OSET
INSTITUTE
Executive Briefing

Murphy's Guide to Likely Dysfunction in the 2020 Presidential Election

The Things That Will Go Wrong Are Already Poised To Do So

This Election Briefing is a guide to the items the OSET Institute has identified as potential issues for the upcoming 2020 Presidential Election. While we are acutely focused on the potential problems of by-mail ballot processing and adjudication, this is an overview of a range of possible issues, which go beyond the recent (and appropriate) focus on by-mail voting. The November 2020 election will present a combination of familiar process and technology issues that have been happening for years (and which are disruptive in their own right), plus a host of new challenges associated with recent changes due to the COVID-19 crisis.

We begin with a survey of what could go wrong, both new and familiar. From there, we examine the potential attacks we are on guard for at this time; and we conclude with our summary forecast of the five things most likely to go wrong, ordered by likelihood and impact. Given that the only constant is change, this assessment will be frequently updated.

Section I: New Murphy's Law–
What Is Likely to Go Wrong Due to COVID-19

Many election administration processes have changed across the country in response to COVID-19 risks. Furthermore, due to many senior citizen poll workers declining to work the polls for health reasons, there is also widespread difficulty in finding adequate numbers of new poll workers, or even temporary workers to support in-person polling places or election headquarters (to assist in processing by-mail ballots, for example). When lack of human resources is combined with altered processes, this creates a compressed time frame for training, combined with a dramatic increase in confusion, mistakes and process errors. Both process errors and technology errors can combine to leave some jurisdictions with chaos on Election Day (as was vividly on display in Georgia's June 9 primary election, for example[1]).

1. A surge in absentee/by-mail voting presents implementation challenges

<u>What it might look like:</u>

- **Jurisdictions' inability to keep up with by-mail voting operations is likely to result in reports of voters not receiving blank ballots they requested**. After the primary election season, election jurisdictions across the country in red and blue states alike are reporting a dramatic increase in

[1] NPR, "Chaos in Primary Elections Raises Fears For November," June 15, 2020. https://www.npr.org/2020/06/15/876474124/chaos-in-primary-elections-raises-fears-for-november

absentee by-mail requests.[2] This is because many states already permitted "no excuse" by-mail voting for any voter; and furthermore, many states that typically require an "excuse" have relaxed their restrictions in direct response to COVID-19 concerns. Some jurisdictions have seen requests go up as much as tenfold. Particularly in jurisdictions that are not accustomed to such by-mail volumes, they cannot always keep up with the pace of requests, which means that some voters will not receive their ballots. This will impact other aspects of voting. (See below.)

- **Jurisdictions' inability to keep up with by-mail voting operations will likely place direct pressure on in-person voting operations.** There is a dynamic relationship between by-mail voting and in-person voting during the age of COVID-19: Ideally, if jurisdictions can keep up with a massive volume of by-mail requests, then that can greatly relieve pressure on Early or Election Day in-person voting. However, if absentee by-mail requests are not processed in timely fashion, then an unexpected surge of voters may crowd in-person polling places, greatly outstripping their capacity to process lines efficiently.
- **A nationwide shortage of poll workers is likely to adversely impact voter service at in-person voting locations.** Due to a nationwide crisis in the recruitment of poll workers, prompted by heavy attrition from the typical senior citizen poll worker population, the number of in-person polling places may need to be reduced, or they may be inadequately staffed. Both would result in long lines for voters.
- **Misjudging the number of in-person voting locations can result in long lines for voters.** The primary season has demonstrated that achieving the right allocation of resources between expanded by-mail voting operations while also preserving an adequate number of in-person polling places is a delicate balance. It appears that some jurisdictions missed the mark, by contracting the number of in-person locations too aggressively, or consolidating locations in too few "supercenters" that were inadequately staffed.[3]
- **Not keeping up with absentee ballot requests can result in increased distribution of provisional ballots to in-person voters, due to absentee ballots not received.** The rapid expansion of by-mail voting, coupled with some jurisdictions' inability to keep up with the pace of requests, means that more and more in-person polling locations may indicate a voter as having "received an absentee ballot," when in fact they may not have done so. In such circumstances, when there is a conflict between voter registration/poll

[2] OSET Institute, "The Bipartisan Truth About By-Mail Voting." https://trustthevote.org/wp-content/uploads/2020/05/27May20_BipartisanTruthAboutByMailVoting_v3.pdf

[3] WAMU/DCist, "D.C. Plans To Open 80 In-Person Polling Sites For November's General Election," July 28, 2020. https://wamu.org/story/20/07/28/d-c-plans-to-open-80-in-person-polling-sites-for-novembers-general-election/

worker records, and what the voter says, poll workers may feel they have no choice but to issue provisional ballots to voters who are actually registered and eligible – and that can adversely impact voter confidence that their ballot will be properly counted.

