in the region, with no Caribbean countries having introduced them. Only 57% of National Authority/Commission/Agency indicated that they use cloud services, with some degree of correlation between the size of the country and its introduction being evident[15].

Further, over 50% have implemented digital identification, and approximately 58% utilize social media with a broader integration in Latin America. In relation to budget allocation, although there are some initial indications as to the priority of digital implementation, over 50% of the respondents indicated that they do not have a dedicated budget nor a dedicated team to enhance the cybersecurity of the democratic process. This is true despite the fact that over 70% of the respondents anticipate an increase in the number of cyberattacks on upcoming elections and 90% of them indicate a deeper collaboration between agencies and a Computer Security Incident Response Team (CSIRT) would have a positive impact in the overall security of the democratic processes.

Concerning overall awareness of possible cybersecurity incidents, over 50% of the respondents are unaware of any such incidents against their electoral processes. One explanation for this measure might be that there are a significant number of events that go undetected. This explanation suggests that more resources should be allocated to identify these incidents correctly and to enhance the awareness of all the stakeholders on the issues underpinning cybersecurity.

Another observation from the survey results is that there are ongoing challenges in terms of awareness and political measures to be taken. Law updates, the establishment of a task force or committee for securing the electoral process, and overall better coordination, were all identified as a need.[16] Additionally, according to the respondents, there is not enough collaboration between organizations in the sampled countries. Although most of them believe that better collaboration would increase the overall security of the electoral process.

A common theme for the respondents represented in the survey is that, although critical, the consideration of cybersecurity in the democratic process loses momentum once elections are over. The topic is overshadowed until the next election cycle, or at the point an attack is discovered. When the latter happens, the lack of defined structures like committees, working groups, or even updated legislation, might lead to insufficient protection and ultimately worsened consequences.
This document, therefore, aims to contribute to the dissemination of good practices and their progressive implementation to prevent cybersecurity incidents in the context of elections.

Degree of digitization of the democratic process

The advancement of tools of information and communications technology (ICT) has the potential to impact democracy nearly as much as any other area, such as science or education. The effects of the digital world on politics and society are still difficult to measure, and the speed with which these new technological tools evolve makes it difficult to track. This digitization has led to, in some countries, a more open and transparent process and in others, a tool to coordinate the voice of people giving rise to use of social networks to raise awareness on key political issues. Some of the things that these digital democratic innovations has facilitated in democratic process include, online voter registration, e-voting, e-petition, online consultations, public engagement and referendums, among other tools.

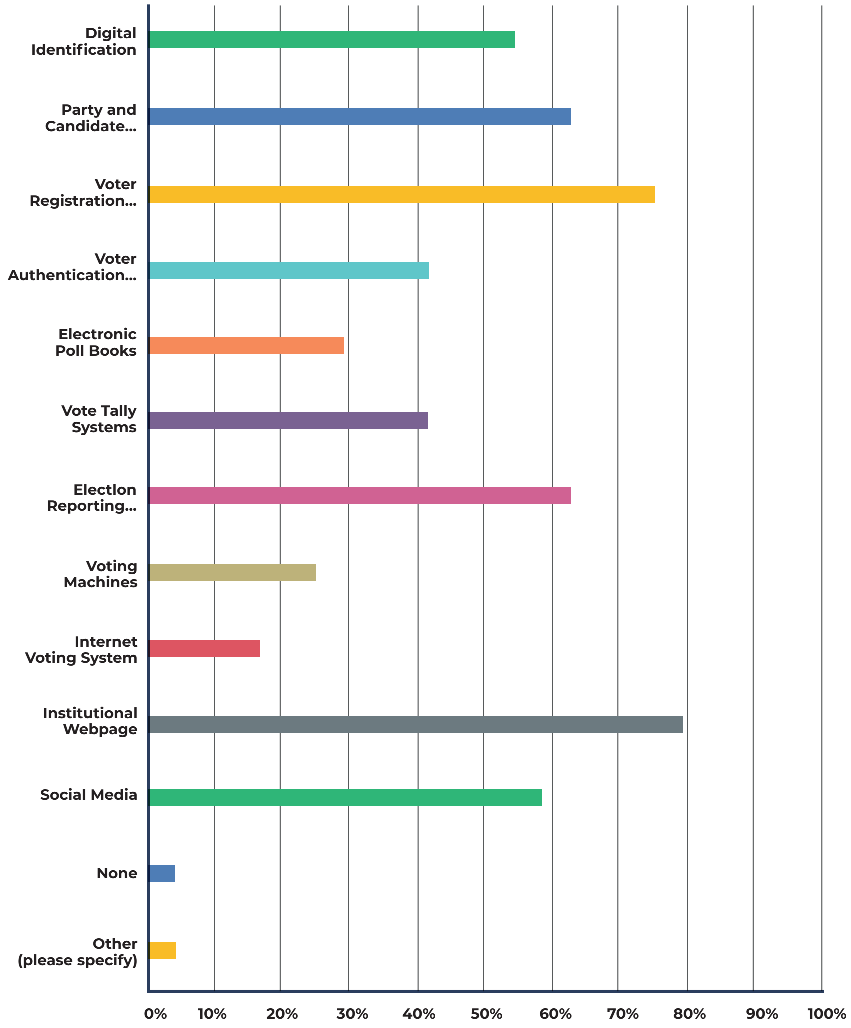


Figure 1-Digital Solutions implemented by the OAS Member States

The first step in order to form a trustworthy snapshot of the cybersecurity landscape around the democratic process in Latin America and the Caribbean region, was to understand the level of digitization of the processes supporting democracy. The results indicated that almost all of the Member States (93%) have digitalized their democratic processes to one degree or another. The most widely used tools, with a penetration of over 75% are: Voter Registration Databases and Institutional Webpages. Whilst 60% of OAS countries, have implemented Party and Candidate Registration and Election Reporting Systems. The third level of digitalisation corresponds to Digital Identification and Social Media (58%).

Legislative Frameworks

As mentioned above, the first step in forming a trustworthy picture of the cybersecurity landscape is to determine what the capacity is in the region for the digitization of information. The second step is to evaluate the status of the Electoral Legislation in incorporating the use of digital solutions, given that those solutions could mandate the tools that would address the cybersecurity-related risks to the democratic process. In this regard, over 50% of the respondents indicated that their countries had not updated their Electoral Legislation to reflect the digital transformation taking place. Improving the status of the Electoral Legislation is an aspect of cybersecurity that must be addressed, given that it is an indispensable first step towards the improvement of the overall cybersecurity posture.

Interestingly, of the over-90% of respondents who have not updated their Electoral Legislation, most believe that it is essential for the amendments to take place in order to reflect the digitization process, which suggests a level of awareness on the challenge. It is worth noting that almost 75% of respondents noted that they anticipate further digitization. The same percentage of respondents were aware that the more an electoral process is digitized, the more overall security will be required. All this suggests that more financial and Human resources should be identified to enhance the security of the digitization tools and processes.

Cyber-threats Against the Democratic Process

As a result of this new shift to incorporate more and more digital solutions to the democratic process, we must consider the potential issues around the ability to protect democratic processes and, by extension, to protect democracy itself by ensuring each election is fair, free, and secure. In 2018, half of all advanced democracies holding national elections had their democratic process targeted by cyber threat activity. [17] (CCS 2019)

Depending on the country's context, some cyber threats fall under the mandate of different levels of electoral administration. In some countries, cyber threats are not even discussed in the context of elections. Threats to the democratic process are often the responsibility of other state actors. For example, it is often considered the responsibility of law enforcement when there is the possibility of high civil unrest. However, once technology is involved, there is value in thinking through a whole-government approach, with an emphasis on interagency collaboration on cybersecurity in elections, no matter at what level. There can be several benefits to establishing a security or election technology task force leading up to an election, for example. Some countries organize interagency collaboration through dedicated forums such as task forces that meet on an ad hoc basis, while others may have a single task force on election cybersecurity. This interagency approach guarantees that all threats are considered and worked through to ensure the integrity of the election results. Below is a graphic describing the intersection of inter-agency collaboration (e.g., in the form of a task force) with the EMBs as it relates to cybersecurity and elections.

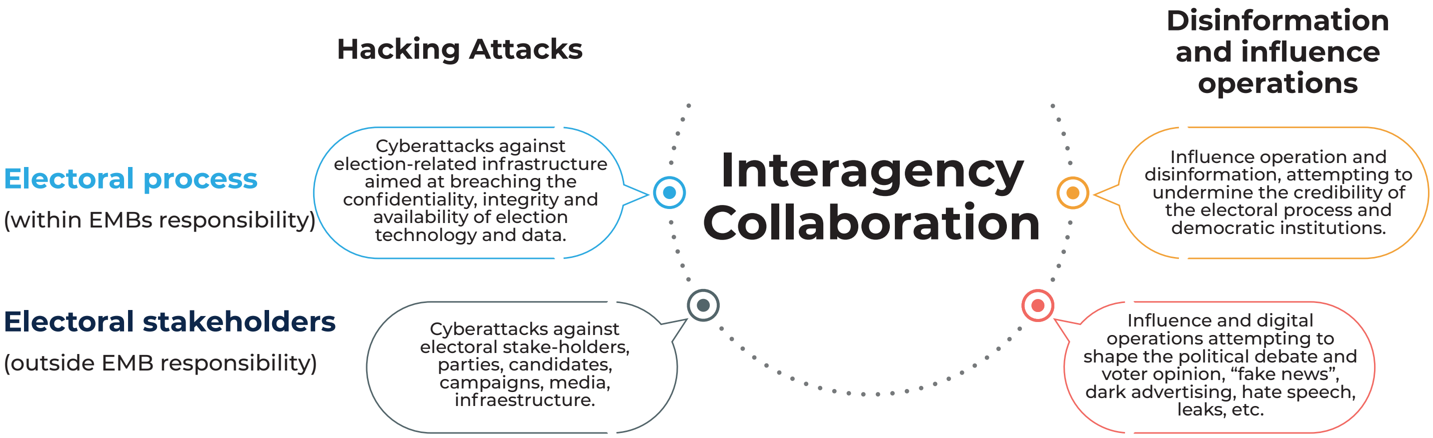

Hacking Attacks
Disinformation and influence operations
Electoral process
(within EMBs responsibility)
Cyberattacks against election-related infrastructure aimed at breaching the confidentiality, integrity and availability of election technology and data.
Interagency Collaboration
Influence operation and disinformation, attempting to undermine the credibility of the electoral process and democratic institutions.
Electoral stakeholders
(outside EMB responsibility)
Cyberattacks against electoral stake-holders, parties, candidates, campaigns, media, infraestructure.
Influence and digital operations attempting to shape the political debate and voter opinion, “fake news”, dark advertising, hate speech, leaks, etc.

Figure 2-Cyber-risks in elections vs EMBs Mandate – Source: International IDEA

The survey results revealed three main findings on cyber threats against the democratic process across OAS member states:

1. More than 55% of the respondents were not aware of any incident. This could be interpreted as an indication that a majority of countries are completely and fully protected against cyberattacks, or it could suggest that there are a significant number of undetected incidents and a lack of awareness of those incidents occurring.

