D.C. hacking raises questions about future of online voting

November 1 2010, By Sean Greene

For the upcoming election, Washington, D.C., was preparing to allow some voters to send their ballots in over the Internet. It's a good thing election officials tested the system first.

Just two days after the District of Columbia Board of Elections and Ethics opened the application for the public to experiment with this fall, the system was hacked. Unbeknownst to D.C. officials, a team of computer scientists from the University of Michigan took control of the website and changed the code to make it play the school's fight song.

The fight-song gag was the part of the hacking that elections officials discovered themselves. More troubling is what they didn't notice.

That was revealed at a recent D.C. Council committee hearing, where J. Alex Halderman, a University of Michigan professor who led the hacking effort in order to demonstrate the system's security flaws, testified that his team had in fact wrested complete control over the elections board's server. Halderman produced 937 pages of names, addresses and PIN numbers of test voters who had signed up to try out the system. Had it been a real election, Halderman said, he could have changed the votes on ballots or revealed voters' supposedly secret choices on the Internet. Additionally, Halderman's crew wasn't the only one rooting around in the D.C. system. They noticed other attacks occurring, originating in China and Iran.

In response, the elections board decided to shelve the idea of having

voters submit ballots online. Eligible voters in the military and others living overseas can still use the system to receive blank ballots, rather than waiting for them in the mail. But they'll have to print the ballots out and mail them back to Washington.

While the D.C. episode was a setback for voting over the Internet, elections experts disagree on what it means for the future. Some say the District's experience demonstrates what computer scientists have been saying for years -- that the Internet in its current state cannot allow for secure online voting. Others, including D.C.'s top elections official, still see potential in online voting. In fact, the state of Arizona and eight counties in West Virginia aren't giving up plans to go ahead with their own online voting experiments on November 2.

The debate over online voting is not new. The U.S. Department of Defense conducted the first pilot project for the 2000 general election. Some 84 citizens used the Voting over the Internet system, the first time that binding votes were sent over the Internet for federal, state and local offices. Voting in the Democratic Party presidential primaries in Arizona in 2000 and in Michigan in 2004 was conducted online. But 2004 also was when concerns about the security of online voting crystallized and another Pentagon pilot project was scrapped.

At least one significant change has altered the landscape since then: Congressional passage of the Military and Overseas Voter Empowerment (MOVE) Act of 2009. Two elements of the federal law could lead to more experimentation with online voting. First, the law mandates that states send ballots to military and overseas voters at least 45 days before an election. Second, the law allows and encourages states to implement pilot programs that test new election technology.

States can safely use the Internet to reduce the time it takes to send ballots out. The question is whether voters can return those ballots online

without the risk of hackers tampering with the results.

Joe Hall, a researcher at the University of California-Berkeley, says it's almost impossible to guarantee that online voting could be done safely. "All an attacker has to find is one hole in a system to mount a serious attack," Hall says. Meanwhile, elections administrators "have to think of all such possible holes and try and plug them."

Still, Arizona used an online system for military and overseas voters in 2008 without any apparent incident and is planning to use it again this year. Likewise, West Virginia pilot-tested its new application in May, when 77 military and overseas voters used it to vote in a primary election. "We have confidence in our system," says Natalie Tennant, who as West Virginia's secretary of state is in charge of elections there.

In a report by Tennant's office which surveyed many of those who used the system, feedback was positive. After the November election, Tennant's office will assess whether to recommend expanding online voting in future elections. "As the wife of a Navy reservist," Tennant says, "I want those who are out in the far reaches of the world to be able to vote in a simple a manner as possible."

Since the D.C. site was hacked, much of the debate has hinged on the underlying technology of online voting. Washington used a system based on open-source software that allows developers anywhere to find mistakes and help fix them.

D.C. elections officials believe that using open-source -- rather than a vendor's proprietary product -- provides the sort of transparent approach necessary for elections, and can be made secure enough to use to transmit ballots. By contrast, West Virginia is using proprietary software that officials there believe to be more resistant to hackers.

Rokey Suleman, executive director of the D.C. board of elections, believes the hacking episode was not as big of a setback as some have made it out to be. In fact, he says it represents an opportunity to push the technology forward. "We are not disappointed that this occurred," Suleman says. "It is an opportunity for the computer science community to work with us."

Suleman says software development will continue over the next 15 months and that he hopes D.C.'s system will be ready to accept voted ballots online by the time of the 2012 presidential primary. "We will do some mock elections and more testing before that," Suleman says, noting that he hopes hackers like the ones at the University of Michigan will try to help make the system work rather than aim to demonstrate that it doesn't.

Some critics aren't convinced. The nonprofit groups Common Cause and Verified Voting used the D.C. council hearing on the hacking to say that states should be extremely cautious about moving toward online voting.

"There are many ways we can help military and overseas voters get their ballots and get them returned without entering this minefield," testified Susannah Goodman, director of Common Cause's national campaign for election reform.

But even some online voting skeptics, including Berkeley's Hall, say it's inevitable that states will want to continue experimenting in this area. The technology to try it is available now, and the desire -- not to mention the new legal requirement -- to serve the population of military and overseas voters is strong.

"I think many of us have started to realize that the momentum won't just go away," Hall says. "I'm starting to see a sentiment that we should do the research that's needed to make pieces of it as secure and trustworthy

as possible before it gets widespread adoption."