- **The US Postal Service's financial crisis could impact reliable operations, resulting in undue delays for outbound and inbound by-mail ballots.** In response to cash flow issues, the newly-appointed Postmaster General is already cautioning mail carriers to "leave mail behind" until the next day in order to reduce costs and labor hours;[4] this is just one example of how increased delays could impact the delivery and receipt of by-mail ballots – which could directly impact the number of ballots from eligible voters that ultimately get counted (perhaps through no fault of the voter at all).

2. A surge in absentee/by-mail voting could reduce transparency, with attendant risks to public faith in legitimacy of results

The surge in ballots cast through the mail means that a significant portion of election administration operations in 2020 could move beyond easy public viewing, unless election officials take methodical and proactive measures to increase transparency and public confidence in election operations.

Unlike in-person voting, which is a public event that easily lends itself to visual monitoring at multiple polling places, processing and scanning of by-mail ballots typically takes place in a centralized location, within the walls of the central elections office. "All-mail" states with experience in these types of elections are accustomed to designing transparency into their implemented operations, for example with windows where the public may observe secure rooms where ballots are opened and processed, or through closed-circuit cameras that allow the public to view operations on a public webpage. However, many jurisdictions that are less accustomed to extensive by-mail voting operations may not take such steps to ensure transparency on processing and counting ballots – and that could increase opportunities for speculation, partisan disinformation, and reduced faith in the legitimacy of outcomes.

What it might look like:

- **A surge in by-mail voting increases the risk that more submitted ballots will be rejected for a variety of reasons, and hence not counted.** It is likely that thousands of by-mail ballots will be rejected for counting, due to various voter mistakes that could potentially be prevented through robust voter education and outreach between now and the fall[5] – but mistakes will likely persist, to the perceived advantage of one party or the other.

[4] The Washington Post, "Postal Service memos details 'difficult' changes, including slower mail delivery," July 14, 2020. https://www.washingtonpost.com/business/2020/07/14/postal-service-trump-dejoy-delay-mail/

[5] Eddie Perez, Twitter, July 16, 2020. https://twitter.com/eddieperezTX/status/1283780212828901387

Partisan legal battles over ballot rejections are a virtual certainty. It should also be emphasized that ballot rejections disproportionately affect seniors, minorities, and new voters. Below are just a few reasons why by-mail ballots might be rejected for counting:

  - Failure to arrive by stated deadlines.
  - Failure to have a postmark on return envelope.
  - Failure to seal envelope(s) in required locations.
  - Failure to provide validating credentials, including signature problems: voters may either fail to sign their name in all required locations (of which there may be more than one); or review teams (typically bipartisan) in the elections office may have concerns about the validity of a voter's signature as compared to the one on file.

- **Increased use of digital ballot scanners in the central office raises the potential for concern over whether scanners are counting votes accurately.** When voters cast paper ballots through hand-fed scanners in precinct locations, they have the opportunity to get immediate feedback about their ballot, and the chance to correct any issues. For example, if a precinct scanner detects that a voter has marked too many choices, of if unclear marks are found to be "marginal," the scanner may reject the ballot and return it to the voter with an information message, so that such issues can be corrected.

  However, such voter-feedback mechanisms do not exist in the centralized, high-speed scanning environment. Batch-fed scanners operate in automated fashion, and the question of what voter marks the scanners are seeing and recording (or not) – and whether they conform with apparent voter intent – presents new challenges.

  Although modern digital scanning voting technology allows human operators to review or "adjudicate" exceptional marks, a complex mix of pixel density, voter behavior (e.g., completely filling in an oval, versus making a clear and unambiguous checkmark), and scanner configuration can have a big impact on whether exceptional marks are flagged for human review or not, and whether the voting system accurately records votes in accordance with voter intent. These concerns recently arose in the Georgia primary election.[6] Again, without sufficient transparency or post-election audits to confirm that the voting system's interpretation of voter choices conforms with those of human auditors, public faith in back-office processing of by-mail ballots could become an issue, particularly in races with close margins.