2. Some of the respondents to the survey anticipate an increase in cybersecurity incidents on the democratic process in the coming twelve months. An evident correlation could be observed between population size and awareness: The larger the country, the more anticipated a rise in the expected cyber threats.

3. Almost 60% of the respondents indicated that their country do not have a cybersecurity task force or committee responsible for securing the democratic process. It is perfectly understandable that, depending on the size and resources of each country, the cybersecurity committee might vary in terms of size and capabilities. Still, the very existence of such a taskforce that is able to respect human rights and guarantees should be considered a first step. The design of these bodies should strike the right balance between being effective and also conscious of the potential infringement of rights that may be involved in the actions they take. 50% of the respondents without a cybersecurity task force or an electoral committee with a cyber remit do not expect to have either before the next electoral cycle.

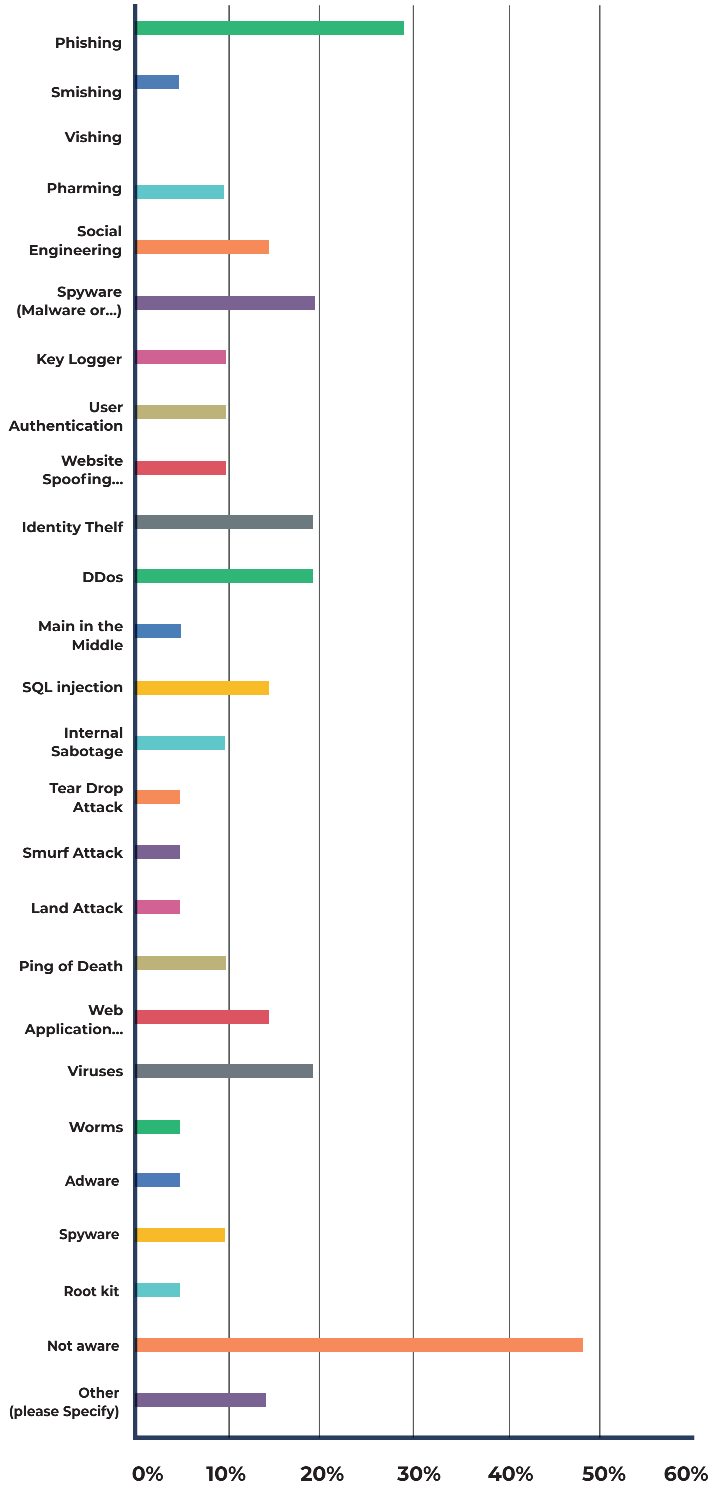


Figure 3 - Types of digital security incidents have been used against the electoral process identified by survey respondents

The three findings mentioned above reinforce the notion that raising awareness on this subject is an urgent need. Cybersecurity needs to become and remain relevant to legislators. Otherwise, the temporal nature of the election cycle means all focus and consideration on cybersecurity in association with the electoral process is concluded until the next pre-campaign, dangerously increasing the chances of undetected successful attacks. It is easy to forget the importance of revisiting useful lessons learned from the overall process in order to avoid repeating those mistakes in the future.

Interestingly, 90% of the respondents strongly agree that better collaboration across government agencies or EMBs and Cybersecurity Agencies would have a positive impact on the overall cybersecurity posture of the electoral processes. It would show that, at an implementation position, there is goodwill. The lack of resources (both Human Capacity and financial), however, remain an inhibitor to progress.

Level of Implementation of Cybersecurity Measures to Protect the Democratic Process

From the results, it emerged that 50% of the respondents indicated they do not have a budget for cybersecurity associated with the democratic process.

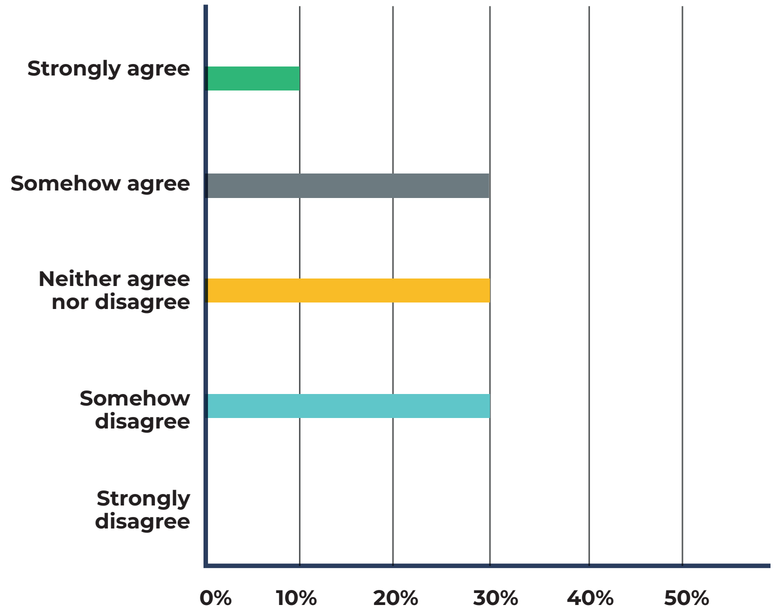


Figure 4 – Question -"Do you agree or disagree with the following statement: 'There are enough resources devoted to cybersecurity for the electoral process in my country.'"

There is a need for further awareness and communication efforts on this subject so that decision-makers can understand the urgency surrounding the inclusion of cybersecurity measures in support of the democratic process, and place cybersecurity at the top of their agendas.

The survey findings also indicate that 35% of the respondents are currently not considering the introduction of incident management processes or contingency plans in the event of an attack for the democratic process. Additionally, more than 40% of the respondents were not aware of coordination efforts between the entity responsible for an election and the local CSIRT when this exists.

Common Challenges

Utilizing the survey results and the challenges faced by stakeholders in the electoral and democracy fields in cyberspace, the following principal categories were identified as common challenges:

- ***Digital Challenges***
- ***Human Capacity***
- ***Political Will***
- ***Legal Framework***
- ***Procedural Measures***

Digital Challenges

The technological or digital challenges can be described as the knowledge or capabilities needed by each stakeholder to pro-actively protect the devices used in electoral activities. For instance, activities such as voter registration, stakeholder communication, the act of campaigning, or even fundraising are subject to threats due to the inability or lack of knowledge stakeholders have in protecting their devices against potential cyberattacks. The lack of awareness and implementation of basic security protocols makes stakeholders prone to phishing, sees them engage with untrusted third parties, and potentially causes them to surrender classified or secret information, which in turn may compromise an electoral system as a whole.

Human Capacity

The Human Capacity challenge consists of the types of actions and activities people perform when engaging with technology in a democratic or electoral setting. These can be associated with errors or the failure to follow cyber-secure protocols, as well as the absence of a high level of scrutiny when implementing these protocols. Common examples include not providing proper and continuous training for staff, having a high-turnover rate within organizations, being unaware of the services available for protection, not having any formal regulations to follow, and, being unable to be vocal on cybersecurity issues. The rules and best practices required to enhance cybersecurity should be in-built into the culture and daily activities of all stakeholders. The absence of best practice, or the lax implementation of best practice, compromise the rigor needed to maintain the credibility of a democratic institution.

Political Will

The need to raise cybersecurity as a part of the political debate is perhaps one of the most pressing challenges for all stakeholders in the region. It is in the interest of all stakeholders to have a greater acknowledgment of the importance of cybersecurity and to ensure that conversations are continually held and regularly revisited to capitalize on more tangible actions on the subject. If there are no active interests, all efforts to enhance cybersecurity may fail.

Legal Framework

Translating active debate into policy and legislation benefits the democratic process and is another fundamental challenge for all stakeholders. It provides for cybersecurity best practices to be enacted into law or policy where necessary. This legal support allows for an organized and coordinated effort that can continually respond to any emerging threats that may compromise democracy and the electoral process. Without this framework, stakeholders will not have sufficient guidance to institute cybersecurity best practices.

Procedural Measures

This effort encompasses multiple layers in which collaboration must be organized and monitored on an ongoing basis. The procedural challenges are complicated due to the fact that cybersecurity, rather than remaining an individual responsibility, becomes a collaborative effort. For instance, stakeholders must be quick to react to attacks and threats and increase their presence and internal audits. If cybersecurity is not integrated into the democratic cycle, the protection of democracy in cyberspace will not be sustainable.

Global Efforts in Cybersecurity and Democracy

As previously introduced, the nature and perception of cybersecurity as applied to democratic processes has evolved throughout the last several years. Initially, the efforts were more technology-based, with an emphasis on "classic cyberattacks" targeting the voting machines or software, the tallying systems, or other coding/cryptography vulnerabilities.[18] (Australia 2017)

Since then, several election interferences have increased the awareness level on information-based attacks such as misinformation, disinformation, fake news, and manipulation of information (as described earlier in the section "The Cybersecurity Connection"). As a result, the same stakeholders have incorporated the topic of information-based attacks in their local dialogue. [19]

As the information-based attacks gained momentum, so did the attention and pressure towards the leading social media platforms and their role in the spread of such attacks. Fortunately, they have taken action towards addressing the problem. Nonetheless, it is critical to implement continued surveillance to guarantee a level of commitment according to the ever-increasing challenges both in a transparent and accountable way. As described in the 2019 Freedom of Expression and the Internet report "it is necessary to insist on the need for their content moderation practices to respect fundamental guarantees of due process, independent authority, transparency, so that they are able to strengthen, enrich, and expand the public debate."[20]

One final aspect worth mentioning when it comes to thwarting information-based attacks is voter education. This document has included the voter as one of the stakeholder profiles. The right to vote implies a responsibility for keeping informed and educated on voting relating matters. There are several tools available to the voter, including the OAS's "Media Literacy and Digital Security" document (OAS 2019) and the various fact-checking initiatives in the region. An educated voter reduces the success of information-based attacks. In essence, all stakeholders of the democratic process would benefit from making an extra effort to facilitate access to educational resources for voters.

