Election Website Tampering: Relevant Criminal Laws and Enhancing Deterrence

BY ZACH ROSENFELD*

INTRODUCTION

Imagine: It is November 5, 2024—election night. All states but Wisconsin have declared their results. With the presidency hanging in the balance, Wisconsin's vote counting stretches into a second day. Suddenly, thousands of Donald Trump votes disappear from the election results websites of three Wisconsin counties. Wisconsin shockingly turns from red to blue on CNN, Fox, and MSNBC. On The New York Times's website, the election predictor needle swings wildly in the opposite direction from where it sat moments before. The Times announces that there has been a tabulation error, revealing that Trump has thousands of fewer votes than initially shown. Kamala Harris has won Wisconsin and, consequently, the election. Protests erupt throughout the country as Republicans insist the presidency has been stolen. Where did the missing Trump votes go?

One week later, a preliminary investigation reveals the cause of this dramatic change: foreign actors hacked those three counties' election results websites, artificially inflating Trump's vote count in an attempt to muddy Harris' legitimate victory in the state. Fortunately, authorities discover the intrusion and correct it. No actual votes were impacted—the hack merely altered the results shown on the counties' tabulation websites. But for the American people, who are now more divided and less trusting of governmental institutions than ever, the damage is done. Trump calls for a new election in Wisconsin, and the Republican Party stands behind him in those efforts. Lawsuits and unrest follow. In order to prevent the violent disruption of the counting of electoral votes, Washington, D.C., becomes a military encampment on January 6, 2025.

Though we may want to believe otherwise, this is not a wildly unrealistic scenario. It is, in fact, shockingly *realistic*. Unofficial election tabulations are critical to the media's ability to

* Georgetown University Law Center, J.D. expected 2025; Tufts University, B.A. 2020. Thank you to Professor Matt Blaze, whose class I wrote an original version of this Note for, and to Anna Reid, Ria Rebein, Madeline Brown, Zachary Morrow, and the fantastic *Georgetown Law Journal Online* team for all their amazing work in helping bring this Note to fruition. Additional special thanks to Jonathan Wroblewski, Director of the Office of Policy and Legislation within the Criminal Division of the Department of Justice, and Professor Glen Nager for reviewing this Note, and Alissa Kempler, Sonia Mittal, and my other mentors within the Office of Policy and Legislation, within the Criminal Division of the Department of Justice and the United States Attorney's Office for the District of Columbia for inspiring my knowledge of the Sentencing Guidelines. Finally, special thanks to Leah Hebron for convincing me to submit this Note.

project election results[1] and can currently be easily breached and tampered with.[2] Unofficial election tabulations are vulnerable to attack, and, as demonstrated by this scenario, the consequences of meddling with them can be enormous. This Note will discuss the current state of, and overlap between, unofficial election tabulations and election-related misinformation. Additionally, this Note will analyze the application of relevant federal criminal laws to the unauthorized modification of unofficial election results, most prominently, The Computer Fraud and Abuse Act (CFAA)[3] and a 2020 law that amended the CFAA, The Defending the Integrity of Voting Systems Act (DIVSA).[4] This Note will further provide an overview of the relevant Sentencing Guidelines for a possible breach of this type. Finally, this Note will describe the state of criminal law in this area and argue that the enhanced protections the DIVSA inadvertently provided against the manipulation of unofficial election results should be utilized to adapt the Sentencing Guidelines to further deter actors in this particularly vulnerable area that is critical to the functioning of our democracy.[5]

I. THE PROBLEM

A. UNOFFICIAL VOTE TALLIES, "ELECTION RESULTS," AND FAITH IN ELECTIONS

The "results that you see on election night coverage are not final and official results."[6] These "unofficial" election results inevitably change and do so at different cadences and for different

---

[1] *See* Lenny Bronner, Emily Liu & Jeremy Bowers, *What the Washington Post Elections Engineering Team Had to Learn About Election Data*, WASH. POST: MEDIUM (Apr. 28, 2022), https://washpost.engineering/what-the-washington-post-elections-engineering-team-had-to-learn-about-election-data-a41603daf9ca; Joe Pompeo, *"Certain Readers May Have a Nervous Reaction": The* New York Times *Election Needle Is Back, With a Few New Safety Features*, VANITY FAIR (Nov. 5, 2018), https://www.vanityfair.com/news/2018/11/the-new-york-times-election-needle-is-back-with-a-few-new-safety-features; *How Does The Times Get Live Election Results?*, N.Y. TIMES (Nov. 7, 2022), https://www.nytimes.com/2022/11/07/us/politics/times-results-pages-how-data.html ("We report vote totals provided by The Associated Press, which collects results from states, counties and townships through a network of websites and more than 4,000 on-the-ground correspondents. . . . [O]ur team of data journalists and software engineers gathers vote tallies directly from the websites of election officials and compares these with our turnout expectations."); *How AP Counts the Vote*, ASSOCIATED PRESS, https://www.ap.org/about/our-role-in-elections/counting-the-vote#:~:text=Vote%20count%20reporters%20and%20vote,up%20and%20down%20the%20ballot [https://perma.cc/KY8T-LHKP] (last visited Oct. 21, 2024).

[2] *See* Brett Molina & Elizabeth Weise, *11-year-old Hacks Replica of Florida State Website, Changes Election Results*, USA TODAY (Aug. 14, 2018, 12:20 PM), https://www.usatoday.com/story/tech/nation-now/2018/08/13/11-year-old-hacks-replica-florida-election-site-changes-results/975121002/ [https://perma.cc/8U9S-SWRQ]; Michael D. Regan, *An 11-year-old Changed Election Results on a Replica Florida State Website in Under 10 Minutes*, PBS (Aug. 12, 2018, 5:00 PM), https://www.pbs.org/newshour/nation/an-11-year-old-changed-election-results-on-a-replica-florida-state-website-in-under-10-minutes [https://perma.cc/J95X-EXEB].

[3] *See* Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030).

[4] *See* Defending the Integrity of Voting Systems Act, Pub. L. No. 116-179, 134 Stat. 855 (2020) (codified as amended at 18 U.S.C. § 1030(e)).

[5] This Note will mainly discuss the problem of unofficial election website tampering in the context of presidential elections, but the impact of tampering in local, state, and other federal elections remains pertinent as well.

[6] Derek Tisler, Elizabeth Howard & Edgardo Cortés, *Roadmap to the Official Count in the 2024 Election*,

reasons in each state and municipality that reports them.[7] Election results are tabulated by local officials on Election Day and reported to the public, but remain unofficial until formally certified and therefore can and do change.[8] Mail-in ballots, recounts, prescribed post-election auditing, errors, and more can impact those tallies.[9] The aggregation of votes from the precinct level to the municipality or county level and thereafter to the state level may also allow for discrepancies

---

BRENNAN CTR. FOR JUST. (Sept. 24, 2024), https://www.brennancenter.org/our-work/research-reports/roadmap-official-count-2022-election [https://perma.cc/P6JN-DZC9].

[7] *See* Christina A. Cassidy, *It's Normal Not to Know the Official Results on Election Night. Here's Why*, PBS (Oct. 27, 2022, 4:58 PM), https://www.pbs.org/newshour/politics/its-normal-not-to-know-the-official-results-on-election-night-heres-why [https://perma.cc/2BHW-922K]; *Election Security Rumor vs. Reality*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/election-security/rumor-vs-reality#:~:text=Election%20results%20reported%20on%20election,certified%20on%20election%20night%20itself [https://perma.cc/NZ7L-VBVU] (last visited Oct. 21, 2024) ("Election night reporting is unofficial and those results may change as ballot counting is completed. . . . The timeline for reporting election results may be impacted by a number of factors, including changes to state or local level policies that affect how the election is administered, changes to when ballots can be processed, or additional protocols implemented to make voting and vote processing safer during the pandemic."). *Compare Unofficial Election Night Results*, ARIZ. SEC'Y OF STATE, https://azsos.gov/elections/results-data/unofficial-election-night-results [https://perma.cc/V2MW-KD5B] (last visited Oct. 21, 2024) ("The first batch of election results will be available after 8:00 p.m. [MST] on election night. After that, the results *are updated sporadically as the counties receive data* from the polling locations.") (emphasis added), *with [ARCHIVED] 2023 Municipal Election Unofficial Results*, BUCKS CNTY., https://www.buckscounty.gov/CivicAlerts.aspx?AID=897&ARC=895 [https://perma.cc/VL4H-UEZV] (last visited Oct. 21, 2024) ("The Unofficial Results for the 2023 Municipal Election, being held on November 7, 2023, will begin reporting around 8:30 PM [EST]. The results *will be updated approximately every 60 minutes.*") (emphasis added).

[8] *See* Tisler et al., *supra* note 6.

[9] *See* Wisc. Election Comm'n, *2022 Post-Election Voting Equipment Audit*, VIMEO (Nov. 10, 2022, at 5:22 PM), https://vimeo.com/769651388 [https://perma.cc/7HA4-9697] (noting, after the 2022 general state election, 10% of reporting units in Wisconsin were automatically selected for auditing, including at least one reporting unit per county and five reporting units for each type of equipment utilized); *Request a Ballot*, N.Y. STATE BD. OF ELECTIONS, https://www.elections.ny.gov/VotingAbsentee.html [https://perma.cc/EDR9-D79G] (last visited Oct. 21, 2024) (stating that you may return absentee ballots in New York by "ensuring it receives a postmark no later than" Election Day); *Election Security Rumor vs. Reality*, *supra* note 7 ("An outage, defacement, or other issue affecting the integrity or availability of the information displayed on such sites would not impact the counting of ballots or the accuracy of the official certified results."); Donovan Slack, *What Are the Recount Rules? We Break Them Down and How They Could Help Donald Trump Win Wisconsin, Arizona or Pennsylvania*, USA TODAY (Nov. 5, 2020, 1:40 PM), https://www.usatoday.com/story/news/politics/elections/2020/11/04/how-recount-wisconsin-arizona-michigan-could-help-trump-win/6163544002/ [https://perma.cc/X6TG-3YT8] (explaining candidates can request a recount at differing thresholds depending on the state in question); Matthew Weil & Christopher Thomas, *Behind the Curtain of Post-Election Canvassing, Audits, and Certification*, BIPARTISAN POL'Y CTR. (Oct. 5, 2021), https://bipartisanpolicy.org/explainer/behind-the-curtain-of-elections/ [https://perma.cc/VKB2-VCDG] (stating "unofficial results are prone to human and technical error and do occasionally reflect mistakes made during data processing on election night"); Kristie Cattafi, *Second Wrong Election Results File Posted to Bergen County Clerk's Site. What Went Wrong?*, NORTHJERSEY.COM (Oct. 5, 2021), https://www.northjersey.com/story/news/bergen/2023/11/10/bergen-county-clerks-office-posts-another-wrong-election-results-file/71530292007/ (demonstrating an unofficial election result tallying mistake).

depending on update cadences.[10] In summation, while these results remain useful, they still remain "unofficial and subject to change" pending formal verification.[11]

Despite their unofficial nature, these results are critical to mainstream media outlets' ability to project the winners of elections.[12] The Associated Press (AP), partially reliant on websites reporting these unofficial results, recognizes the possibility of website errors and attempts to mitigate this where possible by utilizing local reporters, relationships with county clerks and other local officials, and other reporting methods to deliver the results.[13] However, such mitigations are not foolproof. The AP does not specify in its published methodology exactly where its reporters are located and where they get their information.[14] Nor does it explicitly account for the possibility that election officials in those jurisdictions might utilize these unofficial election tabulation websites to inform reporters on the ground.[15] Furthermore, county and municipality websites are critical to AP's election result reporting.[16] Virtually all media outlets will echo that their own displayed "[v]ote results are rigorously checked and verified" and are posted after "checking that vote data is consistent across sources."[17] Still, media outlets do not dismiss the possibility that sources on the ground are receiving their own information from the very same online results websites.

