New American

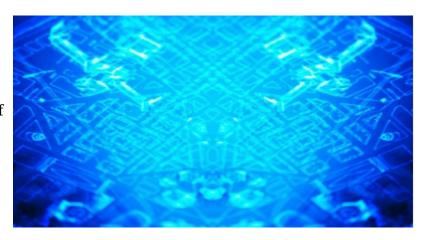Written by **Kurt Hyde** on April 27, 2017

NASS Report: Russians Did Not Cyberattack 2016 Elections

Hillary Clinton's allegations that Russian hackers attempted to help President Trump's campaign were dealt another in a series of setbacks based on facts when NASS (National Association of Secretaries of State) issued a report on the matter last month. The report, entitled "Briefing: Key Facts and Findings on Cybersecurity and Foreign Targeting of the 2016 Elections," was based on unclassified documentation and evidence available to NASS.

The NASS report summarized its findings: "The November 2016 election was NOT HACKED." (Emphasis in original.) It added: "No credible evidence of hacking, including attempted hacking of voting machines or vote counting, was ever presented or discovered in any state, including during recount efforts that took place after the election." The report addressed concerns about hackers who did manage to access online voter registration databases saying, "No voter registration data was modified or deleted" and, "Claims that twenty or more states experienced Russian-led hacks or intrusions into their election systems are false and inaccurate."

The NASS report cited the states' "highly-decentralized, low-connectivity elections process" as a safeguard from large-scale cyberattacks. Hopefully, this sensible, forthright statement by this association, most of whose members are state-level chiefs of elections, will lead to an end of advocacy for Internet voting and other forms of paperless electronic voting.

Readers of *The New American* were warned of the dangers of Internet voting in the October 9, 2000 issue of the print magazine. The article entitled "Voting on the Web" warned of numerous dangers inherent in the Internet technology that could become electoral security weaknesses if Internet technology becomes a vital link in the voting process. That TNA article also reported on attempted cyberattacks during Internet voting's coming-out party in the 2000 Democratic primary in Arizona:

> In an interview with *The New American*, Joseph Mohen, CEO of election.com, admitted that the Arizona Democratic primary was e-attacked. There were two kinds of attacks — denial of service and password-guessing — all of which were successfully thwarted. Nevertheless, the fact that this first-ever, true Internet election was subject to such sabotage attempts shows the profound weaknesses of Internet voting. Attacks on future Internet elections may be prosecuted more successfully.

The NASS report focused only on cyberattacks and did not address other forms of election fraud, such as illegal voting by non-citizens, manipulating the programming of electronic voting equipment via tampering, or centralized election management for setting up of the machines or manipulating the totals after the election.

How Many Illegal Ballots Were Cast by Non-Citizens?

Regarding illegal voting by non-citizens and other forms of illegal voting, such as repeater voting in person or absentee ballots, there has been surprisingly little activity by Republican Party organizations. This is despite President Trump's publicly voiced concerns and is in stark contrast to 1960 when there were credible doubts about the election of President Kennedy and Vice-President Lyndon Johnson. Then Republican National Chairman Thruston Morton issued a call to GOP organizations and concerned citizens to help gather evidence. The *Dallas Morning News* reported on November 18, 1960:

> Morton sent out a call last Friday to GOP organizations in 11 states to seek ballot recounts or investigations to determine whether there were voting frauds or irregularities in their areas.

The New American contacted the Republican National Committee asking if they intend to do anything similar to what the RNC did in 1960 to help gather evidence of potential vote fraud. As of press time, the RNC has not responded to that information request.

With or without help from the RNC and state elections departments, election integrity groups such as True The Vote and Judicial Watch are looking into how many non-citizens illegally voted in the 2016 election. True the Vote founder Catherine Engelbrecht told *The New American*:

> Currently we are aggregating all 2016 state voter registry data and sending over 3,000 FOIA requests to create a master data set that can be used to verify identity, residency, and citizenship status of registered voters. But it is slow-going. Data is still coming in. We are still asking questions and anticipate many additional rounds of FOIAs will be required.

