How NIST has Misled Congress and the American People about Internet Voting Insecurity; or, Internet Voting in the USA: History and Prospects

A Discourse Analysis.

Abstract
Internet voting in the USA has a tragic history. It began in the year 2000. It worked so well that Congress approved a major project for the Department of Defense to provide website based Internet voting for overseas military. But the project was abruptly aborted, and the reputation of Internet voting suffered a blow from which it is yet to recover. In chronicling these events our discourse analysis shows how a coup d'état of the election administration function was executed through the control of Internet voting's meaning.

William J. Kelleher, Ph.D.
The Internet Voting Research and Education Fund
Email: Internetvoting@gmail.com

Paper prepared for the annual meeting of the Western Political Science Association, March 28 – 30, 2013. Los Angeles, California.
Comments are welcome.

Part I: A SHORT HISTORY OF INTERNET VOTING IN THE USA.

Introduction

The defining event for the history of Internet voting in the United States occurred early in 2004. Before then small trials of Internet voting were conducted by the Department of Defense for its overseas military, and by a few political parties, but these uses pale in significance to what happened in 2004. In that year the myth of Internet voting insecurity swept the nation in a matter of days, and has remained the prevailing social meaning of the technology since then. Using a discourse analysis, this paper will describe the emergence of that myth, how it has been sustained to this day, and why it is a myth with no basis in science or fact. But first some historical background is in order.

Remote Electronic Voting Before 2004

The idea of using the technology of electricity to vote has been around for a long while. Thomas A. Edison's first patented invention, in 1869, was an electronic vote recorder for use by legislative bodies. Although demonstrated to Congressional leaders, it was never used.[1] Early in the 20th Century the inventor R. Buckminster Fuller suggested that voting by telephone would be convenient for rural voters.[2]

During the 2006 election Connecticut, Maine, New Hampshire, Oklahoma, Oregon, and Vermont used vote by phone systems.[3] Telephone voting continues to be used in several Canadian provinces.[4] In 1990, during Operation Desert Storm, the Department of Defense (DoD) worked with some states to allow voters to receive and submit their ballots by fax.[5]

Ross Perot's Reform Party might have been the first US political party to employ online voting, in 1996.[6] The Republican Party allowed remote voters in Alaska to vote online in its straw poll in 2000. But a mere 35 votes were cast this way.[7] Also in that year, the Democratic Party offered the option of Internet voting for its members in its Arizona primary. Nearly 40,000 voters, about 46% of the total, used the system.[8]

Concerned about the difficulty of voting from overseas that US voters, especially those in the armed forces, had long complained of, in 1986, Congress enacted the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). The Act granted authority to the executive branch of the federal government to provide a way for US citizens to register and to vote in federal elections from overseas. States were left to their own devices. By Executive Order, the President assigned the Secretary of Defense the administrative responsibilities for UOCAVA. In turn, the Secretary of Defense assigned these responsibilities for implementing the law to the Federal Voting Assistance Program (FVAP), an agency within the Department of Defense.[9] FVAP broadened its vote by fax method in 2003 to offer voting by email to the military in Iraq and Afghanistan.[10]

In the year 2000, FVAP worked with several volunteer states on a pioneering "test of concept." The project was called "Voting Over the Internet" (VOI). The plan was to allow members of the overseas military to vote online in the November election. "Internet voting," is a distinct method of voting. Unlike fax or email voting, Internet voting is website based; that is, the voter can use his or her own equipment to connect with a designated remote server by logging on to a secure website. The challenge for FVAP was to set up a website on which the voter could log on (with user name and password) and retrieve an exact copy of his or her local jurisdiction ballot, then cast votes for every candidate and other issue, and click to return the voted ballot. There were 50 counties presenting ballots among the five states in the trial. FVAP's server was accessed by the overseas voters to vote, and then by the local election officials to download the encrypted digital information. This was the first time any US citizens used true Internet voting to cast an actual vote in a US election.[11]

Of course, no government agency, perhaps in the world, understands security issues as well as the United States Department of Defense. Despite all their security experts knew of online voting threats and how to defend against them, FVAP invited outside "White Hat" hackers to probe the VOI system for weaknesses. In addition, the state of Florida insisted on independently testing the system by its own standards; which it did, and then it gave VOI official "certification."[12]

Although the number of votes cast over the system was tiny, a mere 84, the *concept* of Internet voting for overseas military had proven itself viable. After the election, FVAP conducted a thorough assessment study of the trial. According to Polly Brunelli, FVAP's voting program director, satisfaction levels were very high among local election officials, FVAP managers, and most importantly the voters.[13]

The assessment study compared the use of Internet voting to the vote by mail (VBM) system that the military generally used to date. Several important findings were made. These include that: users had more confidence in the VOI than in the VBM process (4, 2); only voters whose registration was authenticated voted (4, 30); only one ballot per voter was taken by the VOI system (4, 4); VOI provided greater voter secrecy, privacy, and protection against the alteration of ballots than does the VBM process (4, 5-7); VOI facilitated reliable audits and recounts (4, 8); voter enfranchisement was enhanced because many of the frustrations of VBM, which had often discouraged participation, were eliminated. These included delays in the mail, and the rejection of registration forms and/or ballots because they had inaccurate, incomplete, or unclear data (4, 12-15).

Recognition grew in the DoD that Internet voting would be the future of voting for its overseas military, and perhaps all UOCAVA voters. Indeed, though they did not know it at the time, in 2003 FVAP would receive "the Excellence.Gov award for the VOI project from the Federal Chief Information Officers Council and The Industry Advisory Council." Additionally, the computer science experts in the "Caltech/MIT Voting Technology Project rated the VOI voter registration application a best practice for elections."[14] Following the VOI trial, DoD sought authority from Congress to try a much larger test.[15]

The Beginning of SERVE

Section 1604 of the National Defense Authorization Act for Fiscal Year 2002 directed the Secretary of Defense to carry out an expanded demonstration project which would enable uniformed service members to cast ballots through an electronic voting system by the 2004 general election.[16] Using the knowledge gained from the VOI proof of concept, FVAP began work on the Secure Electronic Registration and Voting Experiment (SERVE).

Fifty-five counties from seven states – Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah and Washington – volunteered to participate.[17] According to the EAC report on SERVE, "services for voters included: online voter registration and updating of voter information online; ballot delivery and vote selection; and review of their registration and voting status."[18]

The FAVP team that worked on setting up the SERVE system employed several members of the prior VOI team. Also, private companies were brought in, such as Accenture and VeriSign. These companies had technicians with experience building Internet voting systems, like the one that went so well in Arizona. (Indeed, Arizona adapted that system for its overseas military, and now has the longest running overseas military Internet voting program in the country.)[19]

The SERVE voting process was security conscious from end to end. Each voter had to apply to vote on the system. Once the registration was cleared, he or she was assigned a "digital certificate," or identity code kept in the system to verify the voter's identity when he or she logged on.[20] As with VOI, these controls would help to prevent voter fraud by ensuring that only registered voters voted, and that each voter only voted once.

The central server was located in a well-secured building on Accenture's corporate grounds in Reston, Virginia. System administrators had to use security badges to enter the premises. Access to the server was limited to certificated personnel, each with their own security codes. Reading encrypted data required the codes of at least two authorized personnel. Event logs would keep an exact record of who did what on the server. Regular reviews of these logs assured that if any irregular activity had taken place, it would not go unnoticed. The odds of any "insider attack" succeeding were extremely small.

Separate modules were set up in the central server for each participating local election jurisdiction. Only their authorized personnel could access the central server from their local office. To further tighten security, FVAP provided each jurisdiction with a lap top computer dedicated only to the SERVE project. Using these computers, local jurisdictions could download the encrypted voting data from the central system. The FVAP-issued lap tops were programmed to decrypt only the data for the particular jurisdiction. At least two authorized personnel in a jurisdiction had to log on to access voter data.[21] Here again, security measures made insider shenanigans highly unlikely.

Encryption also makes it impossible for any unauthorized person to know who voted or how he or she voted. Having all the encrypted voter data for each jurisdiction on one lap top, requiring at least two people to use the decryption keys, creates a far more secure situation than having stacks and stacks of thousands of mailed-in absentee paper ballots scattered around an election official's office.

During development, SERVE's operations and security precautions were held to standards already in use by DoD military departments, including the National Security Agency. A diversity of independent subject matter experts combed the SERVE system for security vulnerabilities, and, as with VOI, the State of Florida independently certified SERVE for use by Florida voters.[22]

FVAP plans were to continue its security vigilance throughout the process. As the EAC Report explained, FVAP plans included

> conducting a formal phased risk assessment throughout the system development cycle; monitoring and review of system development process; developing [additional] system security requirements [as needed] to be responsive to risks; collaborative development of system requirements with states and counties; conducting thorough certification and accreditation testing for conformance to both functional and security requirements and doing third party penetration [or, White Hat hacker] testing prior to deployment.[23]

After deployment, intrusion detection systems would immediately alert administrators to any hack attempts so that counter measures could be promptly employed. Third party penetration testing would be conducted at random, without notice to SERVE administrators. System operators would engage in "continuous monitoring of system performance audit logs [which also had] pre-specified alarm conditions, and random third party review of system audit logs were planned as mechanisms to maintain awareness of the threat environment."[24]

FVAP Director, David Chu, used the following table to illustrate, in a report to Congress, the security risks the SERVE team anticipated and the strategies they developed to defend against those threats. Here is that table:[25]

THREAT	**MITIGATION**
Network Security	- Encryption
	- Intrusion Detection Systems
	- Redundant Firewalls
	- Penetration Tests
Privacy	- Digital Signatures
	- Secure Socket Layers
	- Encryption
	- Voter Identity/Ballot Data Separation
	- Voter Ballot Data Verification
Virus, Worm, Trojan horse	- Anti Virus Scanning
	- Digital Signatures

	- Voted Ballot Data Verification
Spoofing	- Secure Socket Layer - Digital Signatures - Voted Ballot Data Verification
Denial of Service	- Large Quantity of Bandwidth, Multiple Carriers - Multiple Internet Service Provider Entry Points - Utilization Monitoring
Voter Fraud	- Digital Signatures

Voters would register and vote in their state of residence. SERVE empowered them to vote in their state's primaries and the 2004 general election.

The voting process would begin with the voter using his or her PC, or any other computer, from any place in the world, at any time of day or night. First, the voter would log on to the secure SERVE website, enter the PIN that was issued at sign up, and request a ballot. Next, his or her name would be automatically checked against the local election authority's registration records. If cleared, an appropriate ballot would appear on the voter's computer screen. He or she would mark the ballot, and click the "vote" button. But that was not the final step. SERVE had a voter verification mechanism. That is, a window would appear showing the vote, and asking the voter to confirm it. Once the voter had verified his or her vote, the vote selections would be permanently stored in the database on the central server for later download by the local election officials.[26]

SERVE would automatically separate the voter's name from the ballot. Then the name would be stored on a list of those who voted, so that there could only be one vote per registered voter. The system would store the vote separately. By storing the separate records of votes and voters, SERVE would act as a back up for the local election officials. This back up data could also be used as an auditing resource. That is, throughout the process state officials could compare their lists of how many persons had voted, and their vote tallies, with those of SERVE. Any discrepancies would be cause for investigation.

Of course, every voting process consists in a division of labor. In the SERVE process, Congress had a role to play by granting authority and funding. DoD and FVAP had roles in the development and supervision of the system and coordinating with the states and local jurisdictions, along with the private contractors involved. Voters also had a role. Besides, hopefully, casting an informed vote, the voters who signed up with the SERVE project had other responsibilities. These included keeping their own PCs free of malware, and protecting their electronic credentials against theft or fraudulent use (such as buying or selling).[27]

Presumably, SERVE voters would have been an especially conscientious and responsible group. Because they were military personnel, they were likely security conscious; and since they had to make the effort to sign up for the SERVE Internet voting project, they probably had more technological user savvy than the typical civilian voter at the time. Nevertheless, FVAP had planned a voter education publicity program to be sure the voters understood the need to protect their machines from malware.

The SERVE system was designed to handle far more votes than the tiny 84 cast in the VOI experiment. SERVE was prepared to process the registrations and votes of up to 100,000 participants. Beyond that, the SERVE technicians aimed to create a show piece of a system, which could be expanded to accommodate roughly six million UOCAVA citizens in the future, without compromising accuracy, vote secrecy, or the voter's identity. Although it was not their mission to demonstrate how a secure, accurate, and convenient Internet voting system could be carried on domestically, the SERVE team understood that this possibility was implied in their work. By the end of 2003 the SERVE technology was ready to conduct the first large scale multi-state online vote in an actual US election. SERVE was prepared for the 2004 primaries, and the November presidential election.

Indeed, to be sure that they had left no technological stone unturned, and that this was no secret operation done by government elites but a fully open process, which is as it should be in a democratic country, the FVAP established a SERVE Security Peer Review Group (SPRG). This group was comprised of 10 members from academia and industry. Some of these specialists were chosen because they were *known critics* of Internet voting. Nothing was kept secret from them, and everything was open for their inspection.[28]

Of course, this was a very risky move. The SPRG members with a bias against the project did not share the enthusiasm of the SERVE team for the vision of all UOCAVA citizens one day voting over the Internet. FVAP was aware that a sharp eyed critic could expose any major flaws in the system. Just one vocal dissenter could become a real party pooper.

Apocalypse Now

As it turned out, there was not just one vocal dissenter, but four! And they didn't simply add their dissenting opinion to the final report, as Supreme Court Justices do when they write a dissenting opinion. These critics went public with a passion to kill the project! That the *potentials* they envisioned and the consequences they imagined *might* happen caused them such alarm that they broke from the protocol for SPRG that the FVAP management had suggested.[29] Rather than the ten members of SPRG filing a consensus report with FVAP, these four critics wrote their own report, and promptly published it in the New York Times. The Times led its story with the conclusions made by the four critics:

> A new $22 million system to allow soldiers and other Americans overseas to vote via the Internet is *inherently insecure* and should be abandoned, according to members of a panel of computer security experts asked by the government to review the program.

> … The system, they wrote, ‘has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber attacks, any one of which could be *catastrophic*.’ Any system for voting over the Internet with common personal computers, they noted, would suffer from the same risks.[30]

That story came out on January 21, 2004. On February 6, 2004, just over two weeks later, Deputy Defense Secretary Paul D. Wolfowitz issued a memorandum ordering David Chu, to halt work on the SERVE project.[31] The New York Times reported the story with the lead,

> Citing security concerns, the Department of Defense yesterday canceled plans to use an electronic voting system that would have allowed Americans overseas to cast votes over the Internet in this year's elections. Paraphrasing the memorandum, a Department of Defense spokeswoman told the Times: ‘The department has decided not to use Serve [sic] in the November 2004 elections. We made this decision in view of the inability to ensure legitimacy of votes, thereby bringing into doubt the integrity of the election results.’[32]

Thus, the dissenting report had its desired effect. Four computer scientists, albeit with the help of the New York Times, caused the termination of an expensive Department of Defense project before it could be put into use. So powerful an essay deserves examination, so that history might understand the reasons and reasoning behind shelving SERVE. What made the SERVE system “inherently insecure”? What potentials did the critics see in the system that might result in “catastrophic” consequences? What did the dissenting essay say that led Deputy Secretary Wolfowitz to doubt the ability of SERVE “to ensure legitimacy of votes”?

The Argument from Potential

The four critics refer to their essay as “The SERVE Security Report” (SSR).[33] In it they stated their mission, their methods, their observations and opinions, and their conclusions. Here is how they understood their mission as SPRG members: “Our task was to identify *potential* vulnerabilities the [SERVE] system *might* have to various kinds of cyber-attack, to evaluate the degrees of risk they represent to the integrity of an election, and to make recommendations about how to mitigate or eliminate those risks.”[34] The key words for understanding the methods these four critics followed are “potential” and “might.” As we will see, they gave those words a very broad interpretation.

