SWCP Portal
October 2018

This year, the real fright night comes a week after Halloween

2018 Election Tricks or Treats

This year, plenty of scary images have already filled our screens. They are not monsters but political candidates, though with the negative advertising, accusations, and photoshopping, it may be hard to tell.

But politicians are not the most frightening things looming over this Halloween season. That arrives a week later with the midterm elections when the *real* tricks or treats take place. And it looks like tricks played on the electorate may be more likely than the treat of a fair, peaceful, and uncontested vote.

Already, unprecedented anxiety hangs over the very electoral process. For the first time ever in the history of our democratic republic stands the question of widespread tampering by our enemies – again. Whatever the official outcome, fear and suspicion of election fraud could taint American politics for years.

These are very serious issues which should be of concern to all citizens. Therefore this issue of the *Portal* will take a look at what the stakes are, how the election could be rigged, what's being done to prevent it, and just what could happen this **November 6.**

Leaderless fumbling in the dark

In spite of **wide-spread acknowledgement** by our intelligence agencies that Russia has tampered with our elections, President Trump does not seem to believe in Russian interference. Unfortunately, this denial has resulted in a lack of coordinated, decisive federal policies to safeguard the democratic process.

As a result, both federal agencies and the individual states have been fumbling around trying to do the best they can. The tech giants and social media have also been left largely to their own devices and have been very reluctant to do anything at all.

Introduced a year ago, the **Honest Ads act**, which would do the bare minimum of including disclaimers in political net ads like those in TV ads, has still not been passed. Facebook has quietly **fought against** it, though it **finally accepted** the necessity of regulation. Google opposes it, too, but says nothing.

In fact, Google does not seem to have done anything to deter fakers beyond a cursory "don't". It's up to **Gmail users** to report fake accounts linked to their own. The company seems to only care about fake Google+ accounts that **impersonate** real users. In fact, the search engine even helpfully lists a slew of pages on how to set up fake Google accounts!

But Microsoft **shut down** *84* phishing websites used by Russian hackers that imitated sites like the US Senate's, while Twitter **eliminated** *70 million* fake or suspicious accounts in just two months.

Facebook also reluctantly tried to clean up its site after the last election by removing a staggering *1 billion* **fake accounts** over a 6-month period, *270* of which were used by the prime Russian hacking front. But this summer, they found **evidence** of new Russian and Iranian fake accounts and deleted *652*.

Even though Facebook has supposedly built up a team of *20,000* humans as well as AI to investigate fake accounts, it is so overwhelmed that it **asked for help** from journalists, governments, and other tech firms. But Alex Stamos, a former Facebook executive who urged them to open up about what really happened in 2016, claims that it's **already too late** to save the 2018 election due to US inaction.

"If the United States continues down this path, it risks allowing its elections to become the World Cup of information warfare," he direly predicts. Indeed, the Russians (and others) have redoubled their efforts helped by new tools. FancyBear, Russia's prime military hacking unit, has developed **new malware** that's nearly impossible to detect or eradicate that can even survive a complete wipe of the hard drive.

Despite all the account deletions and attempts to rein in propaganda, the depth of partisan rancor these days shows that the pots set bubbling by foreign players before 2016 are still furiously boiling.

With all the nasty claims and counter-claims out there, it's not easy to find true, unbiased information. The **League of Women Voters** have long provided solid, non-partisan candidate info and details on how

and where to vote with their PDF **Voting Guide**. To separate fact from fake, there is **FactCheck.org**, which works with Facebook, collects articles from all across the country, while **Ballotpedia** has a more analytical approach. Political fact-checking can be found at **NPR**, and there's always **Snopes.com**.

The vulnerability of electronic voting

It's basically been left to state and local governments to secure the vote. A federal plan wouldn't be simple in any case, as each state mandates its own method of voting and tallying the results, and there can be variations down to the precinct level.

This may prove to be an unexpected advantage, as the variety complicates things for attackers. But one of the lessons of 2016 is that it is not necessary to attack the whole system. Changing in the vote in a few crititcal swing districts is all that's needed, which is why hacking the Democrat's political database was so necessary to the Russian scheme.

The states may be without direction, but not entirely without resources. *$380 million* was **distributed** to the states to shore up elections, divided up by the number of voters. Those funds were used largely to upgrade and secure old systems, yet the Republicans in August **blocked an attempt** to give the states *$250 million* more to finish the job.

Paper ballots have been widely proposed as the best solution. They do create a trail which can authenticate the number of votes but let's not forget the nightmare of **"hanging chads"** in contested districts in Florida during the 2000 presidential election. This caused the switch to electronic voting machines in the first place, costing *two billion dollars*.

Yet little was ever invested on upgrading and patching them during following election cycles. Thus, these **aging machines** jeapardize electoral integrity. Failures in 2012 led to long lines and frustrated voters. In New Mexico, where 1 in 3 went bad, the entire state went back to paper ballots.

But unless the country goes completely "old school" with hand-counts and results sent by courier, the outcome is still at risk because votes are tabulated and communicated electronically. We have traded **security for convenience** and quick results.

At the **DefCon hacker's convention** this year, they found that voting machines are still incredibly vulnerable with many well-known weaknesses that should have been fixed over a decade ago. Ballot counters were also easily hacked to change votes.

Even worse, the poor security on the official websites that display results makes hacking them **literally child's play**, as a number of kids at DefCon easily demonstrated on mock duplicate sites.

Most critically of all, the states' voter registration databases are still vulnerable. The possibility that the actual votes could have been altered was vigorously denied after the last election, but officials were really not that sure. Hackers did penetrate several states' critical systems and the difference in votes and exit polls might indicate that **votes were changed**.

The darkest possibilities

The entire system is not much less susceptible than it was in 2016. Yet it might not take any more interference to achieve the outcome our adversaries want. Putin, it is widely believed, mainly wanted to weaken the US by sowing discord and confusion. By that measure, he's been wildly successful. Yet if our foes can do more, they just might not resist temptation.

President Obama has been widely criticized for not having spoken out more to secure the last election. Excuses given include not wanting to appear partisan in such a heated contest, and the **opposition of the Republicans** in Congress to public statements.

He did warn Putin privately at a summit to stop. But it appears that the president was not much more forceful might be due to **fears** that the Russians had already penetrated our electric power grid.

Two days before Christmas in 2015, the **Russians attacked** the Ukrainian grid – which uses US-based technology with the same weaknesses – shutting it down for *six hours*. Ironically, they did this with an adaptation of the **Stuxnet virus**, created by the NSA and the Israelis to attack Iranian nuclear centrifuges.

The genie now being out of the bottle, this summer it was **revealed** that the Russians have hacked into hundreds of utilities' control rooms. In theory, they can take over the power grid by remote control. One ominous sign is that they have apparently put much more work into those efforts than into penetrating political organizations or voter registration sites.

Officials are as concerned about motivation as how such ability might be used. Our foes could disrupt voting in key precincts or darken the entire nation. Yet the administration has done little more than maintain old coal-fired plants "just in case".

Probably the best advice anyone can give is to vote early, stock up on supplies, and stay under your bed. Might not be a bad idea to save some Halloween candy for comfort, too, in case it's tricks, not treats.

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**
Click on blue terms in PDF file to open links.