Cyberattacks, Foreign Interference, and Digital Infrastructure

Conducting Secure Elections Amid a Pandemic

David Levine, Elections Integrity Fellow, Alliance for Securing Democracy
Beata Martin-Rozumilowicz, Director for Europe and Eurasia, International Foundation for Electoral Systems
October 8, 2020

Introduction

The coronavirus pandemic has introduced an additional layer of complexity into the already challenging task of conducting secure, democratic elections. Prior to the pandemic, many democracies were working to secure their elections from foreign adversaries, often with limited budgets. These challenges have only grown more acute because of the pandemic. Since the coronavirus arrived, much attention has, correctly, been focused on how to administer elections in a manner that reduces the likelihood of voters and pollworkers contracting the virus. However, after reviewing many elections held in Europe and the United States (hereafter referred to as the transatlantic region), including several during the pandemic, we believe that more can and should be done to secure human, physical, and cyber election assets. Both the pandemic and foreign interference threats show no signs of abating; meanwhile the pandemic creates further windows of opportunity for authoritarian regimes to interfere in elections.

This paper is not directed at any one specific country or election. Instead, it seeks to help democratic actors, particularly those in the transatlantic region, conduct more secure elections during these unprecedented times. It examines the challenges that many countries have faced with securing elections, including those posed by malign foreign actors prior to the advent of the pandemic. It then looks at how the pandemic has made securing elections even more difficult by examining how some election officials' responses to the coronavirus have created new vulnerabilities in election infrastructure. Finally, the paper provides solutions to address the election security threats that the current crisis has exacerbated. The integrity of future elections held during the coronavirus pandemic could go a long way towards bolstering or undermining citizens' trust in democratic institutions and elections.

Challenges to Secure Elections before the Coronavirus

The new difficulties caused by the pandemic have not displaced the challenges that election officials throughout the transatlantic community faced before the coronavirus arrived, including the threats posed by malicious foreign actors. While significant attention is focused on countering foreign disinformation and influence operations directed at elections in general, this paper delves into the details and challenges of securing human, physical, and cyber election assets during the current pandemic. Many of these assets, such as online voter registration systems, electronic pollbooks, electronic voting devices, and election night reporting websites, were initially deployed with the aim of making elections easier to participate in and administer. However, some of these assets have introduced additional points of vulnerability for malicious attacks that need to be identified, mitigated, and managed. Malicious actors may also heighten and distort these vulnerabilities through disinformation campaigns in ways that have the potential to undermine public faith and trust in election processes and results.

The evolution of cyberattacks over the past decade illustrates the evolving challenges that democratic actors face in securing election infrastructure. Ukraine's 2014 presidential election is a case in point. Hackers launched a three-pronged attack on the eve of the presidential election against the Central Election Commission (CEC) website, which helps disseminate the election results to the public. They infiltrated CEC computers and deleted key files, rendering the tabulation system inoperable; breached the CEC's computer network infrastructure and released many of the commission's emails and other documents on the Internet; and installed a virus covertly on CEC computers that nearly resulted in a fringe candidate, Dmytro Yarosh, being portrayed as the winner. The final attack was discovered and removed prior to the election results being publicly presented, but not before Channel One in Moscow broadcasted the false results with a fake CEC webpage purporting Yarosh had won the election. Even though election night reporting provides unofficial results before an election is certified, the public can perceive them as official. Therefore, ensuring the accuracy of election night reporting and the protection of election data is critical to maintaining public confidence in elections.

The 2016 presidential election in the United States further underscores the importance of securing electoral infrastructure. Beginning in 2014, the Russian government began attacking the United States to undermine the integrity of U.S. elections and Americans' confidence in democracy. In addition to a wide-ranging disinformation campaign, Russian actors conducted cyber intrusion operations against entities, employees, and volunteers affiliated with a presidential candidate's campaign, as well as against both political party's convention committees, and targeted U.S. election systems by conducting cyberattacks against private technology firms that make election software and election infrastructure at the state and local level. While there is no evidence that Russian actors altered vote totals in the 2016 election, they did target many states' voter registration systems and public election websites, and they were in the position to delete or change voter data in at least one state.