However, the overarching issue of faith in our electoral processes does not rely on media outlets alone. Even assuming media verification is conducted ideally, and no grossly miscounted or defaced results are displayed, that may not be enough to deter bad actors from tampering with unofficial election results websites and consequentially cast doubt on our democratic institutions. As was witnessed during and in the aftermath of the 2020 general election, there is enormous "public distrust in the media, which typically calls elections," alongside diminished "faith in the

---

[10] *See General Election and Voter Information Guide: Election Results*, LIVERPOOL PUB. LIBR., https://lpl.libguides.com/c.php?g=1262870&p=10406752 [https://perma.cc/KH96-3SHM] (last visited Oct. 21, 2024) (claiming that the "unofficial election night results displayed on this [N.Y. state election results] web site are based on the unofficial results reported to us by each County Board of Elections"); Weil & Thomas, *supra* note 9 ("Typically, results are aggregated first at the individual precinct level, then funneled up to the local or county election authority, and ultimately shared with the state.").

[11] *See* Weil & Thomas, *supra* note 9.

[12] *See How Does The Times Get Live Election Results?*, *supra* note 1 (reporting that "vote totals provided by The Associated Press, which collects results . . . through a network of websites and . . . on-the-ground correspondents"); *How AP Counts the Vote*, *supra* note 1; *How Election Data Is Collected*, NBC NEWS, https://www.nbcnews.com/politics/2022-elections/how-election-data-is-collected [https://perma.cc/QAZ2-KLAG] (last visited Oct. 21, 2024) ("Vote data is also collected through state and county websites and feeds.").

[13] *See How AP Counts the Vote*, *supra* note 1 ("Our goal is to have at least two, and in many cases three or more, sources for vote totals from every county. . . . [Partially to] provide a check to help ensure the vote totals we are reporting are correct.").

[14] *See id.*

[15] *See id.*

[16] *See id.* ("Since many states and counties display election results on websites, another group of clerks monitors those sites and enters the results into [AP's system].").

[17] *How Election Data Is Collected*, *supra* note 12; *see also* Zachary B. Wolf, *It's Not Magic, It's Math. Here's How CNN Makes Election Projections*, CNN (Oct. 17, 2020, 10:12 AM), https://www.cnn.com/2020/10/17/politics/2020-election-projections-explained/index.html [https://perma.cc/J8CP-A9YB] (explaining that sources "will be independently obtaining the vote count from around the country").

state and local election officials who underpin American democracy."[18] The conjunction of that mistrust, both in election officials and the media, means the slightest *valid* changes in vote totals, corroborated by independent sourcing across the media, could mean nothing to certain sects of the electorate under the right circumstances.[19] Even constant pronouncements—in courts throughout the country and from nearly the whole of the mainstream media—that mere *accusations* an election was illegitimate were ludicrous[20] could not stop the misinformation that catalyzed the chaos and violence of January 6, 2021. The Department of Justice has signaled that "even simply spreading disinformation suggesting" election results were manipulated "could undermine the integrity and legitimacy of our free and fair elections, as well as public confidence in election results."[21] Even unauthorized access to election-related infrastructure "creates the fog about whether or not they did do anything. And if you're trying to manipulate the election, you may have done as much damage by creating the fear that data was altered than by actually altering it," and some domestic actors might cease on that doubt.[22] The prospect of *actual* interference, even on unofficial result websites, would only multiply the chaos.

Faith in elections is the bedrock of our democratic society, as "a democracy is effective only if the people have faith in those who govern."[23] We utilize elections to solve our political differences at the ballot box rather than through other means.[24] A lack of faith in those institutions can instigate violence.[25] Foreign adversaries are aware of our wide variety of information sources and will seek to exploit that vulnerability if they can.[26] If election results are

---

[18] Brad Brooks, Nathan Layne & Tim Reid, *Why Republican Voters Say There's 'No Way in Hell' Trump Lost*, REUTERS (Nov. 20, 2020, 10:35 AM), https://www.reuters.com/article/us-usa-election-trump-fraud-insight/why-republican-voters-say-theres-no-way-in-hell-trump-lost-idUSKBN2801D4.

[19] *See Fact Check: Vote Spikes in Wisconsin, Michigan and Pennsylvania Do Not Prove Election Fraud*, REUTERS (Nov. 10, 2020, 2:05 PM), https://www.reuters.com/article/uk-factcheck-wi-pa-mi-vote-spikes/fact-check-vote-spikes-in-wisconsin-michigan-and-pennsylvania-do-not-prove-election-fraud-idUSKBN27Q307 (describing voters' concerns upon seeing "vote spikes" for President Biden in certain states over the course of counting votes for the 2020 election).

[20] *See, e.g.*, *id.*; *Fact Check: Courts Have Dismissed Multiple Lawsuits of Alleged Electoral Fraud Presented by Trump Campaign*, REUTERS (Feb. 15, 2021, 10:41 AM), https://www.reuters.com/article/world/fact-check-courts-have-dismissed-multiple-lawsuits-of-alleged-electoral-fraud-p-idUSKBN2AF1FQ/.

[21] U.S. DOJ, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 3–4 (2018), https://www.justice.gov/archives/ag/page/file/1076696/download [https://perma.cc/8Z3G-4TKD]; *see also* Matt Blaze, *Election Integrity and Technology: Vulnerabilities and Solutions*, 4 GEO. L. TECH. REV. 505, 511 (2020) ("Errors in unofficial or final tallies can cast doubt on the legitimacy of entire elections.").

[22] The Daily, *The First Major Cyberattack of the 2024 Election*, N.Y. TIMES, at 23:18 (Aug. 27, 2024), https://www.nytimes.com/2024/08/27/podcasts/the-daily/hacking-2024-election.html?showTranscript=1? [https://perma.cc/VD59-7NVV].

[23] United States v. Miss. Valley Generating Co., 364 U.S. 520, 562 (1961).

[24] President Biden condemned political violence on X, stating, "In America, we resolve our differences at the ballot box. Not with bullets," one day after the failed assassination attempt of Donald Trump at a Pennsylvania campaign rally. *See*, @POTUS, X (Jul. 14, 2024, 9:27 PM), https://x.com/POTUS/status/1812660210013528273 [https://perma.cc/M2S5-ZP9S].

[25] *See, e.g.*, *Editorial: To Ward Off Political Violence We Must Once Again Instill Faith in Democracy*, DAILY CAMERA (Jul. 21, 2024, 5:00 AM), https://www.dailycamera.com/2024/07/21/editorial-to-ward-off-political-violence-we-must-once-again-instill-faith-in-democracy/.

[26] *See* U.S. DOJ, *supra* note 21, at 14 ("Our adversaries will persist in seeking to exploit the diversity of today's information space, and the tactics and technology they employ will continue to evolve.").

reported differently by local election officials than the media, it might only add to the would-be conspiracy. Those changes, being the result of foreign hacking, would likely only add fuel to the fire.

B. THE PROBLEM: HACKING UNOFFICIAL ELECTORAL RESULTS WEBSITES AND SPAWNING MISINFORMATION

Unofficial election result websites are vulnerable to malicious tampering, which can instigate election misinformation. This problem demands a robust response because election misinformation is dangerous and can cause chaos. This Section emphasizes those vulnerabilities through examples from around the world as well as within the United States. It will underline the stakes of those potential breaches and the dangers of misinformation in elections more broadly. Finally, it will call for renewed attention to protect against threats—including specifically unofficial election website tampering—that endanger faith in our democracy.

In 2014, Russian hackers attempted to display a shocking election outcome on a counterfeit election commission server in a foreign country: Ukraine.[27] After its annexation of Crimea, the destabilization of Ukraine remained a fundamental interest of Russia's, which believed election tampering a prudent means to achieve this goal.[28] Though Russia was unsuccessful, certain experts believe "the hackers accomplished their goal" of discrediting the election and muddying the waters.[29] Those same tactics drive foreign actors to interfere in U.S. elections "to spread disinformation and to sow discord on a mass scale in order to weaken the U.S. democratic process, and ultimately to undermine the appeal of democracy itself."[30] Some believe an attack in the United States, similar to the one in Ukraine, could catalyze a "nightmare scenario" in the United States and presumably in Americans' faith in our electoral systems.[31] These "perception hacks," particularly if multi-pronged, can have substantial psychological effects and are a significant national security concern for U.S. national security officials.[32]

---

[27] *See* Andrew E. Kramer & Andrew Higgins, *In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking*, N.Y. TIMES (Aug. 16, 2017), https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html.

[28] *See* Gabe Joselow, *Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past*, NBC NEWS (Nov. 3, 2016, 5:18 AM), https://www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246 [https://perma.cc/HCD5-2UYT] (noting the goal of discrediting Ukraine's election in context of Russia's annexation of Crimea); Ellen Nakashima, *Russian Military Behind Hack of Satellite Communication Devices in Ukraine at War's Outset, U.S. Officials Say*, WASH. POST (Mar. 24, 2022, 10:25 PM), https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/ (pointing to similar goals of Ukrainian disruption from cyberattacks).

[29] Joselow, *supra* note 28.

[30] U.S. DOJ, *supra* note 21, at 2.

[31] *See* Andrew Roth, *How the Kremlin Is Sure to Keep Its Fingerprints Off Any Cyberattack*, WASH. POST (Aug. 2, 2016, 6:24 PM), https://www.washingtonpost.com/world/europe/how-the-kremlin-is-sure-to-keep-its-fingerprints-off-any-cyberattack/2016/08/02/26144a76-5829-11e6-8b48-0cb344221131_story.html.

[32] *See* David E. Sanger & Nicole Perlroth, *'Perception Hacks' and Other Potential Threats to the Election*, N.Y. TIMES (Oct. 28, 2020), https://www.nytimes.com/2020/10/28/us/politics/2020-election-hacking.html.