[6] AP, "Activists cite tabulation flaw in mail-in ballots in Georgia," June 13, 2020. https://apnews.com/66c2b4b36609d83aa5c08235f947ea59

- **A surge in by-mail voting means that additional time will be required to count ballots and release results, which creates a ripe environment for disinformation and other attempts to discredit the legitimacy of the counting process—and ultimately the Presidential Election.** An increasing number of election observers and journalistic outlets have correctly noted that there is a high likelihood that, unless there is a wide margin of victory for a clear winner in the Presidential Election, the release of official results is likely to last weeks, or could even extend into early December. Those same observers have also correctly noted that *the period after November 3 will be a vulnerable time for our representative democracy, as some (including the current President) may not accede to a peaceful transfer of power.*

  During this delicate period, responsible media outlets have a *critical* role to play, by 1) not prematurely calling races, especially if many ballots remain to be counted; and 2) most importantly, by reminding the public that delays are a normal part of counting by-mail ballots accurately and methodically, and are not a sign of problems or so-called malfeasance.

Section II: Typical Murphy's Law— What Usually Goes Wrong, and Probably Will Again

In addition to the new challenges that come with changes due to COVID-19, prudence dictates that the nation should expect the same kinds of lamentable issues that have plagued election administration in the U.S. for years: sub-optimal voting experiences due to human error, technology malfunctions, or both.

1. Poll Workers or election officials are likely to make mistakes

Poll workers or election officials do not always do the right thing, due to insufficient training, human error, and/or lack of resources. This section is limited to problems associated with **human errors**, and does *not* include technology malfunctions.

<u>What it might look like:</u>

- **Poll book issues may lead to check-in delays and long lines.** Manual or digital poll book ("e-pollbook" or "ePB") lookups may take a long time if poll workers are not adequately trained to use check-in tools. In Georgia, for example, many poll workers did not know the "PIN" to open electronic poll books, which immediately prevented them from processing voters as soon as polling sites were opened.
- **Poll workers may apply voter eligibility or ID requirements improperly.** Poll workers may declare that voters fail to meet voter ID requirements, although the voter technically was able to meet official ID requirements; or poll workers may not be helpful to voters in filling out the affidavit for a provisional ballot.

- **Complex technology setup might delay opening of in-person polling places, leading to long lines.** Because many jurisdictions acquired new voting equipment in recent years, or because their poll workers may be new/recently recruited, due to COVID-19, poll workers may be unfamiliar with new election technology. If they cannot correctly set up complex devices and equipment at the start of the day, in-person polling locations may not be able to process voters efficiently. Georgia's 2020 primary election was a dramatic example of how complex new equipment contributed to a chaotic Election Day.
- **Poll workers might improperly declare "cut off" points at the close of polls for in-person voting.** In most jurisdictions, poll workers make a determination that any voters that were in line at the designated close polls time may nevertheless vote, even if the polling place must remain open later to process all voters. These "cut offs" are sometimes improperly applied, and may result in controversy, or sometimes even emergency court orders to ensure that voters in line can vote.

2. Technology malfunctions should be expected

It has become a truism that technology used to support elections in the U.S. typically causes disruptions during every election cycle. The technology-related issues below have already occurred during past elections, and are likely to appear again.

What it might look like:

- **Electronic poll books may have problems communicating with centralized voter registration records, which can lead to bottlenecks and long lines during voter check-in.** Electronic poll books commonly use wireless technology that may be spotty, and if centralized voter registration databases are not properly load-tested, the high volume of communications from multiple polling locations at peak hours can impede performance. Los Angeles County in particular experienced significant disruptions to smooth operations due to e-pollbook issues during Super Tuesday 2020.

  Special Case: voter list modifications. While regular voter list modifications are required, they typically lead to errors in every major election, particularly because many voters who cast ballots in Presidential elections may not be regular voters otherwise. This is part of the voter registration churn issue (i.e. millions are removed from voter rolls every cycle, many for valid reasons; but in 2018, 9.3 million were removed for unknown or unstated reasons).
- **Touch screen voting devices may not correctly mark the voter's choices, which can undermine voter confidence.** Concerns about "vote flipping," which are usually associated with mis-calibrated touch screens, are common. It should also be noted that, since 2016, many states have "refreshed" their old paperless DRE devices with new ballot marking devices that also use touch screens, and they are not immune to voter concerns about their performance.