France's 2017 presidential election is a pre-pandemic success story of how countries can counter foreign electoral interference. Early in the election cycle, France's National Cybersecurity Agency (ANSSI) offered to meet with and educate all campaign staff on the risks of cyberattacks and disinformation, even holding an open workshop on cybersecurity in October 2016. In December 2016, the minister of defense announced the creation of a cyber command agency composed of 2,600 cyber experts. Shortly after President Macron's political movement En Marche! announced that it was the target of an orchestrated attack in February 2019, the Ministry of Foreign Affairs, at the behest of the head of ANSSI, announced cessation of electronic voting for citizens abroad because of the high risk of cyberattacks. ANSSI and the National Commission for the Control of the Electoral Campaign for the Presidential Election (CNCCEP) also frequently informed the news media, political parties, and public about the risk of cyberattacks and disinformation throughout the campaign. And ten days before the vote, Facebook announced that it had suspended over 30,000 fake accounts in France. It was later revealed that the actual number of suspended French Facebook accounts was closer to 70,000.

It is also instructive to review events in the run-up to the Republic of Georgia's October 31, 2020 parliamentary elections. On October 28, 2019, the country experienced a substantial cyberattack—which the United States later blamed on Russia's military intelligence agency—which brought down some 2,000 websites and two television stations. Then in March 2020, just as the pandemic was starting to take hold, another breach of voter data took place. Sources reported that that the "voter information for more than 4.9 million Georgians, including deceased citizens, had been published on a hacking forum." Although it was eventually determined that the data was not from Georgia's Central Election Commission, the event demonstrated that attempts to interfere with democratic elections would not cease during the pandemic.

These high-profile examples created new awareness in transatlantic democracies about the challenges of ensuring secure elections, as well as of the best practices to mitigate such challenges. With attacks such as these continuing to happen, election officials must recognize and respond to the heightened risk that other crises, like the coronavirus, bring to securing election infrastructure.

The Difficulty of Securing Election Infrastructure during the Coronavirus Pandemic

Election infrastructure is comprised of physical, cyber, and human assets, all of which are susceptible to intentional and unintentional threats. Physical assets are things such as ballots, voting locations, and storage facilities that support or provide protection for election activities. Cyber assets are hardware and software such as voter registration systems, election-night reporting websites, and electronic voting equipment. Human assets are personnel with unique training, experience, knowledge, skills, and authority, whose absence could hinder election activities. They include election officials, information technology and security staff, election equipment vendor employees, and temporary staff such as pollworkers. Since the onset of the coronavirus pandemic, securing each of the above assets has become increasingly difficult.

Human Assets

As of September 22, 2020, there were 31,132,906 confirmed cases of coronavirus, including 962,893 deaths, reported to the World Health Organization. These numbers not only affect society at-large, but also elections. In many countries, including the United States, the people who traditionally administer elections at polling places are often older workers who are more susceptible to the coronavirus. These workers often help verify a voter's eligibility, assist the voter with casting a ballot, and protect the voted ballots from any untoward behavior.

Election Management Board (EMB) permanent staff are also at an increased risk of contracting the coronavirus due to their frequent in-person interactions with voters and party and candidate representatives. Without health precautions to prevent their key staff from falling ill, an EMB's ability to defend against cyberattacks decreases due to key experts being out of circulation. It is imperative that election officials throughout the transatlantic community prepare for the possibility of remote work and social distancing at their traditional work sites for as long as the pandemic continues. That way, if one election official is infected with the coronavirus, preparation for any given election can continue unabated. In that same vein, it is imperative that election managers cross-train their staff on different functions and consider how staff from other government agencies could provide election assistance on short notice.

While many countries have used an array of measures to try and limit the risk of spreading the coronavirus during in-person voting, there is still a significant concern that large numbers of pollworkers who have historically helped conduct elections, particularly those in demographics most susceptible to the virus, will not volunteer again until the virus is brought under control. With continuously high coronavirus case numbers in the United States and coronavirus infections rising again in Europe, it is important that every democracy in the transatlantic community recruit and train a surplus of pollworkers (with proper health security and risk mitigation measures being respected), so that each nation can adequately service voters during an election, even if many pollworkers drop out on short notice. Encouraging more mail-in voting could help offset this challenge, but such a change requires proper planning so that it does not create more problems than it solves. Ultimately, a hybrid response that provides voters a wide variety of proven, secure voting options is optimal.