That scenario is less far off than one might think. At a hacking conference in 2018, an eleven-year-old child "successfully hacked into a replica of the website used by the Florida Secretary of State to report election results and changed them."[33] It took that eleven-year-old less than ten minutes to do so.[34] Foreign actors are known to have more money, time, and experience than the average eleven-year-old. This is not a purely theoretical exercise—in 2020, Iran attempted to compromise a U.S. municipal website for reporting unofficial election results.[35] While the hackers succeeded in gaining access to the website, the violation was discovered, and the website was later secured.[36] Russia attempted a similar exercise in 2016.[37] A bipartisan report from the Senate Intelligence Committee revealed, "[i]f the penetration [by the Russians] had been successful, actors could have manipulated the unofficial display of the election tallies."[38] In the 2024 election, there have already been numerous attempts by foreign governments to influence the election, spread misinformation, and hack both major presidential campaigns.[39]

Furthermore, as previously noted, election misinformation and doubt alone can instigate chaos and violence. This occurred in Venezuela's 2024 presidential election, which, due to widely suspected foul play, resulted in a heavily doubted outcome and caused the country to erupt in protests, which have at times turned violent.[40] Another prime example is the 2020 U.S. election. Donald Trump infamously spent months—starting long before Election Day in 2020 and culminating in the January 6 attack on the U.S. Capitol—calling the election he participated in "rigged."[41] The spread of those lies and accompanying misinformation led directly to the

---

[33] Molina & Weise, *supra* note 2.

[34] Regan, *supra* note 2.

[35] *See* Michael McFaul, *A High-level Senate Report Confirms It: Our Elections Still Aren't Safe*, WASH. POST (Jul. 30, 2019, 2:46 PM), https://www.washingtonpost.com/opinions/2019/07/30/high-level-senate-report-confirms-it-our-elections-still-arent-safe/; Sean Lyngaas, *US Military Kicked Iranian Hackers off Municipal Website Reporting Unofficial Election Results in 2020*, CNN (Apr. 25, 2023, 11:51 AM), https://www.cnn.com/2023/04/24/politics/iran-hackers-municipal-website-2020-election/index.html [https://perma.cc/NL9N-UKY4].

[36] *See* Lyngaas, *supra* note 35; Kevin Collier, *Iran-linked Hackers Broke Into Election Results Website in 2020, General Say*s, NBC NEWS (Apr. 25, 2023, 2:17 PM), https://www.nbcnews.com/tech/security/iran-linked-hackers-broke-election-results-website-2020-general-says-rcna81304 [https://perma.cc/LTT5-UT43].

[37] *See* S. REP. NO. 116-290, at 5 (2020); McFaul, *supra* note 35.

[38] S. REP. NO. 116-290, at 16 (2020); *see* McFaul, *supra* note 35.

[39] *See* Ruby Edlin & Lawrence Norden, *Foreign Adversaries Are Targeting the 2024 Election*, BRENNAN CTR. FOR JUST. (Aug. 20, 2024), https://www.brennancenter.org/our-work/analysis-opinion/foreign-adversaries-are-targeting-2024-election [https://perma.cc/XE95-UUDD]; Perry Stein, *FBI Concludes Iran Tried to Hack Campaigns of Trump, Biden-Harris*, WASH. POST (Aug. 19, 2024, 6:01 PM), https://www.washingtonpost.com/national-security/2024/08/19/iran-hack-trump-biden-harris-fbi/.

[40] *See* Joshua Goodman & Regina Garcia Cano, *Venezuelan Opposition Says It Has Proof Its Candidate Defeated President Maduro in Disputed Election*, ASSOCIATED PRESS (Jul. 30, 2024, 2:06 AM), https://apnews.com/article/venezuela-presidential-election-maduro-machado-edmundo-results-acee6c8cd3a8fc88086c2dd71963b759 [https://perma.cc/E6AF-2EVE].

[41] *See* Daniel Funke, *Fact Check: How We Know the 2020 Election Results Were Legitimate, Not 'Rigged' as Donald Trump Claims*, USA TODAY (Jan. 6, 2022, 10:19 PM), https://www.usatoday.com/story/news/factcheck/2022/01/06/fact-check-donald-trump-2020-election-results/9115875002/ [https://perma.cc/8R8T-G3AP]; Mary Clare Jalonick et al., *Jan. 6 Report: Trump 'Lit That Fire' of Capitol Insurrection*, ASSOCIATED PRESS (Dec. 23, 2022, 10:05 AM), https://apnews.com/article/jan-6-committee-final-report-trump-bcfea6162fe9cfa0d120e86d069af0e4 [https://perma.cc/QNW3-J58R]; Jonathan Swan,

violence that occurred on January 6.[42] Even before the election, Trump understood that mail-in balloting would skew mainly Democratic, partially due to the uneven partisan response to the COVID-19 pandemic, and that those ballots, in certain states, might be counted later.[43] Meanwhile, states more likely to be in his corner, like Florida, were expected to complete their tabulations on the evening of the election.[44] Trump, seemingly anticipating the discrepancies between unofficial election tabulations, took full advantage of them to further misinformation and doubt on election methods and outcomes before, during, and after Election Day.[45] Trump's plan to cast himself as the winner regardless of the results almost worked in full, as the states that then-Former Vice President Biden most relied on to win the Electoral College would release their results later than others.[46] However, Fox News' early call of Arizona—a state Trump would have likely needed to win—for Biden disturbed Trump's hopes of declaring a seemingly unperturbed, if not premature, victory on election night,[47] though that did not ultimately prevent Trump from later declaring that he won the election[48] or the subsequent violence of January 6. The underlying point is that, even if challenged, election misinformation can lead to chaos and violence.

It is also worth noting that the manipulation of unofficial election results, while a national concern, is not limited to presidential elections. These same manipulations can be done in any

Scoop: Trump's Plan to Declare Premature Victory, AXIOS (Nov. 1, 2020), https://www.axios.com/2020/11/01/trump-claim-election-victory-ballots [https://perma.cc/28AW-CLCK].

[42] *See* H.R. REP. NO. 117-663, at 8 (2022) ("[T]he central cause of January 6th was one man, former President Donald Trump."); Jalonick et al., *supra* note 41 (quoting Select Committee Chairman Bennie Thompson's designation that Trump "lit that fire").

[43] *See* H.R. REP. NO. 117-663, at 373 (2022) ("The early vote tally favored Republicans on election night because the mail-in ballots, which skewed toward Democrats, were not yet fully counted. . . . The President knew of this . . . .").

[44] *See* Dexter Filkins, *Will Florida Decide the Presidential Race or Throw It Into Confusion?*, NEW YORKER (Oct. 28, 2020), https://www.newyorker.com/news/daily-comment/will-florida-decide-the-presidential-race-or-throw-it-into-confusion (noting that, before the election, Florida election officials believed the "overwhelming majority of ballots [would be] counted by midnight on November 3rd"); Swan, *supra* note 41.

[45] *See* H.R. REP. NO. 117-663, at 373 (2022); Swan, *supra* note 41 (noting in advance of the election, Trump described "plans to walk up to a podium on election night and declare he has won," assuming he had commanding leads in several states).

[46] *See* Filkins, *supra* note 44; Swan, *supra* note 41.

[47] *See* Sarah Ellison, *Trump Campaign Was Livid When Fox News Called Arizona for Biden—and Tensions Boiled Over On-Air*, WASH. POST (Nov. 4, 2020, 8:23 AM), https://www.washingtonpost.com/lifestyle/style/fox-news-election-night-arizona/2020/11/04/194f9968-1e71-11eb-90dd-abd0f7086a91_story.html (describing Trump as "livid" regarding Fox News' Arizona call and noting experts declarations that the call "looms pretty large as a check against claims Trump might make that he's winning"); Swan, *supra* note 41; H.R. REP. NO. 117-663, at 195 (2022) ("When Trump spoke . . . the President's re-election was very much in doubt. Fox News, a conservative media outlet, had correctly called Arizona for former Vice President Joseph R. Biden."); Brian Stelter & Oliver Darcy, *Fox News and AP Scrutinized for Projecting Arizona While Other Outlets Hold Off*, CNN (Nov. 5, 2020, 9:33 PM), https://www.cnn.com/2020/11/05/tech/arizona-fox-news-associated-press-projection/index.html [https://perma.cc/4ECS-ZG2H]; Domenico Montanaro, *AP Explains Calling Arizona for Biden Early, Before It Got Very Close*, NPR (Nov. 19, 2020, 4:13 PM), https://www.npr.org/2020/11/19/936739072/ap-explains-calling-arizona-for-biden-early-before-it-got-very-close [https://perma.cc/6PAD-4TDT].

[48] *See* Ellison, *supra* note 47.

election. Problems with unofficial vote tallies, even at the local level, can have a substantial impact on faith in those elections.[49]

Overall, as seen on January 6, 2021, election misinformation can clearly cause chaos and even violence. With the right mouthpiece and supposed evidence, it can spread quickly.[50] As noted, unofficial election results tabulations are uniquely vulnerable and could be utilized to spew misinformation or cast doubt on election results.[51] The Election Assistance Commission (EAC) has recognized the vulnerabilities of these websites and has attempted to mitigate the risks.[52] These types of breaches and resulting misinformation were enough of a concern after 2020 that the Cyber Security and Infrastructure Security Agency (CISA) has included information on the defacement of unofficial election results on its website.[53] Finally, the DOJ has raised concerns that cyber operations may directly target the "integrity or availability of election-related data."[54] In summation, the possibility of changing unofficial voting tallies is not just a far-off possibility—it has been attempted before, the United States is vulnerable to it now, and the future threat it poses demands a robust response.

II. CURRENT APPLICABLE CRIMINAL LAW RESPONSES

A. CRIMINAL LAW AND DETERRENCE

One available response to unofficial election website result tampering is the existing explicit criminal prohibitions on the conduct. This is, of course, not the sole response available to the government. The government can and should utilize its resources to assist in securing these websites wherever possible. Furthermore, national security,[55] technological,[56] and other laws and

---

[49] *See* Nikita Biryukov, *Lawmakers Eye New Rules for Election Results Reporting*, N.J. MONITOR (May 12, 2023, 3:11 PM), https://newjerseymonitor.com/2023/05/12/lawmakers-eye-new-rules-for-election-results-reporting/ [https://perma.cc/VX74-BGSM]. These problems can summarily result in significant legal action and confusion. *See* Stephen Underwood, *The Vote Totals Changed by Hundreds. Now Hartford Candidates Are Considering Election Complaints*, HARTFORD COURANT (Nov. 17, 2023, 3:51 PM), https://www.courant.com/2023/11/17/after-vote-totals-change-by-hundreds-hartford-candidates-consider-elections-complaints/.

[50] This supposed evidence might include the addition of a large number of votes favorable to one party because of partisan differences in voting methodology or the partisan concentration of a particular environment, such as the Republican-leaning nature of individuals living in rural areas. *See Fact Check: Vote Spikes in Wisconsin, Michigan and Pennsylvania Do Not Prove Election Fraud*, *supra* note 19.

