SWCP Portal
October 2016

Every vote counts, but can they be trusted?

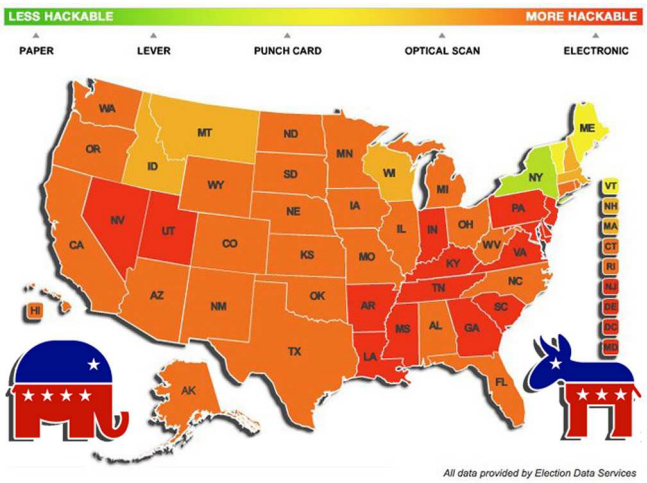
Hacking the US Elections

Many believe that the presidential election of 2016 will be one of the most significant in our history. Rarely have candidates been so lionized or so loathed, and the issues facing our nation are indeed profound. Yet so far, this year has been a political circus unlike anything ever seen.

So just how safe and reliable is the electoral procedure in these divisive times? While voting frauds and gaming the system have always threatened to undermine the democratic process, the recent involvement of the internet opens a new range of potential **vulnerabilities**.

Many of these are just electronic versions of old dirty tricks using phones or mail. But now there's also the threat of hacking electoral software. Yet **social media sites**, ranging from Google, Facebook, and Instagram to Uber, are undettered, urging all potential voters to register ASAP.

New Mexicans can conveniently **register online**, by mail, or in person before **October 11**, which is when early voting is scheduled to start. Absentee ballots can be applied for up to November 4. On Election Day, Tuesday, **November 8**, polls will be open from 7:00 AM-7:00 PM, and employers are required to give staff up to 2 hours off to allow them to perform their civic duty.



Ghosts of Watergate

Dirty tricks have already been used which older readers may find reminiscent of **Watergate**. Back in March, **Wikileaks** launched an **archive** of over *30,000* emails from Hillary Clinton's private server. While clearly intended to damage her, these were obtained from the State Department through the Freedom of Information Act. But they also **published** emails somehow leaked from the Democratic National Committee.

Coming just before their nominating convention, this caused the fall of several **party officials**. Plus it further stirred animosity between the Clinton and Sanders camps. **Oliver Stone**, noted conspiracy theorist, bizarrely claimed it was an "inside job" by the Democrats, while Wikileaks **hinted darkly** that a party staffer had been murdered because of them, even offering a reward that offended the victim's family.

But American intelligence agencies **blamed** the hack on **Russia**, claiming it was much larger than originally known, and the FBI began investigating. While Vladimir Putin applauded the hack as a "public service," he **denied** involvement. It certainly didn't help things when Trump also **denied** Russian complicity even in the first debate, any more than when he actually **suggested** they go after Clinton's emails.

Even more troubling are **reports** of state voter databases being penetrated. Arizona and Illinois were the first ones detected, then **ten**, and now an **unspecified** number of further penetrations.

Voters' data was not tampered with, but the concern is that voter registrations could be deleted, or false information sent to voters. But, there is a limit to how much damage a hacker could do, thanks less to online defenses than to the barely-organized chaos of our electoral process.

Soviet dictator Joseph Stalin famously said, "It is enough that the people know there was an election. The people who cast the votes decide noth-

ing. The people who count the votes decide everything." Luckily for the US, our system is so **decentralized** that it would be next to impossible to rig the people's choice in that manner.

States run their own systems with over *9,000* polling places. While there are some that are vastly insecure, there is no **single point** of vulnerabilty to attack. The entire operation *cannot* be rigged with one crucial hack, which makes it far more difficult to fix an election.

In theory, voting machines could be hacked to change what names are displayed or even miscount the votes. Experts discount that possibility, as it would be hard to do undetected. Yet **many jurisdictions** are still using machines made in the last century. While paper ballots cannot be hacked, the same cannot be said of old, obsolete electronics. Some have unsealable USB ports where any voter could stick in a thumb drive with malware and not be caught.

Only five states are currently completely paperless, nine others have some jurisdictions that are. (New Mexico is not one of these.) States are already on the lookout for flaws, and unprecedented **warnings** have been issued by the FBI.

The Department of Homeland Security is even considering **declaring** the national election a "critical infrastructure" like power plants or Wall Street, allowing it to take over security. In any case, it will have a cyberteam on standby.

From Russia with malware

Intelligence and law enforcement are investigating whether Russia is trying to covertly influence the election. FBI Director James Comey **said** they were looking "very, very hard" at whether the Russians or their minions are trying to disrupt the election. But since much of the evidence is "highly confidential," neither he nor his counterparts in the CIA or NSA will discuss it.

Officials **state** that the Kremlin might not be trying to sway the election but to discredit it, providing fodder to attack US attempts at building democracy around the world, particularly in former republics of the Soviet Union. While there is no "definitive proof" of this, the hacker responsible for the DNC hack, "Guccifer 2.0" is closely **associated** with and protected by Russian state-supported hacking groups , despite denials.

Meanwhile, top members of Congress have **accused** Russia, and called on Putin to stop it, as such activities could only happen with orders from "very senior levels" of the Kremlin. **Claims** that the Republican National Committee was hacked, too, were withdrawn as there is no evidence that they were. Trump continues to **equivocate** on the Russians', and his links with Putin have aroused disturbing **questions**.

Any candidate **believed** favored by foreign parties is likely doomed to lose. But of course, foreigners are not the only ones who may try to tamper with the presidential election.

Domestic terrorists

There are plenty of people right here at home who might want to **wreck** the election. In a contest where Google has been accused of **skewing search results** to ruin one candidate, paranoia and partisanship are already at fever-pitch.

Recently a **denial of service** attack hit *Newsweek* after publishing an article about Trump's illegal dealings with the Cuban regime. Things could turn really ugly in the month until the election.

The hacker activists known as **Anonymous** have laid low so far, only issuing **dire warnings** of one party interfering with results. However, there is **reason to worry** that they could try some dirty tricks themselves in any number of ways.

If either side cries "fraud," the election results could be **contested**. Remember the nightmare of the 2000 election where it came down to a few **hanging chads** in Florida? This one could be even more disputed, chaotic, and prolonged.

Domain Changes Coming

ICANN, the **global internet name and address authority**, is changing the process to update domain name contact records. The changes take effect later this year, and we will cover this in more depth in next month's *Portal*. Stay tuned!