WashingtonPost

The Daily 202: Bipartisan initiative to thwart election hacking gains steam

By James Hohmann September 14 at 7:01 AM

Russian President Vladimir Putin shakes hands with Lebanese Prime Minister Saad Hariri during a meeting yesterday in Sochi. (Michael Klimentyev/Sputnik/AFP/Getty Images)

With Breanne Deppisch and Joanie Greve

THE BIG IDEA: West Virginia Secretary of State Mac Warner's son was wounded by an improvised explosive device in Afghanistan and suffered traumatic brain injury.

When he finally made it home, the Republican asked his boy to tell him about his toughest day in combat.

"He had been wounded. There was a girl who had a leg blown off. They had to call in F-16s to secure their positions," Warner recalled in an interview. "I was expecting those kinds of war stories out of him. But he said, 'Dad, the hardest day for me, without a doubt, was election day in Afghanistan.' It was 110 degrees. Before they went out, they put tourniquets on each of their arms and legs so, if they got hit, they could still turn the tourniquets. They found five IEDs around the one polling place that his platoon was assigned to defend." But Afghans came out to vote any way, even at great personal risk to themselves.

Warner tells his son's story to stress how essential it is for Americans not to take our electoral process for granted and for leaders in both parties to do everything possible to block foreign governments like Russia from meddling in our elections.

He was one of four secretaries of state in Washington yesterday for an election security conference that was organized by the Belfer Center at Harvard's Kennedy School. These election officials, accompanied by their deputies, huddled with cybersecurity experts from Google and Facebook, as well as officials from the FBI, the Department of Homeland Security and the U.S. Election Assistance Commission.

"This is a new issue for us. We're having to respond to stuff we're still learning about," said Connecticut Secretary of State Denise Merrill (D). "The first question we all have is: What are we going to do for 2018 and 2020? We all know we have to do things differently."

She identified an inherent "culture clash" between cybersecurity experts, who are all about confidentiality and secrecy, and elections officers, who prize transparency and openness. "Bringing those two cultures together has been extremely interesting," said Merrill, who chairs a cybersecurity task force for the National Association of Secretaries of State. "We're trying to figure out how best to communicate. We're having to learn a whole new language. We're establishing relationships."

Henry and Lenora Elsesser go over a ballot before voting in Milwaukee last November. (Tom Lynn for The Washington Post)

Yesterday's event took place at Facebook's D.C. office. There were breakout sessions about protecting voter registration lists, recording election results and helping counties administer elections. A crisis communications expert gave a talk about the P.R. aspects of responding to a breach.

Elections are remarkably decentralized in the United States, which is both a strength and weakness of our system. Processes can vary dramatically from county to county.

The former director of information assurance at the National Security Agency, Debora Plunkett, is helping identify potential vectors of attack as elections officials teach her about the contact points in their systems. "These are seasoned professionals who know how to operate in the chaos of Election Day," said Plunkett, now a senior fellow at the Belfer Center.

The highlight of yesterday was a tabletop exercise that simulated a foreign attack on the integrity of an election. An Army major who is enrolled in a master's program at the Kennedy School took point in designing the scenario, with help from eight other students at Harvard and MIT. The six months of planning before an election were compressed into one hour. Then Election Day was compressed into a second hour.

Participants were forced to make hard choices, such as whether to switch from an electronic system to paper ballots. At one point, someone representing a county brought in an email that supposedly had come from the secretary of state. But the secretary hadn't sent the email. It was a test to see whether the group would recognize that their email system had been hacked. Then what do you do next? Call the other counties who might have received the same erroneous email and assumed it was genuine? Stop using email altogether?

Psychological operations were also integrated into the activity. The fictitious enemy disseminated false information, using bots to publicize long lines and sow confusion on social media. Participants needed to decide how to respond to that, as well as protests that grew out of decisions they had made earlier in the exercise.

The conference was closed to the press, but organizers invited me exclusively to attend the opening session and interview participants afterward about lessons they learned.

Then-Defense Secretary Ash Carter and his chief of staff Eric Rosenbach (right) leave Jordan for Iraq in 2015. (Carolyn Kaster/AP)

Eric Rosenbach, the co-director of the Belfer Center, was chief of staff to Defense Secretary Ashton B. Carter from 2015 to 2017. The retired Army intelligence officer spent the Obama years at the Pentagon, including as the assistant secretary who oversaw cyber-strategy. "The thing that bothered me more than all the things I saw in the seven years I was there was this past year was when the bad guys were going after our democracy and our election infrastructure," he said. "It really just bothered me to my core. … I'm not sure we responded as forcefully as we probably should have in retrospect, but you learn a lot when you're going through these things. … I wanted to do something about this from the outside."

Rosenbach said efforts like this are crucial to deter America's enemies. "I'm very worried about the perception that all the other bad guys around the world have after watching what the

Russians did to this election that they can do something similar," he explained. **"I can just see Kim Jong Un rubbing his grubby little hands and thinking, 'Well, you know what, we should go after the Americans too.'"**

During a welcome reception Tuesday evening at the WeWork office space on Capitol Hill, **Rosenbach briefed the 50 or so conference participants in broad strokes about the capabilities and objectives of the Russians, Chinese, Iranians and North Koreans.**

Finally, he warned about "the wild card" risk of "some crazy domestic group" trying to mess with an election. "It could be on either fringe of the spectrum," Rosenbach said. "In some ways, I worry more about that because they know the American system. They could go into a polling place, pose as someone who is a voter but meanwhile they're slipping in a thumb drive (and) they're getting in WiFi networks."

