WINTER 2022 / ISSUE NO.20

$ 15.00 | € 10.00 | 1500 RSD

HORIZONS

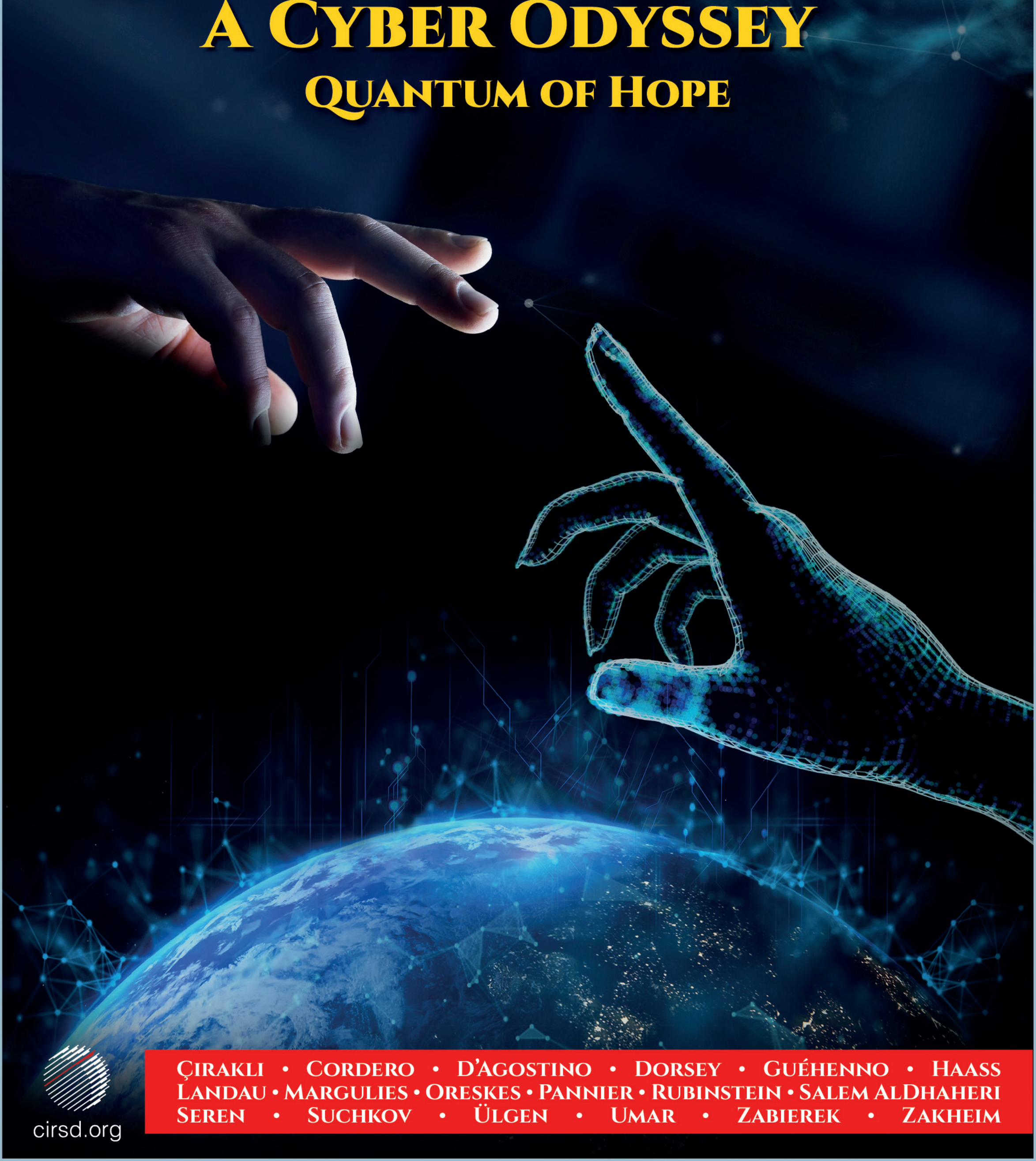
Journal of International Relations and Sustainable Development