- **Ballot printing paper jams.** Especially as consolidated Early Voting and Election Day Vote Centers become more popular (particularly in response to COVID-19 polling location reductions), an increased number of paper ballots are being printed "on-demand," instead of being pre-printed. Paper ballots for hand marking may be generated at the time of voter check-in, and, as noted above, with more jurisdictions using "ballot marking devices," those are also dependent upon printing technology. Any technology issues that prevent ballots from being printed have the potential to stall voting.

- **Optical scanning devices can jam when voters insert ballots, which can create bottlenecks.** Particularly in humid environments, scanners may jam, and because many polling places have only 1 or a few hand-fed scanners to cast the vote, ballot jams can rapidly result in bottlenecks.

Section III: Beyond Murphy— Potential Attacks the OSET Institute Will Be Watching For

1. Disinformation In General: Lies, Lies, Damn Lies

2020 will be a ripe situation for disinformation, because the President of the United States is himself providing air cover to disinformation actors, with claims of "rigging" and "fraud." Other political operators are pouring considerable money into so-called "integrity watch" operations that will be motivated to find problems to justify the expenditures. Disinformation actors will have ample content, due to spurious "suspected fraud" findings, along with the "more of the same" larger numbers of typical dysfunction. [7]

Examples of what it might look like:

- Disinformation actors hack Twitter and use high-profile account names to spread false or misleading information that impacts the election
- Disinformation actors promote fake VR websites
- Disinformation actors deface official election office websites (e.g., "#RIGGED 2020")

2. Disinformation Aggregation: A Mixture of True and False

A particularly worrisome phenomenon is the likelihood that disinformation actors could have "a field day" by aggregating *true* reports of typical dysfunction, *spurious* similar reports, *speculative* "suspected fraud" reports by real people, and *intentionally fabricated* similar reports. The artful combination of just-enough factual information to make something seem plausible, in conjunction with false or misleading information, is a toxic mix – with the capacity to go viral through social media.

[7] Many of the specific examples of potential dysfunction in this section are inspired by the Cybersecurity Infrastructure Security Agency (CISA), "Elections Cyber Tabletop Exercise Package/Situation Manual," January 2020 https://www.cisa.gov/sites/default/files/publications/Elections-Cyber-Tabletop-Exercise-Package-20200128-508.pdf

In addition to that, as noted above, the potential opacity of by-mail ballot processing and counting opens up a field ripe for exaggeration and fabrication—especially when counting will require multiple days and the public visibility will not be 100% consistent.

Examples of what it might look like:

- After legitimate news sources issue reports about a printing vendor making mistakes in printing actual by-mail ballots, disinformation actors create a viral social media campaign telling voters that the local elections office is deliberately excluding certain candidates from by-mail ballots. The story is shared on Facebook by various fake accounts that belong to a group called "Citizens for Election Integrity."
- Disinformation actors spoof actual government websites with official-looking facsimiles, but substitute incorrect/false information for voters (e.g., inaccurate information about early voting locations and hours).
- Disinformation actors conduct social media campaign with a fabricated story that independent attacks against been made against actual state and local government networks.

3. Actual Cyber-Attacks: Penetrating Election IT Infrastructure

We know from 2016 that state voter registration databases were uniformly targeted with some penetration, and we "suspect" (but cannot comment officially) that some local election officials were successfully attacked at least by phishing, and possibly also by way of "VPNfilter" and other pervasive persistent cyber-attacks. There is no reason to expect the 2016 adversaries (and new ones) to stand down in 2020.

However, it takes time and effort to detect and investigate real reports of possible attacks, and professional and/or government assistance is required, including threat intelligence from the intelligence community; so any intelligence community involvement with the Department of Homeland Security (DHS) is likely to result in classification of the findings. As a result, credible reports of cyber operation may come too late to be part of the election news cycle. On the other hand, because the election news cycle is likely to last well beyond November 3, there is more calendar time for leaks to occur that could compromise confidence in election results, before the results are final.

A particular factor for 2020 may be an increased number of jurisdictions (and possibly an increased number of voters) using Internet voting methods from Voatz or Democracy Live, which can return voter-marked ballots electronically, without a paper record. DHS warnings about such systems may decrease usage, but have already increased public awareness of such systems, making them even more valuable targets for disruptive cyber-attacks that are publicly visible and that can decrease voter confidence.

