THE CAPITOL INSURRECTION AND PINEAPPLES ON PIZZA

PAUL ROSENZWEIG

The events of January 6th will echo in American history for years to come. While other essays in this special edition may focus on root causes of the insurrection or legal issues relating to the definition of domestic insurrection, in this brief essay I want to look at the role that cybersecurity efforts played in saving our Nation. Along the way, I will also explore the role Hawaiian pizza played (but more on that later).

Cybersecurity may not have the most obvious nexus to the insurrection, but it assuredly did. To see this most clearly, we might begin with a thought experiment grounded in the assault on the Capitol.

That assault, as others have noted, was more than an assault on a physical building, it was an attack on the counting of the Electoral College votes occurring that day and, more broadly, it was part of a larger effort to overturn the results of the November 2020 election. Fueled by Presidential claims that the election was "rigged" and chanting "Stop the Steal" the rioters on January 6th sought to deny reality – that candidate Biden had clearly won the election securing more electoral votes than Trump and winning the popular vote by more than 7 million votes.

To a very real degree the reason the insurrection failed was that its motivation was bottomed on a false narrative -- #fakenews, if you will. Through the certification process in 51 jurisdictions and through more than 60 lawsuits alleging irregularities in the voting, the results were uniform – though some minor voting irregularities may have occurred (as they do in every election) there was no credible evidence that the certified results were in any way effected, nor was there any credible doubt as to Biden's victory. That fundamental truth was sufficient to withstand the insurrectionists' efforts and to drive the ultimate result -- President Biden's inauguration.

Imagine if that factual grounding had been less certain. Imagine if even vaguely plausible claims of electoral irregularity had been advanced? Might January 6th have unfolded differently?

In the run up to the 2020 election, cybersecurity practitioners harbored two, interrelated fears: that weaknesses in our electoral infrastructure might allow malicious actors (possibly foreign) to manipulate the actual election results and, relatedly, that by spreading disinformation through social media malicious actors would sow doubt on the validity of the election results – even if there had been no manipulation. The perception of insecurity was as great a threat as the insecurity itself.

In the end, happily, neither threat seriously materialized. Both the reality of the security of the election ("the most secure" in American history) and efforts to combat disinformation meant that, ultimately, complaints about election irregularities were unable to gain any purchase outside of a fringe of believers. Had that not been the case, one can readily imagine the possible adverse consequences.

For this tranquility we owe a great debt of gratitude to the Federal government. Their efforts to secure the election were two-fold: to both enhance its actual security and to diminish the impact of disinformation on the perception of security. Despite the lack of active engagement from the White House, the Cybersecurity and Infrastructure Security Agency (CISA) of DHS, in particular, did yeoman's work – work that was, until the untimely and abrupt firing of its Director, mostly unremarked by the American public.

Infrastructure -- Our election infrastructure is primarily owned and operated by the 50 States (along with the District of Columbia) who are responsible for administering elections. To secure this election infrastructure CISA had to build relationships with state and local officials (some of whom were quite skeptical of Federal "assistance") as well as private sector actors (who provide much of the equipment) and non-governmental organizations who were concerned about election security. As part of that effort CISA established an information sharing and analysis center for election infrastructure that was built to share security-related information across the nation so that those responsible for the cyber defense of our election systems could take action.

CISA also offered more substantial assistance to those jurisdictions that wanted it. They created risk assessment tools and developed incident detection and notification standards, that jurisdictions could look to for guidance. More aggressively, if asked, CISA would provide scanning systems to check for vulnerabilities and teams from CISA were available to do penetration testing of local election systems. CISA also gave guidance on how to physically secure voting locations and election facilities from possible threats.

Finally, and perhaps most importantly, working with the Election Assistance Commission, CISA helped state and local jurisdictions transition most election systems in the United States to ones that had paper ballot backups. By the time of the 2020 election, more than 90% of ballots cast in America had a paper-based backup to the electronic recording of a vote. The existence of a clear paper record allowed for post-election auditing and recount processes that validated the accuracy of the reported machine-tallied ballots.

To particularize this rather more pointedly, in 2016 Georgia, which famously became a battleground in the recent election, had a voting system that did ***not*** have a paper ballot backup. By the time the 2020 election season had rolled around a paper backup system was in place. The existence of paper backups allowed the Georgia Secretary of State to confirm the accuracy of the original machine-based count as roughly 99.99% correct.

At bottom then, while the President and his supporters complained vociferously that the Dominion machines used to count ballots in Georgia had been tampered with, they could not maintain that fiction in the face of hard paper records confirming the machines' accuracy. That outcome, in turn, was the result of the hard work done by CISA and others in the Federal government in the years leading up to the 2020 election. Without it, Trump's complaints might have been more plausible and the conflict on January 6th potentially much more devastating.

Disinformation – CISA's efforts on the second prong of their mission -- combatting disinformation – were also quite robust, though it is fair to say that they were not as successful as

the infrastructure work that CISA did. Despite their efforts (and those of private sector actors like Twitter and Facebook) election fictions continued to resonate with the American public.

One can only imagine how much worse the falsehoods might have been, however, without the work that CISA and others did. CISA, for example, published an Election Disinformation Tookit, for election officials to enable them to combat false stories. They also created a Rumor Control website, where Federal officials actively debunked mis- and disinformation about the election and its security (no … dead people do not regularly vote in elections). Speaking to a more popular audience, CISA even created a graphic novel, "Real Fake," that dramatized how malicious actors can use disputes about social and political issues to drive polarization and create doubts about the integrity of the election.

And that brings us back to Hawaiian pizza. You know Hawaiian pizza, I'm sure. It's the one with pineapple on it. You either love it, or as I do, you hate it. There are few, if any, consumers who are neutral on the topic.

CISA used this well-known gastronomic dispute as a way of educating the American public as to how foreign trolls might try to create public polarization. Waging a fake (and joking) "war on pineapple" CISA used this difference of opinion as a means of illustrating the chain of foreign influence operations and the spread of disinformation. The twitter "war" over Hawaiian pizza went viral and served as a humorous way of analogizing to more serious political disagreements that could be distorted and manipulated by malign actors.

* * * * *

Nothing is likely to erase the memory of January 6th from the American mind any time soon. The events of that day were horrific in the extreme. How much worse, however, could they have been if the underlying claims of electoral fraud had not been so conclusively and demonstrably false? Or if at least some portion of the American public had not been sensitized to the possibility of the spread of disinformation? How would our political system have reacted to claims of fraud that were more plausible (even if, ultimately, in error)?

Thankfully, we did not have to confront that question. I do not offer the claim that CISA (and the related election security efforts of other Federal, State, and local officials) was essential to the failure of the insurrection. But I am struck by the fact that our success in thwarting the attempt to overturn the results of the election was, at least in part, the result of groundwork laid over several years before the election by a relatively small Federal agency doing nothing more than trying to advance its overall mission. To the extent that this is true, we should all be thankful that agencies like CISA exist and were able to operate as they did – for without them I do not know if our Nation would have survived unharmed.

**Paul Rosenzweig is a Senior Resident Fellow at R Street Institute and Professorial Lecturer in Law, George Washington University. He is also the Former Deputy Assistant Secretary for Policy, Department of Homeland Security.*