ISSN 2406-0402

9 772406 040003 00020

A Cyber Odyssey

Quantum of Hope



Çirakli • Cordero • D'Agostino • Dorsey • Guéhenno • Haass
Landau • Margulies • Oreskes • Pannier • Rubinstein • Salem AlDhaheri
Seren • Suchkov • Ülgen • Umar • Zabierek • Zakheim

cirsd.org

How Cybersecurity Saved U.S. Democracy

Carrie Cordero

ACCORDING to a 12 November 2020 joint statement of U.S. election officials, the 2020 U.S. presidential election "was the most secure in American history." That success was a result not of accident, but instead of deliberate, sustained, and comprehensive efforts at the local, state, and federal levels to ensure that it was secure from foreign interference. Those efforts to secure the election were borne out of the attempts by the Russian government to influence the outcome of the 2016 U.S. presidential election. In the end, however, the efforts to enhance the cybersecurity of the U.S. electoral infrastructure in 2020 ended up protecting the integrity of the election not only from malign foreign activities, but also from domestic anti-democratic and illiberal efforts to undermine confidence in the 2020 presidential election.

A range of activities designed to protect the American election infrastructure from foreign malign activity ended up providing a bulwark against threatening domestic efforts to undermine and overturn the lawful election result. The U.S. experience in 2020 suggests that cybersecurity itself can play a critical role in protecting not only election infrastructure as a technical matter, but also providing a technical basis to counter illiberal forces as a mechanism to protect the democratic process of conducting a fair election. Cybersecurity itself just may have saved U.S. democracy from careening of the rails, continued sustained efforts to continue to harden election infrastructure cybersecurity and create a cadre of trusted officials, will likely be needed again.

Carrie Cordero *is the Robert M. Gates Senior Fellow and General Counsel at the Center for a New American Security, Adjunct Professor at Georgetown Law, and a CNN legal and national security analyst. She previously served as Director of National Security Studies at Georgetown Law, Counsel to the U.S. Assistant Attorney General for National Security; Senior Associate General Counsel at the Office of the U.S. Director of National Intelligence; and Attorney Advisor at the U.S. Department of Justice. This essay draws, in part, from materials produced as part of the CNAS commentary series on Bolstering American Democracy Against Threats to the 2020 Elections, as well as congressional testimony by the author on foreign interference in the U.S. 2016 election, in June 2019. You may follow her on Twitter @carriecordero.*

Photo: Gulliver Image/Getty Images

On 6 January 2021 a mob stormed the U.S. Capitol, delaying the election's certification

Despite the success of U.S. cybersecurity and intelligence activities in protecting against malign foreign influence, the voting mechanisms and outcome of the 2020 American election has been subject to persistent allegations of fraud and inauthenticity by malicious domestic partisans. These domestic political actors seek to lower voter confidence in the outcome, thereby politically damaging their opponents and undermining confidence in future elections that they lose. As of this writing former President of the United States Donald Trump has not publicly accepted the validity of the 2020 election outcome, and a significant percentage of Americans identifying as Republicans still did not believe that President Joe Biden had lawfully won the 2020 election.

When the U.S. Congress reconvened after the insurrection that delayed the certification of the vote on 6 January 2021, 147 Republicans voted to sustain the false challenges to the vote outcomes in Arizona and/or Pennsylvania. And yet, despite the political support from Republican politicians and their supporters between 3 November 2020 and 6 January 2021 to re-engineer the outcome of the election, these pernicious efforts were largely able to be credibly rebuffed and refuted This ability to confirm the election outcome was a significant downstream effect of the engagement of the cybersecurity community and activities that had been implemented across the country leading up to the 2020 presidential election.

