States are on front lines of 2020 election-security efforts

- By Christina A. Cassidy The Associated Press

- Dec 26, 2019

SPRINGFIELD, Va. — Inside a hotel ballroom near the nation's capital, a U.S. Army officer with battlefield experience told 120 state and local election officials that they may have more in common with military strategists than they might think.

These government officials are on the front lines of a different kind of battlefield — one in which they are helping to defend American democracy by ensuring free and fair elections.

"Everyone in this room is part of a bigger effort, and it's only together are we going to get through this," the officer said.

That officer and other past and present national security leaders had a message to convey to officials from 24 states gathered for a recent training held by a Harvard-affiliated democracy project: They are the linchpins in efforts to defend U.S. elections from an attack by Russia, China or other foreign threats, and developing a military mindset will help them protect the integrity of the vote.

The need for such training reflects how elections security worries have heightened in the aftermath of the 2016 election, when Russian military agents targeted voting systems across the country as part of a multi-pronged effort to influence the presidential election.

Until then, the job of local election officials could had been described as akin to a wedding planner who keeps track of who will be showing up on Election Day and ensures all the equipment and supplies are in place.

Now these officials are on the front lines. The federal government will be on high alert, gathering intelligence and scanning systems for suspicious cyberactivity as they look to defend the nation's elections.

Meanwhile, it will be the state and county officials who will be on the ground charged with identifying and dealing with any hostile acts.

"It's another level of war," said Jesse Salinas, the chief elections official in Yolo County, California, who attended the training. "You only attack things that you feel are a threat to you, and our democracy is a threat to a lot of these nation-states that are getting involved trying to undermine it. We have to fight back, and we have to prepare."

Salinas brought four of his employees with him to the training, which was part of the Defending Digital Democracy Project based at the Belfer Center for Science and International Affairs at the Harvard Kennedy School.

The group has been working actively with former and current military, national security, political and communications experts — many of whom dedicate their time after work and on weekends — to develop training and manuals for state and local election officials. Those involved with leading the training asked for anonymity because of their sensitive positions.

The project's **latest playbook** focuses on bringing military best practices to running Election Day operations, encouraging state and local election officials to adopt a "battle staff" command structure with clear responsibilities and standard operating procedures for dealing with minor issues. The project is also providing officials with a free state-of-the-art incident tracking system.

Eric Rosenbach, co-director of the Belfer Center and a former U.S. Army intelligence officer who served as chief of staff to Defense Secretary Ash Carter in the Obama administration, told the group gathered for the training that it “shouldn’t be lost on you that this is a very military-like model.”

“Let’s be honest about it,” Rosenbach said. “If democracy is under attack and you guys are the ones at the pointy end of the spear, why shouldn’t we train that way? Why shouldn’t we try to give you the help that comes with that model and try to build you up and do all we can?”

Instructors stressed the need for election officials to be on the lookout for efforts to disrupt the vote and ensure that communications are flowing up from counties to the state, down from states to the counties, as well as up and down to the federal government and across states.

Piecing together seemingly disparate actions happening in real-time across geographical locations will allow the nation to defend itself, said Robby Mook, Democratic presidential nominee Hillary Clinton’s campaign manager in 2016. Mook founded the **Defending Digital Democracy Project** with Rosenbach and Matt Rhoades, Republican nominee Mitt Romney’s 2012 campaign manager.

“Find a way to input data in a consistent, efficient and reliable way to ensure you know what is going on and prevent things from falling through the cracks,” Mook told the election officials. “You got to rise above just putting out fires.”

At the training were officials from California, Colorado, Georgia, North Carolina, Oregon, Tennessee, West Virginia and other states. In one exercise, election officials were paired up as either a state or county under an Election Day scenario, charged with logging incidents and trying to piece together what turned out to be four different coordinated campaigns to disrupt voting.

“One of the big takeaways was just how the lack of one piece of information moving up from the counties to the state or moving from the states to counties, if either of those things don’t happen, it can have a significant impact,” said Stephen Trout, elections director for Oregon.

Trout said he would move quickly to acquire, customize and implement the incident tracking system, which would be an upgrade from the paper process currently in use. Dave Tackett, chief information officer for the West Virginia Secretary of State’s Office, said he will recommend some structuring changes at his state operations center, including bringing key personnel into the room and incorporating elements of the incident tracking system like mapping and the ability to assign people to specific incidents.

Local angle

Brad Nelson, director of elections for Pima County, said his office is working with federal and state officials to both ensure their own cybersecurity and combat any misinformation that may arise during the upcoming elections next year.

In terms of the former, those entities, including the county’s communications department, will strive to share accurate information throughout election day, including any issues at polling sites, as well as the correct election results. The votes are not tallied at individual polling locations, but rather at a centralized locations, and are never done on a system that is online, Nelson said.

To ensure cybersecurity, they have set up firewalls on their systems. Although they cannot do the same for candidates and political entities, the secretary of state has provided county offices a cybersecurity handbook for them to share regarding keeping information and accounts safe.

“We’re going to do our best to get the true information out,” Nelson said.

Arizona Daily Star