[51] *See* Weil & Thomas, *supra* note 9.

[52] *See Checklist for Securing Election Night Results Reporting*, U.S. ELECTION ASSISTANCE COMM'N, https://www.eac.gov/sites/default/files/electionofficials/postelection/Checklist_for_Securing_Election_Results_FINAL_EAC.pdf [https://perma.cc/54VW-LDFC] (last visited Oct. 21, 2024).

[53] *See Election Security Rumor vs. Reality*, *supra* note 7 ("Reality: Results displayed via election results reporting websites are unofficial and subject to change until results are certified. An outage, defacement, or other issue affecting the integrity or availability of the information displayed on such sites would not impact the counting of ballots or the accuracy of the official certified results.").

[54] CYBER DIGITAL TASK FORCE, *supra* note 21, at 3 ("Cyber operations could seek to undermine the integrity or availability of election-related data.").

[55] *See Election Security*, U.S. DHS, https://www.dhs.gov/topics/election-security [https://perma.cc/TVX7-8GPV] (last visited Oct. 21, 2024).

[56] *See Voting System Security Measures*, U.S. ELECTION ASSISTANCE COMM'N,

regulations should be promulgated in this area. However, the scope of this Note is limited to the applicability of criminal laws toward these actions. For the purposes of this Note, "deterrence" is limited to the possible punishment for engaging in the malicious tampering of unofficial election website results and the dissuasion associated with those punishments that may make would-be tamperers less likely to commit those crimes. This is in contrast to "preventative" strategies that seek to make the action less possible, such as tightening website security. While this Note's focus is narrow in its coverage of deterrence through criminal law, that coverage should not be taken as a suggestion that preventative measures or other possible deterrence measures have no part to play in election security.

The DOJ has found that criminal prohibitions "help the Department prosecute and deter malicious cyber activity."[57] The Department has made similar assertions regarding the expansion of criminal charges in malign election activity.[58] Thus, criminal law and deterrence in this area are independently worthy of examination.

The deterrence such laws provide against malignant domestic actors is obvious. Criminal prohibitions are often designated, in part, to deter.[59] Supposing a domestic actor sought to muddy the waters with misinformation in support of their own domestic electoral goals, [60] interference may be effective in the short term. Still, such an actor may be identified after the fact and accordingly face steep consequences and reap few rewards.

Deterrence against foreign actors is not as readily grasped. Foreign state actors, particularly those responsible for hacking crimes, may be less likely to face prison time in the United States, given the difficulties of the extradition process.[61] Despite this, indictments are seen by many as "one very public tool in the portfolio of consequences for irresponsible action by a state in cyberspace."[62] Additionally, charges have at times "led to the arrest of those accused and may deter individual hackers from working with particular states."[63] There are natural downsides to

---

https://www.eac.gov/sites/default/files/electionofficials/security/Voting_System_Security_Measures_508_EAC.pdf [https://perma.cc/BQ9N-CW92] (last visited Oct. 21, 2024).

[57] CYBER DIGITAL TASK FORCE, *supra* note 21, at 121.

[58] *See id.* at 7 (describing malign election activity-related criminal charges as "not only . . . a tool the [DOJ] uses to pursue justice, but also [to] help deter similar conduct in the future").

[59] *See id.* at 20, 133.

[60] *See* H.R. REP. NO. 117-663, at 373 (2022); Swan, *supra* note 41.

[61] *See* Rishi Iyengar, *Why It's So Difficult to Bring Ransomware Attackers to Justice*, CNN (Jul. 8, 2021, 12:52 PM), https://www.cnn.com/2021/07/08/tech/ransomware-attacks-prosecution-extradition/index.html [https://perma.cc/BF7W-WG9X] ("'The major challenges in bringing international hacker groups to justice are having to conduct foreign operations through additional layers of bureaucracy of our international counterparts. . . . This includes less access to on-the-ground resources to investigate, gather intelligence and support the prosecution across borders.'"); Luis Sanchez, *Putin: Russia Will 'Never' Extradite Alleged Hackers to US*, THE HILL (Mar. 4, 2018, 2:35 PM), https://thehill.com/policy/national-security/376660-putin-russia-will-never-extradite-alleged-hackers-to-us/ [https://perma.cc/773Z-SYCN].

[62] James Andrew Lewis, *The Russian Cyber Indictments*, CTR. FOR STRATEGIC & INT'L STUD. (Oct. 20, 2020), https://www.csis.org/analysis/russian-cyber-indictments [https://perma.cc/MZ9D-BU56]; *see also* James Andrew Lewis, *Indictments, Countermeasures, and Deterrence*, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 25, 2016), https://www.csis.org/analysis/indictments-countermeasures-and-deterrence [https://perma.cc/849N-KZGJ].

[63] Tim Maurer & Garrett Hinck, *What's the Point of Charging Foreign State-Linked Hackers?*, CARNEGIE ENDOWMENT FOR INT'L PEACE (May 24, 2019), https://carnegieendowment.org/2019/05/24/what-s-point-of-charging-foreign-state-linked-hackers-pub-79230 [https://perma.cc/YA5Z-AFEG].

charging these crimes, such as the publication of specific information revealing intelligence sources and methods.[64] Historically, these downsides have not prevented the federal government from taking such actions.

Similar enhancements and changes in the Sentencing Guidelines have been justified for similar reasons and with similar potential obstacles to implementation. The U.S. Sentencing Commission has justified enhancements against foreign actors, such as trade secret theft,[65] despite the potential limitations on the actual sentencing of those responsible,[66] including barriers to extraditing alleged offenders.[67] However, extraditions of foreign nationals can and do take place,[68] and there are alternatives to foreign extradition as well.[69] Regardless of the possibility of actual consequences for those individuals behind cyberattacks, on the whole, the symbolic nature of charges may have a deterrent effect,[70] which, if nothing else, justifies the existence of these laws and the proliferation of Sentencing Guidelines in these areas.

B. CURRENT LAW

There are numerous laws in this area that could conceivably apply to the scenario posed by this Note, including: "52 U.S.C. § 10307, which prohibits a person acting under color of law from willfully failing or refusing to tabulate a person's vote who is entitled to vote" and "52 U.S.C. § 20511, which provides criminal penalties for defrauding the residents of a state of a fair election by manipulating balloting processes, among other things."[71] Ultimately, this Note finds that The Computer Fraud and Abuse Act (CFAA) and The Defending the Integrity of Voting Systems Act (DIVSA) are far and away more likely to apply to the problem of unofficial vote-tally hacking than these laws. However, a fulsome explanation of why certain laws do not apply remains appropriate.

---

[64] *See id.*

[65] *See* U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b), amend. 711 (U.S. SENT'G COMM'N 1987), https://www.ussc.gov/guidelines/amendment/771 [https://perma.cc/9UAM-XZ4H].

[66] *See* FED. R. CRIM. P. 42.

[67] *See* U.S. DOJ, Just. Manual § 9-15.100 (2018).

[68] *See* Press Release, *Department of Justice Announces Extradition of Iranian National and Unsealing of Charges Against Two Other Men for Exporting Carbon Fiber from the United States to Iran*, U.S. DOJ (Jul. 16, 2019), https://www.justice.gov/opa/pr/department-justice-announces-extradition-iranian-national-and-unsealing-charges-against-two [https://perma.cc/47MB-9E29].

[69] *See* U.S. DOJ, Just. Manual § 9-15.100 (2018).

[70] *See* Tal Kopan, *Hacking Case: Symbolic or Deterrent?*, POLITICO (May 20, 2014, 5:46 AM), https://www.politico.com/story/2014/05/china-hacking-charges-106859 [https://perma.cc/F6PF-LLYW].

[71] JIMMY BALSER, CONG. RSCH. SERV., IF12245, VOTING SYSTEMS AND FEDERAL LAW 1 (2022). While additional other laws may be applicable (specifically 18 U.S.C. § 241, which prohibits conspiracy against the exercise of certain rights, 18 U.S.C. § 242, "which prohibits any person acting under color of law" from doing the same, and 18 U.S.C. § 371, which prohibits "persons from conspiring to commit an offense against or to defraud the United States"), their broad possible applications make them potentially unreliable on their own. *Id.* Furthermore, the lack of specified hacking or vote-tampering provisions in those laws could neuter any additional deterrence that might otherwise be gained.

C. LIKELY INAPPLICABLE LAWS: 52 U.S.C. § 10307 AND 52 U.S.C. § 20511

52 U.S.C. § 10307 outlines "prohibited acts," beginning with the "[f]ailure or refusal to permit casting or tabulation of vote."[72] This section could be construed to implicate meddling with the unofficial tabulation of election results, as it outlines in part, "[n]o person acting under color of law shall . . . willfully fail or refuse to tabulate, count, and report such person's vote."[73] However, this portion of the U.S. Code is derived from Section 11(a) of the Voting Rights Act of 1965.[74] The Voting Rights Act was codified mainly as an enforcement mechanism for the Fifteenth Amendment and was not a general voting law.[75] Precedent further suggests § 10307(a) applies solely to election officials, acting under the color of law and tallying votes.[76] Given that the context of the Voting Rights Act and precedent suggesting this applies solely to officials, § 10307(a) is not sufficiently applicable to the intentional external hacking of unofficial election results.

By contrast, 52 U.S.C. § 20511—signed into law as a provision of the National Voter Registration Act (NVRA)[77]—designates that:

> A person, including an election official, who in any election for Federal office . . . knowingly and willfully deprives, defrauds, or attempts to deprive or defraud the residents of a State of a fair and impartially conducted election process, by . . . the procurement, casting, or tabulation of ballots that are known by the person to be materially false . . . .[78]

This, too, could be construed to implicate meddling with the unofficial tabulation of election results. However, this provision has generally been applied to those working from within the election infrastructure, either on behalf of the state in question, candidates involved in the

---

[72] 52 U.S.C. § 10307(a).

[73] *Id.*

[74] *See* Voting Rights Act of 1965, Pub. L. No. 89–110, §11(a), 79 Stat. 437 (1965); 52 U.S.C. § 10307.

[75] *See* South Carolina v. Katzenbach, 383 U.S. 301, 337 (1966) (noting that the Voting Rights Act is a valid means for carrying out the commands of the Fifteenth Amendment); Chisom v. Roemer, 501 U.S. 380, 383 (1991) ("The preamble to the Voting Rights Act of 1965 establishes that the central purpose of the Act is '[t]o enforce the fifteenth amendment to the Constitution of the United States.'" (quoting Voting Rights Act of 1965, Pub. L. No. 89–110, 79 Stat. 437 (1965))); Duran v. Lollis, No. 1:18-cv-01580, 2019 WL 691203, at *11 n.4 (E.D. Cal. Feb. 19, 2019).