The effective functioning of American democracy is being strained by the recent unravelling of the U.S. social and political construct that lawfully-conducted election outcomes are respected and accepted by both the winning and losing candidates. That being said, the experience and challenges presented by the U.S. 2020 election and accompanying improvements that were made to secure the election from a cybersecurity perspective provided necessary assurances that the election outcome was accurate and fair. This experience provides lessons not only for the U.S., but for the international community interested in ensuring that elections are not only free from both technical cyber intrusion by malign foreign actors, but also fortified against countering disinformation about the security of the election architecture itself.

The U.S. experience in 2020 suggests that cybersecurity itself can play a critical role in protecting not only election infrastructure as a technical matter, but also providing a technical basis to counter illiberal forces as a mechanism to protect the democratic process of conducting a fair election.

The lesson that can be drawn from the U.S. experience in the 2020 presidential election is that accurate technical data and expertise is the best defense to refute international or domestic misinformation and malice to undermine democratic elections. In other words, cybersecurity—and the expertise and credibility of those in charge of it—is turning out to be the best defense against efforts to undermine democratic elections. Security of election administration is paramount for securing democracies and protecting against foreign or domestic efforts to undermine the actual outcome or confidence in the outcome.

How to Endanger an Election

We know the story of the 2016 U.S. presidential election: malign foreign cyber activity directed by the Russian government and its surrogates was conducted against the U.S. population and election ecosystem. The Russian efforts to influence the election were substantially documented in two independent investigations. The first, completed in March 2019 but not released by former Attorney General Bill Barr until 18 April 2019 (and then only in redacted form), was Volume I of the *Report on the Investigation Into Russian Interference in the 2016 Presidential Election*, as a result of the investigation led by Special Counsel Robert S. Mueller III, a former FBI director. The Special Counsel's investigation exposed a sustained, systematic intelligence operation by the government of Russia to interfere in the 2016 election.

According to the Special Counsel's report—and as I described in June 2019 during my testimony before the U.S. House Committee on the Judiciary—the Russian activities started as an information warfare operation intended to affect the election generally, and by 2016 was actively working to help Trump win. According to the report, the operation involved two main efforts. The *first* was a social media operation intended to influence Americans' public opinion. The effort was successful in reaching millions of Americans through social media engagement, false online personas, and ad buys. The *second* part of the influence campaign involved computer hacking to steal and then release information from the Democratic campaign apparatus, including the Hillary Clinton campaign, the Democratic National Committee, the Democratic Congressional Campaign Committee, and the emails of her campaign chairman John Podesta.

In addition, as I also discussed in my June 2019 for-the-record statement, there was arguably a *third* component, which the report discusses as part of the social media operation. This component often gets overlooked: Russian operatives caused real, unsuspecting Americans to organize rallies and gather for political purposes. These foreign operatives pretended to be American grass roots activists. These online operatives made contact and interacted with Trump supporters and Trump campaign officials.

The lesson that can be drawn from the U.S. experience in the 2020 presidential election is that accurate technical data and expertise is the best defense to refute international or domestic misinformation and malice to undermine democratic elections.

Trump campaign officials amplified social media posts produced by the Russian Internet Research Agency (IRA). Individuals influenced by Russian activities organized real-world rallies. As I wrote in my 2019 for-the-record statement, the 2016 activities were a combination of social media engagement, criminal cyber intrusion, and political organization on the ground in local American communities.

The second comprehensive, independent investigation was the five-volume report issued by the Senate

Select Committee on Intelligence, which documented the active measures and social media influence effectuated by the Russian government and its surrogates, American intelligence assessments, the U.S. response to these activities, and the counterintelligence threats and vulnerabilities reviewed by the committee.

Taken together, these collective reports comprising thousands of pages issued by components of two separate branches of the U.S. government established a compelling narrative explaining Russian efforts to influence the U.S. election through direct malign cyber activity, social media information operations, and other attempts to influence U.S. public opinion in the physical world.