Cyber-risk at the International Level

The concrete targets of the cyberattacks against an election are usually the website of EMBs or the voter databases. From a cost/benefit approach, it is often more efficient to launch an attack against these targets, even if the chances of it being successful are very low and focus on subsequently raising doubt about the integrity of an election. [21]

Many attackers know that the resources required to compromise the IT infrastructure of an election are usually fairly high; they either do not have those resources, or they do not see enough return in the investment to make the attack worthwhile. According to a publication by the Government of Canada – 2019 Update: Cyber Threats to Canada's Democratic Process, less than 5% of the cyberattacks against the democratic process targeted such elements of the elections. (CSE 2019)

Even so, the risks of a potential attack against the core IT infrastructure are not negligible, particularly in the event that a country allows the use of remote voting tools. Remote electronic voting, including its deployment, security challenges, and latest developments, is not a topic covered in detail in the present document, but it is worth future attention as its role is relevant and periodically gathers considerable attention.

Traditionally, cyberattacks related to election processes were focused on the electronic devices, software, or network connections involved. However, the intense popularization of social media has allowed for an increased number of information-based attacks, in what could be considered a twenty-first century, refined version of propaganda. According to the Harvard Kennedy School (Harvard 2020), information-based incidents can be categorized as follows:

a. Spreading false or misleading information with the help of fake social media accounts, bots, etc., to discredit candidates, the voting system, or the results.

b. Leaking confidential information about campaigns, vulnerabilities or private communication to undermine the credibility in the system

c. Amplifying or weakening content depending on its source, favoring polarizing or populist opinions trying to change the focus of media and voters, non-relevant topics.

The recent prevalence of this kind of cyber threat also needs to be explained through the appearance of two amplification mechanisms: bots (automatic or semi-automatic actors involving Twitter or Facebook fake accounts) and trolls (individuals who virtually harass, slander or manipulate). (Vilmer 2018) As an example, and according to the same source, there was an incident where a troll factory comprised of a few dozen individuals, which despite its limited size and resources, controlled over 3,800 individual accounts, 50,000 bots, and reached over 150 million people via Facebook and Instagram.

The information-based attacks in the OAS region have also been influenced by the following factors:

a. Economic downturns in several countries in the region.

b. A regulatory framework that is generally less developed and strict than that of Europe or the US.

c. The rapid increase in the penetration of mobile devices, followed by a jump in social media utilization in the region, especially Facebook and WhatsApp. (Vilmer 2018)

While the increase in information-based attacks has been notable in recent years, it is also true that the level of awareness has grown among the stakeholders in the region, with interesting initiatives to prevent disinformation campaigns such as in Brazil, Argentina[22] and Mexico[23] .

Ongoing discussion, debate and raising awareness are essential to be ever-resilient in countering cyber-threats to both elections and the democratic process as a whole. The goal of cyberattacks on elections is to undermine the public's confidence in the democratic process and the electoral system. The missing link in protecting elections from cyberattacks is to fully understand what the "adversary" wants to obtain from the attack.

The Democratic Process: Institutional Infrastructure and their cybersecurity considerations

This document has addressed the security threat to democracy and the processes supporting it. We have seen that the threat is not specific to a region; it is a threat the entire world is grappling with across the political spectrum. The next step is to consider some of the critical components required to facilitate democratic processes. From there, we can consider how to address cyber-risk given varying levels of institutional capacity, and the cybersecurity considerations necessary to mitigate some of this risk.

A Comprehensive Legal Framework

It is essential to consider the legal framework that supports the various institutions that uphold our democracy.

Conceptually, the term Legal Framework for Elections typically refers to a set of laws and rules which include: the applicable provisions in the constitution, the electoral law, laws on political parties as well as regulations related to the electoral law and instructions and regulations issued by the EMBs in charge. Every country and territory's legal framework has particularities when it comes to democratic elections, although there are some key common aspects.

At the global level, for example, Article 21 of the Universal Declaration of Human Rights introduces a set of core principles for democratic elections:

> *"Everyone has the right to take part in the government of his country, directly or through freely chosen representatives.*
>
> *The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures." (UN 1948)*

In parallel, the Council of Europe states that:

> *“The five key principles of electoral law are: universal, equal, free, direct and secret suffrage and they are at the root of democracy.”*[26]

When one thinks about the legal tenants that should be in place, it is worth considering the following:[24]

- Legislation that recognizes the need to provide law enforcement provisions to prosecute digital related crimes impacting the democratic process. These provisions should respect fundamental human rights, such as freedom of expression.

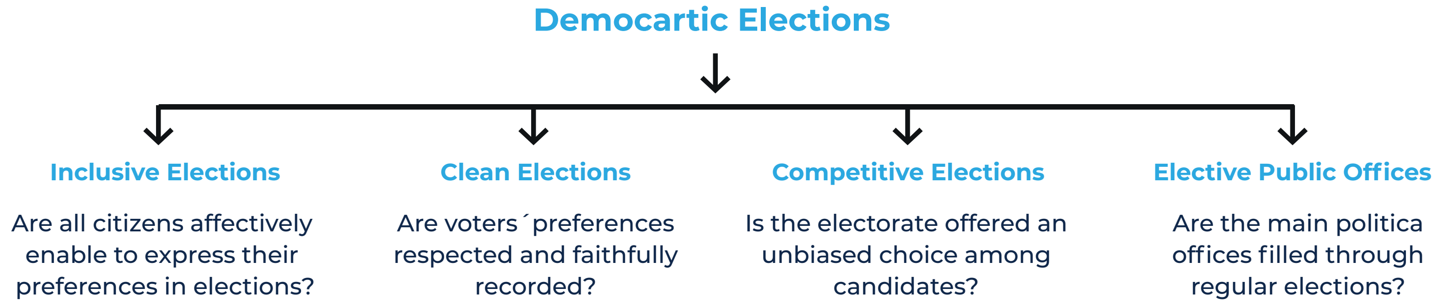
- The maintenance and update of the electoral register, party and candidature registration, and voting registration, including the specific requirements of data handling and data protection.

- Rules on party financing and transparence of funding sources, especially for political advertising.

Additionally, the OAS defines the concept of democratic elections (GS/OAS 2011) when they fulfil the following four basic conditions:

- Inclusive Elections
- Clean Elections
- Competitive Elections and
- Elective Public Offices

Table 1. The Concept of democratic elections I: A first Approximation



Democartic Elections

Inclusive Elections

Are all citizens affectively enable to express their preferences in elections?

Clean Elections

Are voters´preferences respected and faithfully recorded?

Competitive Elections

Is the electorate offered an unbiased choice among candidates?

Elective Public Offices

Are the main politica offices filled through regular elections?

Implementation of Technology in the Democratic Process

To illustrate examples from other countries outside of Latin America and the Caribbean, the implementation of technological solutions in democratic processes became increasingly popular in the early 2000s following the US 2000 General Election scandal concerning punch cards in Florida.[25] During those years, several countries launched e-voting pilots, including France, Germany, the Netherlands, the United Kingdom, and Norway. Each country took a unique approach to the matter, contributing to the ongoing atomization of the technology space.

Some of them, such as the United States, France, and Switzerland, prioritized their non-resident voters. In contrast, others have limited the experiences to the local or regional level, as in the case in Canada and Australia. Several of those countries have since decided to discontinue the pilots, as was the case with the Netherlands, the United Kingdom, Norway, and Germany due to the difficulty in simultaneously securing end-to-end verifiability and privacy.

As an alternative example, however, Estonia has demonstrated steady growth in support of Internet voting solutions, having implemented i-Voting for every binding election in the country for the entirety of the electorate since 2005. (Toots 2016)

In recent years, strong advocates of Internet-based voting solutions, such as Australia and Switzerland, have identified various flaws in these systems and are calling for a gradual and careful introduction of e-voting technologies. (Lewis 2019) Every country is different, and so are the electoral legislations and available cybersecurity infrastructures. What has been valid for one territory is usually not applicable in other cases. A careful approach in terms of the type of election and electorate allowed to use technology for voting is the most advisable option. (Blanco 2018)

Media

Media, including traditional media outlets as well as social media providers, are critical to clear communication. This clear communication becomes even more critical during a cyberattack, and more specifically, a disinformation campaign.   An environment that allows freedom of expression has always been essential to a healthy democracy.

Some of the main functions of the media during an election include providing information on political parties and candidates participating in the process, offering questions for debate, reporting on the voting process, and any other elements that encourage an informed process for the electorate. The impartiality and balanced presentation of the election news coverage—coverage which does not present programs or articles that favor one particular candidate or political party—is important. In other words, media independence should be maintained.

The OAS has worked on strengthening the capacity of media actors in the democratic process and developed a publication Strengthening Electoral Processes and Systems throughout the Hemisphere: The Role of the Media in Electoral Campaigns and the Relationship between Electoral Management Bodies and Political Parties. (GS/OAS 2011) In that document, it was highlighted that:

> *Electoral authorities should develop mechanisms to collaborate with the media to ensure respect for three basic democratic principles: the responsibility to ensure equal access to information, the media's right to inform, and citizens' right to be informed. These rights apply equally to political parties, candidates and even to electoral authorities. Both political parties and candidates have a right to inform the public about their proposals and platforms, and electoral authorities should inform the public about the voting process itself. In carrying out these tasks, the relationship between the media and electoral authorities is clearly an interdependent one.*

More specifically, the OAS recognizes that Electoral Authorities should be especially aware of media advances in the digital age and the appearance of so-called "new media." People are increasingly informed by numerous sources beyond the traditional formats of radio, television, and newspapers. Instead, they are looking to the Internet and other digital media, which has become extremely influential in the way that information is both produced and disseminated.

It is important to recognize that the freedom of the press and a pluralistic mass media system are key elements to guaranteeing free and fair electoral processes. The OAS developed the "Methodology for Media Observation during Elections: A Manual for OAS Electoral Observation Missions," which the various EOMs follow. (GS/OAS 2011) That publication recognizes the important role of the media during electoral processes as, despite the progress observed in the organization of electoral processes in the region, it is crucial to keep in mind that the conditions of access to the media have a significant influence on the conditions to compete in a level-playing field for electoral office.

Community Engagement in Democratic Processes

It is a foundational consideration that any EMBs, or function with a similar responsibility, must uphold the principles of independence and autonomy as the EMBs works through its mandate. In addition to the institutional capacity described earlier, demonstrating independence and autonomy fosters trust and confidence across the institutions and the electorate the EMBs serves.

Both the electorate and the institutions need to have confidence and trust in the independence and autonomy of an EMBs so that they may work together to ensure the successful conduct of any democratic process. It may not be directly clear that collaboration is required here. Still, to ensure the smooth, fair, and transparent conduct of an electoral process, collaboration is essential due to the nature of shared responsibility of national cybersecurity. All stakeholders must understand their roles and responsibilities in an electoral process and the cybersecurity risk attached to it.