[76] *See* La Union del Pueblo Entero v. Abbott, 604 F. Supp. 3d 512, 516 (W.D. Tex. 2022) (bringing a § 10307(a) claim against the governor of Texas); Ruth Bormuth v. Johnson, No. CV 16-13166, 2016 WL 7025173, at *2 (E.D. Mich. Oct. 24, 2016), *report and recommendation adopted as modified*, No. 16-13166, 2017 WL 82977 (E.D. Mich. Jan. 10, 2017) (bringing a § 10307(a) claim against the Secretary of State of Michigan); Buras v. Hill, No. 22-CV-753, 2023 WL 4290073, at *1 (E.D. Tex. May 19, 2023), *report and recommendation adopted*, No. 22-CV-753, 2023 WL 4234393 (E.D. Tex. June 28, 2023) (bringing a § 10307(a) claim against a county commissioner).

[77] *See* Fish v. Kobach, 840 F.3d 710, 715 n.1 (10th Cir. 2016) ("We refer to the sections of the NVRA as they appear in Pub. Law No. 103–31, 107 Stat. 77, 77–89 (1993) (codified as amended at 52 U.S.C. §§ 20501–20511).").

[78] 52 U.S.C. § 20511.

election, or those casting fraudulent ballots. It has generally not been applied to foreign actors or others who might work to manipulate unofficial voting tabulations.[79] Furthermore, the DOJ has formally construed this statute as aimed at fraudulent voting and tabulation of fraudulent votes in federal elections only.[80] Given its constraints and particularized interest in deterring *voting fraud* rather than *unofficial* election result tampering, § 20511 is not an ideal statute to deter this type of breach.

D. LIKELY APPLICABLE LAW: 18 U.S.C. § 1030

The CFAA is the most appropriately applicable law to target malicious actors who would seek to undermine U.S. elections through the tampering of unofficial voting tallies. This was true even before the DIVSA was signed into law in 2020.[81] The CFAA is the principal statute used to prosecute hackers and presumably would be used in prosecuting a wide-scale attack on unofficial result websites in conjunction with 18 U.S.C. § 371, which enacts a prohibition on committing an offense against or defrauding the United States.[82] It was effectively applied, in conjunction with 18 U.S.C. § 371, in indictments against Russian and Iranian actors in response to their plots to subvert the 2016 and 2020 presidential elections.[83]

The CFAA provides protections to "protected computers," which, until 2020, encompassed financial institution protections and computers "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States . . . ."[84] The Supreme Court has interpreted that provision to broadly encompass "all information from all computers that connect to the Internet."[85] Importantly, the CFAA did not previously cover voting machines in many instances, as they are generally not connected to the internet. [86] This changed with the passage of the DIVSA.

---

[79] *See* United States v. Prude, 489 F.3d 873, 875 (7th Cir. 2007) (appealing a conviction under what is now codified as § 20511(2)(B) for casting a ballot when ineligible due to prior offense); Graeff v. Ashcroft, No. 22-CV-971, 2023 WL 2424266, at *1 (E.D. Mo. Mar. 9, 2023) (filing a § 20511(2)(B) claim against the Secretary of State of Missouri); Raskin v. Jenkins, No. 22-CV-2012, 2022 WL 19355739, at *2 (N.D. Tex. Nov. 2, 2022), *report and recommendation adopted*, No. 22-CV-02012, 2023 WL 2777417 (N.D. Tex. Apr. 4, 2023) (filing a § 20511(2)(B) claim against county judge and elections administrator).

[80] *See* U.S. DOJ, FEDERAL PROSECUTION OF ELECTION OFFENSES 60 (Richard C. Pilger eds., 8th ed. 2017) ("Fraudulent voting: § 20511(2)(B)"); Madeline C. Alagia, *Election Law Violations*, 59 AM. CRIM. L. REV. 609, 653 (2022).

[81] *See* Defending the Integrity of Voting Systems Act, Pub. L. No. 116-179, 134 Stat. 855 (2020) (codified as amended at 18 U.S.C. § 1030(e)).

[82] *See* CYBER DIGITAL TASK FORCE, *supra* note 21, at 121 (denoting the CFAA "[t]he principal statute used to prosecute hackers" in a paragraph advocating its amendment to encompass non-internet connected voting machines); BALSER, *supra* note 71, at 1 (noting that the newly updated CFAA was applied in conjunction with 18 U.S.C. § 371 against two Iranian nationals attempting to intrude on election technology in 2020).

[83] *See* BALSER, *supra* note 71; Indictment at 1, United States v. Netyksho, No. 18-cr-00215 (D.D.C. Jul. 13, 2018); Indictment at 11, United States v. Kazem, No. 21 Crim. 644 (S.D.N.Y. Nov. 18, 2021).

[84] 18 U.S.C. § 1030(e)(2).

[85] Van Buren v. United States, 593 U.S. 374, 379 (2021) (citing §§ 1030(a)(2)(C), (e)(2)(B)).

[86] *See* CYBER DIGITAL TASK FORCE, *supra* note 21, at 121.

E. THE DEFENDING THE INTEGRITY OF VOTING SYSTEMS ACT

In October 2020, then-President Donald Trump signed The Defending the Integrity of Voting Systems Act into law[87] as an amendment to the CFAA.[88] The DIVSA expanded its definition of "protected computers" to encompass "voting systems" and, in doing so, expanded the applicable protections to those systems.[89]

The DIVSA was Congress' response to a report promulgated by the DOJ, specifically the Attorney General's Cyber Digital Task Force, published in July 2018.[90] The report noted that the CFAA did not "prohibit the act of hacking a voting machine in many common situations" and instead solely prohibited "hacking computers that are connected to the Internet" or other more detailed circumstances.[91] Given this, had a voting machine been hacked, the government may not have been "able to use the CFAA to prosecute the hackers."[92] Congress responded directly to this report, intending to add protections to voting machines not connected to the internet.[93] In speaking on behalf of this legislation, members of the United States House of Representatives designated that its passage was tied directly to the DOJ's Cyber-Digital Task Force report, denoting the lack of protections afforded to voting machines not connected to the internet.[94] The DIVSA amended the CFAA, protecting those systems. In doing so, the DIVSA utilized the "voting system" definition in the Help America Vote Act (HAVA).[95] HAVA defines a "voting system" to include, in part, the electronic infrastructure required to "report or display election results."[96] Accordingly, by utilizing HAVA's definition, the DIVSA expanded the CFAA's "protected computer" definition to explicitly encompass systems used to report or display election results—like unofficial vote tallying websites—and seemingly did so inadvertently.[97]

Despite the existing protections afforded to internet-connected unofficial election results websites, the DIVSA significantly enhances those safeguards for two central reasons. First, adding protections to "voting systems" allows the U.S. Sentencing Commission to easily promulgate an amendment or targeted guideline subsections that cover hacking in all voting systems, including unofficial vote tallying websites. Second, as noted, deterrence is a significant rationale behind these criminal prohibitions.[98] "Deterrence is one of the primary objectives of

---

[87] *See* Defending the Integrity of Voting Systems Act, Pub. L. No. 116-179, 134 Stat. 855 (2020) (codified as amended at 18 U.S.C. § 1030(e)).

[88] *See* BALSER, *supra* note 71, at 1.

[89] *See* 18 U.S.C. § 1030(e)(14) ("[T]he term 'voting system' has the meaning given the term in section 301(b) of the Help America Vote Act of 2002 (52 U.S.C. 21081(b))").

[90] *See* CYBER DIGITAL TASK FORCE, *supra* note 21, at xiii, 6, 121; *see* 166 CONG. REC. H4581 (daily ed. Sept. 21, 2020) (statement of Rep. Sheila Jackson Lee).

[91] CYBER DIGITAL TASK FORCE, *supra* note 21, at 121.

[92] *Id.*

[93] *See* 166 CONG. REC. H4581 (daily ed. Sept. 21, 2020) (statement of Rep. Sheila Jackson Lee).

[94] *See id.*

[95] *See* 18 U.S.C. § 1030(e)(14) ("[T]he term 'voting system' has the meaning given the term in section 301(b) of the Help America Vote Act of 2002 (52 U.S.C. 21081(b))").

[96] 52 U.S.C § 21081(b)(1)(C).

[97] *See* 166 CONG. REC. H4581 (daily ed. Sept. 21, 2020) (statement of Rep. Sheila Jackson Lee).

[98] *See* CYBER DIGITAL TASK FORCE, *supra* note 21, at 6, 121.

criminal law," and additional prohibitions in the area of malicious cyber activity can help DOJ deter malicious activity.[99] Greater deterrence could be achieved both through naming the crime as one of specific interest and enhancing the applicable Sentencing Guidelines calculation.

The CFAA provides the most appropriate criminal deterrence against tampering with unofficial election results of the relevant and current federal laws in this area. While this presents a novel application of the law, the DIVSA serves to enhance the clarity of that protection by explicitly denoting "voting systems," including mechanisms utilized to "report or display election results" as protected computers and may also be helpful in promulgating additional sentencing guidance or enhancements in this area.[100]

III. CALCULATING AND ENHANCING THE RESPONSE

This Part will attempt to derive the appropriate Sentencing Guidelines, as they currently exist, for the crime of tampering with unofficial election websites and argue for the possible implementation of enhancements in, or the addition of particularized guidance for, sentences based on the DIVSA. In doing so, this Note will first describe the background of the U.S. Sentencing Guidelines and how increased sentences are often thought to deter bad actors. Second, this Note will attempt to determine the most applicable sections of CFAA and the Sentencing Guidelines. Third, this Note will examine what possible punishments current calculations under those guidelines may yield. Finally, this Note will argue that the implementation of the DIVSA is appropriate both to keep the guidelines updated in accordance with current law and to provide for any possible enhancements the Sentencing Commission may deem appropriate for the crime of tampering with unofficial election websites.

A. UNITED STATES SENTENCING GUIDELINES AND DETERRENCE

The United States Sentencing Commission was created by Congress in 1984 to "reduce sentencing disparities and promote transparency and proportionality in sentencing."[101] In the furtherance of its duties, the U.S. Sentencing Commission supports the upkeep of the United States Sentencing Guideline manual, including promulgating additional amendments.[102] Federal judges must consult this manual before sentencing.[103] Judges must calculate the offense level as directed by the guidelines but are free to sentence parties according to 18 U.S.C. § 3553, which describes how to impose a sentence.[104] Amendments to the manual may be promogulated "in

[99] *Id.* at xiii, 6, 121.

[100] 52 U.S.C § 21081(b)(1)(C); *see* 18 U.S.C. § 1030(e).

[101] *About the Commission*, U.S. SENT'G COMM'N, https://www.ussc.gov/#:~:text=The%20U.S.%20Sentencing%20Commission%2C%20a,transparency%20and%20proportionality%20in%20sentencing [https://perma.cc/445Z-Z5ZU] (last visited Oct. 21, 2024); *see* 28 U.S.C. § 991.

[102] *See* 28 U.S.C. § 994.

[103] *See* 18 U.S.C. § 3553(a)(4); United States v. Booker, 543 U.S. 220, 264 (2005) ("The district courts, while not bound to apply the Guidelines, must consult those Guidelines and take them into account when sentencing.").