How to Protect an Election

In 2020, the threats compounded as compared to 2016. Not only were there Russian government efforts—although not on the scale of the 2016 influence campaign—but according to the U.S. intelligence community, Iranian and Chinese government actors also engaged in varying levels of attempted influence on the 2020 election outcome.

Moreover, as election day passed, the greatest threat to public confidence in the election outcome came from domestic politics: Trump and his political allies led an aggressive campaign to undermine confidence in the election and try to overturn the election outcome. This effort came to a head in the events of 6 January 2021 when a mob stormed the U.S. Capitol, causing the delay of the certification of the election by the U.S. Congress. Five people died, including U.S. Capitol Police Officer Brian Sicknick.

In 2020, not only was the Russian government engaged in varying levels of attempted influence on the election outcome, but also Iranian and Chinese government actors.

The improved set of efforts in 2020 by the United States were the result of three main lines of effort: a whole of government initiative, which involved activities at the federal, state, and local levels; technical defenses, which were bolstered by U.S. federal resources and expertise offered; and credible messengers, including senior level American national security and cybersecurity leaders who were willing to provide accurate information in public, regardless of the professional consequences, including, in some cases, political retribution and threats to their own personal safety and that of their families. Each of these components provided a basis upon which the independent U.S. media could accurately report and amplify accurate information regarding the reliability of voting systems, and the legitimacy of the 2020 election outcome.

As Erik Brattberg of the Carnegie Endowment for International Peace explained in a commentary that was part of a series on foreign interference published by the Center for a New American Security (CNAS), America was not alone in 2020 in working to secure elections against foreign influence efforts: "Russia's interference in the November 2016 U.S. presidential election served as a wake-up call for Europe about the rising threats facing free and fair elections." Brattberg outlined how efforts in EU member states to elevate election security as a priority national security issue, assist political parties and campaigns with cybersecurity expertise and resources, and focus on voter education all contributed to building more resilient elections in various European Union member states.

The effort to protect the actual security of the 2020 election and counter post facto allegations that it was unsecure required a whole of nation effort.

Coordinating Government Entities.

American elections are run locally; the U.S. federal government does not administer them and is not in charge of them. The effort to protect the actual security of the 2020 election and counter post facto allegations that it was unsecure required a whole of nation effort that ranged from the Cybersecurity Infrastructure Security Agency (CISA) of the Department of Homeland Security and other parts of the intelligence community to state and local election officials, but also included a range of private sector entities that facilitated the implementation of technical defenses.

As a result of what happened in 2016, local, state, and federal officials took far greater steps over the subsequent four years to ensure that there would not be a repeat performance in 2020. As Deputy Secretary of State for the State of Connecticut Scott Bates wrote as part of the aforementioned series on foreign interference published by CNAS, "the challenge for us as a nation is that it is not the federal government that runs our election system, but that responsibility resides with the 50 states. Thus, it's up to each of the 50 states to defend itself against aggressive nation-states." According to Bates, Connecticut implemented a plan leading up to the 2020 election that, *one*, provided National Guard resources so that assessments of individual municipalities' cybersecurity readiness could be undertaken; *two*, provided and state resources to update computer systems; *three*, supported election cybersecurity education and training, and *four*, put a communications plan in place to counter disinformation.

The U.S. federal government had a meaningful role to play in providing expertise and resources before the election. Leading up to the 2018 midterm elections and continuing through the 2020 campaign season, CISA prioritized election security at the top of its agenda. As former CISA Director Chris Krebs wrote in the same aforementioned CNAS series, the designation of the election systems as "critical infrastructure" was integral to acknowledging that "election infrastructure is of such vital importance to the American way of life that is incapacitation or destruction would have a devastating effect on the country."

CISA was able to convene state and local election officials alongside private sector partners to foster a robust election security community and facilitate the sharing of technical expertise and resources.

