WESTCHESTER COUNTY BOARD OF LEGISLATORS

Voice of the People of Westchester County for over 300 years

MaryJane Shimsky

Legislator, 12th District

Majority Whip
Chair, Committee on Public Works

Committee Assignments:
Appointments
Environment, Health & Energy
Law & Major Contracts
Legislation
Parks, Planning & Economic Development
Public Safety
Seniors & Constituencies
Social Services

MEMORANDUM

TO: Benjamin Boykin, Chair, Board of Legislators
FROM: MaryJane Shimsky, Legislator – 12th District
DATE: August 6th, 2018
RE: *The Weekly Standard:* "Yes, The Midterms Will Be Hacked" by Alice B. Lloyd

Please add the attached *article* to the PW committee.

Tel: (914) 995-2821 • Fax: (914) 995-3884 • E-mail: Shimsky@westchesterlegislators.com

800 Michaelian Office Bldg., 148 Martine Avenue, White Plains, N.Y. 10601 • www.westchesterlegislators.com • 914.995.2800 (main voice)

It's only a question of how, when — and whether we'll notice.

Election meddling may not have been the foremost matter on the president's mind during his hours-long one-on-one with Vladimir Putin in Helsinki, where Putin publicly denied the findings of American intelligence and Trump didn't disagree. But Moscow's interference in our national parties, political campaigns, state election boards, and voter registration software have dominated discussions at state elections meetings and in Washington since 2016. After more than a dozen congressional hearings on the subject, a special DHS commission to monitor election security state-by-state, and one $380-million slice of the omnibus later, are our election systems ready to fight off foreign interference in the midterms?

The movement to replace every last highly hackable touch-screen voting machine with a less corruptible one that leaves a paper trail has new momentum, thanks to an influx of federal dollars and a loss of public faith in the integrity of our elections systems. "There's been an attitude shift," says Lawrence Norden, of NYU Law School's Brennan Center. But it's not enough to fix the problem that makes us vulnerable to the persistent threat of election tampering by Russia or perhaps other nefarious actors. National meetings of secretaries of state—like the one this weekend—and other elections directors' gatherings have all made "cyber hygiene" a topmost priority, Norden said, "Whereas, in the past a lot of people thought of the need for protection against these threats and the warnings about them as hypothetical and exaggerated."

Sometimes panic means progress, and there's plenty to panic about before the midterms. Last week, a 29-page indictment from Robert Mueller's investigation detailed a dozen Russian officers' elections hacking efforts. The 12th officer, the indictment reveals, infiltrated elections databases and gained access to software companies involved in the management of voter registrations. In Illinois, home of "vote early and vote often," Board of Elections officials piped up immediately to say those compromised voter registrations were theirs. Two state elections boards are known to have had their voter registration data infiltrated during the 2016 election. Arizona is the other confirmed victim, although experts contend that bad actors may well have combed through every state's registration database.

The DNC and Clinton campaign hacks get the blame for tipping the scales in 2016. But tactics like explicitly targeting vulnerable voting machines and online voter registrations could reward hackers with more discreet and dependable results—especially now that they've had years to get the hang of it. At least Congress is catching on. They haven't just held hearings. When the omnibus gave states $380 billion to upgrade to safer machines, "A lot of election officials were caught off guard—because they got so used to everyone saying Congress will never do anything."

Even so, it wasn't enough. Only Virginia has replaced its outdated machines, leaving 13 states still dependent on electronic, paperless voting machines. Pennsylvania's officials, for one, have said they want to improve their system but can't afford the upgrade to paper ballots this year, even with federal support. And the five states that still use paperless voting machines statewide—Georgia, South Carolina, Louisiana, Delaware, and New Jersey—have neither the time nor money they need to make anything like a full manual audit by November. Florida, famous for an older elections systems accountability scandal, went digital in the shadow of its disgrace but has since cut back on its paperless voting machines. Their plan is to have moved fully to paper balloting by next year.

Voting machines aren't half the problem, however. The databanks where states and counties store their registered voters' data are likelier targets insofar as that mysterious twelfth indicted official definitely knows how it's done. The post-Bush v. Gore Help America Vote Act required states to maintain voter registration databases, which often include online forms and public search functions. In Illinois's case, hackers climbed through these open windows. But, experts tell me, they made many more undisclosed attempts—not all of them unsuccessful.

The election tampering campaign broadly succeeded if its aim was to sow panic and distrust of the democratic process. Given the quirks of our decentralized elections system, hackers can precisely target high-stakes jurisdictions and—by deleting records, say—can simulate a critical but hardly inconceivable bureaucratic blunder: lost voter registrations.

And, now that they know the danger, what are states doing to protect their registered voters? Quite possibly less than they're doing about voting machines, Norden tells me. Unlike voting machines, which states can't hide, "Registration systems are kept secretly somewhere in state and county elections offices. A number of states have said that they're doing more to upgrade voter registrations systems." But we can't know exactly what—all we can do is hope states are prepared to reconstruct their registrations lists from saved and protected copies.

Altering or erasing registrations effects elections by forcing officials to turn away all-of-a-sudden unregistered would-be voters or by discouraging turnout among those who will look up their registration online only to find that it had, somehow, vanished. Elections officials ought to download their states' and counties' registration data at least daily between now and November, in case they need to rebuild the live database after a breach: The benefit here would be having an offline, uncorrupted copy against which to check the vulnerable live version.

And yet, when I asked the Illinois Board of Elections' spokesman whether the state had started doing a daily download of the its registration database in the wake the reported breach, he did not say. The spokesman, who announced Friday that the twelfth indicted officer was the same guy who'd gotten in Illinois's servers, referred me twice to official documents which make no mention of a daily download.

With midterms fast approaching, it's too late for a new policy to prevent infiltration. Over the next few months, officials have to prepare to detect an attack—and know what to do when they've found one. While we're worrying, our hackers are getting savvier. "2016 shows the first instance of their knowing whom to target," Norden noted. "With a year or two or three to plan your next attack, you can do a lot more damage." Even if they failed to alter our voter registration data, in other words, they learned our systems: While our states still lag behind in terms of tech, the enemy has had nothing but time to improve theirs.