The analysis of Internet voting security is often divided into two sections. One is the website server, its physical environment, and the personnel connected with it (the server side). The other section is the environment of the voters who will vote on the system. This includes the voters, their equipment, the Internet, potential attackers, and law enforcement (client side). In the SSR, the primary concern was with the security threats in the voter’s environment, the client side. The four critics stressed that those who constructed the SERVE *server* understood

> the security problems we describe here, and we have been impressed with the engineering sophistication and skill they have devoted to attempts to ameliorate or eliminate them. We do not believe that a differently constituted project could do any

> better job than the current team. The real barrier to success is … that, given the current Internet and PC security technology, and the goal of a secure, all-electronic remote voting system, the FVAP has taken on an essentially impossible task. There really is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough.[35]

A wide range of threats infest the voter's environment, according to the authors of the SSR, "any one of which could be *catastrophic*."[36] They added, "We can *envision scenarios* in which the computers of SERVE voters have been compromised on a large scale, calling into question all votes cast over the Internet. Regrettably, such a scenario is all too possible."[37]

As a window upon the methodology followed by those writers, this is a telling statement. First, anyone who is concerned with the integrity of the democratic process will surely find it alarming, as those authors did, to contemplate a proposed online election system which would be based on "compromised" computers the use of which would call "into question all votes cast." Deputy Secretary Wolfowitz likely had such a disturbing vision in mind when he ordered a halt to the SERVE project.

However, the quoted statement might also cause alarm to anyone who is equally concerned that public policy criticisms have some foundation in scientific studies, or at least actual experience. Unhappily, that foundation will be found missing throughout the SSR. The expression "We can envision scenarios" is a description of the primary method employed by this "Report." The steps of their method include that they "envision scenarios," and many of them; then they treat each as if it were a statistically demonstrated "possibility," which they in turn rely upon to substantiate their case for setting aside all hopes for Internet voting. As we will see, not studies, but only their subjective imaginations render their scenarios "all too possible."

The authors admit that it is "impossible to estimate the probability of a successful cyber-attack (or multiple successful attacks) on any one election."[38] So, as a substitute for probability studies, the authors use the subjective approach of deeming an attack "quite *easy* to perpetrate." They add that those are "the attacks we are most concerned about."[39] We will discuss how they use "easiness" as a methodological concept below.

Another term in their methodological vocabulary is "could." That word occurs 128 times in the 34 pages of text. (We will also see such variants as "can" and "might.") Because the term refers to possibilities, as opposed to existing conditions, its referent is in the subjective minds of those who use the word, and not in the reality around them. Hence, the attacks the authors envision

> could occur on a large-scale, and could be launched by anyone from a disaffected lone individual to a well-financed enemy agency outside the reach of U.S. law. These attacks could result in large-scale, selective voter disenfranchisement, and/or privacy violation, and/or vote buying and selling, and/or vote switching even to the extent of reversing the outcome of many elections at once, including the presidential election**.**

> With care in the design, some of the attacks could succeed and yet go completely undetected.[40]

Surely, if Wolfowitz had read this paragraph he would have lost a lot of sleep before deciding to stop SERVE.

As if that parade of horribles was not enough to overwhelm every American reader with fear for the safety of their country, should Internet voting be implemented, the authors zone in on party identifiers and political minorities: “It is *possible to imagine* widespread attacks that targeted all voters in a particular party for disenfranchisement, leaving the other party unaffected. Such an attack would have serious consequences.”[41] To be sure!

However, in the present essay, addressed chiefly to professional political scientists, we will question the usefulness for public policy analysis of such head-spinning discourse. Attempts at rational discussions about whether or not a public policy proposal is worthy of implementation are frustrated rather than facilitated by igniting trepidation with seemingly irrefutable claims of catastrophe should the policy be adopted. The use of the word “could,” and its variants, in the SSR appears calculated more to end discourse than to engage in it. No further discourse is possible when a position is based upon arguments that are, to use Karl Popper’s term, “unfalsifiable.” Unfalsifiable arguments are impossible to disprove. Popper uses this concept to distinguish science from religion and superstition. Science continues as an enterprise of learning because it welcomes the refutation of hypotheses. Religions and superstitions reach for the intellectual security of Eternal Verities, which cannot be refuted (at least in the minds of Believers).[42]

One example of an unfalsifiable argument is the well worn admonition, “The End is Nigh,” which has never been disproven. Indeed, one discussion of false Armageddon predictions has it that the first warning on record is found on an Assyrian clay tablet from 2800 BC.[43] Perhaps this exhortation has such endurance with its gullible and naïve adherents because it is impervious to both logical criticism and empirical disproof, thus creating the illusion of Indubitable Truth. By logic, just because the End has not yet occurred, does not mean it will not occur – and soon. Empirically, it is unfalsifiable because with each failure the prediction can simply be moved to “tomorrow.”

The SERVE Security Report attempts to win its case by relying primarily on three unfalsifiable claims. These are:

1. **The Invincible Could**

We have shown some examples of how arguments turning on the word “could” can be unfalsifiable, and we will show more as we proceed.

2. **Success Predicts Failure**

The authors of the SSR write, “the lack of a successful attack [on SERVE] in 2004 does not mean that successful attacks would be less likely to happen in the future.”[44] Here is the same form of argument as “The End is Neigh.” Logically, just because the world did not end on 12-21-12 does not mean that the end would be less likely to happen in the future. On the assumption that it has got to end sometime, each new prediction will be more likely to come true than the prior failed prediction.

Likewise, a successful run of SERVE does not necessarily bode well for the future; "quite the contrary, future attacks would be *more likely*."[45] Thus, with each successful use of online voting, according to this form of imagining, the odds *increase* that a catastrophe will strike. Why would the odds increase? Its simple, "both because there is more time to prepare the attack, and because expanded use of SERVE or similar systems would make the prize more valuable."[46]

In other words, according to these four Ph.D. computer scientists, success is a sure-fire prediction of failure. Contrary to commonsense, each new success does *not* show that more success is possible. Instead, success increases the odds of failure. Lewis Carroll could not have stated the case more clearly than this: "In other words, a 'successful' trial of SERVE in 2004 is the top of a slippery slope toward even more vulnerable systems in the future."[47] Ergo: Internet voting should not even be tried, because it might succeed.

3. **Invisible Attacks**

SSR: "the fact that no successful attack is detected does not mean that none occurred."[48] Here, the argument is that not only does success predict failure, but success can be an invisible failure. With online voting, no one can ever know for certain that the winner of an election is really the one who received the majority of votes, in part, because a hidden code in the computer that tallies the vote could have elected the candidate who actually lost the popular vote.[49]

Logically, this "invisible fraud" argument is invincible. Just because P appears to have won the online vote does not necessarily mean for certain that Q was not the real winner. Armed with this unfalsifiable charge, the four Ph.D.'s, and their followers, can challenge the validity of every online election, and they do not need a scintilla of actual evidence of fraud; indeed, in their method of imagining, the lack of evidence just shows how well the fraud was pulled off.

It is true that in university computer science labs demonstrations have been made of well hidden codes, and even of self-erasing code. True, too, such code can be "extremely difficult to detect" in the tens of thousands of lines of code that online election servers need. However, that code must be installed by stealth to have an effect on an election. So this argument presupposes the failure of every security measure put in place, without having to demonstrate the actual failure. Unfortunately, such dogmatic discourse does not lend itself well to a mature deliberation about so important a public policy proposal as whether or not to implement Internet voting.

Harkening back to Popper, if you can't know the truth or falsity of a proposition, then it is no longer within the realm of scientific knowledge, but has become myth. To say that the security of Internet voting can't be determined because hacks can be done without detection, creates an unfalsifiable proposition. This takes the computer scientist out of the realm of "science," and puts him or her in the myth-making department.

In any large scale election, no one can know for certain that the results represent the will of the majority. Outside a room of 50 people, where everyone can see every raised hand, some *trust* in the process will be required. A large scale election that does not require some trust in the process by the electorate is not possible. US presidential elections draw well over 100,000,000 votes. These are counted in thousands of local jurisdictions. Each jurisdiction passes its count on to a small number of state authorities, which uses the totals to determine the slate of Electors for the state's Electoral College. No one on Earth can ever know *for sure* whether error or misconduct affected the reported results. Indeed, as we will argue again later in this paper, in a representative democracy, like that of the United States, even with checks and balances, some trust is essential to the operation of the system.

To deserve respect and consideration, then, the imaginary vision of an invisible attack in an online election must pass at least two tests of reasonableness. First, a realistic sketch must be made of how a cheater could install the malicious results-changing code without being either foiled or caught by existing security measures. Second, a creditable explanation must be given as to how that code could remain in the server, or a voter's PC, without being detected by existing security measures. But, as we will show, whether as to server-side attacks or client-side attacks, the mere claim of "easiness," and other arguments, made in the SSR fail to meet either of these two tests of reasonableness.

Easy Installation

In addition to its unfalsifiable claims, the SSR frequently comments on how "easy" it is to carry out the various forms of attack they reference. They write, for example, that "The terms Trojan horse, virus, and worm all refer to types of malicious code, differing only in the means by which they get transported to the computer and get executed. … Malicious code is one of the most serious security threats in any application, because it is so *easy* to install, and so difficult to detect."[50]

Despite the condescending praise the four dissenters gave the SERVE construction team, the SSR includes attacks on a SERVE server in its use of the term "easy." While certain that the PCs of voters cannot be relied on to be virus free, the authors caution their readers that the "threat of SERVE-specific viruses should not be discounted."[51] The authors warn with foreboding that the "ability of an arbitrary outsider to learn on a wide scale how voters voted is enough of a threat to democracy that we think this alone justifies canceling the SERVE project. The fact that the attack is relatively easy to mount only strengthens our claim."[52]

But when they say "easy," do they mean "easy" *despite* all of the security measures taken by the builders of SERVE to keep out malicious code, or "easy" if you do not consider those protections? As inspectors of the SERVE system they knew of the many threat mitigating defenses which we discussed above, and which would be in operation during the 2004 election. These would include decryption key management protocols being followed, security guards on duty, and the FBI Elections Division and other law enforcement agencies on high alert and monitoring SERVE's environment, as they would be during an actual election.[53] The authors of the SSR completely fail to engage the law enforcement capacities of the FBI and other policing agencies, just as they pretend that SERVE voters had little or no security protections. How "easy" is it really to commit large scale voter fraud without detection by the FBI? While the SSR imagines that anyone with a computer could sway an election, they neglect to mention the risks to the would-be cheater. Knowing of the possibility that voter fraud can result in arrest, huge lawyer fees, costly fines, time in prison, and all the social and economic consequences of a felony conviction, how many people who are intelligent enough to figure out how to commit such a crime are really dumb enough to try? This supposed "easiness" of election malware installation seems to be solely a product of their method of "imagining."

The SSR creates the impression that voter privacy on SERVE's server could be easily violated. But, specifically to protect the privacy of voters against malicious spyware SERVE was equipped with "Digital Signatures, Secure Socket Layers, Encryption, Voter Identity/Ballot Data Separation," and the means for "Voter Ballot Data Verification." To protect specifically against Trojan horses, viruses, and worms, SERVE had the capacity for "Anti Virus Scanning," and used "Digital Signatures," and "Voted Ballot Data Verification." Thus, the authors of the SSR fall far short of intellectual honesty by proclaiming how "easy" it would be to install malware or spyware on a SERVE server without engaging directly and specifically the security environment and the defenses built into the SERVE system precisely to protect against malicious code in its servers.

The authors assure their readers, without further explanation, that once malware has been installed (magically?), "Even experts with access to the source code of a program may not be able to tell if there is malicious code in it, since it is relatively easy to disguise malicious code so that it is extraordinarily difficult to find."[54] Those authors fail to mention both SERVE's "Anti Virus Scanning" software, and its protocols for the regular review of event logs, which would catch any installation of malware by an insider.

To make it "easy" for themselves, the authors conveniently by-pass any mention of those protocols, and simply speculate generally that "New viruses almost certainly will not be detected by most current virus checking software. Moreover, it is not too difficult for attackers to build new viruses, or to modify existing viruses sufficiently that they will avoid detection."[55] But mere conjectures on the supposed easiness of installation dodge the responsibility of these critics to engage the total security environment, and to specify the short comings of SERVE's security protocols and anti-virus scanning capacity. In the opinion of this writer, no rational public policy discussion should tolerate the avoidance of this intellectual responsibility.

The Specter of DDoS

One of the threats to the convenient use of the Internet is that a website server can be overloaded with visitors, freeze, and become inaccessible to other visitors. This can happen accidentally, as when the server simply receives more visitors than it is equipped to accommodate. However, access to a website can also be slowed or stopped by a deliberate attack. Computer scientists call this a "denial of service" (DoS) attack. A special form of a DoS attack is often referred to as a "distributed denial of service" (DDoS) attack. This occurs when one person, or group, controls many computers and directs them to a particular target.

The SSR correctly states that "the robustness of a website against network flooding attacks is determined largely by the network capacity available to that website."[56] In other words, website hosting servers are constructed to handle an anticipated amount of traffic. If the server is suddenly faced with significantly more visitors than it was built to manage, it will freeze and block further attempts by computers to connect with it. This capacity to handle traffic is also referred to as the server's quantity of bandwidth.

The FVAP anticipated both that it would need sufficient quantity of bandwidth to accommodate thousands of voters at one time, and that a denial of service attack was a threat to be guarded against. Thus, the SERVE builders took not one, but several measures to defend the system's operations under a DDoS attack. According to David Chu, the SERVE system employed a "Large Quantity of Bandwidth, Multiple Carriers, and Multiple Internet Service Provider Entry Points."[57] The system administrators also planned to monitor the utilization of the system so that DDoS attacks could be seen coming, and defensive action taken, before the attack could overload the system. These are standard defenses and strategies.

As members of the SPRG, the authors of the SSR were fully aware of all the security measures taken by the SERVE team. But, in an act of omission that can only be described as disingenuous, the authors of the SSR said nothing about these measures built into the SERVE system. Instead, they simply laid out the bald assertion that, "It seems unlikely to us that SERVE could withstand such a high volume DDoS attack."[58]

Consistent with their "we can imagine" methodology, the SSR writers conjure up a spectacular scenario, treat it as a fact, and base their conclusion that SERVE is defenseless on that "fact." They imagine that

> It is *plausible* that an attacker could gather a 'zombie network' of 10,000 slave computers, and each computer could initiate about 50 new SSL connections per second. Consequently, an attacker could generate 10 to 100 times more SSL traffic than the SERVE website is *likely* to be able to handle. Thus, a DDoS attack against SERVE's SSL web servers *could* render SERVE unreachable to voters and disrupt an election in progress.[59]

Of course, this kind of "reasoning" will always be irrefutable. No matter how many "SSL connections per second" SERVE is equipped to handle, the SSR writers will simply raise the "plausible" number of zombies needed to defeat it in their imaginary scenario. Pitted against imagination, SERVE can never win.

Here are some more "coulds:" "An attacker *could* mount a large-scale denial of service attack that renders SERVE's voting service unavailable on the day of an election. Those voting on Election Day would be unable to vote, calling into question the validity of the election."[60] Of course, the authors of SSR knew that Internet voting is typically spread out over several days as an “early voting” option. So this scary scenario, assuming only one day of voting, is more easily refuted than some of their other imaginings.