In fact, CISA was able to convene state and local election officials alongside private sector partners to foster a robust election security community and facilitate the sharing of technical expertise and resources. As described below, CISA's activities in marshalling the lessons and insights from its work to improve technical defenses proved integral in using its communications capabilities to authoritatively refute baseless allegations of voter fraud and voting machine malfunction and exploitation.

Hardening Technical Defenses.

The decentralization of the U.S. election infrastructure turns out to be an advantage; centralization increases risk. The private sector served a pivotal role in working with government officials to implement cybersecurity initiatives. Some private companies worked to provide cybersecurity related services and resources free of cost to political campaigns and state and local websites. State and local governments, however, often short on resources, had varying levels of modernized hardware and software supporting election administration. The federal government was able to effectively provide technical expertise to states and localities, and coordinate efforts across the country.

Here's how Krebs described CISA's efforts to improve the technical security of the decentralized U.S. election infrastructure:

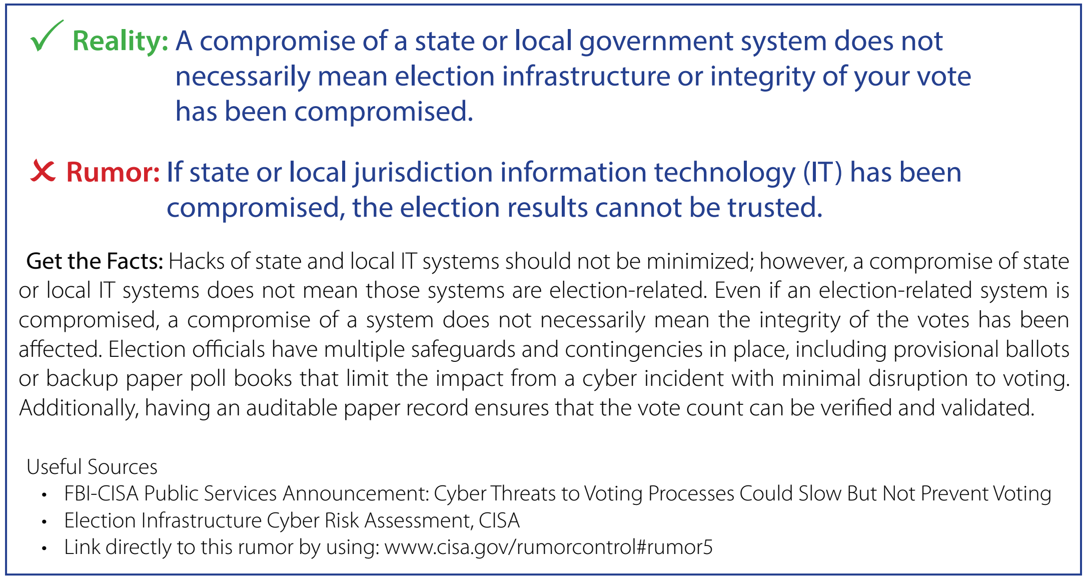
> For both in-person and mail-in voting, we are helping election officials secure the underlying systems and processes by providing a range of services, such as system vulnerability scans on a weekly basis, remote penetration testing for hundreds of jurisdictions and dozens of states, and phishing assessments. There is no question the security posture of election systems is getting better. We have observed improved patch rates, increased adoption of multifactor authentication, more regular backups, and expanded logging of systems, to name just a few. We have worked with the largest election technology providers in the country to pick their systems apart, looking for vulnerabilities, and helped them mitigate those vulnerabilities. We continually work to map out and understand the various systems, mechanisms, processes, and techniques used across the election community to determine where the riskiest bits are and what is effective at managing those risks. One of the best risk management and resilience-building techniques we have found is paper. We continue to encourage states to shift to systems with a paper record associated with every vote—which is essential, because of the ability to audit such records. In 2016, 82 percent of votes cast were associated with a paper record, and for 2020 we project more than 92 percent of votes cast will have a paper record.

