BEYOND "SECURITY":
Addressing the Hidden Crisis in Our Elections

| January 2020

Beyond "Security": Addressing the Hidden Crisis in Our Elections

Voatz, Inc. | January 16, 2020

A quiet but mounting crisis threatens to undermine the integrity of the U.S. election system. It's not the danger of foreign hacking and interference, though the threats are intertwined. Rather it is the dramatic increase in the cost of administering our elections, a figure which has surged since 2016.

This shouldn't come as a surprise: Our election system has become the latest battlefront in the asymmetric warfare which is the hallmark of the 21st century, with our adversaries using relatively modest resources to cause disproportionate harm. Faced with resulting skyrocketing costs of protecting our political system, our leaders must fundamentally rethink how we conduct elections. We should employ a new vocabulary that captures the limits of security and emphasizes instead systemic resilience.

It is a little-known but striking fact of American political life, that no one knows how much it costs to administer U.S. elections.[1] As many as 10,000 jurisdictions have some responsibility (and so spend some money on) administering U.S. federal, state, and local elections, so tallying the cost is a Sisyphean task. Nevertheless, attempts have been made to put a bottom line on the system. In 2001, the Caltech/MIT Voting Technology Project estimated that the previous year's balloting had cost around $1 billion;[2] the same group later assessed that the 2012 elections cost $2.6 billion,[3]

while in 2019 the MIT Election Data and Science Lab calculated the annual price tag at $2 billion.[4]

The 2016 Russian attacks on our political system introduced a major new expense to running an election: the cost of security. It is quickly threatening to dwarf traditional spending. Since 2018, Congress has appropriated roughly $900 million to upgrade the political system's defenses, paying for things such as boosting cybersecurity, bringing on new IT staff and conducting election audits.[5] And that figure does not reflect new state election security expenditures since 2016. These haven't been tallied but the grants came with matching requirements totaling $104 million in new state spending.[6]

Think about that figure: Running elections has traditionally cost somewhere between $2 and $2.5 billion annually, but in the last two years the federal government has authorized spending more than $1 billion on what is essentially a new cost area.

And there is no reason to believe that that amount will decline any time soon. Election security advocates decry the $900 million already appropriated as insufficient, some citing a Brennan Center study released last summer that suggested securing our election system could cost $2.2 billion.[7]

Consider, too, the evolving nature of the threat profile. Russia alone was the adversary in 2016 but last November the U.S. intelligence community warned that "Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions" in 2020.[8] And they're getting smarter about how they vector their attacks: As a January New York Times article noted, foreign hackers' tactics are evolving to keep pace with U.S. defensive efforts; they are, as one intelligence official told the paper, "refreshing" their operations. Worse: "[I]nterviews with dozens of officials and experts make clear that many of the vulnerabilities exploited by Moscow in 2016 remain," the Times reported.[9]

Indeed, while efforts to bolster the integrity of our systems are important, the millions (soon, billions) that we're pouring into those efforts have limited efficacy. In the context of the $4.7 trillion federal budget, $1 or even $2 billion is a rounding error, but if it's not targeted properly – and to the extent that it provides a false sense of security – it is an unconscionable waste. Most of the nation's 10,000 jurisdictions, for example, are tiny and have little or no technical support, meaning

that the bulk of the cybersecurity training never benefits a huge swath of the election system. And much of the new effort focuses on the attack that didn't come in 2016: hacking votes and ballot rolls. While this is important, it elides the vulnerabilities which Russia did exploit four years ago, which remain: using social media and misinformation to exacerbate the widespread polarization which already infects our politics.

This is the very essence of asymmetric warfare: an attack that can cost relatively little to stage and does disproportionate damage, but also puts outsized demands on national resources to defend against in the future. The classic example is 9/11: The terrorists spent between $400,000 and $500,000 to plan and conduct their attack[10] and 10 years after, it had cost the U.S. $3.3 trillion, according to a 2011 New York Times analysis.[11] Similarly, whatever Russia spent in 2016 is trivial compared to the amount the U.S. is now expending in response. Now imagine what Russia (and other countries) are gearing up to spend this year, having seen the return on their initial investment in 2016.

Similarly the voting system is vulnerable to kinetic events like natural disasters. Consider the disruption Hurricane Sandy inflicted on voting in the Northeast a full week prior to the 2012 presidential elections[12], and Hurricane Michael which visited Florida weeks before the 2018 elections.[13] And keep in mind that climate change is only going to make such weather events more frequent and unpredictable.

The unhappy truth few wish to speak is that there is no perfect security solution: Our system will never be invulnerable. So in assessing the weaknesses in and threats to our political system, we need to do more than measure for a larger Band-Aid. We need to rethink how we deliver care to our elections as a whole. What will that entail?