Concerns about pollworker shortages are not merely theoretical. For example, the government of Alabama recently issued an emergency proclamation to help municipalities "that are struggling to find election workers due to COVID-19." Although there is no silver bullet for finding extra workers, several policies could be helpful, including raising the compensation of pollworkers during the pandemic; lowering the age requirement to serve as a pollworker; and allowing polling station workers to serve in places outside their own locality. Election officials could also target certain organizations, such as businesses, universities, social organizations, and sports teams, who might be more civic-minded and willing to pitch in.

Cyber Assets

The coronavirus pandemic has not only made it more difficult to protect election workers, but also election operations. For example, many election officials have worked from home or away from their traditional work sites during the outbreak, often increasing reliance on networks that lack the firewalls of their traditional sites and are more exposed to cybersecurity threats. This added vulnerability creates new targets for those interested in disrupting election infrastructure with cyberattacks. It is therefore critical to ensure good cybersecurity practices for remote environments.

It is important that election officials review the technology their offices are using, such as videoconferencing and chat services, while working away from their traditional worksites. They should evaluate the technology against their own policies and their country's cybersecurity standards and seek assistance as needed from other security experts to ensure that their offices are as secure as possible.

As part of these efforts, election officials need to update their devices regularly. This includes consistently updating devices that are used at home, including laptops, tablets, phones, and home routers. Operating systems, browsers, and other applications used by election personnel should also be patched. If the IT department approves, auto-updates should be enabled. Such steps help address identified vulnerabilities, which prevent bad cyber actors from gaining access to information systems or networks.

Election workers should also know how to avoid phishing attacks, rogue Wi-Fi hot spots, and other malicious activity. If necessary, election officials should seek out the relevant organizations in their countries that can help provide ongoing training on and assessments of these threats. This will help ensure that they stay abreast of the most significant threats and know how to respond in the event of an attack. If possible, election officials should also adopt two-factor authentication. Requiring this for all log-ons is an important way of reducing unauthorized access to sensitive infrastructure.

Physical Assets

In addition to cyber and human assets, securing physical election assets, like voting equipment, amid the pandemic has become a greater challenge. In response to the coronavirus, nations throughout the world, including within the transatlantic community, have increased their reliance on voting by mail. Some countries, such as the United States, South Korea, Poland, and France, have expanded eligibility for voting by mail during the pandemic. Other countries, such as Australia, have encouraged voters to submit their ballots by mail, while some like Germany and Switzerland have resorted to conducting certain elections solely by mail ballot. The increase in voted mail-in ballots could result in official election results not being known until later than is customary due the process of receiving, processing, verifying, and counting such ballots.

Meanwhile, authoritarian regimes are already seeking to undermine democratic elections. For example, both Russia and Iran have alleged that coronavirus precautions, such as expanded mail-in voting, that cause delays in U.S. voting processes are evidence of election malfeasance. One way that democracies can counter such foreign disinformation efforts is to improve the speed and accuracy of counting votes by investing in additional equipment to help tabulate mail-in ballots. As a number of studies have shown, using machines like the ballot optical scanners used in South Korea and much of the United States to initially tabulate the results can be faster and more accurate than hand-counting and, at the same time, offers the possibility of a voter-verified paper trail. Some election officials are also using barcode scanners to more quickly process inbound mail ballots; envelope openers to more quickly open inbound ballots; signature verification software to more quickly and accurately verify the voter returning the ballot; additional hardware (computers, monitors, and scanners) to support the adjudicating of signatures; and a ballot monitoring camera to provide transparency to the public about the operation. Processing, storing, and counting large numbers of mail-in ballots using some of the above equipment requires a lot of space, and even more physical space may be needed due to social distancing precautions in

response to the pandemic. The timely procurement of additional equipment is also necessary to ensure that machine operators have enough time to learn how to use the new machines.

Elections during the Pandemic Cost More

The adjustments made to human, cyber, and physical assets of elections in response to the coronavirus not only require careful planning and execution; they also require more money. In the past, democracies could gradually implement changes to voting procedures that impacted election security to accommodate voters, candidates, election workers, government budgets, and other factors. Now, many countries must keep up with the evolving pandemic just to ensure that their elections are safe. Supplying personal protective equipment and cleaning products, enhancing cleaning protocols, conducting more voter education and outreach, and recruiting and training more pollworkers than is typically necessary can be quite costly. New Zealand, for example, is planning to spend $19 million to fund additional staff and safety measures for its October 2020 parliamentary elections—a cost of around $6.20 for each expected voter. To put that in additional context, if the United States were to match New Zealand's investment for its 2020 presidential election, it would need to spend approximately $750 million more than it has already spent based on its 2016 turnout.

