securing the vote

FAIR ELECTIONS ARE AT THE HEART OF A DEMOCRACY, WHICH IS WHY A UNIVERSITY OF PITTSBURGH INSTITUTE HAS BEEN WORKING TO PROTECT VOTING IN PENNSYLVANIA FROM COMPUTER HACKING THAT WAS ANTICIPATED AND PANDEMIC COMPLICATIONS THAT WEREN'T. BY JEFFERY FRASER

In 2018, a fledgling institute at the University of Pittsburgh began exploring ways to shield the antiquated voting system in Pennsylvania against an insidious menace that David Hickton knew was lurking as the greatest threat to America's political elections. And it wasn't a virus.

As the director of the Institute for Cyber Law, Policy and Security (Pitt Cyber), Mr. Hickton was well-acquainted with the threat. When he was U.S. Attorney for the Western District of Pennsylvania from 2010 to 2016, he had pursued a Russian network of hackers known as Fancy Bear. For several years beginning in 2014, Fancy Bear attacked computers at Westinghouse, the nuclear energy company north of Pittsburgh, and other companies and organizations. Some of the hackers were later indicted as part of a sophisticated Russian cyberattack on the 2016 U.S. presidential election, and according to intelligence agencies, their strategy of disruption continues today.

Mr. Hickton knows that the Russian hackers are cunning in their tactics. Their ranks include military intelligence officers. Their track record includes sowing discord during elections in democracies throughout Europe. And they've been caught probing U.S. state and local election systems, including Pennsylvania's.

"Russia's signature for election hacking is wide, evident, specific," he said. "What they did in the United States is what they've done all over the world. They did it in the 2016 election. They did it in our congressional election in 2018, and they're armed, dangerous and doing it again in 2020.

Jeff Fraser is a Pittsburgh-based freelance writer and frequent contributor to h.

"We have to take that as the landscape we're given and protect ourselves."

Pennsylvania took steps to tighten security last year, adopting election reforms that included mail-in ballots and new voting machines backed up by paper records. The measures were largely based on the recommendations of a panel of experts convened by Pitt Cyber that investigated the state's election process and found it highly vulnerable.

The reforms were cheered as a sign of long-overdue progress in steeling Pennsylvania against an attack intended to disrupt its elections. But the coronavirus pandemic has delivered a new threat, unexpected challenges and uncertainty in a year when Pennsylvanians will elect a president and members of Congress to represent them.

Mr. Hickton described the very structure of the U.S. election system as leaving it vulnerable to cyberattack and concedes a critical advantage to skilled and determined hackers.

In Pennsylvania, for example, every election is, in essence, 67 elections, each run by local county boards of election responsible for overseeing everything from choosing voting machines to tallying the vote. Circumstances are similar in the other 49 states and more than 3,000 U.S. counties.

That leaves each to defend their elections against hacking operations directed by foreign intelligence agencies whose prowess is no match for a county election board, regardless of whether it presides in an urban center or the rural outskirts.

"It's unreasonable to ask county election officials to deal with a nation-state threat from an adversary like Russia," Mr. Hickton said. "But that institutional vulnerability is carried forward to this day."

News reports on foreign hacking activities revealed how investigations in Pittsburgh were among the first to lead to a probe of the criminal cyber network that would eventually turn its attention to the nation's elections.

The network's strategies included spreading misinformation and inciting political and social tensions using social media platforms. Popular targets included key districts in battleground states where no candidate had a clear edge. The U.S. Senate Intelligence Committee reported in 2018 that Russian hackers probed state and local election systems in all 50 states. Special Prosecutor Robert Mueller reported the targets included technology firms that make and administer election hardware and software, including software used for voter registration and electronic polling stations.

Pennsylvania's aging electronic voting machines were ripe for attack. Replacing them with models that add a paper record of every vote cast was at the top of the list of recommendations made by the Blue Ribbon Commission on Pennsylvania's Election Security launched by Pitt Cyber with support from The Heinz Endowments. Until this year, some 83 percent of voting machines in the state were only able to electronically record votes.