Information and Communication Technologies (ICT) influence the day-to-day lives of billions of citizens in the sectors of education, health, finance, and more. Similarly, ICTs are also having a comparable influence and impact in numerous elements of both electoral and democratic processes. For instance, electoral campaigns are run significantly differently; the public accesses news and information through social media platforms, as well as dialogue and debate, takes place predominately online. The engagement with all stakeholders has changed under the influence of ICT, and the resulting digital mechanisms used for democratic processes can lead to challenges, which can in turn influence to various degrees the stakeholders that are integral to the democratic process.

Those charged with the responsibility to manage and support an electoral process must demonstrate independence both from incumbent and opposition parties. The reality of this challenge must not be underestimated. This chapter offers some ideas for EMBs to consider regarding the fostering of trust through transparency and accountability across various identified stakeholders.

It is through solid stakeholder engagement that institutions can begin to mitigate the risk of the threat. The mitigation of risk and creation of trust are the ultimate objectives of engagement with the community and specific stakeholder groupings. The intent of the engagement and its scope should be clearly defined from the beginning. This engagement is an opportunity for the EMBs to be strategic in order to maximize whatever resources that may be available for the elections. There are significant reasons why engagement with stakeholders is key for the good conduct of a democratic process. For example:

1. An EMBs that holds the trust of all stakeholder groups through transparent processes and demonstrable autonomy and independence ensures good conduct within the democratic processes.

2. An EMBs makes it possible to ensure every stakeholder understands their responsibilities as well as those of their peers.

3. An EMBs can share cybersecurity messages and best cybersecurity practices, thus improving the cyber risk profile for the country.

4. An EMBs fosters collaboration amongst stakeholders.

Engagement with identified stakeholders should be sustained throughout the cyclical periods of the democratic process. Stakeholders should always understand why the engagement is taking place; those leading the engagement should be upfront about the purpose and objective of the exercise. One way to do this is to offer an invitation to participate that fully explains the intent of the engagement right at the start. If stakeholders continue to remain engaged, the EMBs should keep the scope and objectives of the engagement exercise at the forefront of every communication between the EMBs and the relevant stakeholders.

Whether a nation chooses to establish a separate entity with responsibility for democratic processes (see the summary for all consultations in Annex II) or simply elects a function within government, we can assume that there is the intent to follow good practices in order to foster the perception of independence across an electorate. It is necessary, if not vital, to uphold the principle of independence for this responsibility because it provides for the establishment of voter confidence in the democratic process. Without the confidence of the voter in the process itself, the engagement of those same people is likely to be minimal, resulting in a disengaged electorate, which is a sign of an unhealthy democracy.

The main objective for any EMBs is to hold a consultation that is premised on transparency and accountability. In order to reach this objective, the identified authority must establish a position of trust across all identified stakeholders and different sectors they each represent.

It is through sustained long-term engagement and clear communications throughout the entire cycle of a democratic process that an entity in-charge or function in-charge can ensure there is no perception of any bias within its operations and retain autonomy and independence.

Engaging with Stakeholders

In a governmental context, cybersecurity has largely been associated with the intelligence communities, sometimes seated within the military. As it is becoming more understood by the world, and there is an acceptance that cybersecurity is not solely a technical consideration for intelligence communities; it instead requires a multidisciplinary approach with people at the core. We have noticed an increase in entities or agencies being set up outside of traditional intelligence communities in order to enable the entity to engage with the public more directly.[26]

It is not often the case for an entity of this kind to exist within the individual countries of the world. The existence of an organization focused on cybersecurity is not a blanket provision that will solve all of the problems addressed in this document. In some cases, the geography is so disparate that a national agency may not be the right answer to the challenge of cybersecurity. In the absence of an agency as described above, the EMBs may seek to collaborate with other accredited cybersecurity professionals to engage stakeholders in the run up to an election period or part of the continuous engagement throughout the lifecycle of the democratic process. Collaboration is essential, especially if a separate entity is not established to manage and oversee the conduct of a democratic process because time and resources will be dramatically impacted. Through collaboration, the outreach could be more effective and efficient by including expertise in cybersecurity at the start.

Essential Stakeholders to Consider

It is difficult to be comprehensive when deciding which stakeholders should be included in an engagement program. There is no single listing that can serve a group of countries as diverse as the membership of the Organization of American States. The following is a categorization that may suggest the breadth of stakeholders that should be consulted and invited to participate in such a program of engagement and communication. A more detailed description of the stakeholder groupings can be found in Annex I.

- ***Political Actors***
  Political Candidates, as well as Political Parties, must be part of the cybersecurity conversation as it relates to the democratic process. Not only must they become aware of the risk, but they must ensure that they operate with a data mindset and an understanding of the proper conduct and execution of political campaigning. They must be made aware of insider risk and ensure that best practice is adopted in terms of all matters relating to data protection and privacy.

- ***General Public***
  It is important to ensure the general public, the 'voter,' has a basic understanding of cybersecurity risks and the essential skills required to be an informed digital citizen. Direct engagement with the general public should not be demographically targeted. A general

increase in the awareness of the risk and threat across the board should be considered and implemented where possible. The involvement of civil society in this regard would be of considerable benefit to raise awareness amongst the general public.

• ***Government actors involved in the process***

Civil Servants who have some responsibility in the conduct and execution of a democratic process, but who may not necessarily be cybersecurity experts or hold basic knowledge of cybersecurity risk, are a valid stakeholder group. By engaging them in a conversation about the risk and crisis management planning, they will be better equipped to face a crisis should it occur. This grouping could also include elected representatives and elected officials who may not be aware of the cybersecurity risk they face.

• ***Media and Internet service Providers – Print, Radio, Broadcast***

Media outlets must be included in any engagement program so that they can be better informed on the risk landscape. They must be prepared to plan internally for any cybersecurity attack that they may face during the actual democratic process and in time preceding an election. The media (inclusive of social media) contribute significantly to public debate both online and through traditional broadcast channels, so their involvement is necessary should be considered part of the region's critical infrastructure.

• ***Incident Response Organizations***

- Incident Response Teams

It is crucial that the national incident response capability, if it exists, is part of this conversation. Not only is it important for the national CSIRT to understand its role and responsibility on special occasions such as general elections, but it is of greater importance for the critical national infrastructure stakeholders to understand the role of the national CSIRT team. It is best to engage also smaller incident response teams, such as regional teams and sectorial ones, so in their preparatory process and scenario setting, a chain of command or chain of communication can be established.

The national CSIRT entity could hold their own consultations with their constituents, reminding each constituency of their specific terms of reference for each team. This activity would encourage clarity on referrals to responders and Law Enforcement Agencies. Constituency consultations could also drive crisis management planning with scenario exercises deployed to ensure the sustainability of plans. Through the national CSIRT agency consultations, there will be an increased urgency to establish robust links between the constituents and various media houses to ensure message handling in the case of an incident.

- Critical National Infrastructure (CNI) providers

Typically, CNI is considered to be service providers of transport, utilities, and border control. It is important to engage with these service providers to ensure that they are aware of the cyber risk in and around any democratic process. It is important to encourage stakeholders to engage with cybersecurity experts and run regular audits and crisis scenarios to effectively draft up a crisis management plan in the instance one of their services is attacked during a period of democratic importance.

Engagement with this sector, either directly or through the national CSIRT agency, should be used to encourage crisis management planning, audit checks, and regular scenario exercises focused on democratic processes (elections or referenda).

The value in ensuring all these various stakeholders are part of the engagement plan lies in establishing a mutual understanding of the roles and responsibilities for each actor in the process. It helps illustrate the roles and responsibilities of the various actors and when or how it is of the essence to escalate to the next reporting line. Communication may lead to the identification of gaps of information across the stakeholder groupings.

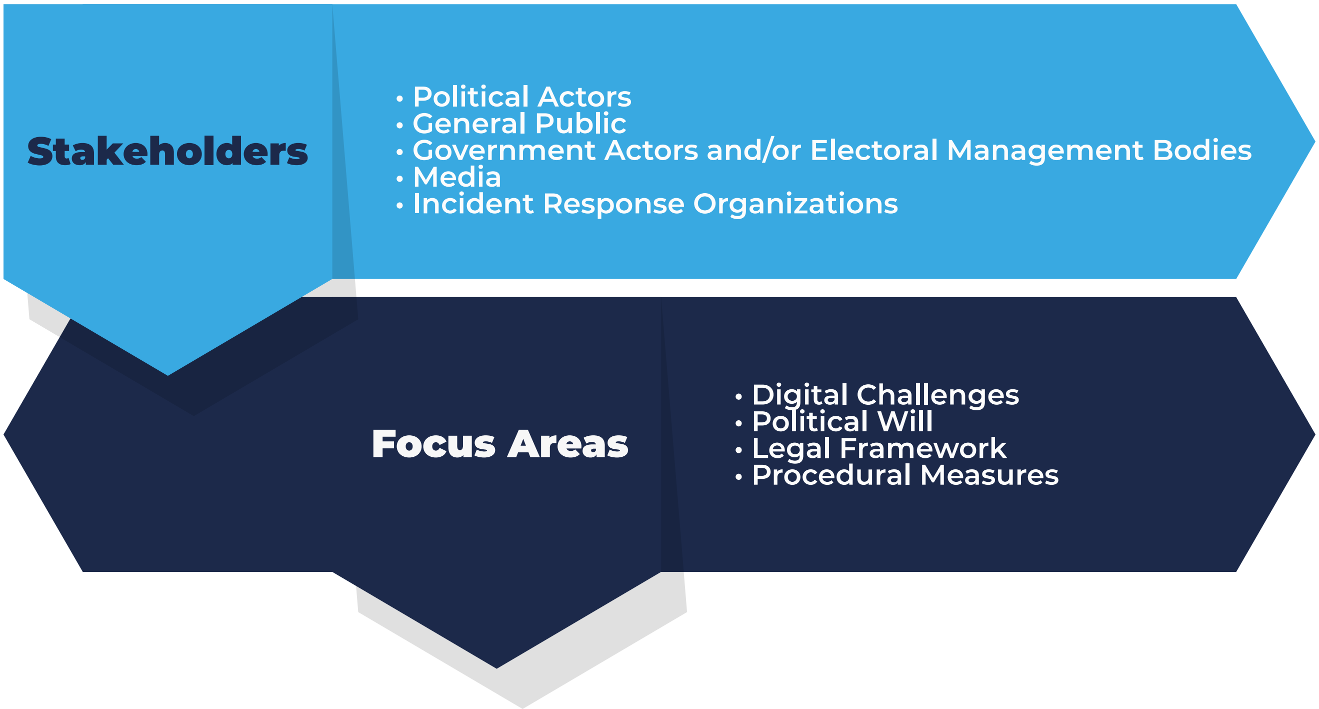
Facilitating the Dialogue and Considering Next Steps - Recommendations

These recommendations were developed while taking into account the process outlined throughout this document. The process included a careful review of the cybersecurity threat landscape in the democratic process, a reflection on the power of information in the digital era, and the identification and engagement of stakeholders and the associated challenges, which have been broken down into:

- Digital Challenges
- Human Capacity
- Political Will
- Legal Framework
- Procedural Measures

The recommendations were then defined and classified by stakeholder grouping with the main purpose of facilitating the reader to identify the stakeholder grouping and have a guideline of what steps to consider in order to increase their cybersecurity readiness.