Examples of what it might look like:

- Threat actors use phishing campaigns to penetrate state and local government systems.
- Threat actors include ransomware payloads in malicious attachments to eMails. Ransomware could "lock up" data for voter registration, or results data used for Election Night Reporting, for example.
- Threat actors disrupt online voter registration, leading to a denial of service.
- Threat actors disrupt online absentee ballot request tools, leading to a denial of service
- Threat actors alter voter registration data, which leads to mass confusion for both by-mail voting (i.e. impacts to outbound mailing and verification of voter records) as well as in-person voting (i.e. to impacts poll book printing or e-pollbook configuration).
- Threat actors alter voter registration data shared with by-mail printing vendors, which results in mass numbers of "undeliverable" mail, due to maliciously-altered names and/or addresses.
- Cyberattacks on non-election-specific critical infrastructure, such as the power grid, city traffic lights, etc.[8]

4. Pseudo-Attacks: Impersonation That Leads to Disruption (Even if Detected)

There are many parts of the election process vulnerable to pseudo-attacks, which involve impersonation activities that are based on actual voter information that is at least *partly publicly visible*, and which can be used to disrupt the activities of actual voters. Such attacks undermine voter confidence and election legitimacy.

Examples of what it might look like:

- Voter lists can be manipulated via the "front door" rather than requiring cyber-attacks. Most registered voters' personal information is available to threat actors, who can use that information to impersonate a voter to a VR system, in order to change that voter's registration so that the actual voter's experience will be disrupted. For example, a change of name, address, or absentee status can all be used to impede voters. These impersonation attacks can be done at scale in any state, via online voter registration or paper-based voter registration, or both. Scale attacks can be stealthily executed over time, with increasing scale to avoid detection until the time of the adversary's choice; or they could be done at very large scale over short time frames, to essentially swamp the system's

[8] For a dramatic example of how Election Day chaos could be generated without needing to actually attack any election-specific assets, see NBC News, "How a fake town and real hackers battle test officials for Election Day 2020," November 6, 2019. https://www.nbcnews.com/tech/security/how-fake-town-real-hackers-battle-test-officials-election-day-n1077836

processing of requests, thereby creating a denial of service that creates delays in processing real requests.

- Voter impersonation can also be used to change mailing addresses to redirect by-mail ballots so that not only is the voter impeded, but the attack has the additional "bonus" inflammatory effect of feeding claims that errant by-mail ballots are being "harvested" and fraudulently voted.
- Voter impersonation can also be used in the absentee ballot request process, to direct the absentee ballots to be mailed to another address, without the voter's knowledge; or to make several such contradictory requests for each of many voters, so that local election officials do not actually know which is a legitimate request, or where to mail the absentee ballot.
- Fraudulent ballots that have the surface appearance of being authentic are also relatively easy to manufacture in bulk, with deleterious effects – even if the many safeguards associated with by-mail voting would almost certainly detect those ballots as inauthentic and prevent them from being voted.[9] Even if ultimately detected as fraudulent, threat actors' efforts to mass-mail such ballots could both swamp a jurisdiction's intake process, and also create claims of fraud that could be used in disinformation aggregation campaigns (e.g., actual attack plus amplification via disinformation by the same team).

  Even if caught, large numbers of very obviously fraudulent ballots could have many benefits to disinformation operators, and could also serve to disenfranchise a targeted voter if local election officials cannot easily, and with confidence, find the real voter's ballot in a large set of fake ones.[10]

5. Capacity Attacks: Overwhelming Systems to Cause Disruption

In addition to process-based capacity attacks (i.e., so many absentee ballot requests or absentee ballots that local election officials cannot handle them in a timely manner), technology can also be employed to undermine capacity. The classic case is termed a "distributed denial of service" (DDOS), which is an attack on network-connected systems such as state election services web sites; related county web sites; election night reporting systems; and the Internet-connected back end systems that coordinate a county-wide real-time connected electronic poll book

[9] OSET Institute, "Stop the Nonsense About 'Counterfeit' By-Mail Ballots – Here are the Facts," https://www.osetfoundation.org/blog/2020/6/30/ballotnonsense

[10] Another similar example of a possible pseudo-attack that could be performed in bulk (and also easily trapped and stopped in bulk) involves the "Federal Write-In Absentee Ballot" (FWAB) that any overseas or military voter is entitled to use. The FWAB which is essentially a "made-at-home" ballot where the voter can simply list the name of a contest for office, and the name of the candidate of their choice, for as many or few of the contests that they are eligible to vote for. It is not hard to create a false FWAB and combine it with the required signed affidavit for a real voter (voter lists are readily available to adversaries), or for large numbers of spurious voters. It is also not hard to create signatures that will not match – even if election officials will detect these on signature verification. Even though it is likely that these fraudulent ballots would be caught, the attack can swamp the capacity of an elections office to process real ballots.

system. While DDOS attacks can be mitigated, the initial impact can be substantial, with real impact if such is timed properly.