[104] *See* 18 U.S.C. § 3553; U.S. SENT'G GUIDELINES MANUAL § 1B1.1 (U.S. SENT'G COMM'N 2023); *Booker*,

light of congressional action, decisions from courts of appeals, sentencing-related research, and input from the criminal justice community."[105] Said amendments become effective if Congress does not modify or formally disapprove of them before November 1 of the year the amendment or modification is submitted.[106]

Amendments to the U.S. Sentencing Guidelines can create particularized enhancements, additional offensive level changes, or incorporate laws after passage.[107] For example, an amendment to the Sentencing Guidelines might add a new "4-level enhancement" in response to the passage of legislation.[108] Importantly, sentencing enhancements have been and may be utilized to further an underlying goal of deterrence.[109] And, as noted, deterrence is an essential element of criminal law.[110] Additionally, and perhaps most importantly, the DOJ has recommended utilizing deterrence in the area of malicious election interference to prevent such actions from occurring.[111] Given the deterrence justification for certain sentencing enhancements, this Note posits that greater delineation between specific sentences is necessary to ensure further particularized deterrence for voting system breaches, including meddling with unofficial election results. Furthermore, it encourages the Sentencing Commission to adopt sentencing guidance or enhancements for these particular crimes as appropriate.

B. UNOFFICIAL ELECTION RESULT TAMPERING UNDER THE EXISTING SENTENCING GUIDELINES

This section will examine how best to apply the Sentencing Guidelines to the scenario posed at the introduction of the Note, to see what the possible sentencing outcomes might look like under current law. In doing so, it will examine which sections of CFAA would best be applied to the crime of malicious tampering of unofficial election websites. It will then go on to examine what Sentencing Guideline enhancements are appropriate, as directed by the Manual.

---

543 U.S. at 264.

[105] *Policymaking*, U.S. SENT'G COMM'N, https://www.ussc.gov/policymaking [https://perma.cc/VTP2-7V5X] (last visited Oct. 4, 2024).

[106] *See* 28 U.S.C. § 994(p).

[107] *See* U.S. SENT'G COMM'N, AMENDMENTS TO THE SENTENCING GUIDELINES 14, 58 (2023), https://www.ussc.gov/sites/default/files/pdf/amendment-process/reader-friendly-amendments/202305_RF.pdf [https://perma.cc/VY74-YBVK].

[108] *See id.* at 14.

[109] *See* 18 U.S.C. § 3553(a) ("The court, in determining the particular sentence to be imposed, shall consider . . . the need for the sentence imposed . . . to afford adequate deterrence to criminal conduct"); U.S. SENT'G GUIDELINES MANUAL ch.1, pt. A, cmt. n.2 (U.S. SENT'G COMM'N 2023) ("[I]n promulgating guidelines, the Commission must take into account the purposes of sentencing as set forth in 18 U.S.C. § 3553(a)."); 28 U.S.C. § 991(b)(1)(A); *see also* United States v. Milligan, 77 F.4th 1008, 1014 (D.C. Cir. 2023) ("Our affirmance of the sophisticated-means enhancement also coheres with its central object: deterrence."); Peugh v. United States, 569 U.S. 530, 557 (2013) (Thomas, J., dissenting) ("Congress directed the Commission 'to consider' whether fraud guidelines were "'sufficient to deter and punish'" particular offenses, in light of increases to statutory maximum penalties for certain fraud crimes other than bank fraud.") (quoting U.S. SENT'G GUIDELINES MANUAL app. C, amend. 653 (Reason for Amendment) (effective Nov. 1, 2003)).

[110] *See* CYBER DIGITAL TASK FORCE, *supra* note 21, at xiii, 6, 121.

[111] *See id.* at 7.

The U.S. Sentencing Guidelines Manual instructs the presiding court, as the law requires, to "determine the kinds of sentence and the guideline range as set forth in the guidelines."[112] The guidelines further direct the court to a statutory index to determine a statute's accompanying offense guidelines.[113] If a statute is not listed, the guidelines instruct that the most analogous guideline should be applied.[114]

As stated, this Note aims, in part, to examine the current potential sentence for scenarios similar to the one posed in its introduction. Several sections of the CFAA could be applied in the scenario posed at the beginning of this Note, depending on the exact nature of the intrusion. Particular possibilities include 18 U.S.C. § 1030(a)(2)(C) and (a)(5)(B) or (C). Section 1030(a)(2)(C) prohibits unauthorized access to and the subsequent collection of information from a protected computer.[115] Section 1030(a)(5) prohibits, among other things, intentionally accessing "a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage"[116] or "damage and loss."[117] In the similar Iranian hacking case previously mentioned wherein the breachers attempted to compromise voting-related websites, including "state voter information websites," § 1030(a)(2) and (5)(A) were among other provisions used to charge the hackers.[118]

Appendix A of the United States Sentencing Guidelines Manual directs the utilization of § 2B1.1 in conducting a guidelines calculation for § 1030(a)(2) and (5).[119] Section 2B1.1 outlines guidelines calculations for property damage or destruction, fraud and deceit, and forgery, among other things.[120]

When conducting a guidelines calculation, both parties may make arguments to the court about whether including specific provisions from that calculation is appropriate,[121] and the court may make individualized determinations that differ from other judges in similar cases.[122] As the

---

[112] U.S. SENT'G GUIDELINES MANUAL § 1B1.1(a) (U.S. SENT'G COMM'N 2023) (*citing* 18 U.S.C. § 3553(a)(4)).

[113] *See* U.S. SENT'G GUIDELINES MANUAL § 1B1.2(a) (U.S. SENT'G COMM'N 2023).

[114] *See id.*; *see also* U.S. SENT'G GUIDELINES MANUAL § 2X5.1 (U.S. SENT'G COMM'N 2023).

[115] *See* 18 U.S.C. § 1030(a)(2)(C).

[116] 18 U.S.C. § 1030(a)(5)(B).

[117] 18 U.S.C. § 1030(a)(5)(C). Section 1030(a)(3) is less likely to be utilized given its prohibition on access to a nonpublic computer by the "Government of the United States," (which is separate from the term "government entity," which also includes states, provinces, municipalities) which implies the "Government of the United States" is, for all intents and purposes, the federal government (not state or local websites). *See* 18 U.S.C. § 1030(e)(9).

[118] Press Release, *Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election*, U.S. DOJ (Nov. 18, 2021), https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed [https://perma.cc/Q22S-2VHF]; *See* Indictment at 2, 8, United States v. Seyed Mohammad Hosein Mousa Kazem and Sajjad Kashian, No. 21 Crim. 644 (S.D.N.Y. Nov. 18, 2021).

[119] *See* U.S. SENT'G GUIDELINES MANUAL app. A (U.S. SENT'G COMM'N 2023).

[120] *See* U.S. SENT'G GUIDELINES MANUAL § 2B1.1 (U.S. SENT'G COMM'N 2023).

[121] *See, e.g.*, Government Sentencing Memorandum at 14, United States v. Wren, No. 21-CR-00599 (D.D.C. Oct. 10, 2023) (arguing for the application of particular guidelines provisions).

[122] *See e.g*, Michael Kunzelman & Alanna Durkin Richer, *In Jan. 6 Cases, 1 Judge Stands Out as the Toughest Punisher,* ASSOCIATED PRESS (June 12, 2022, 11:49 AM) https://apnews.com/article/capitol-siege-only-on-ap-donald-trump-government-and-politics-sentencing-de394dd56b3251aac5a50014f4d6afa7 [https://perma.cc/TMF4-7KH6].

crime of meddling with unofficial election tabulations has not yet been formally sentenced,[123] it is difficult to say exactly what provisions would be utilized. Furthermore, the guidelines advise broad upward sentence considerations given judges' ultimate discretion. "In a case involving stolen information from a 'protected computer', as defined in 18 U.S.C. § 1030(e)(2), [where] the defendant sought the stolen information to further a broader criminal purpose."[124] Importantly, as previously noted, all computers connected to the internet may be considered "protected computers."[125] Because of this, any overall "broader criminal purpose" receives the same upward consideration under the guidelines, with no particularized enhancement or sentencing guidance for the invasion of voting systems.[126]

C. ATTEMPTED APPLICATION OF THE EXISTING GUIDELINES

This section aims to address how that range is reached and when it might most likely apply. It does this in part through the consideration of prior similar crimes and an in-depth examination of the Sentencing Guidelines. It goes on to apply the guidelines directly to the hypothetical scenario posed in the introduction of the Note.

First and foremost, to address how best to improve the Sentencing Guidelines in this area, we must fully understand where the existing guidelines lead us. As noted, sentencing is incredibly context-dependent and can vary greatly depending on the case.[127] This is particularly true given the existence of a broad upward enhancement for utilizing information from a protected computer for broader criminal purposes, giving judges additional sentencing discretion.[128] However, given that the provision that currently criminalizes the hacking of unofficial election websites is the same as that protecting all internet-connected devices, [129] one can presume the application of the guidelines would be similar to its application in those areas. There are additional existing enhancements that are also worthy of discussion and potential application, including designated enhancements related to whether or not the computer breached is "used to maintain or operate a critical infrastructure, or [is] used by or for a government entity in furtherance of the administration of justice, national defense, or national security" or caused "a substantial disruption of a critical infrastructure."[130] As noted, the Sentencing Guidelines and their outcomes aim, in part, to deter. In the discussion of the law, as it relates to the criminal

---

[123] Even the previously denoted attempts at meddling by Russian and Iranian officials have not led to sentencings as those indicted officials could not be tried *in absentia*. *See* FED. R. CRIM. P. 43.

[124] U.S. SENT'G GUIDELINES MANUAL § 2B1.1 cmt. n.21(v) (U.S. SENT'G COMM'N 2023).

[125] *See* Van Buren v. United States, 593 U.S. 374, 394 (2021).

[126] *See* U.S. SENT'G GUIDELINES MANUAL § 2B1.1 cmt. n.21(v) (U.S. SENT'G COMM'N 2023).

[127] *See* 18 U.S.C. § 3553; U.S. SENT'G GUIDELINES MANUAL § 1B1.1 (U.S. SENT'G COMM'N 2023); United States v. Booker, 543 U.S. 220, 264 (2005).

[128] *See* U.S. SENT'G GUIDELINES MANUAL § 2B1.1 cmt. n.21(A)(v) (U.S. SENT'G COMM'N 2023) (denoting upward departures "[i]n a case involving stolen information from a 'protected computer', as defined in 18 U.S.C. § 1030(e)(2), [where] the defendant sought the stolen information to further a broader criminal purpose").

[129] *See Van Buren*, 593 U.S. at 378.