One big focus right now for everyone involved in the effort is getting security clearances for secretaries of state so that the people who administer elections can be more "read in" about the precise nature of foreign plots. Warner from West Virginia, who took office at the start of this year, expects that people are going to start getting full clearances in the next couple of weeks. A DHS undersecretary assured them that their applications are being expedited.

"Cybersecurity is now part of the job description," said Rhode Island Secretary of State Nellie Gorbea (D). "We need to do it in a way that people trust by being as transparent as we can. …. This is more than a one-time thing."

Robby Mook speaks to the traveling press corp aboard Hillary Clinton's campaign plane above Cedar Rapids, Iowa, last October. (Melina Mara/The Washington Post)

The co-chairs of the Belfer Center's "Defending Digital Democracy" initiative are Robby Mook, who was Hillary Clinton's campaign manager in 2016, and Matt Rhoades, who managed Mitt Romney's campaign in 2012. Both participated in the tabletop exercise.

There is, of course, consensus among intelligence professionals that Russia went after Clinton and the Democratic National Committee last year as part of an extensive effort to interfere in the election, but the Chinese also hacked Romney's campaign in the fall of

2011. That forced Rhoades to spend precious dollars to harden security systems that he couldn't devote to winning the primaries.

"We were concerned about how partisan this issue had become," said Mook, explaining how they decided to collaborate.

"There's tons of things we disagree on," added Rhoades, "but we 100 percent agree that American voters should decide our elections. No one else."

Both guys are now working on a "playbook" to share with campaigns at all levels about best practices for protecting data and training staff.

The Belfer Center is also working to produce a set of best practices for what local governments should do when a breach occurs. They're thinking about packaging yesterday's tabletop exercise in a way that could be disseminated to elections officials around the country, so that individual states can do it on their own.

"We're never going to get the threat of an attack on the election system down to zero percent, but you can mitigate the risk and think about how to react to it," Rosenbach said. "You have to rehearse these things over and over again."

Eugene Kaspersky, Russian programmer and CEO of Russia's Kaspersky Lab, poses at his company's headquarters in Moscow. (Pavel Golovkin/AP)

RUSSIAN CYBER-ESPIONAGE IS NO LAUGHING MATTER:

-- The U.S. government banned the use of Kaspersky security software in federal agencies on Wednesday. Officials said that at least half a dozen federal agencies run Kaspersky on their networks. Ellen Nakashima and Jack Gillum report: "Acting Homeland Security Secretary Elaine Duke ... ordered the scrub on the grounds that the company has connections to the Russian government and its software poses a security risk. 'The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security,' [the department said in a statement]."

-- A shuttered "Heart of Texas" Facebook group that had over 225,000 followers and organized anti-Clinton, anti-immigrant rallies across the state last year was found to have links to Russia. Business Insider's Natasha Bertrand reports: "In late October … the group transformed from a nativist, anti-Clinton meme machine to an organizing force when it created a Facebook event for a 'Texit statewide rally' titled 'Get ready to secede!' … The event called on Texans to protest 'establishment robbers' and 'higher taxes to feed undocumented aliens' in major [Texas] cities. It further claimed that a 'Killary Rotten Clinton' victory would lead to an influx of 'refugees, mosques, and terrorist attacks.' It is unclear how many people showed up to the protests. The group's efforts came on the heels of a similar Russian effort [reported this week]: an anti-Muslim protest in Twin Falls, Idaho, titled 'Citizens before refugees.'"

-- A salesman in Brazil said his family photos were stolen and used to concoct a fake Facebook profile that helped spread Russian propaganda during the U.S. election. He was made aware of the fake page only after a New York Times story featured it last week as an example of fake social media accounts that were used during the campaign, and he recounted being particularly disturbed by the theft "because he used the privacy settings on Facebook to limit access to his profile." (New York Times)

-- Special counsel Robert Mueller's investigation has a "red hot" focus on the Kremlin's effort to influence U.S. voters through Facebook and other social media sites. Bloomberg's Chris Strohm reports: "Mueller's team of prosecutors and FBI agents is zeroing in on how Russia spread fake and damaging information through social media and is seeking additional evidence from companies like Facebook and Twitter about what happened on their networks[.] … The ability of foreign nations to use social media to manipulate and influence elections and policy is increasingly seen as the soft underbelly of international espionage, another official said, because it doesn't involve the theft of state secrets and the U.S. doesn't have a ready defense to prevent such attacks."

House and Senate investigators are also likely to make social media sites a focus of their probes: Senate Intelligence Committee Chairman Richard Burr said Tuesday that it's "probably more of a question when" than if his panel will hold a hearing with Facebook officials. And Rep. Adam Schiff, the top Democrat on the House Intelligence Committee, said they have also "been in discussions with the technology companies," including Facebook.

-- Another front: "RT, Sputnik and Russia's New Theory of War," by Jim Rutenberg in this Sunday's New York Times Magazine: "How the Kremlin built one of the most powerful information weapons of the 21st century — and why it may be impossible to stop."