DDoS attacks can be stopped by several different means. One is to switch servers, as SERVE was prepared to do. Another is to trace the attack to its source and block traffic from there. The servers being used by the attacker can also be shut down. So, this Election Day argument is weak. But, perhaps anticipating this refutation, they offer another alternative scenario.

Imagine this – a “last-day denial-of-service attack.” The attacker cleverly lies in wait to disenfranchise all the procrastinators and late deciders. What “possibilities” are implied by this scenario? “With SERVE, there is the *possibility* that the disenfranchisement rate could rise to close to 100%.”[61] Although this “possibility” is drawn from thin air, as opposed to any sort of research or experience, they recommend killing the project, because “we consider last-day denial-of-service attacks a significant threat to the security of SERVE's elections.”[62] Of course, by demanding that SERVE be shelved, they become responsible for disenfranchising 100% of the UOCAVA voters who, for a variety of reasons, could not vote by mail.

Given all these “possibilities” and imaginings, one may wonder if there are any actual facts upon which rational people can assess the kind of threat that DDoS attacks really pose to elections using Internet voting. The SSR refers to only *one case* of an election being disrupted by a DDoS attack.[63] In 2003, the New Democratic Party of Canada (NDP) held its officer elections, and offered online voting as an early voting option along with other ways of voting. During one of the days of voting the online process was slowed, but not stopped, by a DDoS attack. The technicians operating the system blocked the attack within 45 minutes.[64]

There are only two other examples of an election using Internet voting being disrupted by a denial of service attack, which occurred after the SSR came out. Ironically, in another NDP officer election event access to the website was slowed. But the exact cause of the problem has not been fully determined. It might have been caused by a DDoS attack, or it might have been a result of too little bandwidth being clogged up by an unexpected surge of legitimate voters. Either way, the problem was resolved when the traffic slowed.[65] An Internet voting option has been offered in about 50 different municipal elections in Canada over the past decade, and *not one* instance of a DDoS attack, or other security issue, has been reported.[66]

The EAC “Survey of Internet Voting” repeated an allegation of a DDoS attack on an online voting trial for students in Austria, during the 2009 Austrian University Elections. However, no facts were given as to how long the voters were denied access, if at all.[67] In its survey of over 30 Internet voting trials around the world, the EAC Survey did not mention any other instances of a denial of service attack even being alleged.

When *facts* such as these are compared to the *imaginings* in the SSR, the threat of denial of service attacks appears less frightening. The facts indicate not that DDoS attacks can be dismissed as insignificant, but that the professionals who set up the Internet voting systems can be relied upon to include effective defenses and mitigation strategies, such as they did with SERVE. Unfortunately, the myth of Internet voting vulnerability to DDoS attacks has other perpetrators, as our discussion of NIST will show.

E-commerce and Internet Voting

The New York Times quoted the SSR's claim that "e-commerce grade security is not good enough for public elections."[68] In support of that claim the authors of the SSR argue, *inter alia*:

> In a commercial setting, people can detect most errors and fraud by cross-checking bills, statements, and receipts; and when a problem is detected, it is possible to recover … In contrast, voting systems must not provide receipts, because they would violate anonymity and would enable vote buying and vote coercion or intimidation. [But] it is still vital for the system to be transparent enough that each voter has confidence that his or her individual vote is properly captured and counted, and more generally, that everyone else's is also.[69]

Here, again, those authors omit to engage what they knew to be the measures taken by FVAP to meet that criterion of transparency and voter confidence. As noted above, SERVE provided a method for voter verification. After marking the ballot, the voter would send it to the server, and the server would put up a confirmation widow showing the voter the vote that the system had for recording. The voter then had an opportunity to correct any errors.

Without elaboration the SSR simply dismisses SERVE's voter verification process with the contemptuous remark that "The mere presence of a confirmation screen does not prove that the vote was recorded correctly."[70] But, of course, the voter does not ask for "proof," but only reasonable assurance that his or her vote was counted as cast. For opponents of Internet voting like the SSR authors, nothing could ever satisfy their requirements of "proof." Because SERVE was never used, follow up studies on voter confidence in this verification method could not be conducted.

Another difference between e-commerce security and SERVE's security is that e-commerce websites are online 24 hours a day, seven days a week, and 365 days a year. This gives hackers an endless amount of time to poke at the systems for security vulnerabilities, and to experiment with different attack strategies. An online voting platform that is only up for two or three voting days does not offer such opportunities. Also, in such a lengthy time, the chances of disgruntled or greedy employees turning against their employers is greater than it would be with a small team of personnel who have had security clearances by the US Department of Defense, and who are working intensely on a very short term project. E-commerce employees working at routine jobs are also more likely to be distracted, or to make mistakes over the long haul, than are skilled technicians on high alert for a short time.

Like other opponents of Internet voting, the SSR reminds its readers of the multitude of news reports of alleged "hackings" of government and commercial websites. However, the circumstances that enabled the hacks to happen are rarely examined, nor is light shed on the differences in the types of hacks. A superficial defacing of a commercial website's home page is given the same coverage as an unauthorized withdrawal from a victim's savings account. Thus the occurrences of really serious crime are inflated in the minds of the public.

Yet the explanation is rarely given that the victim may have enabled the crime by his own carelessness. People who open every email and uncritically click on the links they present, or who download free screen savers or other "freebies," visit websites with free music or porn, or who fail to purchase quality commercial virus protection systems are far more likely to fall victim to online crime than are the more prudent folks.

Recently, the New York Times gave prominent coverage to a report that the Chinese military was engaging in industrial espionage by hacking into the computer systems of US corporations.[71] But the 3000 word Times story was written in an upside down fashion. That is, it led with the sensationalistic announcement of all kinds of hacks on US corporations, but only towards the end did it introduce a little education. By far, most of the attacks were not cold hackings coming from out of nowhere. The Chinese sent trick emails to corporate officials who then clicked on links, which instantly let in the malware. For example, Coca Cola was in negations to buy a Chinese company. One email posed as part of the business communications, and Coke was hacked. But in other instances, sharp employees knew better than to click on links in email. They turned over the emails to security, and saved their companies from the headaches Coke executives had. If the Times had given as much attention, in this and other such articles, over the years to educating its readers on how to avoid being fooled by trick emails, perhaps many system penetrations could have been prevented.

Despite the stream of e-commerce hacker news, in the context of understanding Internet voting security issues, the SSR's references to common computer crime is a Red Herring. In addition to what has been said about the lack of public education about security self-protection, election officials cannot be held responsible for the victims of computer crime any more than they can be held responsible for the victims of purse-snatchings when these happen to voters going to and from polling places, or auto theft that happens while the voter is waiting in a long line to vote. Computer crime exists; but that is no reason to forgo online voting. If election officials make an effort to educate voters as to their responsibility to protect themselves, and to inform voters about how to protect themselves during the election process, the amount of online election crime could be significantly reduced, if not eliminated. Experts in computer security could help election officials to prepare such an education program.

While the New York Times eagerly printed the catchy quote, "e-commerce grade security is not good enough for public elections," its reporter made no effort to inform his readers as to how they can protect themselves, and he asked no questions challenging the comparison of online commerce and online voting, nor did he ask why the SERVE security measures could not be relied upon. Apparently, while cries of impending catastrophe make a sensational story (news that's "fit to print"), educating readers about how the doom can be avoided is too dull an endeavor.

More of the specific claims of Internet voting insecurity will be examined in the discussion of NIST's unfortunate role in this propaganda war on that voting technology. But first some accounting will be given for how the myth of Internet voting insecurity, based on the claims in the SSR, swept the nation in the days that followed the publication of the allegations by the New York Times.

Part II. THE BIRTH OF A MORAL PANIC

Wolfowitz's order on February 5, 2004, to halt the SERVE project was the direct cause of SERVE's demise. The New York Times states what is known of that order: "Paraphrasing the memorandum, a Department of Defense spokeswoman said: 'The department has decided not to use Serve [sic] in the November 2004 elections. We made this decision in view of the inability to ensure legitimacy of votes, thereby bringing into doubt the integrity of the election results.'"[72]

However, there are unanswered questions about that order, to which a complete history of Internet voting in the US should have answers. For example, what factors weighed most heavily in Wolfowitz's reasoning? His order to Chu clearly implies a lack of confidence in SERVE's security measures. The focus on "legitimacy of votes" can entail several items. It might mean the concern that votes could be changed on the voter's machine, without the voter or the FVAP authorities knowing. Another concern Wolfowitz might have had is that the votes cast could be coerced or cast by someone who has bought or stolen the voter's credentials. He might have been worried that the final tally would be unreliable, both because the SERVE server could be hacked and the votes changed on it without detection, or because he did not trust the system's capacity for auditing. Besides the SSR, what other reports, studies, or publications, or who influenced him is not available in public records. The order was not made public.[73] Whether he was personally convinced of SERVE's supposed vulnerability, and based his order on that conviction, or he gave the order to quiet public outcry, is currently unknown. There was public outcry, and we will examine the main causes of it.

Unfortunately, Wolfowitz has not elaborated on his reasons for shutting down the SERVE project. Wolfowitz is reported to have also said in the memo that he would reconsider his decision only if researchers can prove that integrity can be maintained.[74] Apparently, that proof was never forthcoming. While the record is clear as to what the SSR arguments against SERVE were, there is no record as to what, if any, FVAP personnel pled to Wolfowitz in SERVE's defense. Indeed, while the press and other news media gave widespread coverage to many of the specific, and most sensational, charges made against SERVE by the four critics, there is no public record of any intellectually equivalent rejoinder in defense of SERVE.

The January 21st article in the Times, which originally announced the SSR's claims, gave several reasons why voting on SERVE "could be catastrophic."[75] The information the

Times publishes is, in many cases, all that the public learns of an issue. Thus, if the Times, and all the secondary publications following it, give a one-sided sensationalistic report, calculated to alarm and frighten readers, then that will likely be all that enters the minds of the public. The Times story included such emotionally weighted phrases about SERVE as:
"inherently insecure and should be abandoned;"
"Trojans, viruses and other attacks [are possible, and] could be carried out on a large scale;"
"unacceptable risks of election fraud;"
"malicious software [could] monitor the users' activities, scan them for private information;"
"introduces greater risks just to gain convenience;" and,
"How do we recover if an election is compromised?"
For many readers, these phrases might sound like a Paul Revere alarm that another government boondoggle is coming, and concerned citizens should demand it be stopped before the "catastrophe" of a corrupted election befalls the nation. (Indeed, a New York Times editorial says no less two days later.)

But in reply to such disturbing charges as those, and that using SERVE "could enable hackers to disrupt or even alter the course of elections," a FVAP spokesperson gave an arid and tepid response. Representing DoD and FVAP, Glenn Flood told the Times that the four critics were a "minority" of the 10 SPRG members, and that they "overstated" the security risks. An official for Accenture, the lead contractor on the project, said the critics drew "unwarranted conclusions." She also claimed that five of the other six SPRG members told her they would not recommend shutting down SERVE. The Times reporter quoted one of the six non-dissenting SPRG members as saying the four critics were simply reflecting "the professional paranoia of security researchers."

That's it. No energetic, hard hitting, blow-for-blow riposte from the SERVE side; at least nothing that made it into that report by the Times, or other public sources. While opinions can differ, considering the *emotional appeal* of the discourse presented in the Times story, one can understand why such a lethargic defense did nothing to slow the momentum set in motion by the alarming report in the Times. More on how that momentum of public opposition to SERVE was sparked and kept fueled can be learned from an insider's account.

Introducing Avi Rubin

About two years after Wolfowitz issued his February 5, 2004, halt order, Avi Rubin, one of the four SSR authors, published a memoir of that period.[76] He writes about how, before being invited to join the SPRG, he was a leading figure in the publicity campaign against the burgeoning use in the US of DREs, or direct recording electronic voting machines. The use of those machines was prompted by the passage of the Help America Vote Act of 2002.[77] Following the infamous "hanging chads" in Florida in the 2000 election, the Act, among other things, made nearly four billion dollars available to states as reimbursement for upgrading their voting technology. Rubin became a leading critic of the DREs when he published an essay exposing what he saw as numerous security flaws in the source code of a popular DRE model built and sold by the Diebold Corporation.

An anti-e-voting activist, Bev Harris, discovered in 2003 that the source code was on a Diebold website, and unprotected. She posted the link for all to see on her blog as a prank. When Rubin heard this, he downloaded the source code to his office computer at The Johns Hopkins University. Once Rubin had written out his critique of the Diebold code, he devised a strategy for publicizing his exposé. Prior to teaching, he had worked for six years at AT&T, where he fortuitously underwent "media training."[78] Given this training, Rubin "sensed that his exposé was going to be a public relations hot potato."[79]

He put his PR training to good use. He writes,

> From the beginning, my plan was to break the story in the New York Times. I wanted this story in the hands of a reporter I could trust to get it right, someone who was … sensitive to the political ramifications. If the first story doesn't get it right, any misinformation it contains is likely to be repeated countless times. The reporter I trusted most was John Schwartz, who covered technical issues for the Times.[80]

Rubin had provided Schwartz with technical advice in the past. On July 24, 2003, the New York Times ran the Diebold story.

Rubin had learned from his media training that "the second day after a news release is the big day for media coverage. That's when all the stories that follow the original one appear."[81] Sure enough, the next day, his local paper, the Baltimore Sun, made his report "its lead story on the front page."[82] Not only that, to his delight the story was printed "above the fold," where readers could see it in vending machines. Beyond that, the following "Sunday the Sun put the story on the front page again."[83]

After making the deal with Schwartz, Rubin contacted "the vice president at the CNN national desk, Nancy Lane."[84] They arranged to interview Rubin "in a studio in Baltimore" on the day the Times broke the story.

A man of foresight and energy, Rubin made further preparations. He informs his readers that the day before the New York Times was to run the exposé, "I had prepped Adam and Yoshi," his two grad student research assistants.[85] The trio spent several hours in a Johns Hopkins classroom polishing, memorizing, and rehearsing the key phrases that Rubin wanted to feed the media (and, hence, the public).

He had learned from his public relations training at AT&T that the more complex a statement to the press is, the more likely they are to get it wrong when they present it to the public. To control the message, you have to keep it simple. "The main idea is to boil your information down to no more than three short, simple, and memorable messages … that will stick in the minds of readers and [TV] viewers."[86] Rubin writes, "we practiced ways to work these quotes into our answers, even if they didn't directly answer the questions asked. … I grilled them for hours." The effort paid off, and the trio was "amused and gratified" when "many of these quotes turned up verbatim in news stories over the next few weeks."[87]

Once the Diebold story came out, Rubin shot to celebrity status. His memoir is replete with detailed accounts of all his TV appearances. He writes, for example, "I was on The Today Show a couple of times and on NBC's and CBS's national evening news shows, and … on The Daily Show with Jon Stewart."[88] He also fully discusses his radio and press interviews, his speeches, and the articles he was asked to write for magazines and newspapers. He became so famous, according to his narrative, that one story on his blog, about serving as a voluntary poll worker, received "forty thousand hits," and became the subject of even more stories in the press.[89] Later, Rubin was called for a meeting with members of the House of Representatives, which he notes was covered by the "NBC Nightly news."[90]

Potential, not Experience

Rubin candidly reports receiving much criticism from other computer scientists about his methods for analyzing the security vulnerabilities of DRE voting machine code. For example, lawyer and Carnegie Mellon computer science professor Michael Shamos, conveyed to Rubin that "the lack of fraud in previous electronic elections made the concerns about it unrealistic."[91] But Rubin rejects this method of trying to assess the likelihood of fraud from the study of what happens in actual situations. He writes, "I believe in assessing *vulnerability*, not past performance. *Potential*, not experience."[92]

To further illustrate his methodological point, Rubin writes that he was questioned by Ohio congresswoman, Marcy Kaptur, about his claim that hacked DRE code could be used to the advantage of a political party. "Diebold's base of operations was in her home state."[93] He frankly admitted to her, a Democrat, that in his examination of the DRE code, "we had not seen even the slightest indication that the [Diebold] voting machines were rigged to favor one party over another. In fact, [he and his two assistants] hadn't seen any evidence of tampering at all. Our point had to do with potential fraud."[94]

Rubin saw his methodological approach soundly rejected in a Maryland court. In *Schade v Lamone*[95] an anti-e-voting group in Maryland sought an injunction to try to stop the state from using the Diebold machines in the 2004 November election, or at least to compel Diebold to make its machines print a paper record of the votes. Rubin submitted his Diebold analysis as evidence, and testified as an expert witness for the Plaintiffs. Michael Shamos testified as the expert witness for Maryland, the Defendants.

