defenseone.com

Obama's Cyber Legacy

By Joseph Marks

He did (almost) everything right and it still turned out wrong.

The Obama administration made an unprecedented all-fronts effort to secure cyberspace. So, why are we less secure?

For eight years, cyberspace proved the Obama administration's most unpredictable adversary, always twisting in new directions and delivering body blows where least expected.

The administration took the cyber threat seriously from day one, launching reviews, promulgating policy, raising defenses and punishing cyberspace's most dangerous actors. That included imposing sanctions against Russia and North Korea and indicting government-linked hackers from China and Iran.

But, in the end, cyberspace won.

President Barack Obama will leave office this week following an election in which digital breaches ordered by Russian President Vladimir Putin helped undermine the losing candidate Hillary Clinton, sowed doubts about the winner Donald Trump's legitimacy and damaged faith in the nation's democratic institutions.

When the history of the Obama administration's cyber policy is written, that fact will likely loom larger than anything else, numerous cyber experts and former officials told Nextgov, overshadowing years of hard work to prepare the government and the nation for an age of digital insecurity. It will also likely overshadow the dozens of instances in which Obama officials got the big cyber questions, more or less, right.

“He set himself up with all the tools, but he blew this,” said Paul Rosenzweig, a deputy assistant secretary at the Department of Homeland Security during the Bush administration.

“Going into the final, they had a B-plus,” said Jason Healey, a three-decade cyber policy veteran who’s led cyber initiatives at the White House and in the financial sector. “Unfortunately, they blew it on the final.”

This assessment is unnerving for many top cyber watchers who credit the Obama administration with making substantial progress preparing the government, military, law enforcement and the private sector to operate in an emerging and incredibly complex domain.

“The Obama administration has done a good job laying out the traditional government markers of thoughtful policy consideration ... the fundamental building blocks of what makes the traditional American policy apparatus function,” Rosenzweig said. “They’ve invested intellectual capital and a lot of effort and time in them. On the negative side, despite these efforts, we aren’t actually any better off in terms of cybersecurity.”

Are We Better Off Than We Were Eight Years Ago?

That question—are we better off in cyberspace now than we were eight years ago—was a particularly troubling one for cyber experts consulted by Nextgov.

Their answer, by and large, was a qualified no.

“We’re better off in terms of policies and institutions to deal with cybersecurity, but worse off with regard to the threat landscape and the actual security environment,” said Tim Maurer, co-lead of the Cyber Policy Initiative at the Carnegie Endowment for International Peace.

“There’ve been improvements on protecting us from attacks on critical infrastructure,” said Adam Segal, director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations. “I think those are much less likely than before. But, overall, the progress has not kept up with the pace of the threat.”

Even Michael Daniel, the president’s cybersecurity coordinator, whom many experts credited with shepherding major advances during four-and-a-half years in the post, was not entirely sanguine.

"I think we're clearly more capable and I think in many ways, we're more aware and we are safer in many ways," Daniel told Nextgov. "But our vulnerability has continued to expand as well ...The landscape is more serious and more dangerous."

The Good

There's a lot to place on the positive side of the Obama administration's cybersecurity ledger.

On the top of most former officials' lists is a September 2015 agreement between Obama and Chinese President Xi Jinping to halt purely commercial hacking.

Prior to that agreement, former National Security Agency Director Gen. Keith Alexander described Chinese cyber theft of U.S. companies' trade secrets and intellectual property as "the greatest transfer of wealth in history." FBI Director James Comey declared there are "two kinds of big companies in the United States ... those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."

Within months after the agreement, Chinese corporate hacking dropped precipitously, according to U.S. intelligence agencies and private-sector cybersecurity firms. The cyber firm FireEye, which was conducting an average of 35 investigations of Chinese cyber espionage per month for different corporate clients in the years prior to the agreement, is now conducting about 10 such investigations per month, FireEye Chief Technology Officer Grady Summers told Nextgov recently.

That's just the top of a long list of accomplishments.

DHS built and continually upgraded its Einstein cyber threat detection and prevention system, which now protects more than 90 percent of federal agencies.

The White House issued directives establishing internal government cybersecurity policies and procedures for responding to cyber incidents and attacks.

The National Institute of Standards and Technology established a cybersecurity best practices framework widely adopted by the private sector.

The Defense Department stood up an independent U.S. Cyber Command, with offensive and defensive capabilities, which reached its initial operating stage in October staffed with more than 6,000 cyber warriors.