Importantly, the range of technical defenses includes the least technological but a critical aspect of providing a verifiable result: paper ballot backups. From 2016 to 2020, the percentage of states with paper ballot backups significantly increased, not all states had paper ballot backups available for all voters in 2020. The existence of paper ballot backups is something that all election administrators should work to facilitate, as the availability of the backup can facilitate an actual recount, if needed, as well as a bulwark against allegations that machines are at fault and cannot be verified.

Amplifying Credible Messengers

The presence of cybersecurity activities provided credible government officials with a basis upon which to offer accurate information to the public, but also to be believed. The assurances by public officials were not just empty assurances that election results could be trusted—they were assurances based on the facts of how elections are verified through extensive processes, and on the enhanced understanding and attention that state and local officials had dedicated to improving the cybersecurity of the election technology infrastructure since 2016. In addition, the credibility of the message was enhanced when the messengers themselves ranged from unelected national security leaders to elected and partisan state election officials.

At the U.S. federal level, senior national officials, including FBI Director Chris Wray, National Counterintelligence Executive William Evanina, and CISA Director Chris Krebs provided the public with non-partisan, unclassified information regarding the nature of the foreign threats to the 2020 election. As the election drew near, these leaders released video messages outlining the threat posed by foreign adversaries and communicating the



✓ **Reality:** A compromise of a state or local government system does not necessarily mean election infrastructure or integrity of your vote has been compromised.

✗ **Rumor:** If state or local jurisdiction information technology (IT) has been compromised, the election results cannot be trusted.

Get the Facts: Hacks of state and local IT systems should not be minimized; however, a compromise of state or local IT systems does not mean those systems are election-related. Even if an election-related system is compromised, a compromise of a system does not necessarily mean the integrity of the votes has been affected. Election officials have multiple safeguards and contingencies in place, including provisional ballots or backup paper poll books that limit the impact from a cyber incident with minimal disruption to voting. Additionally, having an auditable paper record ensures that the vote count can be verified and validated.

Useful Sources

- FBI-CISA Public Services Announcement: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- Election Infrastructure Cyber Risk Assessment, CISA
- Link directly to this rumor by using: www.cisa.gov/rumorcontrol#rumor5

Example A

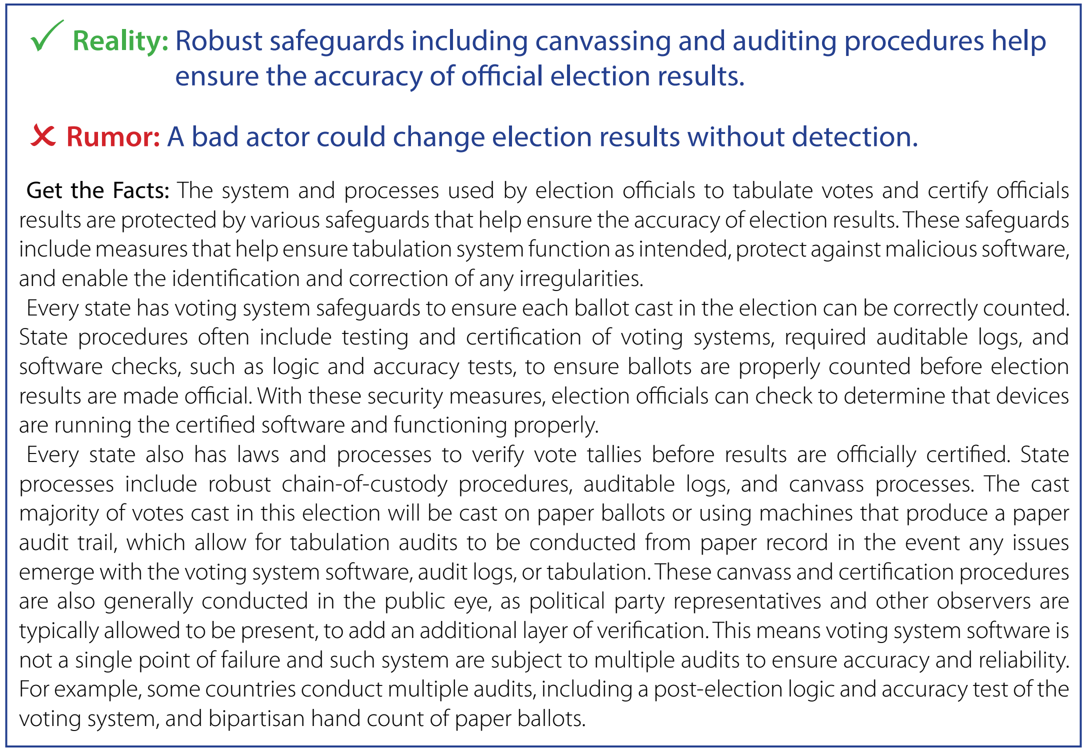
national security community's attention to preventing foreign interference from Russia, Iran, and China from successfully impacting the election.