A summary table on the logic and different categories of the list of recommendations is shown below:



Stakeholders

- Political Actors
- General Public
- Government Actors and/or Electoral Management Bodies
- Media
- Incident Response Organizations

Focus Areas

- Digital Challenges
- Political Will
- Legal Framework
- Procedural Measures

Since certain stakeholders share some characteristics, part of the recommendations are present in more than one profile, especially in matters regarding awareness, training, or independence.

Digital Challenges

Digital challenges can be described as the knowledge or capabilities needed by each stakeholder to pro-actively protect the devices used in electoral activities and the democratic system.

Political Actors

1. Be aware of what the best cybersecurity practices are for all devices you use, such as mobile devices and laptop or desktop computers.

2. Be aware of the best cybersecurity practices are for software, in particular web browsers and email programs.

3. Understand local data protection and privacy regulations, particularly as they relate to data stored about local constituents.

General Public

1. Be aware of what the best cybersecurity practices are for all devices you use, such as mobile devices and laptop or desktop computers.

2. Be aware of the best cybersecurity practices are for software, in particular web browsers and email programs.

3. Learn about the tools and services that exist to verify information during an election cycle, such as the OAS's paper "Media Literacy and Digital Security."

Government Actors or EMBs

1. Be aware of what the best cybersecurity practices are for all devices in use by EMBs members, such as mobile devices and laptop or desktop computers.

2. Be aware of the best cybersecurity practices are for software, in particular web browsers and email programs.

3. Consider key information infrastructure systems critical assets and segregate them, enabling redundant access control (electronic and analog).

4. Establish relationships with social media and Internet service providers to ensure that information can be 'fact-checked' or verified and corrected as needed.

5. Help identify more financial and Human resources to enhance the security of the digitization tools and processes.

IRO

1. Provide standards and guidelines for key stakeholders on minimum cybersecurity baseline such as Implement 2-Factor Authentication (2FA), password protection best practices, software/firmware updates, and conduct thorough penetration tests and code audits.

2. Establish talent recruitment for cybersecurity specialists.

Human Capacity

The Human Capacity challenge consists of the types of actions and activities people perform when engaging with technology in a democratic or electoral setting. These can be associated with errors or the failure to follow cyber-secure protocols, as well as the absence of a high level of scrutiny when implementing these protocols.

Political Actors

1. Implement password best practice, as well as keep software/firmware versions updated and consider adopting Cloud Solutions from a reputable vendor to aid in end-to-end security.

2. Inform CSIRT/IRO and EMBs your official social media accounts and any suspicious communication, event, or incident.

3. Establish strong ties and relationships with social media and Internet service providers. Identify collaborators (where necessary) and set up a collaborative partnership to establish an engagement program where necessary.

4. Implement 2-Factor Authentication (2FA) for Internet supported devices and accounts.

General Public

1. Keep informed of the threat landscape through official channels and report to the CSIRT/IRO and EMBs of any suspicious communication, event, or incident during the electoral process.

2. Consume relevant information from multiple sources on democratic processes.

3. Verify election information before sharing on social media.

Government Actors or EMBs

1. Implement good 'cyber hygiene' such as 2-Factor Authentication (2FA), password good practices, and timely software and firmware updates, and manage the supply chain for information systems that support democratic processes.

2. Given that auxiliary systems are increasingly targets for cyberattacks, avoid "critical nodes of failure" that, if compromised, take down the entire system such in the case of a DDoS attack.

3. Develop mechanisms to collaborate with the media to ensure respect for three basic democratic principles: the responsibility to ensure equal access to information, the media's right to inform, and citizens' right to be informed.

Media

1. Advise CSIRT/IRO and EMBs of your official social media accounts and inform CSIRT/IRO and EMBs any suspicious communication, event, or incident.

2. Monitor incidents facilitated by bots, trolls, and automated publishing tools.

3. Enhance fact-checking through official sources or trusted parties.

4. Establish strong ties and relationships with social media and Internet service providers and maintain communication channels to facilitate the reduction of misinformation to the public.

IRO

1. Implement a unified approach to data integrity, in compliance with cybersecurity standards, and maintain controls over technological solutions and the data.

2. Implement technologies compatible with the EMBs systems and conduct combined security trials, ensuring technical compatibility with EMBs digital solutions.

3. Prepare a code of conduct to be signed by staff and associates regarding social media platforms and implement policies (that adhere to privacy principles) on network monitoring, log files analysis, user privilege segmentation, and a no-black-box approach to reduce insider threats.

Political Will

The need to raise cybersecurity as a part of the political debate is perhaps one of the most pressing challenges for all stakeholders in the region.

Political Actors

1. Make cybersecurity a national security priority with a public-private approach. This level of priority will ensure sustainability throughout cyclical periods allowing for increased intensity during an election period.

2. Keep the topic of cybersecurity in democratic processes “trending” to counterbalance the tendency for it to be overlooked outside of an electoral period. Introduce cybersecurity and promote information manipulation prevention as an integral part of the compulsory education curriculum.

3. Collaborate to develop, build, and sustain thorough data protection regimes and commit to the safeguard of Internet neutrality.

4. Support the creation of official communication channels to update real-time on democratic process-related incidents (both hacking and information manipulation). Take into account cyberattacks and information manipulation to other democratic processes leading up to their election period.

5. Commit to the establishment of a specific group of judges and prosecutors specialized in cybersecurity and information manipulation to solve urgent matters within 48 hours.

General Public

1. Get involved in reputable Civil Society cybersecurity-related movements to promote transparency and openness during democratic processes.

2. Leverage influence by being an active part of the political debate, legislative consultations through Civil Society

Government Actors or EMBs

1. Work with elected authorities in non-electoral periods to create awareness regarding the importance of cybersecurity.

2. Maintain independence from political, lobby, and large corporations' pressure.

Media

1. Actively pursue your government to increase resources for capacity building and training for media actors in cybersecurity.

2. Keep the topic of cybersecurity in democratic processes topic "trending" to counterbalance the tendency to be overlooked outside of the electoral period through the publication of articles and other relevant topics to keep the public informed.

3. Remain vigilant in the safeguard of Internet neutrality and freedom of speech.

4. Enhance fact-checking through official sources or trusted parties and participate in internationally recognized rankings for evaluating media reliability.

IRO

1. Build trust with voters and the different media through permanently available communication channels.

2. Secure computer resources, regardless of the political party.

3. Collaborate with key stakeholders to develop, build, and sustain thorough data protection regimes.

4. Delimit political interference in the IRO.

5. Appoint politically independent chief auditor and cooperate with international and regional bodies and/or independent observers.

Legal Framework

Translating active debate into policy and legislation benefits the democratic process and is another fundamental challenge for all stakeholders.

Political Actors

1. Strengthen legal frameworks for the protection of personal data, transparency of election advertising, and information manipulation[27].

2. Revise the relevant legislation to address cybersecurity concerns in democratic processes.

General Public

1. Stay aware of any cybersecurity issues being debated in all levels of government and offer feedback to your representative.

Media

1. Take an active part in the legislative consultation processes to introduce cybersecurity-related regulatory updates

IRO

1. Introduce the required legal framework for cybersecurity and risk mitigation in democratic processes based on the latest available version of recognized standards such as the ISO 27K family.

2. Establish an internal group in charge of presenting legal improvement proposals and take part in the electoral legislative update committees.

3. Develop legal instruments to support the establishment of a permanent framework for cybersecurity such as a Taskforce and a dedicated cybersecurity budget.

Procedural Measures

This effort encompasses multiple instances in which collaboration must be organized and monitored on an ongoing basis. The procedural challenges are complicated due to the fact that cybersecurity, rather than remaining an individual responsibility, becomes a collaborative effort.

Political Actors

1. Establish a clear structure in the newly created independent body, so that this body can be agile in the responses to cybersecurity attacks.

2. Establish a reporting system to report any suspicious behavior or potential campaign cyber incident.

3. Support civil society and quality journalism, regardless of the ideology, to ensure transparency and openness for debate during any democratic process.

General Public

1. Quickly report to the EMBs/IRO any suspicious behavior or potential incident/manipulation campaign

Government Actors or EMBs

1. Conduct periodical hacking and information manipulation simulations coordinated with the CSIRT/IRO and the media as part of the training activities.

2. Jointly with the Agency responsible for cybersecurity design and implement a comprehensive Risk Assessment and Management policy and protocols.

3. Design, implement, and update a Risk Mitigation Plan well in advance of the elections with the advice from the IRO.

4. Increase internal controls/audits to minimize insider threats and establish a secure communication plan with an updated Content Management System (CMS) and share it with the CSIRT/IRO.

5. Develop an engagement program and associated communication plan and budget. This program would include a communication protocol for attacks, enhancing transparency as much as possible, without being counterproductive in terms of leaking details that might help potential intruders.

6. Implement measures for responsible disclosure of cyberattacks and incidents of information manipulation attempts.

7. Coordinate with CSIRT/IRO to increase official website resilience against cyberattacks and establish a permanent working group with the EMBs to enforce cybersecurity protocols. This working group should coordinate with the media group's representatives (traditional media, private corporations, civil society, and multilateral organizations) to keep them updated in real-time about relevant news/incidents.

8. Implement security-cross checks to critical infrastructures and implement strict access controls to physical cites of information systems, especially servers that support democratic processes.

Media

1. Digital platforms should consider democratic processes as a profitable business unit subject to conforming to rigorous ethics.

2. Carefully adhere to information and data privacy standards.

3. Create and maintain an official database of fake accounts and non-reliable media groups, social media profiles, private companies, and organizations.

4. Quickly report to the EMBs/IRO any suspicious behavior or potential incident/manipulation campaign.

5. Establish a relationship with EMBs and IRO to keep them updated in real-time about relevant news/incidents if discovered to encourage swifter response to incidents.

6. Encourage digital platforms to cooperate with independent researchers and academia to improve the response to information manipulation.

7. Improve the detection and response timing to information manipulation, especially regarding bots, netbots, and anonymous accounts.

IRO

1. Design, implement, and update a detailed cyber-surveillance protocol for both cyber threats and information manipulation activities.

2. Implement early detection mechanisms and coordinate with the EMBs risk mitigation and cyber response policies.

3. Jointly with the EMBs design and implement a comprehensive Risk Assessment and Management policy and protocols

4. Create a designated Incident Response Team for democratic processes and develop communication plans that are targeted per stakeholder grouping with information on cybersecurity incidents and information manipulation attempts.

5. Establish cybersecurity awareness messaging campaigns to keep the public informed and create a designated person/group to monitor the occurrences of misinformation and reporting.

6. Establish a permanent working group with media groups' representatives (traditional media, private corporations, civil society, and multilateral organizations) to keep them updated in real-time about relevant news/incidents.

7. Establish a permanent working group with the EMBs to enforce cybersecurity protocols.

8. Conduct hardening exercises and information manipulation simulations coordinated with the EMBs and the media as part of the training activities to improve cyber incident response plans.