The court stated, in part, that while the witnesses for the Plaintiffs "indicate catastrophic, doomsday-type scenarios, nevertheless, the Court is impressed with Dr. Shamos's testimony this will not occur. The Court is confident the votes of Plaintiffs will be counted."[96] The court opined, "No system is infallible. No machine is infallible. Under oath, all experts agree systems such as these [DREs] are much more secure and less vulnerable than the paper ballot, and even the opt scan ballots."[97]

The court also observed that "the overwhelming factual evidence clearly shows there have been no verified incidences of tampering with these machines anywhere in the United States. The votes have been counted accurately. Recounts have occurred with complete accuracy, and there is no reason to believe this will not continue."[98] During the hearing, said the court, in sworn testimony "All experts agreed the use of paper ballots is the least accurate of all systems and lends itself to the most chicanery. On the other hand, the experts seem to agree, if untampered, the Diebold-type voting machines are the most accurate in recording and counting votes."[99] The petition for an injunction was denied.[100] The decision was upheld on appeal.[101]

Rubin was stunned by his experience in the hearing. In his view, the lawyers were not there, as he was, to find "objective truth."[102] "I walked out of the courthouse and wandered the streets of Annapolis."[103] Showing his pique, Rubin contemptuously dismissed the lawyers, the expert witnesses who testified in favor of the DREs, and the judge as more of those "technically illiterate people" found "throughout the legal system."[104] Because of that experience, Rubin rejects the US legal system as a source of "objective truths," and says that only by funding research institutes, like the one he had just founded, can the truth be known.[105]

Rubin and his cohorts were unswayed by such criticism, whether from courts or colleagues. David Jefferson, a veteran anti-e-voting activist and one of the four SERVE critics, had also heard many similar criticisms from his colleagues. In an interview he said, "I think they believe our concerns are exaggerated – either that it's not really possible to undermine the election to the extent we say it is or it's all theoretical and academic."[106] Undaunted, they followed the same methodological principles in their estimations of SERVE's "potential" security flaws. In their SERVE Security Report, perhaps with some defiance, they listed many of their previous criticisms of DRE security vulnerabilities to hackers and insiders. "All of these criticisms, which we [still] endorse, apply directly to SERVE as well."[107]

The Election Integrity Movement

Judge Manck's characterization of Rubin's testimony in *Schade* as based on unrealistic "catastrophic, doomsday-type scenarios," coincides with much that has been said in the present analysis about the vacuity of the SERVE Security Report's fanciful methodology. The imagined dangers to democracy of DREs that Rubin divined were belied by the judge's finding of fact in *Schade* that "there have been no verified incidences of tampering with these machines anywhere in the United States."

Thus, one wonders whether the only intellectual foundation of the anti-e-voting "election integrity" movement in the US, informed by Rubin, consists of no more than Rubinesque divinations of *possibilities* that have never been realized. If so, such unreasoned hysteria would be sadly reminiscent of the socially unwise rhetoric of groups like the Anti-Saloon League prior to the ratification of the Eighteenth Amendment in 1919. Laws based on ill-reasoned foundations, like those prohibiting the sale and consumption of intoxicating beverages, and, worse, those permitting slavery, tend to have consequences that have proven antithetical to the public good. Since politics is their field of study, political scientists are well positioned in our society to carefully scrutinize activist demands for "election reform," and to alert law makers and the public when they find that those demands are based on irrational Rubinesque foundations. By doing so, this profession might help public policies to stay the course of Reason.

The *Schade* decision was rendered in September of 2004. That was too late to lend any assistance to the defense of the SERVE project. Wolfowitz had ordered the project stopped in February of that year. But our digression into the *Schade* case helps to amplify our sketch of the kind of reasoning that lead to the demise of SERVE. We will continue using Rubin's memoirs of the period to further explain the original steps that resulted in the current widespread doubt about the security of Internet voting.

SPRG

Two weeks before the New York Times broke Rubin's Diebold "exposé" (which was done on July 24, 2003), the first Security Peer Review Group (SPRG) meeting was held to discuss the SERVE system. As we have said, SPRG was a 10 member group of computer scientists who were invited by FVAP to inspect the system. There was a second team, which included the CIA and the National Security Agency; but they made their suggestions privately, and did not call for terminating SERVE.[108] Still working furiously on his Diebold report, Rubin "was only able to attend by phone."[109] He writes that the SERVE team "seemed unafraid to share openly the details of the system. Those details, unfortunately, horrified me."[110] But he was too busy with the Diebold essay to do anything about SERVE at that time.

The second SPRG meeting was a two day affair held in Reston, Virginia in early November 2003. "After the second day of review, several of us determined that if we failed to act, SERVE would almost certainly be adopted and implemented."[111] That is when the four dissenters decided to write their exposé alerting the public. "We set at it immediately, working late into the night and continuing over the next couple of weeks, firing drafts back and forth to each other over e-mail."[112]

Having hit the news stands about six months before he and the other three started in on their SERVE Security Report, Rubin's Diebold exposé was still "a public relations hot potato." But Rubin had already learned many lessons from this experience about maximizing public exposure for his exposés. So he took the lead of his SSR co-authors. He writes, "I convinced the others to work again with John Schwartz of the New York Times."[113] As before, Schwartz was given the exclusive.

Rubin notes that he and his cohorts "had hoped to manage the release of the report to the media carefully, as had happened with the Diebold report."[114] Unfortunately, Schwartz failed to get the story on the front page of the New York Times. But that was not much of a set back, for, as Rubin understood, "the second day after a news release is the big day for media coverage." And so it was. The second day reports mimicked the Times's model of leading with the emotionally alarming allegations of "easy" to execute dangers to democracy, followed by a reserved response in defense of SERVE.

The Washington Post ran the story on their front page the day after it came out in the Times.[115] The Post headline was, "Pentagon's Online Voting Program Deemed Too

Risky."[116] Above the fold, the alarming lead sentence declared, "A Pentagon program for Internet voting in this year's presidential election is so insecure that it could undercut the integrity of American democracy and should be stopped immediately." The story quoted Avi Rubin and Barbara Simons as saying "their biggest fear is that this year's experiment would be a hit, leading to widespread Internet voting for the 2008 presidential election. That is when the kind of Internet attack they envision could emerge, possibly from foreign subversives."

Coming just two years after the 9/11 Al Qaeda bombing of the Twin Towers in New York City, many readers likely found the "vision" of "foreign subversives" attacking "American democracy" to be a credible scary scenario. Perhaps aiming for "balanced reporting," the Post quoted a couple of SERVE team members as pleading it's only "an experiment," and could yield useful knowledge. But to this rather pedantic defense, Barbara Simons countered, "calling the program an experiment ignores the fact that voters will be casting votes that will count. If there is a question about the legitimacy of those votes, she said, the election could be undermined. It is no favor to overseas voters to let them think they have cast ballots when they have been fleeced, she said." No defense matching the emotional punch of "fleeced" voters was given.

Also the day after the Times story broke, CNN reported the news.[117] On its web page CNN's lead sentence said, "A federally funded Internet-based voting system due for release in less than two weeks is inherently flawed and should be scuttled because of weak security, according to a report by a team of computer scientists." Then, "According to the report, the online nature of SERVE could easily allow a hacker to tamper with the voting results. … Among the type of hacks the researchers outlined are ones that would overwhelm computers with a denial-of-service attack."

For the appearance of balance: "The backers of the SERVE system downplayed the findings Wednesday, saying other experts disagree." Then the tepid Glenn Flood quote, "This is a minority report from one of the peer-review groups … of about 10 or 11 members, only four of them decided that concerns were warranted." This was hardly enough to calm the emotions aroused by the lead.

Computer World, a widely read print and online IT magazine, also reported on the SSR the day after the New York Times broke the story. The lead sentence: "A federally funded Internet-based voting system scheduled for use in the 2004 primary and general elections has several unresolvable security vulnerabilities that leave it open to widespread vote tampering and privacy breaches."[118] Quoting SPRG member David Wagner, who favors the methodological terms "easy" and "could," the article goes on,

> For instance, it would be relatively easy for malicious hackers to insert spoofed Web pages that appear to belong to the SERVE system but are actually designed to alter votes or prevent them from being cast. A voter using a PC infected with a virus or worm could easily jeopardize the integrity of the system … An attack on the main SERVE system or any of the PCs being used by voters, using any of these methods, could seriously compromise the results … And the particularly dangerous part is that

> … SERVE is susceptible to large-scale election fraud that could be launched from outside the reach of U.S. law and go completely undetected.

Then Avi Rubin added, “I think that a dedicated and experienced hacker could subvert the election rather easily … I don't think that Internet-based voting such as SERVE can be made secure enough for use until we can develop computer systems that are not vulnerable to viruses and Trojan horses, and until we can develop an Internet that is resistant to denial-of-service attacks.” As usual, failing to challenge any of the “easys” or “coulds,” or to respond to any of the specific charges, and completely missing the emotional punch their presentation carries, Glenn Flood is quoted as repeating his standard reply that FVAP “welcomes” the input, but these are only four critics out of the ten-member SPRG, etc.

For some semblance of balance, the Computer World article closes with a quote from the SERVE website (since taken down) explaining that to protect voter information and ballot integrity the SERVE system “uses the latest security technology available.” But the article does not use this quote to challenge the critics of the system; instead, it criticizes the website for making such “claims without offering specifics.”

Building Momentum

The reports by the Washington Post, CNN, and Computer World represent the scores of second day stories that came out in print, on the air, and on the World Wide Web. Like a fish story, the re-telling of the SSR allegations grew and grew. Just as an earthquake on the ocean floor can cause a tsunami that wreaks havoc on land dwellers in its path, so that combination of re-publications of SSR allegations sent a wave of meaning throughout the minds of the US public that wreaked havoc on the possibilities for Internet voting in this country. Without any rational challenges, the “ease” of hacking, and imminent likelihood of all the “coulds” became folk lore, accepted without doubt.

On January 23, 2004, the New York Times published an editorial designed to fuel the flames of opposition to SERVE ignited by its piece two days earlier.[119] The editorial singles out “Aviel Rubin” for special mention as among the “Four computer scientists brought in by the Pentagon to analyze a plan for Internet voting by the military.” Then, as if they were heroic whistleblowers, rather than a dissident minority, the Times mentions that these four were the only ones to issue a report among the ten 10-member advisory committee. No mention was made of the second “committee.”

Suspending all critical judgment, the editorial repeated the methodological terms of the report, such as “potential,” “possibilities,” and “could,” to alert the world that

> the *potential* for hackers to steal votes or otherwise subvert elections electronically is too high. … the *possibilities* for compromising the secrecy of the ballot, voting multiple times and carrying out vote theft on a large scale would be limited only by the imagination and skill of would-be saboteurs. Viruses *could* be written that would lodge on voters' computers and change their votes. Internet service providers, or even foreign governments that control network access, *could* interfere with votes before

> they reached their destination. … the advantages of the Pentagon's Internet voting system would be far outweighed by the dangers it would pose. [Emphasis added.]

Although no science, nor actual experience, was cited in support of all its "coulds" and "possibles," the great newspaper righteously demanded that "Congress should suspend the program." Unhappily, for anyone who values a more balanced public policy debate, not one question was asked in this diatribe about the methods these four "scientists" used to arrive at their alarming conclusions. Only the conclusions were published. There was not a word about the opinions of the other experts and the entire SERVE team in defense of SERVE. Not even a tepid quote of Flood. Indeed, the editorial gave the impression that the frightening possibilities it enumerated was the one and only way to understand Internet voting.

Two weeks later, Wolfowitz issued his halt order, and SERVE was done for. Although it is not known exactly why he took this momentous decision, the unquestioning publication of the alarmist and sensationalist SSR by the New York Times, Washington Post, and other sources, plus the follow up editorial by the Times, no doubt contributed to his decision.

Once again, Rubin had hit another PR home run. He boasts that the SSR story took him on another round of celebrity appearances on TV, with more interviews by the newspapers and radio. He was called back to Congress, and invited to meet with the commissioners of the EAC.[120] Of course, in all this, the public only heard his divinations of all the dangers to democracy Internet voting invites. None of the pro-SERVE SPRG or FVAP members enjoyed such celebrity. Needless to say, there were no public debates or exchanges of opinion, and while Glenn Flood was occasionally quoted towards the bottom of printed articles, only the sensational allegations of the SERVE critics received widespread media publication.

In May of 2004, Rubin's PR insider, New York Times reporter John Schwartz, published an unabashed encomium on Rubin in the Times.[121] Completely oblivious to the lack of science or factual experience in Rubin's methods, Schwartz proclaimed that Rubin

> has become the face of a growing revolt against high-technology voting systems. … His critiques have earned him a measure of fame, the enmity of the companies and their supporters among election officials, and laurels: in April, the Electronic Frontier Foundation gave him its Pioneer Award, one of the highest honors among the geekerati.

Schwartz ends his plaudits by quoting David Jefferson's tribute to Rubin as "the most important figure in the United States in articulating the security problems with electronic and Internet voting."

Following Wolfowitz's order, a wave of "end of SERVE" news stories continued the public education about the issue. Given the fact that Wolfowitz had ended the project, the message to the public was that the allegations of security vulnerabilities were effectively confirmed by Wolfowitz's order. For example, the NBC report led with,

> Citing security concerns, the Pentagon has canceled Internet voting that would have involved as many as 100,000 military and overseas citizens from seven states in November, a Defense Department official said Thursday.
>
> The announcement comes two weeks after four outside security experts urged the program's cancellation in a scathing report. They said hackers or terrorists could penetrate the system and change votes or gather information about users. At the time, the Pentagon said it felt confident enough to proceed. … But Deputy Defense Secretary Paul Wolfowitz has since decided to scrap the system because Pentagon officials were not certain they could 'assure the legitimacy of votes that would be cast,' said a Pentagon official who spoke on condition of anonymity.[122]

In announcing the decision, the NBC report also enumerated some of the specific threats:
"The experts specified these central risks, among others:
•There is no way to verify that the vote recorded inside the system is the same as the one cast by the voter.
•It might be possible for hackers to determine how a particular individual voted, 'an obvious privacy risk.'
•The system may be vulnerable to attacks from many quarters, some undetectable. Stealth programs as trojan horses that harvest data are sometimes installed on public computer terminals."

In Computer World's announcement, Barbara Simons was given a platform upon which to proclaim the most hysterical statement of this epoch. Simons was quoted as saying, "Our great fear is that there will be a major move to Internet voting, which I personally feel is a threat to our democracy. The bottom line is we could have our president selected by [hackers in] Iran."[123]

Nothing was said in SERVE's defense in this article. Apparently because "Polli Brunelli, director of the Federal Voting Assistance Program, wasn't available for comment."