In 2020, CISA created a webpage entitled Rumor Control as part of its public communications strategy to counter disinformation originating from malign foreign activity directed against the upcoming November 2020 presidential election. This website was integral to these efforts to combat misinformation—whether foreign or domestic in origin.

There, on a rolling basis, CISA posted accurate, verified information dispelling myths and other inaccurate information about the election, shooting down myths that were arising with increasing frequency as the election neared with real-time information about how voting systems actually work (see Example A).

But Rumor Control became even more important in the days after the election, using its expertise, credibility, and platform to counter domestic efforts from the incumbent president, his political surrogates, and political allies in certain key states where the vote count was close (see Example B).

Krebs shared the information that was published on CISA's Rumor Control website on his personal Twitter account and used his own professional credibility as a cybersecurity professional willing to work across party lines to counter the post-election attacks on the credibility of the election outcome.



✓ **Reality:** Robust safeguards including canvassing and auditing procedures help ensure the accuracy of official election results.

✗ **Rumor:** A bad actor could change election results without detection.

Get the Facts: The system and processes used by election officials to tabulate votes and certify officials results are protected by various safeguards that help ensure the accuracy of election results. These safeguards include measures that help ensure tabulation system function as intended, protect against malicious software, and enable the identification and correction of any irregularities.

Every state has voting system safeguards to ensure each ballot cast in the election can be correctly counted. State procedures often include testing and certification of voting systems, required auditable logs, and software checks, such as logic and accuracy tests, to ensure ballots are properly counted before election results are made official. With these security measures, election officials can check to determine that devices are running the certified software and functioning properly.

Every state also has laws and processes to verify vote tallies before results are officially certified. State processes include robust chain-of-custody procedures, auditable logs, and canvass processes. The cast majority of votes cast in this election will be cast on paper ballots or using machines that produce a paper audit trail, which allow for tabulation audits to be conducted from paper record in the event any issues emerge with the voting system software, audit logs, or tabulation. These canvass and certification procedures are also generally conducted in the public eye, as political party representatives and other observers are typically allowed to be present, to add an additional layer of verification. This means voting system software is not a single point of failure and such system are subject to multiple audits to ensure accuracy and reliability. For example, some countries conduct multiple audits, including a post-election logic and accuracy test of the voting system, and bipartisan hand count of paper ballots.

Example B

On 12 November 2020, CISA published a joint statement from the Elections Infrastructure Government Coordinating Council and the Election Infrastructure Sector Coordinating Council Executive Committees confirming the integrity of the election mechanics and refuting allegations of voting machine manipulation or error. On 17 November 2020, Trump fired Krebs, who was the subject of threats of violence for his efforts to publicly refute false election narratives.