Conclusion

In short, three predominant challenges emerge in the region:

- **Awareness** for every stakeholder involved in the democratic process.

- **Legislative frameworks that make provisions** for the coordination of cybersecurity policies in democratic processes with a sense of urgency, as cyber threats in the field are clearly on the rise.

- **Continuity:** The inherent nature of a democratic process tends to put the cybersecurity aspect of it in the spotlight before the election and on Election Day, losing most of its visibility during the rest of the democratic cycle.

The findings of the OAS survey suggest that there is an increasing awareness of the threat landscape across the Americas and the Caribbean regarding the need to improve cybersecurity practices and the associated implications of cyber threats for an election. Awareness is increasing among policymakers, though limited resources mean that progress is limited to the political cycles alone. It is important that the mind-set around political planning shifts to a more encompassing holistic approach. In this context, the need for a closer examination of this subject is not only recommended but needed for the region.

Much of the threat and risk may be mitigated through traditional legislative, technical, and operational approaches, as well as by supporting increases in the capabilities and capacities of each stakeholder group. In order to strengthen the integrity of the democratic process, it is also important to encourage an increased awareness and real understanding of the benefits and the risks that technology brings to the table among society at large. This awareness, together with the skills to be able to decipher events around political campaigns, is critical to supporting democracy in our region. Conclusively, Democratic Processes are strengthened by ongoing dialogue between the various stakeholders, during and even outside the electoral period.

The media as a sector has an opportunity to encourage and foster independent and fact-based debate in order for any democracy to function in a healthy way. If the independent media increases their understanding of the cyber risks our democracies are facing, ensuring their own cybersecurity profile is as resilient as can be, they can be a driving force of the fact-based debate that the world so desperately needs.

Lastly, it is important to acknowledge that progress is dependent on there being both Human Capacity and financial resources in order to drive the ambition of better cybersecurity practices in the democratic process. It is important for there to be political will in order for the adequate or appropriate legislative frameworks and budgets assigned to counter the increasing threat to the core of our democracies.

Annex I

Stakeholders

mong the stakeholders identified we include: (a) Political Actors, (b) General Public, (c) Government Actors and/or EMBs, (d) Media, and (e) Incident Response Organizations (IRO). The following provides a detailed description of each stakeholder group identified for the purposes of this document and their role in the democratic process.

Political Actors

Political Actors are considered as elected officials, or any person means elected at a general or special election to any public office, by the vote of the appropriate electorate, political parties, and political party officials. Their role is indispensable in that they are the only ones responsible for proposing, enacting, and approving legislative changes. Their power is usually curtailed by:

- The constitution.

- An independent judiciary with the power to declare legislative acts unconstitutional (e.g., constitutional court, Supreme Court).

- Deliberative initiatives or direct popular measures (e.g., initiative, referendum, recall elections). However, these are not always binding, and legal power usually remains with representatives [wiki].

General Public

General Public covers ‘voters,’ who ‘are people who have the legal right to vote in elections, or people who are voting in a particular election’ according to Collins dictionary.[28] They are the ultimate holders of a territory’s sovereignty, and as such, the final goal should be that of keeping them away from manipulations and attacks, so they can exercise their right freely.

Government Actors and/or Electoral Management Bodies (EMBs)

An EMBs is “an organization or body that has the sole purpose of, and is legally responsible for, managing some or all of the elements that are essential [to] conduct elections and direct democracy instruments—such as referendums, citizens’ initiatives and recall votes—if those are part of the legal framework.”[29] Including:

- Determining who is eligible to vote;

- Receiving and validating the nominations of electoral participants (for elections, political parties and/or candidates);

- Counting and tabulating the vote, among others.

The guiding principles [of these types of entities] should be independence, impartiality, integrity, and transparency.

An EMBs can manage additional aspects such as media coverage, educational activities, or dispute resolution. Nonetheless, if the EMBs related activity does not include any of the aforementioned essential aspects, it cannot be considered as one and should be contemplated as a media coverage surveillance commission, a civic education commission, or an electoral court, respectively.

Depending on the territory, the EMBs can be (and probably should be) part of the Commission responsible for Cybersecurity in the Democratic Processes. (IFES 2018)

Media

The digitization of our society, especially through the emergence of social media, has had a huge impact on the role the media play in democratic processes.   Media groups wield great influence over public opinion, and this influence can be due to the representation of a particular group of people, the resources and prestige, the reach, or the access to financial means.

We have included in this category social media platforms such as Facebook, Twitter, Instagram, WhatsApp, Telegram, etc. Given that their cooperation is also indispensable in terms of actively and quickly collaborating with Governments, EMBs and CSIRT in the event of an attack. In that regard, initiatives like Facebook's Mark Zuckerberg's hearing in 2018 related to the Cambridge Analytica and the reported 5 billion USD fine to be applied certainly sets the tone for a future in which Tech Giants have to implement better privacy measures to protect the user and its related data.

Incident Response Organizations (IRO)

For the purposes of this document, an Incident Response Organization includes a CSIRT (Cybersecurity Incident Response Team) or CERT (Computer Emergency Response Team) is an expert group in charge of dealing with computer security incidents. It can be of public, private, or hybrid (public-private) nature. Many of the most relevant CSIRTs, including the public ones, are part of the FIRST (Forum of Incident Response and Security Teams) organization.[30]

Concerning the cybersecurity of Democratic Processes, the role of a CSIRT is critical to give a response in a timely and technically sound manner to any event that could arise.

The CSIRT team can be embedded into an Election Security Committee (ESC) or Task Force, which has the ultimate responsibility to safeguard the integrity and safety of the democratic process.

The establishment of correctly designed and implemented dynamics and tasks between the EMBs, the CSIRT, and the technology vendors will have an enormous impact on the overall cybersecurity of the electoral processes.

Annex II

Summary of Activities

Workshop I

Date: November 29 - 30, 2018

Location: Mordan Hall, St Hugh's College, Oxford, United Kingdom

Number of Attendees: 19

Countries involved: Antigua and Barbuda, Barbados, Belize, Brazil, Colombia, Costa Rica, Guatemala, Guyana, Jamaica, Mexico, Nicaragua, Paraguay, St Vincent and the Grenadines, Suriname, and Trinidad and Tobago.

Main findings:

- Identification of member states' common points regarding the Democratic Process: steps of the process (e.g., voter registration database, voting devices, tally systems, results report), democratic actors (e.g., constituents, politicians, parliamentarians, electoral authorities), critical infrastructure, threats, among others. By defining the common points, it would be clearer the scope of the guideline.

- Roles and responsibilities: participants highlighted the importance of including the roles and responsibilities of the different national actors with regard to the cybersecurity of democratic processes. Additionally, they stressed the importance of discussing cooperation and collaboration mechanisms.

- Risk-based approach that considers not only the technical aspects, but also social ones.

- Importance of confidence and trust in the system: participants mentioned that "building trust" is a key for the democratic process, and that this should be somehow reflected in the title of the document. The word "resilience" was also brought to attention.

- Good Practices + General Principles: the guideline could include experiences from the region and other countries as a good practice on cybersecurity and democratic processes. Some participants also suggested that basic principles to promote cybersecurity on the democratic process should be considered.

- Regional guideline adaptable to national and local needs: Although the guideline will be written to a regional audience, participants suggested that the guideline could be used as a model to create their national and local cybersecurity guide for democratic processes.

Workshop II

Date: February 27-28, 2019

Location: Oxford Martin School, University of Oxford

Number of Attendees: 30 (10 F and 20 M)

Countries involved: Antigua and Barbuda, Barbados, Bolivia, Chile, El Salvador, Guatemala, Jamaica, St Lucia, St. Vincent and the Grenadines, The Bahamas, and Trinidad and Tobago.

Main findings:

- Risk assessments should go beyond elections and also examine how they are financed and communicated.

- Building trust – collaboration and best practices.

- Emphasis on the internal operations of the parliamentarians and how they manage their own information.

- Electoral processes should be considered a Critical Infrastructure.

- In relation to AI- it is becoming an invisible facilitator. AI removes Human Capacity responsibility and it is important that we as Human Capacities do not lose our skills and capabilities.

- Need to think about the democratic process holistically, including the supply chain for electoral processes, including third party systems.

- One of the risks if cybersecurity is not enforced is not just the possibility of the system being hacked but that trust in the system is eroded.

- The guide should have an assessment tool, security protocols; this should cover all the players in the electoral process including the support agencies such as the first responders, regional authorities inclusive of the media. Should have codes and rules for observing agencies.

- It's one person- one vote. So hacking is not the only issue but the ability to have multiple votes. The guide needs to be simple and clear, especially if the legislatures themselves may be older and not adapted to technology. There must be recommendations for data protection laws and cybercrime laws.

- The laws are not current and needs updating. There is no finance campaigning laws.

- Media regulations may need to be updated but you won't be able to always change.

Workshop III

Date: March 18-19, 2019

Location: OAS Main Building, Washington DC, US

Number of Attendees: 13 (3 F and 10 M)

Countries involved: Antigua and Barbuda, Brazil, Canada, Colombia, Grenada, Mexico, Paraguay, and United States.

Main findings:

- The participants identified fake news, misinformation, social engineering, and denial of service and malware attacks, among others, as some of the most pressing risks for the electoral processes.

- In terms of solutions, the participants emphasized the importance of implementing communication policies, allocating of a specific budget to address cybersecurity concerns, and developing a risk-based approach in order to combat fake news, misinformation, and cyberattacks, as well as an increased coordination between all relevant parties.

- Intervention needs to be well coordinated and maybe an implementation of a common center with key personnel.

- Participants agreed on the need of a risk matrix to identify what is necessary to formalize procedures based on documented procedures. It would be useful for an impact evaluation, adopted control measures and the implementation of plans for improvement.

- Should include terms and define what is embracing (e.g., cyber does not include fake news).

- Should include misinformation, fake news and social media topics.

- Recommendations on surveys: countries should consider extending to a longer time lapse the dissemination of surveys.

- Use of civil society for the technological audit process of the system (shared responsibility, more trust in the process).

- Stablish which will be the audit institutions (citizenship, experience, technical capacity, etc.).

- Should include importance of verification of identity.

- Importance of a multiregional nature: to face the differences among the region and adapt to each country's reality.

- Importance of the use of technology in a legal framework.

- ISO 2705: Risk analysis is general and should set the basis. The guide should include a catalog/ check list to have a list of threats.

- Define a clear Role of the EMBs in Cybersecurity

- Create check list or Incident Respond Procedure that indicate how to escalate threats especially when it involves the National Security Forces or Police. What happens when you detect a threat? (include check list).

Webinar

Date: July 11, 2019

Location: https://vimeo.com/347556001

Number of Attendees: 67

Countries involved: Antigua and Barbuda, Argentina, Barbados, Canada, Chile, Colombia, Costa Rica, Dominica, Dominican Republic, Ecuador, Spain, United Kingdom, Guatemala, Honduras, Jamaica, St Kitts and Nevis, Republica de Moldavia, Mexico, Panama, Peru, Suriname, Trinidad and Tobago, United States, and Uruguay.