By this time, of course, it was too late for anyone to try to defend SERVE, or to challenge the methods of those who condemned it. The public had its education on this policy issue. Internet voting was well on its way to "folk devil" status in the US. With one exception, Internet voting would go untried by any US election district or the DoD from 2004 to 2010.[124]

Internet Voting in the US After the Shelving of SERVE

The Michigan Democratic Party offered an Internet voting option to members for its caucuses in February 2004. The decision was made after a full debate over the issues of accessibility and security. This debate took place before the four SERVE critics burst into the public discussion on Internet voting. Times were different then. Writing prior to the publication of the SERVE Security Report, political scientists R. Michael Alvarez and Thad Hall observed that the consensus of the experts in the 2001 Cal Tech/MIT study, and "other studies," was optimistic. In their view, at the time, the rise of Internet voting seems "inevitable: Internet voting is the future of voting in the United States."[125]

Indeed, the Michigan experience bore out the optimism. Alvarez and Hall later studied the event. They found that there were more online voters in these caucuses than in any prior Internet voting trial. Of the 162,929 votes cast, 28.57%, or 46,543, were cast online. 14.41%, or 23,482 votes were sent in by mail, and 57.02%, or 92,904 votes were cast in person. Turnout was "much higher" in this year than in either 2000 or 1996.[126]

At a time when the "digital divide" was still considered a problem, and mindful of those who did not have a PC or access to a computer at the time, the party provided lap tops in public libraries, churches, and other places.[127] A CBS News survey of the online voters in the Michigan primary found that 67% said they used Internet voting for the convenience. 90% of these said they voted from home, and 8% from work. Despite the national media stock in trade predictions of doomsday and catastrophe, Alvarez and Hall report that "there were no successful attacks from pranksters and hackers."[128] The two political scientists did not find any voter disenfranchisement caused by offering online voting, but did observe that problems at polling places resulted in frustrating voters.[129]

After the successful use of Internet voting in Michigan, the behavior of government officials reveals how powerful the taboo on Internet voting had become. There were probably more violations of the incest taboo in the US between 2004 and 2012, than there were violations of the taboo against Internet voting. The temptation was there, the DoD and state governments did everything they could to tip toe up to the "sinful" act without actually committing it.

For example, in 2004, DoD's Federal Voting Assistance Program enabled overseas military voters to *request* ballots and *receive* blank ballots electronically. But it was not a streamlined process. First the voter had to apply to use the Interim Voting Assistance System (IVAS), and make a request for a ballot. Then FVAP had to check the voter's registration status with the local jurisdiction. If valid, the voter was notified by email. Then the voter would log on to the FVAP website to download and printout the appropriate blank absentee ballot. But after that, the voter had to use traditional mail to send the completed printed ballot back to the local election official.[130]

State participation and laws varied. Some states would accept the return of voted ballots by fax or email. But, of course, military personnel had to be located in areas where fax machines were available. To return the voted ballot via email, the voter had to have a scanner attached to his or her PC, or do the whole thing in an office that had the equipment. To comply with the taboo on using Internet voting, voted ballots would not be accepted via the FVAP website. Just to complicate the process, unlike SERVE, no voter registration could be done electronically from overseas through FVAP. The unregistered voter had to register with his or her jurisdiction through snail mail. FVAP provided a postcard, but no electronic means for voter registration.[131]

Returning voted ballots by traditional mail adds 5 to 10 days to the process. If the ballot arrives past the deadline, it is not counted. If the voter made some error on the ballot, it might be returned for correction. This can happen, for example, when the voter signs his or her name in some way that varies from the signature on file (such as “W. Jones,” rather than “William Jones”). If the soldier moves in the course of his or her service, the returned mail could be delayed and the voter disenfranchised.[132]

Of course, SERVE – the Secure Electronic Registration and Voting Experiment – was designed to reduce the cumbersome process of registering and voting for overseas military from days or weeks down to minutes. Who would have benefited from SERVE? By Election Day, in November of 2004, there were roughly 150,000 combat troops in Iraq.[133] Add to that another 150,000 Americans providing some kind of support to the troops, either logistical or diplomatic, in that war-torn country, and the result is roughly 300,000 eligible US voters in that country. The war in Afghanistan then was still in its infancy, with about a tenth as many Americans of voting age, or roughly 30,000.[134] The 100,000 Americans who had volunteered to vote online in the SERVE project included some of these folks in combat zones.

The needless problems for overseas military voters continued to fester long after SERVE’s demise. In 2009, the Pew Center found that more than one-third of states did not provide military voters stationed abroad with enough time to vote.[135] FVAP estimates that of those who requested absentee ballots in 2010, “29 percent of active duty military voters — roughly 120,000 troops — never got their ballots.”[136] Only tinkering with various forms of electronic ballot request and ballot return by fax, email, or snail mail has been done to try to contain the spread of the inevitable frustration and disenfranchisement of overseas military voters. The technology is readily available to end this persistent disenfranchisement once for all, but the courage to break the taboo on Internet voting is lacking in the DoD, FVAP, and throughout the entire nation.

In 2009, President Obama signed the Military Overseas Voter Empowerment Act (MOVE). Among other things, MOVE required states to provide absentee ballots to overseas military voters for federal elections at least 45 days before the election would be held.[137] States were also required to provide some form of electronic communication for overseas military voters to use to request and receive an absentee ballot. In compliance with the taboo on Internet voting, voting on a secure website, in the style of SERVE, was not required. Thus, the states were encouraged to tip toe up to the edge of Internet voting, like FVAP, but not to cross over into the forbidden zone. Under this taboo, online registration is allowed, online ballot request is allowed, even online marking of a ballot is allowed, but then the ballot must be printed out for sending by fax or snail mail, or in a growing number of cases, copy and pasted into an email format.

Ever vigilant for deviations from the taboo, the New York Times growls when it sees anyone getting too close to the edge, but it has not condemned the tip toeing like it did SERVE. Commenting on the MOVE Act, a Times editorial warned that allowing the email return of voted ballots is getting too close for comfort to violating the taboo the Times had helped set in place. The first paragraph reads,

> Internet voting is in its infancy, and still far too unreliable, but states are starting to allow it and the trend is accelerating because of a new federal law that requires greater efforts to help military and other overseas voters cast ballots. Men and women

> in uniform must have a fair opportunity to vote, but allowing online voting in its current state *could* open elections up to vote theft and other mischief.

The Times, like other opponents of Internet voting, sometimes stretches the meaning of the term “Internet voting” to include the use of email and fax, so that all the technologies can be criticized with the same charges of insecurity. For example, the Times writes, “Massachusetts recently enacted a law allowing service members to vote by e-mail overseas. According to Verified Voting, a group that works to ensure reliable elections, 16 states allow some form of Internet voting.” But the differences in the technology compel the use of the distinct terms. The terms “email and fax voting” have referents that are quite distinct from that of website based “Internet voting.” Morse code is sent over telephone lines, but no one calls it talking on the phone.

In the same article, the Times then considers the Rubinesque *possibilities* opened up by the MOVE Act: “E-mail *can* be intercepted, and voting Web sites *can* be hacked or taken down by malicious attacks.” Nothing is said, of course, about the fact that none of these things has actually happened in an election using the technology. The Times worries that often “it is not possible to ensure a secret ballot when votes are cast online or by e-mail.” But the editors ignore the fact that the same problem exists with the current method of marking paper absentee ballots and returning them by traditional mail.

Disregarding military law enforcement’s capability of controlling crime, the newspaper editors warn that voter coercion “is a particular concern for military voting, where soldiers *could* come under pressure from commanding officers about their choice of a candidate.” They do not mention that this has not been a problem using paper absentee ballots. While approving of electronic requests for blank ballots, and sending them to voters electronically, the editors remind their readers of where the taboo line is drawn, “Right now, those ballots should not be returned online.”[138]

While the Times did not mention the finding made by the judge in the *Schade* case that no misuse of DREs has ever been shown to have occurred in the US, it did give a platform to law professor and anti-e-voting activist John Bonifaz to twist the truth, returning voted ballots by fax or email “basically takes the hazards we’ve seen with electronic voting [by DREs] and puts them on steroids.” Opponents of Internet voting, with a little help from the Times, often deliberately try to stretch the worries Americans have been made to feel about DRE insecurities and fraud to include the return of voted ballots by fax or email. Continuing to conflate the distinct technologies, the Times article declares that the “coming election will be the first in which Internet voting will play a major role, now that 33 states [up from 16 in January] have passed measures to allow their voters to cast ballots over the Internet.”[139]

Of course, if the Times does not trust military officers to respect the democratic process, then voting machine vendors are even less trust worthy: “Critics of the new guidelines say they are flawed because they allow voting machine vendors to do some of the performance and security testing themselves.” For balance, the Times does quote election officials in three states (Florida and the two Carolinas) that have used email and fax return of voted ballots without problems. One of them added that “those soldiers are real happy, too, that they don’t have to lose their right to vote.”

The New York Times holds special favor for Representative Rush Holt (D-NJ), because he introduces bills that require paper records of voted ballots, which “would in effect ban Internet voting.” One of his bills in 2009,

> would require paper ballots to be used for every vote cast in November 2010. It would help prod election officials toward the best of the currently available technologies: optical-scan voting. With optical scans, voters fill out a paper ballot that is then read by computer — much like a standardized test. The votes are counted quickly and efficiently by computer, but the paper ballot remains the official vote, which can then be recounted by hand.[140]

The Times does not discuss the error rates or other reliability, or security, issues of optical-scan machines.

The editorial declares, “Electronic voting machines that do not produce a paper record of every vote cast cannot be trusted.” But evangelizing for paper based voting technologies is something new for the great newspaper. Paperless lever voting machines were so well liked in the state of New York that they had been in use from the 1890s to 2010. Without objection from the Times, New York City used them for at least a half century. The state only gave them up and purchased DREs when the Department of Justice sued New York for being out of compliance with HAVA.[141]

In 2008, Florida crept the closest of any state to real Internet voting without quite crossing the taboo line. Okaloosa County has several military installations, and over 20,000 active duty service members and dependents registered to vote in the county, many are overseas voters. The County set up a trial program anticipating that about 700 military voters, from Germany, Japan, and the United Kingdom (not Afghanistan or Iraq), would cast their votes online. But the voters still had to go to a polling place on base, and use a dedicated computer in a special kiosk. They could not vote from just anywhere. Using those computers, they would log on to the County’s secure website, mark, and send their ballots. Then the computer would print out a record of the vote, without the voter’s name or identity, and he or she would check the paper and deposit it in a box.[142]

David Dill, founder of the anti-Internet voting lobbying organization, VerifiedVoting.org criticized the process for not disclosing the “full details of the system.”[143] But the harshest criticism came from the New York Times; indeed, the Times wanted to kill the project for being too SERVE-like, and therefore “bad.” “Florida’s secretary of state should deny Oskaloosa’s request [to set up the trial], and Congress should ban Internet voting in federal elections until a reliable and *fully tested* system is developed.”[144] Of course, the standard they use, “fully tested,” is a neat piece of trickery, because it is unsatisfiable. That is, no matter what test is done, the Times will simply move up its standard of “fully” another notch. Since that standard can never be satisfied, the Times will always have an excuse to condemn Internet voting.

Case in point: The entire Okaloosa County system underwent a lengthy and thorough inspection by an independent team of security experts, led by Alec Yasinsac, Dean of the School of Computer and Information Sciences at the University of South Alabama and co-director of the Security and Assurance in Information Technology Laboratory. They recommended some improvements, and these were made. Then the Florida Bureau of Voting Systems Certification tested the system completely before certifying it. It was studied and approved by the Florida Division of Elections. Testing was continuous. For example, before voting each day the tamper proof seals on the equipment were checked. Also, the integrity of the kiosk voting software was validated each day. Sensitive materials were kept under 24 hour watch.[145]

But this was not "fully" enough for the Times. Also, those editors knew that "a reliable and fully tested system" will never be "developed" if every trial is shot down before it is tried, as the Times would have it.

This Times editorial starts out with an irrelevant and mean slurring of the state's reputation: "The words 'Florida' and 'Internet voting,' taken together, should send a chill down everyone's spine. … Internet voting is fraught with problems, including the *possibility* that a hacker could break in and alter the results."

Upon what evidence does the Times base its claim for this alleged Rubinesque "possibility"? Upon the word of Prof. Rubin himself – "In 2004, a group of academics reviewed an Internet voting system that the Pentagon was considering. The system was scrapped after the group identified numerous security flaws. There was a very real possibility, the professors warned, that the system could be used to steal votes."

Reflecting what seems to be its annoyance at the nation's move towards a paperless economy and culture, the Times continued to present its readers with only one side of this public policy issue. It offered no discussion of the successful use of Internet voting outside the US. The Times does not mention that the four SERVE critics, like David Dill, had never built an Internet voting system, but only condemned such systems from their armchairs, while the experts who have actual experience have demonstrated by their successes that it can be done. Instead, the editors drag out the old Rubinesque "slippery slope" fear producer: "The issue here goes beyond a single county. If the Okaloosa experiment goes forward, other counties around the country may decide to implement their own programs, with just as little public scrutiny and debate."

Even though Okaloosa County did not cross the taboo line, because it came so close the New York Times did its very best to shame and embarrass County officials by name, as well as those in the rest of the state, by painting them as reckless. This is one way of enforcing the taboo across the nation. How many election officials, especially elected officials, want to risk a public scolding from the New York Times?

The efforts of the states to comply with both the MOVE Act and the taboo against Internet voting have had disappointing results. A recent Chapman University study of how well the email/fax return of voted ballots is working concludes that the “absentee ballot data for 2012 paints a bleak picture for military voters.”[146]

A Coup d'état

The perpetrators, and enforcers, of the taboo on Internet voting appear to have successfully executed a coup d'état over the election administration system in the United States. They now control how elections will be conducted; and, it won’t be online. The cabal consists of anti-Internet voting lobbying groups like Dill’s 501c4 VerifiedVoting.org and the 501c3 Overseas Voting Foundation (or OVF, which specializes in keeping Internet voting out of the military). Whenever a “public outcry” is needed to pressure Congress, or some state legislature, Verified Voting has several power houses waiting on call. These include the Electronic Frontier Foundation (which gave Rubin its Pioneer Award), Moveon.org, and Common Cause. Following their study of how public attitudes towards electronic voting were manipulated, political scientists Hall and Alvarez observe “These organizations were able to shape the debate over electronic voting quite successfully.”[147] Of course, the ultimate power of the cabal comes from the New York Times, which can trigger a flood of secondary online and print press with its opinions. Without the support of the Times, those special interest groups would not be able to use fear mongering to counteract the public’s desire for more convenient voting. The Times has been the single greatest force for instilling the Internet voting taboo in the minds of the American people and their elected officials.

Natalie E. Tennant: A Profile in Courage

Despite the powerful forces railing against Internet voting, our country has had at least one outstanding profile in courage. In 2008, Natalie E. Tennant was elected Secretary of State in West Virginia.[148] Having a husband who is a career officer in the military, she knew first hand about the problems members of the military have had voting from overseas. Determined to do something about it, Secretary Tennant persuaded the state legislature to approve a true Internet voting trial to include five volunteer counties. Two private companies, Scytl and Everyone Counts, offered their expertise for free, as a demonstration of what can be done. A system not unlike SERVE’s was constructed. Overseas military voters could log on to the secure voting website with a PIN and password. Online voting was made available for the 2010 primaries. Overseas military voters could use their own PC, and vote any time during the three day voting period, from anywhere. The process worked so well that Secretary Tennant persuaded the legislature to approve expanding it to several more counties for the general election, which it did.