First, we should utilize new terminology to more accurately reflect the effort to strengthen our election systems. "Security" is too narrow a concept, connoting as it a defense rather than a holistic notion of both protection and recovery. "Resilience" is a more useful term: We cannot harden our entire system, so we need to move beyond traditional conceptions of securing our elections and start to think about hardiness when the inevitable breaches come.

Resilience refers to the system's ability to rebound from unexpected events – not simply 2016-style attacks but incidents involving other vulnerabilities including

natural disasters (such as hurricanes), bureaucratic inertia (the time and cost of certifying voting technology – a process which does not, incidentally, test the security of voting systems – is a perverse disincentive to fixing identified problems), and human error (such as the mistakes which plagued Durham, North Carolina in 2016[14] and Northampton County in eastern Pennsylvania last fall[15]). Having a resilient system can mean anything from not having to rerun voting, in the extreme case, to avoiding disruption to voters being able to complete the voting process and have their ballots counted as they intended.

There are several factors to consider regarding minimizing the possibility that a breach becomes catastrophic. Areas where voters and votes congregate – whether big polling stations or major tabulation centers – are natural targets. Can these functions be dispersed to minimize the damage a penetration could cause? Second, fake news and polarization, combined with potent social media networks, remain a critical vulnerability. Is there a way – whether through new technology, new legislation or public education – to mitigate against the virality of weaponized misinformation? Third, while the specific nature of disruptions is unforeseeable, some broad effects can be anticipated. To what extent do states and localities have robust backups and plans in place to respond to disasters, whether manmade or natural?

Where possible, we should leverage modern technology to bolster resilience. Current voting machines deployed in dozens or hundreds of locations, for example, can be cumbersome to reprogram if an error – manmade or malicious – is discovered during the voting window. By contrast, modern smartphone technology provides for a more nimble but still secure solution. That is because the secure software distribution platforms operated by public app stores allow for the ability to deploy state of the art malware-prevention measures on modern smartphones. Updated software can be quickly downloaded to resolve a previously undetected problem. Not incidentally, employing smartphone technology would also dramatically diffuse voting locations, mitigating against both systemic human attacks, natural disasters and prohibitive costs. That's because, according to the Pew Research Center, 81 percent of U.S. adults own smartphones (up from 35 percent as recently as 2011).[16]

Crises bring opportunities. Right now the U.S. faces both, but skillful and prescient leadership will help our elections system not simply survive these tests but emerge stronger – and more resilient.

[1] See, for example, "Election Costs: Who Pays and With Which Funds?" by Katy Owens and Wendy Underhill, National Conference of State Legislatures, March 2018
[2] "Securing the Vote: Protecting American Democracy," The National Academies Press (2018)
[3] *Ibid.*
[4] "How Much Are We Spending on Election Administration?" by Zach Mohr, Martha Kropf, Mary Jo McGown Shepherd, JoEllen Pope, and Madison Esterle, MIT Election Data and Science Lab
[5] "The Cybersecurity 202: Pressure still on McConnell after $425 million election security deal," by Joseph Marks, The Washington Post, December 17, 2019
[6] The $425 million passed in December 2019 had a 20 percent state match, or $85 million; the previous tranche of $380, enacted in March 2018, had a 5 percent match requirement, or $19 million. See "The Cybersecurity 202: Pressure…" in The Washington Post and "States move quickly to tap into money for election security," by Christina A. Cassidy, Associated Press, August 21, 2018
[7] "What Does Election Security Cost?" by Lawrence Norden and Edgardo Cortes, The Brennan Center for Justice, August 15, 2019
[8] "JOINT STATEMENT FROM DOJ, DOD, DHS, DNI, FBI, NSA, AND CISA ON ENSURING SECURITY OF 2020 ELECTIONS," November 5, 2019
[9] "'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020," by Matthew Rosenberg, Nicole Perlroth and David E. Sanger, The New York Times, January 10, 2020
[10] "9/11 panel: Al Qaeda planned to hijack 10 planes," CNN, June 17, 2004
[11] "One 9/11 Tally: $3.3 Trillion," by Shan Carter and Amanda Cox, The New York Times, September 8, 2011
[12] "Using Hurricane Sandy as a Lesson for Future Elections," by Thomas Kaplan, The New York Times, November 12, 2012
[13] "Hurricane Michael forces Florida to ease voting rules in hard-hit counties," by Ray Sanchez and Keena Willard, CNN, October 21, 2018
[14] "No evidence of cyber attack in Durham's 2016 elections, feds say," by Will Doran, The News & Observer, December 30, 2019 and "Durham County elections officials blame human error, not hacking, for 2016 delays," by Joe Johnson, The News & Observer, June 13, 2019
[15] "A Pennsylvania County's Election Day Nightmare Underscores Voting Machine Concerns," by Nick Corasaniti, The New York Times, November 30, 2019
[16] Mobile Fact Sheet, Pew Research Center, June 12, 2019