State leaders, particularly Republicans who refused to go along with the false allegations of voter fraud and election machine malfunctions, also served a critical role in combatting domestic political disinformation about the election outcome.

For example, the fact that Georgia Secretary of State Brad Raffensberger was an elected Republican who publicly countered the false election fraud narrative added to his credibility that the election outcome in Georgia could be trusted. Raffensberger and other Georgia election officials spoke out publicly against Trump's false public accusations of voter fraud as well as private pressure he directed at them in phone calls—all at the risk of what became persistent threats to their safety and that of their families. The Raffensberger family continued to receive death threats for the Georgia Secretary of State's role in upholding the credibility of the election outcome for many months after the election and even after the presidential inauguration of Joe Biden.

The U.S. Justice Department launched a task force intended to investigate and prosecute threats against election officials as threats increased—whether directed against elected officials, political appointees, non-partisan poll workers, or other election officials at state and local levels. As recently as late October 2021, the Florida Supervisors of Elections, currently with a Republican majority, issued a letter pleading with political candidates to "tone down the rhetoric and stand up for our democracy" in the face of "disinformation, misinformation, and malinformation" that has led to threats directed against election officials and undermines confidence in democratic institutions.

Cybersecurity's Continued Role

Election integrity measures do not only involve the technical aspects of administering elections. In addition to securing the technological aspects of election administration, bureaucratic and administrative processes that take place after votes are cast are functions that provide voter confidence in the result. As Matthew Weil and Christopher Thomas of the Bipartisan Policy Center explained in an October 2021 paper on election integrity, a variety of "security and integrity measures" are currently in place at the state and local levels in order to provide redundancy and accuracy of election outcomes. These include but are not limited to establishing a proper chain of custody, records of tabulations, and audit trails. Ensuring an election in which citizens have confidence involves not only actually securing the election technology and mechanics, but being able to provide transparency about the process and rules that are followed.

The 2016 activities were a combination of social media engagement, criminal cyber intrusion, and political organization on the ground in local American communities.

In the U.S., threats to elections are multifaceted. Over the long term, the success of the Russian 2016 influence and intrusion campaign provides foreign adversaries with substantial evidence that the investment can be low, but the reward can be high for engaging in activities intended to affect not just American elections but the fabric of U.S. society itself. According to the U.S. intelligence community, Russia and Iran tried their hand at more limited acts of interference in 2020. It would not be surprising if these or other countries with interests of their own targeted U.S. elections in the future with either malign cyber intrusion activity or perhaps a more pernicious social media influence. Thus, the U.S. national security and intelligence components will need to continue to be vigilant about identifying and countering malign foreign influence on future elections.

At least in the short term, however, the U.S. political environment is so damaged that disinformation about the integrity of the election infrastructure will remain a persistent part of the national political conversation. Even in an off-year election, for example, the Republican candidate for Governor of Virginia that took place in early November 2021 (he ended up winning) made "election integrity" a centerpiece of his campaign, with calls to audit Virginia's voting machines, despite no credible facts that Virginia's voting systems are unsecure. This current and unfortunate political environment places cybersecurity and other national security officials—who would generally prefer to avoid engaging in dialogue concerning the election for fear of being perceived as partisan—squarely with the responsibility of countering damaging allegations of vote tampering, equipment malfunctions, and other fabricated statements about the election infrastructure.

The U.S. political environment is so damaged that disinformation about the integrity of the election infrastructure will remain a persistent part of the national political conversation.

In the future, cybersecurity officials at the federal, state, and local levels will be able to look at the 2020 election as an example of how—in the face of persistent efforts to paint voting infrastructure as insecure—the work that went into securing the election ecosystem provided a factual, credible basis upon which to effectively counter malign domestic forces intent on undermining and overturning the election. Continued engagement of cybersecurity experts who work to coordinate government entities, harden technical defenses, and bolster those that are credible messengers will provide an invaluable service to the country by not only securing elections, but protecting democracy.