After the election, Secretary Tennant sent the legislature a reoprt on the project. In the counties where Internet voting was offered, of all the voters who requested that their absentee ballots be delivered electronically, 76% voted on the secure website. In the counties using standard mail as the absentee ballot transmission method, 58% of the requested ballots were returned. As the report observes, there was a higher rate of participation with Internet voting. Also, there were no reports of security breaches or voting fraud. Contrary to the ill-founded worries of the New York Times, there were no reported cases of military brass pressuring soldiers to vote one way or another. Indeed, a survey showed extremely high voter satisfaction, and many said they would use the system again.

Based on her experience, Secretary Tennant has become an advocate for Internet voting in the USA.[149] However, she has had to pay a price for her courage and advocay. For example, she participated in a panel discussion in which there were several prominant anti-Internet voting activists and she was the only discussant who favored the technology – and, who had actual experience using it. After quite a bit of interrupting, badgering, and being accused by the OVF CEO of using her overseas military voters as "guinea pigs," Secretary Tennant declared in her closing remarks, that if this is what it takes, "I'll continue to sit up here and take the attacks, take the arrows ... and things like that!"[150] Of course, public humiliation for violaters is another means of enforcing the taboo on Internet voting.

Also Rans

In 2009 there were three noteworthy uses of online voting in public elections, but these were less significant than the West Virginia experiment. The New York City School Board conducted one trial. Website voting was open to parents for six days to cast "advisory votes for [unpaid] members of their community education councils." This was not for actual public officials.[151]

The City of Honolulu offered telephone voting and website based voting for its Neighborhood Board Election in May 2009. However, these are also only advisory positions.[152]

Another online voting project was held in 2009 for the Board of Supervisors of the King Conservation District in the State of Washington. While these elections were for paid elected officials, the system of online voting used fell safely short of violating the taboo on Internet voting. Voters had to find their way to voting kiosks distributed across the County, and vote on dedicated lap tops.[153]

The DC Hack

Much ado has been made of the one and only Internet voting system in the world known to have been penetrated by hackers. In 2010, the Washington DC Board of Elections and Ethics contracted to construct an Internet voting system with a nonprofit group that had no experience building such a complex system. Partly to reassure itself that the system would work, the Board held a practice mock election a month before the November election.

The Board publicly invited anyone to test the security of the system. Someone did. University of Michigan computer science professor, Alex Halderman, and a team of graduate students probed the system in every way they could think of. After 36 hours they found a way in. Once in, they discovered all the identities and passwords of registered voters. They found stored passwords for administrators of the system. They used these to access all the approximately 900 votes that had been cast on the system. They changed the votes and wrote in a variety of silly names, like "Bender," a robot cartoon character. Then they installed the UM football team “fight” song, which played after someone voted. Of course, the penetration alert system failed. None of the responsible administrators noticed the hack, until fans of other teams complained in emails that their school’s fight songs were not being played. Since Halderman and his team had taken control of the security cameras in the “secure” room where the server was kept, they were able to see the expressions on the faces of the administrators and security guards after they learned of the deed.[154] The myth of Internet voting insecurity had its most potent reinforcement.

Part III: ASSESSING THE PROSPECTS FOR INTERNET VOTING

Assessing the prospects for Internet voting in the United States requires an examination of the claims made about its security. For, if elites and public believe the technology is unacceptably vulnerable to manipulation and abuse, then its prospects are poor. But this can change if the claims of insecurity are publicly and authoritatively shown to be without intellectual foundation.

We have seen that the fears of insecurity have been aroused in elites and public by methods of opinion manipulation, which have lacked intellectual integrity. But because well respected institutions, such as the New York Times, are leading the campaign against Internet voting, and no equivalent force is opposing it, the prospects for moving to the new technology are, at present, nearly nil. If the prospects for Internet voting are to improve, an institution that can command a degree of respect like that given the Times, must come forth and, using Reason and the Scientific Method, counter the Times’s strategy of stimulating unfounded Fear.

The Voice of Science

Article 1, section 8, of the US Constitution enumerates the specific powers of Congress. Among these are: “The Congress shall have power … To regulate Commerce … To coin money … and fix the standard of weights and measures.” The Framers had learned from unhappy experiences under the Articles of Confederation that without uniform standards for money, the new nation’s economy had little chance of thriving. They had also learned that without uniform “weights and measures,” the growth of science and technology, industry, and commerce would be crippled by chaos. Out of its continuing efforts to exercise these powers responsibly, in 1988 Congress created the National Institute of Standards and Technology (NIST), which is currently a non-regulatory agency within the Department of Commerce.

Throughout the history of the US, NIST, and its predecessor agencies, have worked in close collaboration with industry, science, and the military to fulfill its mission. That mission is “to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.” Without an agency to perform these functions, the United States might never have become the giant it is in science and industry; indeed, NIST has such a vital role in the progress of science that it can aptly be understood as the voice of science in the USA.[155]

Appreciating the importance of NIST as a research and standard setting institution, and respecting its past accomplishments and the professional competence of its staff of researchers and technicians, when Congress established the Election Assistance Commission (EAC), in the 2002 Help America Vote Act (HAVA), it mandated that the Director of NIST be the Chair of the EAC's Technical Guidelines Development Committee (TGDC).[156] In a display of foresight, Congress also mandated that among the responsibilities of NIST is to provide the EAC technical support on the research and development of, among other things, "remote access voting, including voting through the Internet."[157]

NIST, then, has the authority and power to set straight the New York Times, and all the other purveyors of irrational fear. Only NIST can present itself as having the confidence of the United States Congress to apply the highest standards of the Scientific Method to a particular problem, and to command respect for its pronounced findings. Were the Times to obstinately contradict the scientific findings of NIST, it would risk looking ridiculous, and chance the loss not only of prestige, but of advertisers, subscribers, and readers. Thus, if there is no science behind the Internet voting insecurity scares, as we allege, then NIST is singularly situated to falsify or to verify this claim.

NIST Speaks

NIST has, indeed, spoken on Internet voting; and we will now examine attentively the findings of this honorable Paragon of Science; for, surely, nowhere else will we see the methods of science and the application of Reason so well displayed. The main pronouncements by NIST on Internet voting are found in its 2011 report, "Security Considerations for Remote Electronic UOCAVA Voting" (NIST 7770).[158]

Unhappily, in NIST 7770 the agency has not performed its duties well. Indeed, the agency appears to have been captured by the proponents of the taboo on Internet voting. Although expected to conduct independent scientific research for Congress and the nation, this report reveals little or no research beyond their reading of the infamous SERVE Security Report (SSR). While the EAC, Congress, the states, and the people of the United States look to NIST to be a leader in the field of scientific research, the reality is that, in its election technology division, NIST is a mere sycophant to the leaders of the bloodless coup over our nation's election administration process. NIST 7770 has no scientific content, but mindlessly puppets even the most absurd Rubinesque divinations. An examination of this document will reveal it to be a model of misfeasance.

NIST 7770 advises Congress and the states against the implementation of Internet voting. This advice is based on the report's findings in three principle subject areas.[159] These are:

1. **Software Attacks**

"First, remote electronic absentee voting from personally-owned devices face a variety of potential attacks on voters and voters' personal computers. Since the voter's personal computer is outside the control of election officials, it is extremely difficult to protect against software attacks that could violate ballot secrecy or integrity or steal a voter's authentication credentials. These are serious threats that are already commonplace on the Internet today."

2. **Voter Authentication**
"Second, remote electronic voter authentication is a difficult problem. Current technology does offer solutions for highly-secure voter authentication methods, but these may be difficult or expensive to deploy. Personally-owned computers may not be able to interface with these methods, such as having the necessary smart card readers for cryptographic authentication using Common Access Cards or Personal Identity Verification cards."

3. **Auditability**
"Third, it is not clear that remote electronic absentee voting systems can offer a comparable level of auditability to polling place systems. Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution."

1. Software Attacks: Voter Education and Responsibility
We will examine each of these points, starting with the first; Software Attacks. Software attacks can occur against the voter's PC or the voting website server. The SSR's primary argument was that because the voter's PC was too vulnerable to malware and spyware, those PCs could not be trusted to be used securely in Internet voting.[160] By putting its focus on PC "software attacks," NIST 7770 is in lock step with the SSR.

But the NIST statement contains an ambiguous phrase, which seems to go well beyond the SSR. The report states, "Since the voter's personal computer is outside the control of election officials, it is extremely difficult to protect …" Does this mean that if the PCs were within the control of election officials, they would be easier to protect? That was the case in Okaloosa County, when overseas military voters went to an office on base and voted on a dedicated lap top computer in a kiosk. But the statement might be hinting at more than what they did in Okaloosa County. It could be read as suggesting that unless the voter's PC is within the control of election officials, Internet voting cannot be trusted.

This could be accomplished, for example, by requiring every voter to submit his or her device to the remote access of the election officials so that they could scan the machine for malware. Of course, if this government intrusion into each PC was made a requirement of law for Internet voting, it would not likely be acceptable to defenders of the secret ballot, or of privacy generally. By setting up a standard that would be an anathema to the public and thus impossible to fulfill, NIST would be guaranteeing the results it appears dedicated to bringing about – preventing the implementation of Internet voting.

Also, a standard that makes election authorities responsible for the security of the voter's PC implicitly rejects the original policy of the Department of Defense and its agency for overseas military voters, the Federal Voting Assistance Program. When DoD's FVAP constructed the SERVE system, they understood the threats to voters, but their policy was to leave the responsibility of maintaining the voter's equipment to the voter. SERVE would be able to protect itself from penetration by malware in the voter's computer. The voter was responsible for protecting his or her machine from malware and spyware that could, in NIST's words, "violate ballot secrecy or integrity or steal a voter's authentication credentials."

But FVAP did not intend to simply leave the voters to the mercies of predators. FVAP planned to actively engage the voters in a program of security education, so that they would know that they needed to protect themselves, and how to do it. Such education could be enough to prevent all, or most, of the common computer crime that opponents of Internet voting worry about. Because they were fully briefed, the four critics of SERVE knew of FVAP's plans for voter education, but they deliberately kept it out of their discussion. The NIST report, like its parent the SSR, also does not consider the role of voter education as a security measure in the Internet voting process.

However, before Wolfowitz's order to shelve SERVE was issued in February 2004, the director of the SERVE project for FVAP, Carol Paquette, responded directly to the charge that the online environment of the voter's PC was too insecure to be trusted for voting online. She explained to Kim Zetter of Wired (a popular print and online magazine), "We absolutely understand that the Internet is insecure." She said of the voters, "If they're using computers at work [however,] in most instances those computers are going to have firewalls and protection [from viruses]." She assured Zetter that, "Election officials will advise home voters to install antivirus software and run a virus check before election day. After all, this is a pretty important thing they're going to be doing, *and the voter also bears some responsibility for the act of voting.*"[161]

Paquette's statement, "the voter also bears some responsibility for the act of voting," is not only the policy set by FVAP for the SERVE project, it is a policy followed by the United States, and every state, for as long as we have had the Union. Voters have always been expected to make their own way to the polls, and back home again. Except in the most extraordinary Civil Rights cases, the government has not provided voters either with transport or with a safe escort to and from the polling place. The government does not provide protection against the elements for voters who must wait in long lines. Nor does the government, as mentioned before, accept responsibility for any of the common crimes that can befall a voter. No voting jurisdiction in the US accepts liability for the victims of purse-snatchings when these happen to voters going to and from polling places, or auto theft that happens while the voter is waiting in a long line to vote. Even the act of registering to vote must be performed under the voter's own initiative, and is not done automatically for him or her by the government. The individual voter bears these responsibilities for the act of voting.

To the extent, if any, that NIST's ambiguous phrase is hinting that the government should have the responsibility for the security of the voter's electronic voting device as a condition of allowing Internet voting, then the proposal should be rejected as a tactic for preventing the implementation of Internet voting. Such tactics are tried in other parts of the report, as we will see. NIST presents numerous specious arguments in support of its claims that "it is extremely difficult to protect against software attacks that could violate ballot secrecy or integrity or steal a voter's authentication credentials."

Software Attacks on Secrecy

NIST 7770 notes that, at least in theory, there are two primary categories of attack on voter secrecy; client side and server side. In other words, secrecy can be violated by attacks on the voter's PC or on the voting website server. As to the server side, NIST suggests the reasonable requirement that "Voting systems must protect the confidentiality of sensitive information stored on those systems."[162] The NIST report candidly acknowledges that servers can be made reasonably secure, especially compared to vote by mail systems. "Compared to mail-in voting, remote electronic voting systems have the potential to provide much greater technical controls for maintaining ballot secrecy."[163] While secrecy is protected somewhat in vote by mail systems by using separate envelopes within envelopes, small scale violations by misbehaving election workers are still possible.

But with properly organized online voting systems, server access "control mechanisms and cryptographic technologies can provide strong protections against [server side] attacks on ballot secrecy."[164] Using prudent decryption key management and carefully vetted personnel can protect against insider attacks that could violate vote secrecy and voter identification privacy.[165] The report recognizes that sophisticated servers have the capacity to keep votes and voter identity separate. In other words, Internet voting systems that are constructed by real professionals can be relied upon to protect the vote and voter data stored in the servers. The fatal secrecy problems are far more on the "client side" than on the "server side."

Credential Stealing

The NIST report states hypothetically that "an attacker can potentially steal the victim's authentication credentials (e.g., a password or PIN)."[166] As the authors of this report know, few elected policy-makers or citizens who are concerned about the integrity of elections would support an online voting process if that would enable widespread stealing of voter credentials, and the multiple voting by crooks that would follow. Thus, assessing the prospects for Internet voting in the US depends upon evaluating the likelihood that the alleged threats to the process would actually occur.

While the report asserts in Rubinesque fashion that this crime "can potentially" be done, one of the important facts it omits to mention is that there are *no known instances* of this election crime ever having been committed in any online vote around the world. Lacking such experience, small wonder that the report omits any estimation of the probability that this crime will be attempted; or, if attempted, how likely a wrongdoer would be to succeed at using the credentials of other voters to cast multiple votes without being detected.

The NIST report is defective, in part, for its numerous omissions. For example, it fails to explain who would want to engage in credential stealing, why it would be done, or how the many practical difficulties could be overcome. It also fails to show how much damage this crime could cause an election. Could an online election outcome be determined by multiple voting resulting from credential stealing, or, assuming it could succeed, would it only be a potential nuisance factor?

We will argue here that there is no reason to believe that the threat of multiple voting by a credential thief, is any greater for an online election than in the current practices of absentee voting, or voting by mail. We will also reflect upon how easily this could be done on a large scale. To put the report's hypothetical propositions in a fuller and more realistic perspective, we will carefully consider the practical details the commission of this crime would have to manage.

We will see throughout this examination of the NIST report that once its Rubinesque "possibilities" are juxtaposed with practicalities, the likelihood of the possibilities is greatly reduced. Indeed, NIST's advice against Internet voting is based entirely upon unrealistic hypotheticals. The report suggests two major methods for stealing voter credentials in an online voting system. These are keylogging and phishing.

Keylogging

As the report says, there are several types of malware that can be installed on a voter's computer. One form of malware installs a keylogging program.[167] Keyloggers send the hacker every key tapped on the user's keyboard. As a voter logs on to the voting website, he or she types in the necessary password and PIN. Then the hacker has it, too.

Keylogging is sometimes used by thieves to steal banking information. With that information, the crook can log on to the bank account any time and execute unauthorized withdrawals. Such banking credentials are re-useable. However, the first practical problem a fraudster faces with keylogging voter information is that under some circumstances he cannot use the information he has collected. During an online election, the key strokes can only be taken while the voter is logging on to vote. If each voter is only allowed to vote once, then by the time the credential thief goes to vote, it will already have been done, and he will be refused ballot access by the website. Keylogging only works in systems that allow multiple uses of the credentials; otherwise, it is useless.