[130] U.S. SENT'G GUIDELINES MANUAL §§ 2B1.1(19)(A)(i), (iii) (U.S. SENT'G COMM'N 2023).

legal deterrent against tampering with unofficial election results websites and tabulations, it seems prudent to make an approximate calculation of sentencing for these crimes.[131]

Two relatively analogous cases involving the breach of, and tampering with, government websites illustrate the range of possibilities in applying the Sentencing Guidelines. In 2013, in the case *United States v. Jeremey Hammond*,[132] the defendant successfully hacked into numerous government websites, including those belonging to the "Federal Bureau of Investigation's Virtual Academy, the Arizona Department of Public Safety, the Boston Police Patrolmen's Association, and the Jefferson County, Alabama Sheriff's Office."[133] Hammond's overall adjusted offense level was thirty-one, and his criminal history category was four, leaving him with a recommended guideline sentencing range of one hundred fifty-one to one hundred eighty-eight months (approximately twelve and a half to fifteen and a half years).[134] After submitting a guilty plea and a statutory maximum was taken into account, Hammond received a sentence of ten years. [135]

Separately, in the 2018 case *United States v. Billy R. Anderson*,[136] the defendant "pled guilty . . . to two felony counts of computer fraud for obtaining unauthorized access to and committing defacements of the websites for the Combating Terrorism Center at the United States Military Academy in West Point, New York ('West Point'), and the Office of the New York City Comptroller."[137] Anderson's applicable offense level was thirteen, with a criminal history category of one.[138] Accordingly, his recommended incarceration range under the Sentencing Guidelines was twelve to eighteen months (one year to one and a half years).[139] In 2019, Anderson was sentenced to three months in prison.[140] The variation between these cases' sentences is wide, in part because of variations in their criminal history and a wide variation in

---

[131] A calculation is useful despite any approximation being just that, an approximation, which may vary significantly depending on the arguments, facts, and parties involved.

[132] 12 Crim. 185 (S.D.N.Y. Feb. 21, 2013).

[133] Press Release, U.S. Att'y's Off., S. Dist. of N.Y., *Jeremy Hammond Sentenced to 10 Years in Prison for Hacking into the Stratfor Website and Other Company, Federal, State, and Local Government Websites*, FBI (Nov. 15, 2013), https://archives.fbi.gov/archives/newyork/press-releases/2013/jeremy-hammond-sentenced-to-10-years-in-prison-for-hacking-into-the-stratfor-website-and-other-company-federal-state-and-local-government-websites [https://perma.cc/JEN8-BGHX].

[134] *See* Sentencing Memorandum on Behalf of Jeremy Hammond at 4, United States v. Hammond, No. 12 Crim. 185 (S.D.N.Y. Jan. 7, 2014).

[135] *See* U.S. DOJ, *supra* note 135.

[136] No. 18-CR-00596 (S.D.N.Y. Feb. 26, 2019).

[137] Press Release, U.S. Att'y's Off., S. Dist. of N.Y., *California Man Pleads Guilty to Hacking Websites for the Combating Terrorism Center at West Point and the New York City Comptroller* (Oct. 2, 2018), https://www.justice.gov/usao-sdny/pr/california-man-pleads-guilty-hacking-websites-combating-terrorism-center-west-point-and [https://perma.cc/M9PM-TXEM].

[138] *See* Transcript of Sentencing at 26, United States v. Anderson, No. 18-CR-00596 (S.D.N.Y. Feb. 26, 2019).

[139] *See id.*

[140] *See* Press Release, U.S. Att'y's Off., S. Dist. of N.Y., *Hacker "AlfabetoVirtual" Sentenced to Prison for Hacking Websites of the Combating Terrorism Center at West Point and the New York City Comptroller* (Feb. 26, 2019), https://www.justice.gov/usao-sdny/pr/hacker-alfabetovirtual-sentenced-prison-hacking-websites-combating-terrorism-center#:~:text=Berman%2C%20the%20United%20States%20Attorney,the%20websites%20for%20the%20Combating [https://perma.cc/N33H-DZDU].

offense levels. However, using these cases as guideposts for their respective offense levels, we can estimate a hypothetical calculation for the existing guidelines under the central scenario that catalyzes this Note.

Given the wide range of possible considerations, the Sentencing Guidelines leave open the possibility of sentences ranging anywhere from ten to sixty-three months in prison. The following is an estimated guidelines calculation followed by relevant explanations under the hypothetical scenario devised in the introduction to this paper.

A base offense level of six rather than seven is appropriate under § 2B1.1(a).[141] The application of § 2B1.1(b)(10)(C), a two-level enhancement for the utilization of sophisticated means, is also appropriate.[142] If the resulting offense level under § 2B1.1(b)(10) is less than twelve, the guidelines direct that the offense level be increased to twelve.[143] At this point, a possible deviation in sentencing levels is present. Under § 2B1.1(b)(19)(A), the greatest of one of three options is to be applied, if any are applicable.[144] If a defendant is convicted under § 1030 and "used by or for a government entity in furtherance of the administration of justice, national defense, or national security," the guidelines call for an increase of two levels.[145] If, however, a defendant is convicted under § 1030(a)(5)(A), the guidelines call for an increase of four levels.[146] Finally, if the offense "caused a substantial disruption of a critical infrastructure," an increase of six levels is required, or, if the offense level is less than level twenty-four, an increase to level twenty-four is called for.[147] Accordingly, much depends on whether or not election result tabulation websites are considered "critical infrastructure" or relevant to "the administration of justice, national defense, or national security" under the guidelines.[148] While the guidelines do not define "the administration of justice, national defense, or national security" explicitly, for the purposes of § 2B1.1(b)(19), "'[c]ritical infrastructure' means systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters" and can extend to both publicly or privately owned entities like gas and oil production capabilities and telecommunication networks.[149]

At this point, one can only speculate if the breach of an unofficial election website would apply under the meaning of "critical infrastructure" or serve the "administration of justice." Critically, in *United States v. Hammond*, despite breaching the FBI's Virtual Academy website as well as those belonging to the Arizona Department of Public Safety and a Sherriff's Office, this provision did not apply.[150] Furthermore, in *United States v. Anderson*, Anderson's final

---

[141] *See* Sentencing Memorandum on Behalf of Jeremy Hammond at 4, United States v. Hammond, No. 12 Crim. 185 (S.D.N.Y. Nov. 12, 2013).

[142] *See id.*

[143] *See* U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b)(10) (U.S. SENT'G COMM'N 2023).

[144] *See* U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b)(19)(A) (U.S. SENT'G COMM'N 2023).

[145] U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b)(19)(A)(i) (U.S. SENT'G COMM'N 2023).

[146] *See* U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b)(19)(A)(ii) (U.S. SENT'G COMM'N 2023).

[147] U.S. SENT'G GUIDELINES MANUAL §§ 2B1.1(b)(19)(A)(iii), (B) (U.S. SENT'G COMM'N 2023).

[148] U.S. SENT'G GUIDELINES MANUAL § 2B2.3(b)(1)(A) (U.S. SENT'G COMM'N 2023).

[149] U.S. SENT'G GUIDELINES MANUAL § 2B1.1 cmt. n.15(A) (U.S. SENT'G COMM'N 2023).

[150] Sentencing Memorandum on Behalf of Jeremy Hammond at 4, United States v. Hammond, No. 12 Crim. 185 (S.D.N.Y. Nov. 12, 2013); U.S. DOJ, *supra* note 137.

sentence suggests that he did not breach critical infrastructure when defacing the websites for the Combating Terrorism Center at the West Point and the Office of the New York City Comptroller.[151] Accordingly, a final offense level would likely land at any one of the following: twelve,[152] fourteen,[153] or sixteen.[154] Further, assuming a criminal history category of one, the resulting sentencing guideline ranges would be ten to sixteen months under offense level twelve, fifteen to twenty-one months under offense level fourteen, or twenty-one to twenty-seven months under offense level sixteen.[155] Accordingly, under the hypothetical provided, an offense breaching an unofficial election result website and meddling with that website would yield, at most, two years and three months in prison under the Sentencing Guidelines and imputing the assumptions as stated. Alternatively, assuming a damaging breach of "critical infrastructure" occurred, a sentence under the guidelines with an offense level of twenty-four would yield fifty-one to sixty-three months incarceration (up to five years three months).[156]

D. IMPLEMENTATION OF THE DEFENDING THE INTEGRITY OF VOTING SYSTEMS ACT TO THE U.S. SENTENCING GUIDELINES MANUAL

Whether any of the previously denoted sentences would be appropriate is outside the scope of this Note. However, at the very least, the U.S. Sentencing Commission should consider such a question and promulgate an amendment specifying where it stands on that issue. In addition, regardless of any enhancement in offense level for these particular crimes, the Sentencing Commission should promulgate an amendment to explicitly implement the DIVSA to the U.S. Sentencing Guidelines Manual. The passage of this new legislation is a plausible justification for promulgating an amendment to the Sentencing Guidelines.

Furthermore, amendments may be justified through recent trends and updated information as the guidelines are explicitly flexible.[157] Recent amendment briefs have pointed to policy priorities and statistics in support of their promulgation.[158] The Sentencing Guidelines have yet to be updated to incorporate the newest definition of a "protected computer," which, as noted, now encompasses "voting systems."[159] The need for this updated definition also offers a critical opportunity to further deter meddling with unofficial tabulations and elections more broadly,

---

[151] *See* Transcript of Sentencing at 26, United States v. Anderson, No. 18-CR-00596 (S.D.N.Y. Feb. 26, 2019); U.S. DOJ, *supra* note 138.

[152] Assuming none of the possibilities under USSG §2B1.1(b)(19)(A) were applicable.

[153] Assuming USSG §2B1.1(b)(19)(A)(i) was applicable.

[154] Assuming USSG §2B1.1(b)(19)(A)(ii) was applicable.

[155] *See* U.S. SENT'G GUIDELINES MANUAL ch. 5, pt. A (U.S. SENT'G COMM'N 2023).

[156] Assuming USSG §2B1.1(b)(19)(A)(iii), and therefore USSG §2B1.1(b)(19)(B), was applicable. *See id.*

[157] *See, e.g.*, *2023 Amendments in Brief*, U.S. SENT'G COMM'N (Nov. 1, 2023), https://www.ussc.gov/sites/default/files/pdf/amendment-process/amendments-in-brief/AIB_818.pdf [https://perma.cc/M79V-9E7K].

[158] *See id.*

[159] *See* U.S. SENT'G GUIDELINES MANUAL § 2B2.3, cmt. n.1 (U.S. SENT'G COMM'N 2023) (denoting a "protected computer" means a computer described in 18 U.S.C. § 1030(e)(2)(A) or (B) and neglecting to include §1030(e)(2)(C) as a part of that definition); *see also* 18 U.S.C. § 1030(e)(2)(C).

which the U.S. Sentencing Commission should take advantage of. The Sentencing Guidelines often utilize particularized subsections of the U.S. Code to specify offense-level changes or other departures from the guidelines.[160] Additionally, the Sentencing Commission has promulgated similar enhancements against foreign cyber threats,[161] with, presumably, similar chances of conviction and sentencing in those cases.