Examples of what it might look like:

- Threat actors overwhelm online voter registration systems or online absentee ballot request systems at scale, with fraudulent requests.
- Threat actors use "robo-call" facilities to swamp important phone communications for election operations (e.g., numbers used for poll workers to request technical assistance, or to call in unofficial vote counts.) The Iowa primaries provide an illustrative use case for non-malicious capacity outages.

6. Pseudo-Suppression Attacks: Dirty Tricks to Stop Voters from Voting

Prior elections have seen a number of "dirty tricks" tactics to impede voters from casting a legitimate ballot, or to make them think they have voted when in fact they have not.

In 2020, tactics like this are even more of interest when conducted not by domestic political actors working for perceived political gain, but rather by foreign adversaries with much greater capability and capacity, and who conduct the attacks to implicate domestic political actors.

Such attacks on in-person voting operations would be especially effective in 2020, since, due to COVID-19, many jurisdictions have a much smaller number of voting places. In such an environment, any method of hampering voting place operations could have a disproportionately large effect, and a substantial negative impact on public confidence in the election process. Finally, we have seen in recent primaries that likely non-malicious capacity problems have led to suspicions of suppression; they provide a model for malicious threat actors to similarly suppress the vote in November.

Examples of what it might look like:

- Robo-calls with spurious information about how to vote
- Robo-calls soliciting participation in spurious vote-by-phone methods
- Spam campaigns for spurious email voting
- Spurious claims of closed voting locations
- False bomb threats intended to close a voting location

Conclusion and Short List

The 2020 Presidential Election has rightly been anticipated to be one of the most divisive and consequential elections in recent U.S. history. Turnout is expected to be record-setting, partisans on both sides are displaying extremely high levels of motivation and commitment, and the election is taking place in the midst of unprecedented challenges: a global pandemic; widespread social unrest; and conditions that have radically upended election administration across America. The nation's typical challenges in recent years, which have led to long lines for voters, concerns about the integrity of results and ragged election administration in general, still persist – but they have been greatly compounded by public health concerns, disruptions to in-person voting, a dramatic increase in by-mail voting, and baseless claims from the President about so-called "fraud" and "rigged elections." The President has not committed to accepting the legitimacy of the election results. These conditions are startling and dangerous for our democracy. For the same reason, we hope that this Executive Briefing is valuable and helpful to election officials, policy makers, the media and other stakeholders in making preparations to protect our democracy and public faith in the legitimacy of November's election results.

In this Briefing, we have illustrated a combination of threats, ranging from implementation challenges, lack of resources, process changes, and human error; to technological vulnerabilities, whether inherent to deployed voting systems, or exploitable by motivated malicious actors who might make cyber-attacks; as well as historically low levels of voter trust that have created multiple opportunities for disinformation campaigns, especially through social media.

While the Briefing is comprehensive and includes dysfunctions that range widely in terms of likelihood and severity of impact, we conclude with this short list of what we believe are most likely and most impactful. We will revisit this list with issues to watch in specific battleground states, as we get closer to September. Finally, we also caution that the possibility of more dramatic and worrisome -- though perhaps less likely -- attacks should not be ignored.

Most Likely Dysfunctions to Anticipate in the 2020 Presidential Election

1. High volume of absentee by-mail ballot requests, which leads to delayed mail deliveries and voters without ballots.
2. In-person polling place dysfunction (including long lines for voters and inoperable election equipment), due to poor poll worker training on operational procedures and consolidation of in-person polling places due to the pandemic; and difficulty in recruiting adequate skilled poll worker staff.
3. Long lines for voters, due to delays with electronic pollbook check-in, including some that might be credibly claimed to be DDOS attacks.
4. Errors in voter record lists which may be imputed not only to prejudicial intent, but also to a repeat of 2016-like cyber-attacks on voter registration systems.
5. Disinformation actors leveraging real incidents for disinformation campaigns, including spurious additional incidents.