Countries are implementing a range of measures to help ensure that voting during the coronavirus pandemic can be done safely. Many are purchasing materials such as personal protective equipment, protective screens, and sanitation supplies to protect voters, election workers, and others who visit elections offices or polling places. A number of countries are modifying workplaces and polling locations to ensure social distancing, whether that means putting markings on floors to indicate where people should stand, printing additional signage, or having additional people on hand to remind the public of these changes. In cases where typical voting facilities cannot sufficiently accommodate social distancing, election officials are seeking out additional facilities that can safely accommodate voters and their workers. And after such changes are implemented, many election officials are notifying voters and the public of these adjustments through mailings, newspaper, television, and digital ads, and other means.

Working to address each of the aforementioned considerations in a relatively short period of time is critical, but it is already straining some election officials' budgets. In the United States, the coronavirus pandemic has drastically changed voting behavior. Millions more voters are requesting mail ballots—far more than were expected to prior to the pandemic—and the costs associated with this are significant. For example, the elections board in Macon-Bibb County, Georgia, indicated that it was already short of cash, even before its August runoff and the November general election. A flood of absentee ballot requests increased election expenses, and the county's budget has shrunk as the coronavirus has slashed tax revenues. For Macon-Bibb County and other election jurisdictions that are similarly situated, this makes financing the administration of future elections, let alone securing them, a major challenge.

EMB Responses and the Creation of New Vulnerabilties in Election Infrastructure

As election officials rush to modify their election systems to account for the coronavirus, they must build or adapt human, cyber, and physical infrastructure in ways that can handle the strains of large, closely contested elections while remaining secure. Otherwise, their hastily adopted alterations could create new vulnerabilities in the infrastructure that underpins their elections. If election infrastructure is expanded or changed, security and resiliency measures should be part of their design, not introduced after the fact.

For example, Poland's governing Law and Justice party initially proposed conducting its May 2020 presidential election with full postal voting for the first time, as the country was under lockdown at that point to limit infections. In preparation for this scenario, the Polish Postal Service requested personal data of Polish citizens via email without any additional protection or a password. While email is convenient for sharing information, it has limited security protections and should not be used for sending sensitive information, such as personal data. Since email can be viewed or tampered with at multiple places in the transmission process and is often used in cyberattacks on organizations, some Polish local authorities voiced their concerns about potential privacy violations and refused to provide the requested data. Putting the security of its citizens' personal information at risk in this manner could have made the Polish election vulnerable to a hack-and-leak operation.

Furthermore, to print the ballots for the full postponed postal election, the Polish national government contracted a firm that did not have the capacity to ensure the security of the ballots. A few days after the hiring of the firm was announced, copies of the ballots were leaked, and an angry presidential candidate demonstrated how easy it would be to copy the ballots and submit multiple votes. Vendors often build and maintain much of a country's physical and cyber election infrastructure by doing things such as printing ballots, creating election websites, and maintaining voter registration databases. Such roles can make them targets for adversaries. Therefore, it is imperative that EMBs require vendors to follow good cybersecurity practices. EMBs should include these cybersecurity practices in tender specifications, build processes that allow vendors to report cyber incidents to election officials, conduct background checks on their personnel, and maintain supply chain integrity, among other things. Fortunately, a few days before the Polish election was to set take place, an agreement was reached to delay the election, and it was subsequently rescheduled and administered in June with voting in polling stations under health protection measures.

Another instructive example is Ukraine's efforts to adopt internet voting. Initially, the presidential administration announced their intention to introduce full-scale Internet voting for their next elections (nationwide local elections have now been scheduled for October 2020), even though it had not conducted any previous pilot projects or introduced any technology into their elections other than the website results page previously discussed. Although it was partially posited as solving health concerns raised by the coronavirus, such a move presented clear risks to the integrity of the electoral process. There were not adequate timelines put in place to procure and adequately test an Internet voting system, let alone introduce and educate the electorate on it. It is a stark example of how new vulnerabilities can be introduced when EMBs seek to introduce hasty responses to the coronavirus.