The promulgation of an amendment certainly could have a deterrent effect on domestic actors who might seek to utilize misinformation to serve personal or political ends.[162] However, as noted, the extent to which additional deterrents would be needed in this area of domestic criminal law is up for debate. Admittedly, the lack of breaches of unofficial election results websites may be evidence that domestic actors are currently sufficiently deterred from engaging here. However, domestic non-hacking-related attempts to destabilize unofficial tabulations, mainly carried out by former President Trump and his allies, have continued in advance of the 2024 election.[163] Moreover, this is, by its very nature, a prospective scenario. Recent events suggest that individuals might be willing to take advantage of the vulnerabilities in our election systems for their own gain.[164] It would seemingly be impossible, at least for the purposes of this Note, to measure the existing deterrent effect of the current laws and the Sentencing Guidelines in such a specific area. However, at the very least, it is clear that attempts by domestic actors to hack into government websites at large have not been so effectively deterred that such actions are never attempted.[165] If, under current law and the existing Sentencing Guidelines, there is not enough deterrence to prevent hacking into significant and secured government websites like those belonging to the FBI and West Point's Combating Terrorism Center[166] on occasions that *lack* larger potential political gains, it is not inconceivable that a politically motivated actor might consider doing so to a local and unsecured county election tabulation website for broader purposes.

---

[160] *See, e.g.*, U.S. SENT'G GUIDELINES MANUAL § 2B1.1(13) (U.S. SENT'G COMM'N 2023) ("If the defendant was convicted under 42 U.S.C. § 408(a), § 1011(a), or § 1383a(a) and the statutory maximum term of ten years' imprisonment applies, increase by 4 levels."); U.S. SENT'G GUIDELINES MANUAL § 2A3.4 (a)(1) (U.S. SENT'G COMM'N 2023) (applying base offense level "20, if the offense involved conduct described in 18 U.S.C. § 2241(a) or (b)"); U.S. SENT'G GUIDELINES MANUAL §2B1.1 cmt. n.21(A)(v) (U.S. SENT'G COMM'N 2023) (denoting upward departures "[i]n a case involving stolen information from a 'protected computer', as defined in 18 U.S.C. § 1030(e)(2), the defendant sought the stolen information to further a broader criminal purpose.").

[161] *See, e.g.*, U.S. SENT'G GUIDELINES MANUAL § 2B1.1(b), amend. 711 (U.S. SENT'G COMM'N 1987), https://www.ussc.gov/guidelines/amendment/771 [https://perma.cc/9UAM-XZ4H].

[162] *See* Swan, *supra* note 41; H.R. REP. NO. 117-663, at 373 (2022).

[163] *See* Adam Rawnsley & Asawin Suebsaeng, *Inside Trump's Plot to Corrupt the 2024 Election with 'Garbage' Data*, ROLLING STONE (Dec. 8, 2023, 9:30 AM), https://www.rollingstone.com/politics/politics-features/trump-election-plans-corrupt-voter-registration-eric-eagleai-1234920083/ [https://perma.cc/S2FX-E4TN] (describing how efforts to move states away from stable voter file systems may precipitate delays to count ballots and "the longer it takes to count overall ballots and get an unofficial winner, those all feed into the potential for chaos and even incitement to violence by election losers").

[164] *See id.*; Swan, *supra* note 41.

[165] *See* Sentencing Memorandum on Behalf of Jeremy Hammond, United States v. Hammond, No. 12 Cr. 185 (S.D.N.Y. Nov. 12, 2013); U.S. DOJ, *supra* note 137; Transcript of Sentencing, United States v. Anderson, No. 18-CR-00596 (D.D.C. Mar. 26, 2019); U.S. DOJ, *supra* note 138.

[166] *See* U.S. DOJ, *supra* note 138; U.S. DOJ, *supra* note 137.

Again, while it is seemingly impossible to effectively measure deterrence in this specific area of the law, historic government website breaches under the same laws and guidelines, and the clear mission by some to manipulate the election infrastructure in the hopes of metastasizing misinformation to their benefit, points towards the possibility that domestic actors are not currently effectively deterred from acting in this area. Regardless, the U.S. Sentencing Commission would be well placed to attempt to examine the relevant information and determine the degree of deterrence, or lack thereof.[167] Current laws and guidelines have not been effective in deterring foreign actors from attempting to breach these systems.[168] An amendment in this area could further deter foreign and domestic actors from engaging in malicious election interference behavior and demonstrate the seriousness with which the United States takes interference in its election systems, including unofficial election results. Furthermore, it would allow the Sentencing Commission to specifically articulate what it believes the appropriate consequences should be for such breaches.

Given its delineation of voting systems in a separate subsection,[169] the precedent of using those delineations to shape the Sentencing Guidelines, [170] and its creation of an independent need for an amendment to the Sentencing Guidelines in this area,[171] the DIVSA offers an opportunity for the Sentencing Commission to efficiently add particularized guidance on how to approach sentencing for these types of election crimes, including the act of tampering with unofficial election results. Currently, unless they are considered "critical infrastructure," the Sentencing Guidelines do not afford voting systems, including unofficial election tabulation, any greater protections, and, therefore, deterrence than that afforded to all devices connected to the internet.[172] Given the relevancy of these issues, the continued threat of such interference, and, perhaps most critically, the relative ease with which the Sentencing Commission can promulgate these amendments[173] compared to Congress's legislative process and build-up and adoption of a federated website security infrastructure, this Note calls on the Commission to take an explicit stance on meddling with voting systems. In doing so, the Commission would further the national interest of deterring unofficial election tabulation meddling and election interference as a whole.

---

[167] *See, e.g.*, *2023 Amendments in Brief*, *supra* note 157.

[168] *See, e.g.*, Lyngaas, *supra* note 35.

[169] *See* 18 U.S.C. § 1030(e)(2)(c).

[170] *See, e.g.*, U.S. SENT'G GUIDELINES MANUAL § 2B1.1(13), cmt. n.21(A)(v) (U.S. SENT'G COMM'N 2023); U.S. SENT'G GUIDELINES MANUAL § 2A3.4(a)(1) (U.S. SENT'G COMM'N 2023).

[171] As noted, the Sentencing Guidelines' definition of "protected computer" is outdated. *See* U.S. SENT'G GUIDELINES MANUAL § 2B2.3 cmt. n.1 (U.S. SENT'G COMM'N 2023) (denoting a "'protected computer' means a computer described in 18 U.S.C. § 1030(e)(2)(A) or (B)" and neglecting to include §1030(e)(2)(C) as a part of that definition); *see also* 18 U.S.C. § 1030(e)(2)(C).

[172] *See* Van Buren v. United States, 593 U.S. 374, 378 (2021).

[173] The Commission promulgates amendments through its regular cycle and said amendments become effective if Congress does not modify or formally disapprove of those amendments before November 1 of the year the amendment or modification is submitted. *See* 28 U.S.C. § 994(p).

CONCLUSION

In the movie *WarGames*, a 1983 thriller, "a rebellious high school student nearly starts World War III when he accidentally accesses the computer system controlling the United States nuclear arsenal, mistaking the system for an interactive video game."[174] By many accounts, this movie's fictionalized scenario catalyzed congressional action that would later lead to The Computer Fraud and Abuse Act.[175]

This Note also outlines a hypothetical scenario—that foreign actors may breach unofficial voting results websites and change them, sowing discord and weakening "the U.S. democratic process, . . . undermin[ing] the appeal of democracy itself."[176] As shown, this threat is very real.[177] The federal government takes threats that might undermine democracy, including the breach of unofficial election websites, seriously and has resultantly proliferated significant guidance for citizens and state and local officials, crafted various reports, and responded with the passage of legislation.[178] Still, the threat of unmitigated chaos in light of a potential breach of websites remains significant. The possibility of election misinformation from these sources caused by foreign or domestic interference may only continue to undermine faith in the electoral process and, as a result, catalyze violence. This Note is limited in how it chooses to address and examine the potential threat, but every bit of protection is necessary when faith in democracy is at stake.

This Note analyzes how existing criminal laws and subsequent Sentencing Guideline calculations might react to such a scenario and how that response might be improved within the confines of those laws and guidelines. Specifically, this Note calls attention to the CFAA and the DIVSA as critical components of the criminalization of and resulting deterrence against this malicious behavior.[179] While these breaches have yet to be actualized to the extent hypothesized in this Note's opening scenario, it is shockingly realistic and possible. While the threat may seem far off, deterrence is, by its nature, prospective. All reaches of the government should work in

---

[174] CONG. RSCH. SERV., R47557, CYBERCRIME AND THE LAW: PRIMER ON THE COMPUTER FRAUD AND ABUSE ACT AND RELATED STATUTES (2023), https://crsreports.congress.gov/product/pdf/R/R47557 [https://perma.cc/SUE7-4TXA] (quoting Roger Ebert, *WarGames*, ROGEREBERT.COM (June 3, 1983), https://www.rogerebert.com/reviews/wargames-1983 [https://perma.cc/TDJ4-4CXH] (reviewing and summarizing plot of WarGames)).

[175] *See id.* (citing Jay P. Kesan & Carol M. Hayes, *Mitigate Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 492 (2012) (explaining there is evidence the CFAA was signed into law "partially in response to the situations depicted in the action film WarGames")); Ivan Evtimov, David O'Hair, Earlence Fernances, Ryan Calo & Tadayoshi Kohno, *Is Trusting a Robot Hacking?*, 34 BERKELEY TECH. L.J. 891, 904 (2019) ("According to popular lore, President Reagan saw the movie WarGames and met with his national security advisers the next day to discuss America's cyber vulnerabilities. The CFAA is said to be the result of their deliberations.")).

[176] CYBER DIGITAL TASK FORCE, *supra* note 21, at 2.

[177] *See id.* at 3.

[178] *See, e.g.*, *Election Security Rumor vs. Reality*, *supra* note 7; CYBER DIGITAL TASK FORCE, *supra* note 21, at 12; BALSER, *supra* note 71, at 1; Defending the Integrity of Voting Systems Act, Pub. L. No. 116-179, 134 Stat. 855 (2020) (codified as amended at 18 U.S.C. § 1030(e)).

[179] *See* CYBER DIGITAL TASK FORCE, *supra* note 21, at xiii, 6, 121.

concert to prevent this activity wherever possible. Accordingly, this Note recommends the Sentencing Commission make use of its powers to promulgate an amendment to the Sentencing Guidelines and articulate specific consequences for attacks on voting systems utilizing the delineation available through the DIVSA to do so. Despite the fact these changes will arrive too late to impact the 2024 election, the threats outlined here will not dissipate with time. And while this may seem a minimal change, the obligation to deter against such a fundamental threat to our stability and the relative ease with which that deterrence can be implemented both speak in its favor. In describing the state of the law and making this recommendation, this Note calls attention to a threat all too real to a particularly vulnerable area that is critical to the functioning of our democracy.