The State Department worked with dozens of other nations to establish peacetime norms in cyberspace and to work out how international law applies there.

And the Treasury Department developed a set of cyber-specific sanctions the White House used to punish Russian hackers in December.

The Bad and the Ugly

There were also bad moments, however, that went beyond Putin’s election meddling.

There were breaches of email systems at the White House, State Department and Joint Chiefs of Staff, reportedly committed by Russian government-linked hackers. Hackers reportedly linked to the Chinese government stole sensitive security clearance documents on more than 20 million current and former federal employees and their families from the Office of Personnel Management.

There were also private-sector breaches, led by North Korea’s destructive cyberattack against Sony Pictures Entertainment, but also including major data breaches at Target, J.P. Morgan, Yahoo and the denial-of-service attack against the internet optimization firm Dyn, which knocked websites including Netflix and The New York Times offline for hours.

Disclosures by NSA leaker Edward Snowden fundamentally damaged attempts to cooperate with Silicon Valley on cybersecurity. It also pushed adversaries and some allies toward a narrow and insular view of managing the internet that has made cooperation on cybersecurity significantly more complicated.

Cyber crime against consumers and the private sector did not significantly ebb during the past eight years. Despite a “cyber sprint” to shore up federal networks in the wake of the OPM breach, the government still relies inordinately on outdated technology. And decades-old inefficiencies in government technology acquisition and hiring have not been substantially repaired.

Most importantly, cyber watchers, say the government never successfully managed to establish a broad policy to deter cyberattackers. If anything, as the Russian election meddling suggests, attackers only grew bolder.

“They didn’t get out of the reactive side to the proactive side,” said Bruce McConnell, a former deputy undersecretary for cybersecurity at DHS who now leads the EastWest Institute.

“As many good things as I do think the administration implemented, there are some really bad events that happened and the reality is there have been no game changers in terms of making everything more secure,” said Jacob Olcott, a former counsel to the House Homeland Security Committee who’s now a vice president at the cybersecurity risk consultant BitSight.

“You can be the best performer but if you have a bad day, you’re going to get dinged bad,” Olcott said.

A Complicated Landscape

The Obama administration’s cybersecurity efforts were hampered by a few fundamental facts.

To begin with, unlike combat in air or at sea, the internet as a domain of conflict is controlled largely by the private sector. The government’s ability to enforce security measures is limited, especially outside industries such as energy, electricity and transportation DHS has labeled critical infrastructure.

Cyberspace is also best viewed as a domain of conflict rather than an issue unto itself like health care or homelessness. As a result, experts say, it makes more sense to view the administration’s failure to halt or counteract Russia’s election meddling as part of a broader failure to contain Russian aggression in Crimea and elsewhere rather than as a purely cyber failure.

Finally, the target is continually shifting.

The greatest fear during the first part of the Obama administration, expressed by intelligence officials and congressional leaders, was a destructive cyberattack against critical infrastructure that caused major loss of life and destruction of property. That never happened and, if it had, the breaches and influence operations that did occur might pale by comparison.

Moving Faster Than the Threat

If there is one fundamental reason for the Obama administration’s inability to claim victory over cybersecurity, experts and former officials tell Nextgov, it is this: The threat grew and mutated faster than the administration’s ability to deal with it.

“Government moves at 60 miles per hour and internet innovation moves at 6,000 miles per hour,” former DHS official Paul Rosenzweig said. “Hackers are ahead of defenders, defenders are ahead of legislators and legislators are ahead of regulators.”

If the Trump administration or future administrations are going to get ahead of that threat, it will require a fundamental rethinking of how cyberspace is secured.

That may mean requiring some critical infrastructure sectors to share more information with government regulators about their cyber protections and cyber hygiene, former DHS official Bruce McConnell said.

It will certainly require making officials, including cabinet secretaries, ultimately accountable for the cybersecurity of their departments, Olcott said, and investing heavily in top-grade technology and a more efficient government acquisition system.

Perhaps most importantly, it will require developing a more encompassing cyber policy than the Obama administration was able to manage, one that specifies where the government will stand when there are tradeoffs between privacy, security and relationships with other nations and with the private sector, said Jason Healey, now a senior research scholar at Columbia University.

“We don’t have a couple decades to work through these things,” the Carnegie Endowment’s Tim Maurer said. “We need to accelerate at a speed that conventional government activity has a hard time keeping up with.”

D