Possible Solutions to Addressing Election Security Threats

Due to the uncertainty around the pandemic, many election officials have been forced to make significant changes to their elections in short periods of time. Such changes have included quickly scaling up vote-by-mail operations, expanding early voting opportunities, consolidating Election Day polling places, and recruiting scores of new workers—all of which could create more vulnerabilities. As countries move to hold key elections across the transatlantic region in the coming months, there are several actions they can take to secure their elections and address the threats analyzed above.

1. Implement proper assessment and risk mitigation planning.

It is recommended that election authorities conduct joint coronavirus risk assessments together with the appropriate cyber and health authorities and that based on such risk assessments, they develop mitigation plans that are fully integrated into the EMB's operational plan. This may require additional funding to conduct, so proper planning for these measures should be done in a timely fashion.

2. Ensure voter registration databases are secure during the pandemic.

Due to the pandemic, many election officials and their staff have been working from home, and there's a greater risk that people who are teleworking will become the victims of a cyberattack, like a spear phishing campaign or a ransomware attack. In that vein, if election officials remotely access election infrastructure such as the voter registration database, it is imperative that they do this in as secure a manner as possible. Voter registration systems are often critical and interconnected components of states' election infrastructures, and as the 2016 U.S. presidential election demonstrated, foreign adversaries are capable of targeting and infiltrating them. Therefore, for those countries that use digital voter registration databases, there are several steps they should take to ensure they are more resilient. Those include requiring multi-factor authentication and passwords that are consistent with good practices; monitoring all voter registration database login attempts and backing up their databases on a regular basis; possessing a current offline version of the database; and having an information and communications technology system that has sensors installed to monitor activity and alert election officials to any potential compromises.

3. Use paper-based voting methods.

Some people have argued that a fully digital voting process will protect election workers that might otherwise contract coronavirus from tabulating the paper ballot votes. However, a recent study asserts that the virus can survive on paper or cardboard for only 24 hours. Paper-based voting systems are also the most secure. Paper ballots can be verified more easily by voters, secured more effectively by most pollworkers, and reviewed or audited more accurately after an election than electronic ballots. In the event that any election-related infrastructure, such as electronic voting machines (for example, ballot scanners) or election night reporting websites, is breached by bad actors or experiences technical glitches, paper ballots can be used to verify the election outcome and, thereby, can help ensure public confidence in the election.

4. Ensure the public can observe the election process, including procedures modified in response to the coronavirus.

In response to the pandemic, many democracies are adjusting their voting procedures, which can directly impact the security of their elections by creating new vulnerabilities that lack measures to protect against malign adversaries. These changes should be shared in a timely and proactive manner with the public and viewable to them, as well. When the public can see that the adjusted procedures for conducting an election are beyond reproach, it makes it much more difficult for foreign adversaries or other bad actors to either interfere with the modified election infrastructure or foment doubt about the adjusted election procedures among large segments of the electorate.

5. Implement robust post-election audits to validate the results of elections conducted amid the pandemic.

One way to mitigate any mistakes that could arise from changes to elections due to coronavirus-related concerns is to conduct robust post-election audits. As places such as the state of Colorado have shown, reviewing statistically significant samples of voted paper ballots to verify the winner of the contest helps to ensure that any issues with the tabulation of the election results are caught and corrected. The gold standard is the risk-limiting audit (RLA), which is generally performed by comparing a random sample of cast paper ballots against the expected results. Such audits provide a very high likelihood that a reported outcome is the same as the result that would be obtained if all ballots were examined by hand by ensuring that a different reported outcome has a high probability of being observed and corrected. That said, RLAs can take a good deal of time, expertise, and resources to plan and implement, and many election authorities could find it easier to first conduct a smaller, more traditional audit of a certain percentage of ballots before trying an RLA. While smaller audits may not be as foolproof, they are certainly better than no audit at all.

6. Ensure that the election night reporting system data is accurate and protected.

The attack on Ukraine's 2014 presidential election underscored the importance of ensuring that election night reporting system data is accurate and protected. Before the coronavirus pandemic, allowing public observation of the actual tabulation of results was a great way to retain credibility in the face of such attacks. However, because of the coronavirus and the need to socially distance to reduce the risk of contracting the virus, it could be harder to observe the tabulation of results in-person. Election officials will therefore need to develop other resiliency measures to deploy in the event of such attacks, whether that is establishing redundant election night reporting sites that could be made available in the event the main site is attacked, live-streaming the tabulation of results in a secure manner, or developing a comprehensive communications plan to reach out to the public in the event of a similar attack.