Some countries, such as Estonia and Australia, actually allow a voter to vote multiple times, and the system only counts the last vote. This provides some protection in cases of coercion and vote buying. Perhaps a credential thief could succeed in this type of process by using the credentials to "re-vote." But even here, if the official website has a re-vote challenge question, such as "in what year did you first register to vote," the crook will not have the information he needs to pull off the crime. Also, Australia uses an independent verification website. A voter can log on and see what vote is recorded under his or her name. If a voter is alerted by email or SMS of a re-vote being recorded, he or she could promptly report the irregularity. Thus, while keylogging “can possibly” be done, the stolen voting credentials would be useless.

Phishing

A second way to steal voter information, discussed in the report, is through phishing.[168] Suppose a spammer sends out thousands of emails during the days in which online voting is being conducted. The email is made to appear to be from some trusted organization, such as the political party the voter is registered with, and states something like this: “Don’t forget to vote. Our democracy depends on your participation. For your convenience, click on the link provided here and vote now!” Some gullible and unsuspecting voters will click on the link. Then they will find themselves on a web page that appears official. They enter their password and PIN, and cast a vote. Not only is the vote wasted, but the criminal has the information he needs to vote on the official website multiple times, once for each duped voter. But, while hypothetically it “could” be done, this tactic also has practical problems, which NIST failed to consider.

First, the crook must obtain a list of email addresses. Rather than buy a spammer’s list of general email addresses, he will want to buy a list of email addresses for registered voters. Such lists are commercially available and legal to sell.[169] These lists can be tailored to various marketing requirements – voting districts, party membership, age, gender, etc. However, they are not cheap. Political campaign organizations pay several thousand dollars for this information. So, the prudent crook will have to balance the costs of committing this crime against the benefits he might derive from it.

If a crook has a lot of extra money, or wealthy backers, he can buy a custom email list; otherwise, he might have to shop around for a cheaper, and perhaps stolen, list. Shopping around for a cheaper list with the email addresses of registered voters could very well bring him to the attention of the FBI. Law enforcement authorities are well aware of phishing scams, and will be monitoring the sale of voter information carefully around election time. They might set up a sting operation by offering such lists for sale, to catch unwary crooks. A patriotic employee of a company that sells voter information might report a suspicious customer to authorities. However, whether making a legal or an illicit purchase, the cost of such a list will be a deterrent to most people who are thinking about phishing as a way to steal voter credentials. (Probably, the costs of conducting a phishing scam will eliminate most teenagers.) As we will see, those with the money will also be deterred, because the return on the investment is very poor, and the risk of being caught is very high.

Multiple Voting in a Local Election

To illustrate what NIST should have done to make a rational threat assessment, we will conduct a thought experiment. Suppose an online election in Los Angeles County is being held over a three day period, so that every one in the county will have time to vote. In this case, credential stealing could pay off because the crook has time to use the voter credentials.

Suppose that thousands of dollars is no obstacle for this crook, and that he obtains a list of emails for all the 4.6 million registered voters in LA County. His plan would be to make up a fake website that looked like the official one being used for voting in that jurisdiction. He will send out his trick email praising democracy, and giving a link for the voter's convenience. When duped people click on the link, and log on to the website, they will give him their PIN and password, and then waste their vote. Then he will use this information to impersonate voters and cast multiple votes. With this scheme, keylogging will not be necessary. But this crime is easier to speculate about than to commit in practice.

The villain will not know what the official website looks like until it goes online just hours before the voting is to begin. He will have to work fast to duplicate it. Another difficulty is that in LA County different precincts have different candidates for different offices, and different issues. For example, the LA County Board of Supervisors has five Supervisorial Districts; there are 18 Congressional Districts, and 88 cities.[170] When a voter logs on to the official website, it will know the voter's precinct and present an appropriate ballot. Our fraudster will not have time to set up so sophisticated a site, so he will have to use a more generic look-alike. A generic site would surely arouse suspicion among some experienced voters. To paraphrase Lincoln, you can only fool some of the people some of the time. Just one call or email to the authorities would be enough to end the scam.

Despite the risks, suppose that on the first day of voting the crook scrambles madly to construct his generic website and post it online. Once that is done, he sends out his 4.6 million emails. However, LA County will have a voter education program running in print in newspapers, and on billboards and buses, on TV and radio, and online. That publicity will state that the voter should never trust an email with a link to the County voting website, no matter what the source, and that the County will never send voters such an email. An email address for reporting suspicious activity to the FBI will also be provided.

In practice, then, many of the crook's trick emails will be disregarded or deleted by voters who paid attention to the County's voter education publicity. More importantly, not just one, but perhaps scores of voters will alert the authorities to the scam, many by simply forwarding the trick email to the FBI. Those officials will have the server hosting the fake website shut down within minutes of learning about it. The crook will have thrown away thousands of dollars on the list he bought, and the authorities will have enough evidence to track him down. The overwhelming odds of detection and capture are enough to stop any sane potential bad guy from attempting this foolhardy crime.

Nevertheless, let us pretend, as the NIST report would have us do, that this crook is somehow able to dodge the authorities. Imagine that by the end of the first day of voting he has suckered 10,000 voters to give him their PINs and passwords. Now what will he do?

Bars to Automated Multiple Voting

During the next two voting days he will work furiously to log on and vote as many times as possible. Although the cheater has all these sets of credentials, automated multiple voting is unlikely to succeed. It can easily be prevented by placing a simple security question on the voting web page, such as "how much is 2+2, or 3+9, etc." The challenge problem can be chosen at random by the server, so that it is unpredictable for each voter who logs on. Alternatively, a few letters randomly selected by the server, and scrambled so that malware cannot read them but are readable to humans, can be placed on the web page, and voters instructed to type them into a box. Voters can answer the question, or retype the letters, but not an automated program.

Another problem for the imposter voter using multiple voter identities is that the LA County official voting website server will likely be programmed to detect multiple votes coming from the same computer, or IP address. It can then present a challenge question, such as "in what year did you first register to vote," or "what is your current address." The crook will have to take the time consuming task of checking his voter registration list for that information, provided he paid to have such information included on the list. The more time he spends on log in, the less time he has to cast multiple votes.

Hypothetically, if all goes well, working alone, how many fraudulent votes could he cast in two days? To cast 1000 fraudulent votes in two days, he would have to log on and vote about 21 times per hour. But that would require, on average, nearly three votes per minute, which is not humanly possible. At one vote every five minutes, he could cast 12 votes per hour. Working without stop for two days, he "could" cast 576 fraudulent votes. If he had accomplices he could cast more votes.

What damage could he cause? The trickster would have limited control over which LA County candidates or issues he could vote on. Because he cannot select or control or predict who will be duped by his fake website, he can only vote in those elections for which he has randomly obtained the voter credentials. His tricks might or might not fool enough voters to give him a controlling number in closes races. All his expenses and risk taking could result in his having no influence on any close elections.

The only candidates that would be on all the LA County ballots would be those for a presidential or gubernatorial election. If there are state-wide initiatives or referenda to vote on, these would also be on every ballot. Otherwise, he would have a smattering or potpourri of randomly appearing propositions and local, state, and congressional races to vote on.

Thus, in this thought experiment, the very best a crook could do is cast a measly few hundred votes in a presidential or gubernatorial election. If one guy working furiously without stop for two days could cast 576 fraudulent votes, then five guys working furiously for two days might be able to vote 2880 times. Giving them a lot of generous assumptions, hypothetically, they "could" provide the winning margin for some congressional races or ballot measures, and an extraordinarily close gubernatorial election. But in a presidential contest, that is still an insignificant number when the total vote exceeds 130,000,000, and the winning margin, as in 2012, is over four million votes.

Since this crook cannot control which congressional or local elections he can vote in, but must accept randomly given opportunities, he might or might not be able to swing one of these elections.

How many rational persons would pay the costs, and incur the risks of fines and imprisonment, for such uncertain opportunities? And, why would any sensible person do this? Would any malware writer or website maker take pay to go on such a suicide mission? The NIST report does not answer these questions; indeed, it does not even ask them.

Even if Fortuna favored the bad guys, using electronic technology in the LA County election would not have enabled them to cast as many fraudulent votes as, for example, the organized effort did in the Miami mayoral election of 1997. There, a group of candidate enthusiasts, among other things, stole absentee ballots from mail boxes, and cast about 5000 votes. Their candidate won. But the scheme was immediately detected, and within four months the crooks were convicted, jailed, the bad votes subtracted from the total by court order, and the election set right.[171]

The fraudsters in the LA County example would need a gang of 8 to 10 operatives to cast as many fraudulent votes as were cast in Miami. But, the same rule of criminology would apply in this hypothetical as elsewhere; that is, the more members of a conspiracy there are, the more likely they are to be detected. Once detected, all the fraudulent votes and PINs of the victims will be on the computers of the crooks. A court can either order those votes deducted from the totals, as was done in Miami, or subtract the bad votes and let the victims cast their votes anew.

The report concludes its section on credential stealing by claiming that "it is difficult to estimate the likelihood of such attacks or how motivated potentials attackers would be to conduct these types of attacks."[172] No it's not. It's not difficult, if one bothers to think it through. While *possible* in an unselfcritical imagination, realistically the crimes of keylogging and of phishing for voter authentication credentials are highly unlikely to be attempted, and if attempted, nearly impossible to pull off without early detection by alert law enforcement. Such considerations as high risk and uncertainty of reward would dampen the motivation of any rational potential hacker. As to scale, the damage they can do to an election is no worse than existing threats to elections using paper mail-in ballots.

Therefore, the threat of these crimes is no reason to forego the convenience to voters and election administration as well as the enhancements to democracy that online voting systems offer. NIST has failed to fulfill its fiduciary duty to Congress and the American people by not fully analyzing the practicalities of carrying out the threat of voter authentication credential theft before presenting it as a reason to discourage the implementation of Internet voting.

Complex Thought Experiments

The practicalities of executing some types of election crimes in an online election can be extremely complex, and require a very high degree of technical sophistication. There are numerous contingencies involved. But these practicalities must be considered if estimates of the likelihood of the crimes being successfully committed are to have any intellectual bases. Without this sort of exercise, the execution of the crimes could appear to naïve and unthinking persons to be as easy as writing the names of the crimes.

Ballot Integrity

NIST states correctly that a vote loses its "integrity" if it is "modified by unauthorized parties."[173] Also, as we have seen, the SERVE Security Report alleges that hackers can "change votes," and listed "vote switching" as among the types of attack that "could succeed and yet go completely undetected."[174] Seeming to take its marching orders from the SSR, the NIST report states that hackers "can potentially … even change the victim's vote without the victim noticing."[175] And later,

> Ensuring the security of personally-owned computers remains a very serious open issue. At this time, there is relatively little jurisdictions can do to ensure that voters' computers are free from malware capable of changing ballots cast from those machines. Attackers have demonstrated an ability to infect large numbers of machines with malicious software.[176]

We have already addressed the false and misleading statement that "there is relatively little jurisdictions can do to ensure that voters' computers are free from malware." Voter education around election time can do very much to reduce the number of infected computers. As to the phrase "large numbers," elsewhere the report provides a slightly more specific statement of what that might realistically be. It cites estimates that up to 15% of computers around the world are infected with some sort of malware.[177] That, of course, implies that 85% are uninfected.

If there were 130,000,000 voters in an online presidential election, and 15% of their computers were infected with malware, that would be 19,500,000 infected machines. If such an election can turn on four or five million votes, then maybe there is good reason for alarm. It would be terrible, indeed, if millions of votes in a presidential election, for example, could be changed on the machines of voters, "without the victim [or election officials] noticing." This hypothetical threat, of itself, would be enough to stop any prudent member of Congress, or other person, from agreeing to implement an Internet voting system – that is, so long as the scary story was not critically examined. We will do that now. What would it take to pull off this crime? How easy is it to infect in mass the computers of voters with vote changing malware? Also, once infected, how likely is it that their votes can be changed in mass so as to affect election outcomes? Can that be done without anyone, like the voter or law enforcement authorities, noticing?

First, this crime is not easy to commit. Writing vote changing malware requires a high degree of technical skill and training. Such programs cannot be written simply by typing in "change all votes for Obama to votes for Romney." This code writing is far more complex than that. The malware not only must hide its operation from the voter, it must trick the voting server into accepting its vote as that of the voter who has logged on to the official website.

So long as the ballot being used has uniform positioning for candidates and issues, the vote changing program can work automatically in the infected computers. However, there are other challenges the program must be able to overcome. For example, different jurisdictions have different offices to be filled and different issues to be voted on. So the vote changing program would have to be tailored to the voter's specific jurisdiction. Not only that, but in the interest of fairness, jurisdictions routinely shuffle candidate and issue positions on their ballots. They do this because the first place on ballots is slightly favored by voters, and "voting fatigue" sometimes results in voters disregarding candidates and issues at the end of the lists.

To work automatically on each voter's computer, then, the vote changing program would have to be sophisticated enough to "read" the individual voter's particular ballot. This means the malware would have to interpret all the incoming data to the computer and identify when a ballot was being presented and then intercept the voters returning data and change it to suit the malware writer. Suppose the voter votes for 'X,' but the bad guys want 'Y.' The bad guys intercept the 'X,' and send 'Y' to the server. If the website has a voter verification function, as SERVE had, then the malware will have to intercept the message "You have voted for Y," and change it to appear "You have voted for X." The voter will be fooled, and click 'send.' While extremely complex, writing a program that can do all of this is not impossible.

Although an important fact to consider in the current public policy discourse, the NIST report fails to mention that to date there are *no* documented cases of vote changing malware ever changing even one vote in any online election in the world. Nor does the report give any consideration to the practicalities of executing this type of attack. It does not offer any assessment as to the likelihood of such an attack occurring in any kind of US election, and does not try to estimate the actual damages that such an attack could cause, if attempted. The Rubinesque assertion of what "could" be done – votes changed in mass without voter or official knowing – can be read as implying that this is highly likely to be done with ease in any kind of election; local, state, or federal. We will show below why that implication is false, and that this type of attack is extremely difficult to carry out successfully, has a very uncertain pay off, and is thus highly unlikely to even be attempted by people with rational minds.

We agree that vote changing malware can be written and widely disseminated in a bot network. A botnet is a collection of computers under the control of one operator. An unlawful botnet can be aggregated by a bot master who tricks PC owners into letting his malware into their computer. This can be done when people download freebies or visit websites that have the malware in them. Botnets can consist of tens of thousands of machines. But the larger they are, the more likely it is that law enforcement agencies will be able to track down the crooks.[178] Assuming that botnets with vote changing malware are possible, we will consider the practicalities of two scenarios: one in which criminal conspirators want to change the votes in an election in a single jurisdiction; and, the other in which the crooks want to swing a presidential election their way.

A Single Voting Jurisdiction

Suppose the voting website for Los Angeles County goes online at 10 pm on Monday. Voting will begin at midnight, and continue through Tuesday, Wednesday, and end at midnight on Thursday. (An extended voting period is common practice with online voting. To keep the complexity to a minimum, we will assume that no re-voting is allowed in this example.) Without insider information, or prior access to a demo site or a previous implementation, the botnet master and his gang will not know what the official website looks like until 10 pm on Monday, and will not be able to try it out, to see how it communicates with voters, until after midnight. In order to get the changed vote accepted on the website, adjustments in the vote changing program might be required before it is installed into the slave computers. During this time, voting will already have begun.