Engelbrecht added:

> Indiana just purged nearly 500,000 voter registrations from their rolls. The story behind the story is that in 2012 True the Vote and Judicial Watch worked together to sue Indiana and Ohio for not keeping their voter rolls clean. These were multi-year courtroom battles that we settled in two historic consent decrees in both states — but it took suing them to get them to do their jobs. What won those cases was our ability to use True the Vote's past research to prove that citizens were having to do the job of government. It caused Indiana to cancel the registrations of a stunning 10% of its voter rolls. Consider the implications if 10% of our nation's voter rolls are inaccurate.

Learning how many illegal ballots were cast in November looks like it will be a long battle and the mainstream media is all but ignoring this aspect of the 2016 presidential elections.

Was There Tampering With the Electronic Ballots?

Regarding tampering or manipulating of the electronic voting equipment during set-up, fortunately there are quite a few jurisdictions in this country where the electronic voting equipment has a paper trail, and some partial recounts were accomplished in Michigan and Wisconsin with no significant differences between the electronic totals and the recounts of the paper ballots.

University of Michigan Professor J. Alex Halderman and graduate student Matt Bernard were quick to point out in their presentation *Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election* that finding no evidence of hacking is not the same as finding evidence of no hacking. For example, when attempting recounts on paperless voting systems, there was no evidence one way or the other. The researchers also mentioned severe obstacles to obtaining permission for recounts, such as in Pennsylvania. Professor Halderman also mentioned his concerns because of the relatively small number of people who accomplish the software set-ups of the electronic voting equipment for each election. Having such a small cadre of people accomplishing this key function increases the risk of a central point

of attack for manipulation, especially for equipment that doesn't have a paper trail.

Halderman also voiced his dismay with how infrequently the paper trails are actually used for some form of audits of elections even though the voter-verified paper trails are available. Not taking advantage of the paper trail when one is available to verify vote totals increases the risk of election fraud because it significantly decreases the risk of detection.

Was There Tampering With the Totals?

This past fall, on Alex Jones' Infowars program, Bev Harris, founder of Black Box Voting, and computer professional Bennie Smith publicly unveiled a computer application named Fraction Magic. Fraction Magic can read actual election results and alter the vote totals and subtotals all the way down to the precinct level to fit a desired outcome and do so with believable numbers. Harris reported testing Fraction Magic on Alaska's election results from the 2004 general election, and she was able to produce the altered results in four seconds.

Fraction Magic proves that it is technologically possible for people with inside access to election results to alter the results quickly and silently. The safeguard against this form of electoral fraud is public access during vote counts and immediate public disclosure of precinct election results. Practices such as this were the rule in traditional American elections.

The good news is that many precinct vote totals are still being released to the public immediately after the results are known. The bad news is that public access to witness the vote counting has been greatly reduced, and there appears to be a silent movement to stop the practice of making precinct results public immediately. As far as the 2016 election results are concerned, it is highly unlikely that manipulation of election results made any difference, but if we don't reverse the current movements of not allowing public access to vote counts and the stopping of immediate public disclosure of election results, it will become feasible for a small group of insiders to quickly and silently alter election results in a manner similar to those used by Hitler and Stalin in their sham elections.

For learning more about fraudulently manipulating vote totals, see TNA online article "American Elections Are Vulnerable to Wholesale Vote Fraud."

While it is highly unlikely that Russian hackers cyberattacked the 2016, this is no thanks to the liberal elements who have been advocating Internet voting and other forms of electronic voting sans paper trail. And it will be a long time before the volunteer groups that are looking into the possibilities of illegal voting by non-citizens will learn how many of such ballots were cast in the 2016 general election even though this is a task that should have already been done by the government agencies that conduct our elections.

Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful
perspectives within the pages of "The New American" magazine. Delve into a
world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture,
and technology, we bring you an unparalleled array of topics that matter most.

What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.

Subscribe