7. Give voters as many secure choices as possible to cast their ballots.

Elections that offer only in-person voting on a single day are at a higher risk for coronavirus spread because there will likely be bigger crowds and longer wait times. Such elections are also arguably higher risk from a security perspective because any issues that arise are harder to detect, investigate, and/or recover from in a timely manner. A single day of in-person voting may also not ensure that all those who wish to vote can successfully do so. Depending on the county and its election, providing many secure choices for voting could include offering longer voting periods (more days and/or hours), more opportunities to vote by mail, or opportunities to vote outside of traditional polling stations. Even before the pandemic, some countries took innovative steps to increase participation while retaining adequate security. For example, in Sweden, legislative changes ahead of its 2004 election meant that in addition to voting by mail, eligible voters could vote ahead of Election Day in places such as libraries and shopping malls. This expanded access to the ballot while also ensuring the integrity of the vote.

8. Communicate accurate information about elections to the public widely and proactively.

Election officials should have an explicit communication strategy that includes a way to share information about the pandemic and how the election is being secured in response to the virus with voters. This will help ensure confidence in the election process and reduce the likelihood that bad actors, including foreign adversaries, can amplify mis- and disinformation in a manner that successfully undermines confidence in a country's election and democratic processes more broadly.

9. Work to ensure that all government agencies involved in the administration and security of a country's elections are accessible, flexible, communicative, and supportive of one another.

Clear, timely communication between different government agencies is critical to better identifying and responding to election cyber threats. To learn how to better work together and problem solve, government agencies can turn to their counterparts in other countries that have gone through similar experiences. These peer networks can help governments build more robust responses to the issues they face and provide them with examples of how to coordinate across and support different government agencies during elections. In North Macedonia's July 2020 parliamentary elections, such efforts may have helped thwart a large-scale cyberattack from bringing down the country's CEC results system. Similar assistance is being provided to Georgia's CEC ahead of the country's October parliamentary elections.

10. Ensure that all individuals involved in the administration of elections know what to do in the face of cyber threats from foreign adversaries.

This includes ensuring all individuals have access to cyber training, maintain good cyber hygiene, and know to say something when they see something. Ensuring the cybersecurity of elections is a shared responsibility. Anyone who has access to an elections system, no matter how minor, bears some responsibility for the cybersecurity and integrity of the election. As this paper is the latest to note, "security through obscurity" is no longer a viable option. Instead, training of election management bodies and their partners should be done on a consistent, ongoing basis by security experts with knowledge in the field, many of whom can be found at key academic institutions, think tanks, and other private sector and civil society organizations.

11. Harness resources, guidance, and knowledge from international institutions, such as IFES, the Alliance for Securing Democracy, the National Democratic Institute, the Council of Europe, the European Union, and the Organization for Security and Cooperation in Europe.

For example, after Ukraine decided to pursue internet voting, the international community quickly intervened and countenanced a more nuanced approach, suggesting that Ukraine review the examples of other countries that had piloted Internet voting to identify both pitfalls and emerging good practices. In particular, IFES advocated and undertook a feasibility study into the question of internet voting and made a series of recommendations. Before considering remote internet voting, or any other technology solution, the EMB should first identify the key issues in the election process that it is trying to mitigate or address with a technology solution. While implementation of new technologies presents certain opportunities, lack of preparation or due diligence could also be a cause of extensive damage to public trust and the integrity of an election itself.

Conclusion

Cyber operations and malign foreign influence campaigns already presented a serious threat to democratic elections prior to the advent of the coronavirus crisis. The pandemic has further complicated this situation by forcing many countries to quickly adjust some of their traditional voting processes. In some cases, countries have deployed novel technology solutions shortly before an election, making proper planning and resource allocation, both human and financial, more challenging. These quickly deployed procedural changes have, in some cases, made countries more susceptible to foreign interference in the electoral process.

As countries' authorities and election management bodies make changes to their election processes in response to the coronavirus, they must carefully consider the election security risks such changes introduce, while ensuring that elections carried out during the pandemic are accessible, secure, and legitimate. Doing otherwise risks making elections more vulnerable to adversaries and undermining public confidence in the democratic process.