State law required Pennsylvania counties to upgrade in 2019 to modern machines that leave a paper trail for auditing in time for the upcoming elections. This year's primary was to be the first test of those machines for most.

The importance of having auditable backup ballots was underscored last year, however, when Northampton County switched to new voting machines that had paper ballot backups, and a software glitch occurred in an election for county judge. At the end of the night, electronic tabulations gave one of the two front runner candidates only 164 of the 55,000 votes cast, a shocking result in a contest expected to be razor-close. Because the new machines allowed re-tabulation of the vote from backup paper ballots, the candidate who originally had 164 votes was eventually found to be the winner of the election by a slim margin.

But the risk posed by hackers is broad, imperiling the entire state election infrastructure, federal investigations conclude. "You don't have to change tabulation of votes if you cast doubt upon the legitimacy of the process," said Christopher Deluzio, Pitt Cyber policy director.

Voter registration is a critical part of the state election architecture. Deleting or changing data in registration rolls could affect whether people are able to vote when they show up at their polling place.

The election security commission's recommendations included adding another layer of encryption and using multifactor identification to secure voter registration records. Accordingly, Pennsylvania's voter registration system was being overhauled in Harrisburg as June drew to a close, but it was uncertain what precautions would be taken to harden the system against attack, though the threat was clear.

The U.S. Senate Intelligence Committee warned that Russian intelligence directed an "unprecedented level of activity" against state election systems, largely to scout for vulnerabilities. The committee report noted, for example, that in Illinois, the hackers were found to be in position to delete or change voter data had they chosen to.

"If Russia is in full possession of the voter rolls in one state, it is quite possible that you turn up to vote and your name has been wiped from the rolls," Mr. Hickton said. "Now, you have a choice. Are you going to stand there until that's cleared up? Are you going to go to court for permission to cast a provisional ballot? Or, are you going to go back to work? Creating disruption, creating delay, creating lack of certainty of our elections is all Russia has to do."

The voter registration system is particularly important this year, when Pennsylvanians are for the first time able to

Noah Purdy

David Hickton, director of the Institute for Cyber Law, Policy and Security at the University of Pittsburgh, in his office at the institute, which is also known as Pitt Cyber.

"THERE ISN'T ANY BASIS FOR A CLAIM OF WIDESPREAD, INSTITUTIONAL ELECTION FRAUD."

David Hickton, director of the Institute for Cyber Law, Policy and Security

vote by mail if they don't want to do it in person. By May, nearly 1 million had applied for ballots. And as long as the registration rolls are tamper-proof, the risk of fraud is low, Mr. Hickton explained.

"Election fraud has been alleged repeatedly over many years," he said. "The hype around it is more extreme than the facts. Mail-in, in particular. There isn't any basis for a claim of widespread, institutional election fraud.

"There are rogue operators on both sides of the political aisle engaged in chicanery. But on a wholesale basis, the only election interference that can be demonstrated is by the Russians."

Mail-in ballots are expected to play a prominent role in elections held during the COVID-19 pandemic. The pandemic forced the rescheduling of the primary, and uncertainty over the trajectory of the outbreak prevents knowing what its impact will be on the November general election, when it could coincide with the seasonal flu.

Also, some of the commission's recommendations for tightening election security in Pennsylvania remain just that. One recommendation calls for conducting post-election audits considered the gold standard in ensuring accurate vote count, and which are now possible with the backup paper ballots from the new voting machines. Pennsylvania began pilot testing the auditing method last year, but state officials have not yet required the audits to be used in upcoming elections.

COVID-19 quickly exposed ambiguities in the state election code that leaves everyone guessing about who has the authority to declare an election emergency and postpone or suspend voting. In March, as virus cases escalated, Gov. Tom Wolf and the state general assembly negotiated a deal to move the primary to June.

"Crisis averted, in some respects," Mr. Deluzio said. "But legislators would be wise to codify emergency power, and the limits and contours of it."

Other contingency planning for responding to or recovering from an election crisis was still taking shape when the pandemic arrived. Much of the planning is confidential. Details are not publicly known. But there's a good chance it will be tested in coming months. h