Written by **C. Mitchell Shaw** on June 8, 2017

National Association of Secretaries of State: "Election Was Not Hacked"

Since the revelation of a highly classified NSA report Monday asserting that Russian intelligence agents targeted voting machines and the computer systems of election officials, the received wisdom seems to be that the election was hacked. The facts, however, stand in direct opposition to that received wisdom.

The Intercept's report on the leaked NSA document included excerpts and quotes from the document. The sum of those excerpts and quotes is that Russian state-sponsored hackers launched a cyber-attack on at least one U.S. voting software company and sent spear-phishing e-mails to more than 100 election officials ahead of the 2016 presidential election.

While this NSA report was leaked and not officially released, it is similar to other reports the intelligence community released late last year and early this year. One similarity is that what the report does say is less telling than what it does *not* say. An example of that can be seen in *The Intercept's* article:

> The NSA analysis does not draw conclusions about whether the interference had any effect on the election's outcome and concedes that much remains unknown about the extent of the hackers' accomplishments. However, the report raises the possibility that Russian hacking may have breached at least some elements of the voting system, with disconcertingly uncertain results.

So, without actually *claiming* that Russian hackers swayed the election, the NSA document leaves the reader with the *impression* that that's what happened. But that impression is wrong, according to the National Association of Secretaries of State (NASS). And since NASS represents the people responsible for securing and maintaining the election systems — including voting machines — they are in a much better position to know whether those systems were hacked.

In March, NASS released a briefing entitled "Key Facts and Findings on Cybersecurity and Foreign Targeting of the 2016 U.S. Elections." The briefing, based on "all unclassified documentation and evidence available to the National Association of Secretaries of State (NASS)," lists five points. The first point — under the subheading, "The November 2016 election was NOT HACKED" — says:

> The voting process was not hacked or subject to manipulation in any way. 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. A joint DHS-DNI report details the foreign cyberattacks that took place against U.S. government, political and private sector entities that were attributed to Russia. Election officials remain concerned by

> unfounded conjecture that a lack of such tangible evidence indicates that hacking might have been overlooked or hidden from discovery, despite collaborative efforts with our intelligence services, cybersecurity firms, network defenders and state and local officials.

Since the NSA report doesn't really add anything new, it also does not seem to have changed NASS's opinion on the issue. A statement by NASS on Wednesday said, "The NSA report is concerning. However, we have yet to see any evidence that would call into question the outcome of the 2016 elections in any state or locality." Rather than retract its previous statement in light of the leaked NSA document, NASS linked that briefing at the bottom of its most recent statement.

As the NASS briefing points out, "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." Furthermore the idea that "a lack of such tangible evidence indicates that hacking might have been overlooked or hidden from discovery, despite collaborative efforts with our intelligence services, cybersecurity firms, network defenders and state and local officials" is merely "unfounded conjecture."

The briefing goes on to assert that "Russian intrusions into state and local election boards in 2016 were limited to TWO INCIDENTS that did not involve systems used in vote tallying." (Emphasis in original.) And while the FBI found that in both of those cases — in Arizona and Illinois — "foreign-based hackers attempted to mine data from voter registration systems," in the final analysis, "no voter registration data was modified or deleted."

The briefing also says, "Additional state voter registration systems were targeted by cyber hackers, but NO ADDITIONAL SYSTEMS were accessed or breached." (Emphasis in original.) Laying waste to one of the liberal mainstream media's favorite claims, the briefing says, "Claims that twenty or more states experienced Russian-led hacks or intrusions into their election systems are false and inaccurate," since "targeting does not equate to gaining access or actual breaches."

Since Internet connectivity is a major concern where hacking is a possibility, the briefing points out that the "highly-decentralized, low-connectivity elections process" used in the United States "provides BUILT-IN SAFEGUARDS against large-scale cyberattacks." (Emphasis in original.) As the briefing explains, "Our national intelligence agencies concurred with secretaries of state in concluding that our diverse and locally–run election process presents serious obstacles to carrying out large-scale cyberattacks to disrupt elections, and that standalone, disconnected voting systems present a low risk." This point should put to rest two phantoms that occasionally raise their heads: Internet voting and nationalized, centralized elections. Since the lowest risk among voting machines is "standalone, disconnected voting systems" and the decentralization of the voting process makes it a harder target, Americans should firmly refuse both Internet voting and the idea of federal centralization of the voting process.

Perhaps one of the most important points of the NASS briefing touches the fringe of that last issue. The briefing states, "Just OVER HALF of all states took advantage of voluntary cybersecurity assistance provided by the U.S. Department of Homeland Security" and explains that "33 states and 36 county jurisdictions had taken advantage of [DHS's] voluntary assistance and services by Election Day on November 8, 2016." (Emphasis in original.) DHS involvement in helping secure the election process may be fine and well as long as it truly is "voluntary" for the states. Unfortunately, that is not always the case.

In December, Georgia Secretary of State Brian Kemp — who had declined the DHS's offer of assistance — sent a letter to DHS to ask "why [it] was attempting to breach" the firewall protecting his computer infrastructure. As Kemp reminded DHS in his letter:

> Georgia was one of the only few states that did not seek DHS assistance with cyber hygiene scans or penetration testing before this year's election. We declined this assistance due to having already implemented the security measures suggested by DHS.

It appears that — in keeping with its heavy-handed approach in general — DHS was unwilling to take no for an answer. On November 15 — days *after* the election — "an IP address associated with the Department of Homeland Security made an unsuccessful attempt to penetrate the Georgia Secretary of State's firewall," according to Kemp's letter. Kemp also reminded DHS of the fact that its attempted penetration of the firewall was both unwanted and unsuccessful:

> At no time has my office agreed to or permitted DHS to conduct penetration testing or security scans of our network. Moreover, your Department has not contacted my office since this unsuccessful incident to alert us of any security event that would require testing or scanning of our network. This is especially odd and concerning since I serve on the Election Cyber Security Working Group that your office created.

On December 13, Kemp followed up on his letter to DHS by writing to President-elect Trump to ask him to investigate the matter. In that letter, he revealed that the attack on November 15 was not a one-off. In fact, in his letter, Kemp wrote that there have been at least 10 such attempts in as many months and that "these scans correspond to key election dates and times when I was speaking out against DHS' plans." This would not be the first time a department of the federal government targeted someone for political reasons.

So while there is still no real evidence that Russia hacked the election (or, for that matter, even attempted to do so), there is ample evidence that DHS has attempted to hack the systems of at least one state. It seems that while the Deep State would have Americans focus their concerns on foreign hacking of elections, the Deep State itself poses at least as much danger to that process.