Main findings: The main lesson learned was the identification of critical stakeholders. Discussion also held a representative of the Commonwealth Secretariat who was a participant in the webinar.

Face-to-Face

Date: 25-26 July, 2019

Location: Washington D.C., US

Number of Attendees: 5

Countries involved: N/A

Main findings: During this session with the consultants who are developing the Guide, we discussed chapter by chapter the findings and main discussion points to be included in the guide. Concrete feedback on the proposed chapters was provided including recommendations to ensure that the guide aligns to the OAS pillars on democracy and Human Capacity rights. The input received in addition to the survey results was incorporated into the updated draft.

Workshop IV

Date: September 30 – October 1, 2019

Location: Hyatt Regency Hotel, Port of Spain, Trinidad and Tobago

Number of Attendees: 40 (19 F and 21 M)

Countries involved: Antigua and Barbuda, Barbados, Belize, Chile, Colombia, Dominica, Ecuador, Grenada, Guyana, Mexico, Nicaragua, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

Main findings:

- There is a need to have a stand-up cybersecurity team during election

- Media independence is critical

- Social responsibility and awareness of the issues is needed

- Capacity building should be sustainable and long term for actors within the democratic process

- There should be a mechanism to implement the best practices once the guide is published

- Technology literacy of the citizens, elected representatives, etc. is critical

- Skilled personnel in digital security are needed in the democratic process

- Some participants challenged that there should be a process of strengthening cybersecurity instead of responding to incidents after the fact.

- There needs to be a balance between technology, legislation and civil liberties such as freedom of expression

- There is also a need to balance the right to information and the role of media and the liberties

- Elected representatives should consider:
    - Managing their social media presence
    - Interference of state actors
    - Legislation to address online interface with representatives
    - Enabling capacity through legislative provisions
- Voters:
    - Any threat to the confidence of the EMBs is a political threat
    - There needs to be protection in the legislation for voters when there is a breach

Annex III

Bilbiography

“2018 CIRA Canadian Internet Security Survey – Spring edition,” Canadian Internet Registry Authority, https://www.cira.ca/resources/cybersecurity/report/2018-canadian-cybersecurity-survey-spring-edition.

“2018 CMO Cybersecurity Survey: Key Findings,” Cyberthreat Alliance, June 2018, https://www.cyberthreatalliance.org/wp-content/uploads/2018/06/2018-Cybersecurity-Survey-Key-Findings_Final_06222018.pdf.

“2018 Deloitte-NASCIO Cybersecurity Study - States at risk: Bold plays for change,” a joint report from Deloitte and the National Association of State Chief Information Officers (NASCIO), 2018, https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/DI_2018-Deloitte-NASCIO-Cybersecurity-Study.pdf.

“2018 HIMSS Cybersecurity Survey”, Healthcare Information and Management Systems Society, 2018, https://www.himss.org/2018-himss-cybersecurity-survey

“2018 UN E-Government Survey 2018,” United Nations, 19 July 2018, https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.

“2019 Internet Security Threat Report,” Symantec, February 2019, https://www.symantec.com/security-center/threat-report.

“Cisco 2018 Annual Cybersecurity Report,” Cisco Corporation, February 2018, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

“Compendium on Cybersecurity of Election Technology,” European Commission, 2018. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645

“Cybersecurity: Protecting Local Government Digital Resources”, International City/County Management Association and Microsoft, 25 October 2017. https://icma.org/cyber-report

“The Cybersecurity Campaign Playbook, European Edition,” Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2018. https://www.belfercenter.org/publication/cybersecurity-campaign-playbook-european-edition.

“Cybersecurity regained: preparing to face cyber-attacks - 20th Global Information Security Survey 2017-2018,” EY, 2017, https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf.

Defending Digital Democracy Project, Harvard Kennedy School, Belfer Center for Science and International Affairs, accessed 16 February 2020, https://www.belfercenter.org/project/defending-digital-democracy.

“Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe”, Organization of American States, 2018, http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

“Guidelines for reviewing a Legal Framework for Elections,” second edition, OSCE Office for Democratic Institutions and Human Rights, 2013, https://www.osce.org/odihr/elections/104573?download=true.

“INTER-AMERICAN DEMOCRATIC CHARTER (Adopted by the General Assembly at its special session held in Lima, Peru, on September 11, 2001),” Organization of American States, 11 September 2001, https://www.oas.org/OASpage/eng/Documents/Democractic_Charter.htm.

“International Electoral Standards: Guidelines for reviewing the legal framework of elections,” Institute for Democracy and Electoral Assistance (IDEA), 1 June 2002, https://www.idea.int/es/publications/catalogue/international-electoral-standards-guidelines-reviewing-legal-framework?lang=en.

IFES: International Foundation for Electoral Systems, https://www.ifes.org/publications/cybersecurity-elections

“Media Literacy and Digital Security: Twitter Best Practices,” Organization of American States, 13 September 2019, https://www.oas.org/en/sms/cicte/docs/20190913-DIGITAL-ENG-Alfabetismo-y-seguridad-digital-Twitter.pdf.

“Methodology for Media Observation During elections: A Manual for OAS Electoral Observation Missions,” General Secreteriat of the Organization of American States, 2011, http://www.oas.org/es/sap/docs/deco/ManualMedia_WEB.pdf.

“Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions,” General Secretariat of the Organization of American States, 2010, http://www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf.

“Promise and Problems of E-Democracy: Challenges of Online Citizen Engagement,” OECD, 2003, http://www.oecd.org/gov/digital-government/35176328.pdf.

“Protección de la Infraestructura Crítica en América Latina y el Caribe”, Organization of American States and Microsoft, 2018. https://www.oas.org/es/sms/cicte/cipreport.pdf

“Tendencias sobre ataques de ciberseguridad,” LACNIC, 30 October 2018, https://www.lacnic.net/3366/1/lacnic/.

“Universal Declaration of Human Rights,” United Nations, 10 December 1948, https://www.un.org/en/universal-declaration-human-rights/.

ACE Project Electoral Knowledge Network: “Electoral Management,” EMBs definition, last accessed 16 February 2020, https://aceproject.org/ace-en/topics/em/ema/ema01

Emefa Addo Agawu, “How to Think About Election Cybersecurity: A Guide for Policymakers,” New America, 3 April 2018. https://www.newamerica.org/cybersecurity-initiative/policy-papers/how-to-think-about-election-cybersecurity/
Panizo Alonso L., Gasco M., Marcos del Blanco D.Y., Hermida Alonso J.A., Barrat J., Alaiz Moreton H., “E-voting system evaluation based on the Council of Europe recommendations: Helios Voting,” IEEE Transactions on Emerging Topics in Computing. 19 November 2018, DOI: 10.1109/TETC.2018.2881891

Australian Cybersecurity Centre, “ACSC Threat Report 2017,” Australian Signals Directorate of the Australian Government, October 2017, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

Jean Baudrillard, “Simulacra and Simulations (The Body, In Theory: Histories of Cultural Materialism,” University of Michigan Press, 1983.

DYM del Blanco, LP Alonso, JAH Alonso, “Review of Cryptographic Schemes applied to Remote Electronic Voting systems: Remaining challenges and the upcoming post-quantum paradigm,” Open Mathematics, 23 February 2018, DOI: 10.1515/math-2018-0013

D.Y. Marcos del Blanco: “Ciberseguridad Aplicada a la E-Democracia: Análisis Criptográfico y Desarrollo de una Metodología Practica de Evaluación para Systemas de Voto Electrónico Remoto y Suaplición a las Soluciones Más Relevantes,” thesis, 2018 (in Spanish).
https://buleria.unileon.es/bitstream/handle/10612/7959/Tesis%20David%20Marcos%20del%20Blanco.pdf?sequence=1

Jakob Bund, “Cybersecurity and democracy Jakob Bund, Hacking, leaking and voting”, European Institute for Security Studies, November 2016. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_30_Cyber.pdf

Canadian Centre for Cyber Security, “Global Trends and the Threat to Canada,” Government of Canada, 26 March 2019, https://cyber.gc.ca/en/guidance/global-trends-and-threat-canada-0.

Communications Security Establishment, “2019 update: cyber threats to Canada’s democratic process,” Government of Canada, 2019, http://publications.gc.ca/site/eng/9.872398/publication.html.

Council of Europe Venice Commission, “European Standards of Electoral Law in Contemporary Constitutionalism,”Council of Europe Publishing, ISBN: 92-871-5909-2 , 2005. Available from: https://books.google.es/ks?id=7xo7NUSrthIC&pg=PA17&lpg=PA17&dq=European+Standards+of+Electoral+Law+in+Contemporary+Constitutionalism&source=bl&ots=2uuCmyGSNn&sig=jKw-Za0JHjs26MQN83xpY6QfxU&hl=es&sa=X&ved=0ahUKEwiJ6vfZx7bSAhXHaRQKHZ3GCa4Q6AEISzAG#v=onepage&q=European%20Standards%20of%20Electoral%20Law%20in%20Contemporary%20Constitutionalism&f=false.

Katherine Ellena, Goran Petrov, “Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies,” International Foundation for Electoral Systems, 17 October 2018, https://www.ifes.org/sites/default/files/2018_heat_cybersecurity_in_elections.pdf.

David Fidler, “Transforming Election Cybersecurity,” Council on Foreign Relations, 17 May 2017.
https://www.cfr.org/report/transforming-election-cybersecurity.

Luciano Floridi, “Marketing as Control of Human Interfaces and Its Political Exploitation,” published online 10th August 2019, https://www.academia.edu/attachments/60279708/download_file?st=MTU4MTg4NzE1Myw3MS4yMzEuMjE2LjEw&s=profile.

Frost & Sullivan. “2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk”. https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf **Password protected**

Nellie M. Gorbea, “Elections Cybersecurity in Rhode Island”, Rhode Island Department of State, April 2018, https://vote.sos.ri.gov/Content/Pdfs/cyber_security_ri_2018.pdf.
V. Hahanov, E. Litvinova, M. Brazhnikova and A. Hahanova, “Cyber democracy and digital relationship,” 2016 13th

International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv, 2016, pp. 545-548, https://ieeexplore.ieee.org/document/7452110.

Dr. Sven Herpig, Julia Schuetze, Jonathan Jones: "Securing Democracy in Cyberspace: An Approach to Protecting Data-Driven Elections" October 2018. https://www.stiftung-nv.de/en/publication/securing-democracy-cyberspace-approach-protecting-data-driven-elections.

Human Rights Council of the United Nations General Assembly, "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development – Oral Revisions of 30 June," A/HRC/32/L.20, United Nations, 30 June 2016, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.

Brooks Jackson, "The Florida Recount of 2000," FactCheck.Org, 22 January 2008 https://www.factcheck.org/2008/01/the-florida-recount-of-2000.

"33 ataques por Segundo: Kaspersky Lab registra un aumento del 59% en ataques de malware en América Latina," Kapersky Lab, 11 September 2017, https://latam.kaspersky.com/about/press-releases/2017_33-attacks-per-second-increase-in-malware-attacks-in-latin-america.

S.J. Lewis, O. Pereira and V. Teague. "Trapdoor commitments in the SwissPost e-voting shuffle proof". The University of Melbourne, 2019. https://people.eng.unimelb.edu.au/vjteague/SwissVote.

Wade Payson-Denney, "So, Who really won? What the Bush v. Gore studies showed," CNN, 31 October 2015, https://edition.cnn.com/2015/10/31/politics/bush-gore-2000-election-results-studies/index.html.

Thamy Pogrebinschi, "Does digital democracy improve democracy?" openDemocracy, 2 March 2017, https://www.opendemocracy.net/en/democraciaabierta/does-digital-democracy-improve-democracy/.

K. Reinasalu, "Handbook on E-democracy," □pace theme publication, January 2010.

V. Teague. "Faking an iVote decryption proof". University of Melbourne, 2019. https://people.eng.unimelb.edu.au/vjteague/iVoteDecryptionProofCheat.pdf.

Maarja Toots, Tarmo Kalvet, and Robert Krimmer, "Success in eVoting – Success in eDemocracy? The Estonian Paradox," Electronic Participation: 8th IFIP WG 8.5 International Conference, pp. 55-66, https://doi.org/10.1007/978-3-319-45074-2_5.

J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, "Information Manipulation: A Challenge for Our Democracies," report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018.

Footnotes

1. In 2016, Bloomberg released a story about a Colombian hacker, Andres Sepulveda who claims he hacked and spied in the elections in Colombia, Costa Rica, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, and Venezuela for almost eight years. 'How to hack an election'- https://www.bloomberg.com/features/2016-how-to-hack-an-election/

2. Antigua and Barbuda, Bahamas, Belize, Bolivia, Brazil, Colombia, Costa Rica, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Vincent and the Grenadines, Saint Lucia, Suriname and the United States of America.

3. See the website for the OAS Department of Electoral Cooperation and Observation, available at https://www.oas.org/en/spa/deco/.

4. For example, see the collection of essays by French sociologist Jean Baudrillard, "The Gulf War Did Not Take Place."

5. IACHR, The Inter-American Legal Framework regarding the Right to Freedom of Expression. Office of the Special Rapporteur on Freedom of Expression of the Inter-American Commission of Human Rights. 2009, par. 8.

6. Ibid., par. 80

7. Ibid., par. 57

8. IACHR, Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts, cit., pág. 17 –"In general, the executive branches of the region control dimensions of the state that are essential for the development of these types of campaigns. For example, from the management of the education system or cultural promotion avenues. In these cases, it is essential that the authorities in charge of these departments address the problem of misinformation through awareness, education, and training campaigns. They should be focused on offering citizens tools to distinguish true from false information, become aware of their own participation in the processes of replication of information, and warn about the impoverishment of the public debate that misinformation generates. While this recommendation is addressed to the executive branch, it would be desirable for all actors involved in the phenomenon to develop education and awareness campaigns".

9. For the purposes of this document - disinformation is understood to be "the mass dissemination of false information (a) with the intent to deceive the public and (b) with the knowledge of its falsity" - IACHR, Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts, pg. 3

10. The French government has described the manipulation of information and perhaps have taken the hardest stand against this by introducing regulatory frameworks for this; see http://www.gouvernement.fr/en/against-information-manipulation; The Canadian government has also addressed the issue of 'fake news' highlighting the threat to its very people; see https://www.loc.gov/law/help/fake-news/canada.php.

11. In Trinidad and Tobago, targeted election campaigns drove a particular part of the electorate not to bother casting their paper ballot on Election Day affecting the result of the election in a pre-determined manner – see https://www.opendemocracy.net/en/dark-money-investigations/they-were-planning-on-stealing-election-explosive-new-tapes-reveal-cambridg/

[12] See, e.g., IACHR, Freedom of Expression and the Internet, cit, pars. 137-142; IACHR, Standards for a Free, Open and Inclusive Internet, cit, ch. 4law updla.

[13] For example, Internet intermediaries, social network providers, data brokers, search engines, etc.

[14] The countries represented in the survey include: Antigua and Barbuda, Bahamas (The), Brazil, Canada, Chile, Colombia, Costa Rica, Ecuador, Grenada, Guatemala, Haiti, Mexico, Panama, Peru, Saint Vincent and the Grenadines, Trinidad and Tobago and the United States.

[15] The bigger the country, the more likely it is that it has introduced cloud services.

[16] It must be noted that such legislative updates should take into account current international human rights standards

[17] According to Canada's Communication Security Establishment, this represents about a three-fold increase since 2015; they expect the upward trend to continue. See https://cyber.gc.ca/en/cyber-threats-and-democracy.

[18] The Institutions authoring those original documents tend to be Multilateral Organizations or top-level Universities and think tanks. Some of the most relevant examples include:
1. "Promise and Problems of e-democracy" by the OECD
2. "Handbook on E-democracy. □pace theme publication" by Reinasalu "Cybersecurity and democracy" by the European Union Institute for Security Studies (EUISS).

[19] Noteworthy benchmark publications covering the matter include: "Information Manipulation: A Challenge for Our Democracies," report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, "Cybersecurity in Elections" by IFES, "Transforming Election Cybersecurity" by the Council on Foreign Relations, "The Cybersecurity Campaign Playbook, European Edition. Defending Digital Democracy" by Belfer Center for Science and International Affairs, Harvard Kennedy School, "Cyber Threats to Canada's Democratic Process" by the Communications Security Establishment of the Canadian Government or the "Guia para garantizar la libertad de expression frente a la desinformación deliberada en contextos electorales" by the Organization of American States (in Spanish).

[20] IACHR, Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts, cit., pág. 13.

[21] Damien Bancal, a French Cybercrime expert, analyzed over 30 sites belonging to 11 candidates for the latest French Presidential campaign, unveiling over 200 flaws, including SQL injections and WordPress sites still using the original username and password in the administrator account.

[22] An example of a fact-checker website in Argentina - https://chequeado.com/

[23] An example of a fact-checker website in Mexico - https://verificado.mx/

[24] For additional sources and further reading, OSCE's "Guidelines for reviewing a Legal Framework for Elections" and Institute for Democracy and Electoral Assistance (IDEA)'s "International Electoral Standards: Guidelines for reviewing the legal framework of elections" provide an in-depth analysis on the Legal Framework for Democratic Elections with comprehensive requirements and recommendations as a key resource.

25. More information on the US 2000 election scandal can be found at "Fact Check: The Florida Recount of 2000" https://www.factcheck.org/2008/01/the-florida-recount-of-2000 and in CNN's article "So, Who really won? What the Bush v. Gore studies showed." https://edition.cnn.com/2015/10/31/politics/bush-gore-2000-election-results-studies/index.html

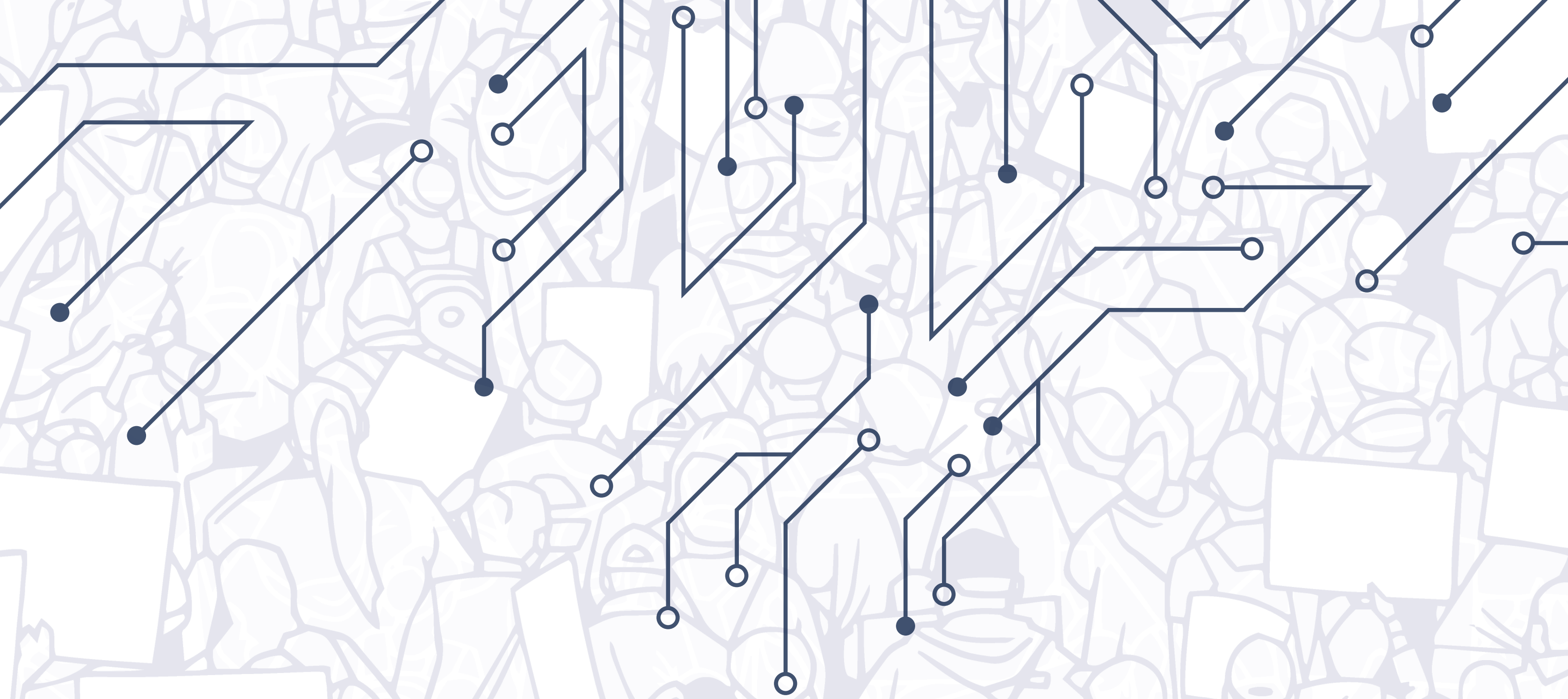
26. We have seen this in the United Kingdom, with the establishment of the National Cybersecurity Centre in 2016, which remains part of (GCHQ), with a mandate to be the agency responsible for cybersecurity matters, backed up with very sophisticated capacity in GCHQ when required but also independent enough to engage with the general public.

27. See IACHR, Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts, cit., page 15 - "One of the essential conditions to combat the phenomenon of misinformation implies transparency and publicity of the entire electoral process. Most electoral regimes in the region already include transparency obligations, especially at the head of political parties. Likewise, many also include special obligations, such as pointing out that certain messages or notices are issued within the framework of electoral campaigns, hired by a certain political party, electoral alliance, or third parties, and so on".

28. As defined by Collins Dictionary; see https://www.collinsdictionary.com/dictionary/english/voter

29. As defined by the ACE Electoral Network; see https://aceproject.org/ace-en/topics/em/ema/ema01

30. Website for FIRST: https://www.first.org/



Cybersecurity Considerations

for the **Democratic Process** for **Latin America** and the **Caribbean**

Cybersecurity Considerations

for the Democratic Process for Latin America and the Caribbean

ORGANIZATION OF AMERICAN STATES

OAS

More rights
for more people