Of course, this malware program could only be effective on those machines which were used for voting *after* the malware was installed. Obviously, the malware could not be effective on those machines that were used for voting before it was installed. So the opportunity to change the votes of the earliest voters will be lost.

Suppose these crooks want to increase the number of Republican winners of congressional districts on the ballot for LA County voters. To succeed, the plot will require sophisticated preparation and planning. It cannot be done by just anybody.

Currently, only three seats of the 18 districts to be voted on are held by Republicans.[179] So, how would clever crooks plan their attack? First, they will have to determine which of the remaining15 districts have a chance at being winnable by a Republican.

In 2012, Democrats won two districts by more than 70% of the vote. They won four other districts by 35% or more. If, as the NIST report says, only 15% of computers on average are infected by malware, then that number suggests the probable success the crooks will have at building up their botnets in the three LA County precincts. Indeed, 85% of the computers in the targeted districts might not be infected. Assuming the crooks could control 15% of the votes in a given district, they still could not win in these very safe districts. Clearly, political realities limit what vote changers can do. Few crooks, with their reason in tact, would risk fines and prison to attack safe districts, which they have no chance of changing. They would have to focus on closer contests.

Republicans lost by 30% or less in three LA County races in 2012. They lost by 4% in the 26th district, and by 26% in the 27th district. They lost in the 32d district by 30%. Suppose, then, that the vote changers reckon that with luck they have a fighting chance at cheating successfully in these three districts, if they can lower the Democrat's vote total by 15%, and raise the Republican's total by that amount.

In a perfect world, for them, they could make the margin of victory in the three targeted districts just large enough so as not to arouse the suspicion of pollsters or seasoned observers. But since the earliest votes have already been cast, the bad guys will not know what the voting trends are. They won't be able to fine tune their votes, but will have to make all their slaves in the three districts vote for the Republican candidate for Congress. The uncertainty here is that this move could result in unexpected lopsided victories, no victory, or the ideal of a close victory.

Suppose that there are 300,000 registered voters in each of the three districts. The bot herders in the gang will have done all they could to build up their herd. They will have purchased email lists divided by districts, so they can focus their trick emails on the three particular districts. But they still have to work within severe constraints. They cannot force folks to take their bait.

Also, amidst the campaigning and election related publicity, County officials will have conducted a public education campaign. So along with other political information, the attentive public will learn about phishing, trick websites, untrustworthy freebies online, and the need to have professional security services scan their computers for malware before voting.

In some of the three congressional districts the voter education program will have been more effective than in others. That is, if on average 15% of machines are infected, then perhaps only 5% or 10% will be infected in one or two districts, while 25% or more are infected in another district. Whether the needed number of voters is fooled by the bot herder's ruses is a matter of chance, and luck. Just as you can lead a horse to water, but not make him drink, so spammers can try to entice email recipients to click on a link, or download their malware, but they cannot make them do it. The bad guys will have no control over which districts will have the requisite number of infected machines to assure victory for the Republicans. These contingencies render botnets an unreliable tool for election fraud.

Yet another contingency is that if the margin of victory is so far beyond what seasoned observers had predicted or expected, then the election's integrity will be cast in doubt. For example, if the vote changing in the 26th district gives the Republican a 25% margin of victory, when the experts were predicting a narrow win for the Democrat, protests will surely follow. The US Constitution, Article 1, section 5 states that "Each House shall be the judge of the elections, returns and qualifications of its own members." If the fraud is so obvious that local experts would protest, Congress might not accept the "winner." In that case, all the efforts, expenses, and risks taken by the crooks would be for naught.

In addition, the cheaters will have to reckon what their chances are of being caught. Of course, such an underhanded endeavor as vote changing cannot be undertaken risk free. The FBI will be on high alert for election fraud during the election. Botnet activity can be observed, and herders are often caught and prosecuted. In the course of tricking voters into going on websites loaded with malware, or luring them to download free videos, etc., containing malware, the FBI might be alerted for a variety of reasons. Security companies might be asked by customers to scan suspicious websites for malware, or the companies may notice their customers are being infected by one source, and the company alert the FBI. Anyone on the Internet can alert the FBI to suspicious activity. Thus, the FBI or other law enforcement agencies could investigate the bad guys, and arrest them before they change any votes; or, wait until they do change some votes and arrest them for the more serious charges. Crooks never know when they are being observed, or about to be arrested. Even if the crooks are off shore, their servers can be shut down.

Finally, besides disregarding all the practicalities involved in committing this crime, the NIST report fails to ask why anyone with the skill and intelligence needed to launch this particular form of attack would do so. Would they do it as a prank, just for fun? How likely is it that a few technicians with professional level programming skills would take on such a task, with all the risks they would incur to their freedom and fortune, for their own amusement? On a scale of one to ten, ten being the most likely, would the likelihood of them doing this as entertainment rate a zero, or a .5? Clearly, there would have to be some other motive. Since no one enjoys any immediate gain from winning an election, except the candidate and his party, there would be no immediate gain for the crooks. How likely is it that non-candidate tricksters would be policy wonks, or party zealots, willing to risk everything just to see a like-minded candidate win? Would this possibility rate as much as a 1 or a 2?

If they did it for *money,* then the crooked computer technicians would receive an immediate reward for their efforts and risks. But who would pay them? If they were paid to target the three congressional elections, how likely is it that the three Republican candidates would conspire and pool their funds to pay the programming experts? Would even one candidate take such a risk? Would local party elites? Whoever pays them, there would have to be some shopping around to find corrupt yet highly skilled programmers and bot herders. What are the odds that the FBI would learn of such shopping around? Could that likelihood be between 8 and 10 on our scale? The FBI might even set up a sting operation for morally challenged candidates to get trapped in. Knowing of the risks involved, and having their rational faculties intact, how many candidates are likely to attempt such a crime? Probably no more than do in the current polling place process; which is very few.[180]

The price for such vote changing services would be very high. The more operatives involved, the higher the price. The more races to be won, the more money the programmers will demand. Even if there was only one technical expert, would he agree to win one seat for one Republican candidate for one million dollars? Or, three seats for three million? While there are plenty of candidates who can afford such a fee, how would the payment be made – half now, half after the victory? What if there was no victory? Would the programmer refund the money? How many sensible Republicans would make so risky an investment?

We have presented an abbreviated analysis of the myriad of practicalities involved in carrying out a vote changing scheme in just one jurisdiction. Considering the difficulty of the technical challenges of writing the program and adapting it to a county Internet voting server, only a few highly skilled technicians could do the work involved. Finding such talent that is also willing to conspire to commit numerous federal felonies would not be easy, and would itself be very risky. Why would any skilled technician engage in such a risky enterprise, and which is so uncertain of success? Raising the funds to pay such criminal characters could be problematic, and risky. Of course, the more conspirators there are in a criminal conspiracy, the more likely it is to be detected. So a conspiracy to change three congressional elections in LA County is not only highly unlikely to happen, but if it did, its detection would be highly likely. The same would be true of any county.

The persons at NIST who were responsible for presenting the idea of a vote changing attack as if it were inevitable, and likely to go undetected, in an election based on Internet voting appear to base their claim on a Rubinesque divination, rather than upon any science or experience. That same divination can be seen in the SERVE Security Report. The four SERVE slayers imagined the breath taking fantasy that, "Such attacks [as 'vote switching'] could occur on a large-scale, and could be launched by anyone from a disaffected lone individual to a well-financed enemy agency outside the reach of U.S. law … even to the extent of reversing the outcome of many elections at once, including the presidential election."[181] Since these mentors of the NIST writers mention a presidential election as being under imminent threat in an online election, we will do what NIST avoided doing, and test that hypothesis in a thought experiment.

A Presidential Election

If the difficulties of winning a congressional election by unlawful vote changing are formidable in the limited context of LA County, how hard would it be to swing a presidential election that way? Aping the four SERVE critics, the NIST report assures Congress and the American people that "Attackers have demonstrated an ability to infect large numbers of machines with … malware capable of changing ballots cast from those machines."[182] While no record of such an event is cited, presumably, such a "large number of machines" would be enough to sway a presidential election. Regrettably, however, while omitting to mention that there are no known cases of this attack ever having been done, the report also shirks its responsibility to discuss any realistic scenario of how this could be done. Why avoid that discussion? Perhaps because the NIST report writers know that no such scenario can pass the laugh test. Let us reflect on some realities.

To win a presidential election, one of the candidates must take at least 270 of the 535 electoral votes available. While there are over 4000 voting jurisdictions in the US,[183] the crooks know that they will not have to control the computers used by voters in all of those places. Indeed, most states are relatively safe for one or the other political party. Coastal states are likely to give their electoral votes to the Democratic Party, while the Republicans can usually count on receiving the electoral votes of several Midwestern and Southern states. As campaign managers know, the outcome of the contest will be determined by a few battleground, or swing, states.

Suppose that a presidential election is so close that whoever wins just four swing states can win the race. Let us say that Florida, with 29 electoral votes, Ohio, with 18, North Carolina, with 15, and Virginia, with 13 are at issue. Because these are winner-take-all states, the bad guys will just want to change enough votes to win each state's electoral votes.

Of course, online elections would not be conducted monolithically in any US state. The administration of elections is usually divided up among counties, or boroughs, parishes, townships, and independent cities. Many of these political units would have their own website hosting servers, and all would format their own ballots. In Florida there are 67 counties. Ohio has 88 counties. North Carolina has 100 counties. And, The Commonwealth of Virginia is divided into 95 counties and 39 independent cities. The crooks who want to control a presidential election have a lot of work cut out for them.

Suppose further that there are six or seven major companies that provide Internet voting services, and that each has various models of online voting servers. Within each state, there will be a variety of products and services among the political units. These wrongdoers will have to be prepared to adapt their vote changing malware to every different server model there is on the market.

As prudent crooks, they will want to focus on just the number of the most winnable counties in each state needed to secure the necessary electoral votes. So as not to waste their resources and efforts, they will need to know which of the 389 political units are so one-sided for one party that even with a vote changing operation, there is no way they could change enough votes to win. But since there are so many voting jurisdictions to consider, how will the criminals know which ones they are going to be the most likely to succeed in?

Perhaps they had better try to recruit a political scientist or two to advise them of the major swing counties in each of the swing states. Of course, shopping for corrupt political scientists might be even more difficult and risky for the crooks than shopping for corrupt computer scientists was for them in LA County. Just one report to the FBI by an honest political scientist could result in all the conspirators paying lawyer fees, fines, and losing freedom.

At this point in our analysis of the practicalities, it seems that to swing a presidential election there will have to be quite a crowd of co-conspirators involved. Besides political advisors, the bad guys will need a highly skilled malware programmer for each county they need to win. If they decide to attack just 10 select counties in each of the four states, then they will need 40 top notch malware writers to adapt that program to the particular server being used.

Barbara Simons's much publicized frightening vision of a lone hacker in Iran controlling the outcome of a US presidential election seems somewhat off the mark when the political realities are brought into consideration. Even if the Iranian crook were to assemble the team he needs to succeed, how could he do so and still fly under the radar of the FBI, the Department of Homeland Security, and the CIA?

As in the example of LA County, each of the malware writers will have to wait until voting begins to see how the server for that county communicates with voters as they log on, vote, and verify their vote. They will not have to hack the server, but just quickly adapt their malware program to the server in use. All the contingencies that applied in the attack on LA County will apply to each of the 40 attacks required to swing a presidential election.

To build their bot herd, the attackers will have to buy lists of the email addresses for all the registered voters in the 40 counties. While selling such lists is legal, buying them could raise suspicions. The crooks will be praying that the companies selling the lists don't have patriots in them who would report their suspicions to authorities.

Whatever the odds are that the FBI would get wind of the conspiracy in LA County can be multiplied by at least 40 in the case of a presidential election. In other words, all the conspirators would understand that the enterprise upon which they are embarking will be 40 times as risky as was the vote changing project in LA County. The world might not have that many qualified technicians who were also so reckless and foolish.

How could the search for such recruits be conducted in secret? Every person who was offered a part in this plot, even if he turned it down, would risk later arrest as a co-conspirator who abetted the crime, unless he or she immediately informed the authorities of the offer. Co-conspirators who aid and abet a crime by not reporting it risk the same punishments as those who actually commit the crime. The old rule of criminal investigation applies here; that is, the more conspirators there are, the higher are the chances of being detected, caught, prosecuted, imprisoned, etc.

Now, as to the costs: whether forty million dollars, or fifty, or even one hundred million dollars, political campaigns often spend far more than that on presidential elections. But to estimate the likelihood of this crime being attempted, the point is not how much money is needed, but rather how could people who are such talented and worldly entrepreneurs, as to be able to raise amounts like that, be so foolhardy as to do it for so high risk a crime with such an uncertain outcome? Unless one's theory of human nature is based on a Batman movie, the combination of entrepreneurial talent and foolishness required for this crime seem contrary to human nature.

The NIST report fails to speculate as to who in the real world would attempt such a suicidal crime. Would the governments of Russia or China? Would a Mafia organization in one of those countries, or in the US, try it? If detected, the US would surely retaliate with severely damaging economic sanctions. It could insist that every one of its allies stop doing business with the offending nations. All trade with those countries, and all travel to and from them, and even communication, could be halted.

What could a rouge nation gain from such a high risk crime if they succeeded? Would they do it to have a Republican Party foreign policy rather than a Democratic one? Are the risks worth that? Surely, only a government gone as mad as Hitler's Third Reich in the 1930s would even consider such a crime. What could a Mafia hope to gain? Would a presidential candidate promise to call off the Department of Justice Organized Crime Unit if the Mafia wins his election for him? A president who tried that would enrage the nation, and be impeached in a minute by Congress. He might even be tried for treason.

Why would a terrorist group like Al Qaeda try it? Would they join forces with Iran to try and elect a Muslim president? Could that *really* be done “without detection”? Would Americans sit happily on their couches praising the wonders of democracy as a newly elected Ayatollah harangues them on Inauguration Day? Barbara Simons seems to think so. Should the Untied States of America forego the enhancements to our democracy offered by online voting, out of the fear that an Iranian band of religious extremists might try to change some votes?

As we have shown here, the chances of successfully controlling a presidential election are slim for any would-be vote changing attacker. While NIST researchers are paid from US taxes to do their own thinking and scientific research, this NIST report seems to be based more on memos from Avi Rubin and Barbara Simons. No public policy discourse can produce an outcome beneficial to the political system based on this kind of mindless input. Congress and the political science profession, both of which understand the needs of the political system better than any other groups, have extended NIST an unwarranted excess of deference by allowing the NIST 7770 to stand unchallenged. If the demand was made of NIST that it do better than this – surely it could.

2. Voter Authentication

Among its reasons for rejecting Internet voting is that “remote electronic voter authentication is a difficult problem.” There are two major reasons for this problem. One is the condition of voter registration records. Currently, the states are converting their paper based records into digital form.

Section 303 of the 2002 Help America Vote Act (HAVA) requires that each state have a centralized electronic Statewide Voter Registration System.[184] This computerized list will contain the name and registration information of every legally registered voter in the state and assign a unique identifier to each legally registered voter in the state. This voter information must be cross checked with the records in the state’s Department of Motor Vehicles, and all other record keeping state agencies, such as the welfare department, the department of corrections, agencies that keep vital records, and with the national Social Security Administration. Once this task has been completed, Internet voting servers will be able to instantly check a voter’s registration status in the relevant state data base, and the results will be reliable.

The second problem is that it is difficult to know if a person who logs on to vote is really the voter he claims to be. Voter authentication credentials can be lost, stolen, bought or sold, or a voter can be under coercion, and the system server will not be able to know this. But this is a law enforcement problem in every form of election. We have argued above (see Credential Stealing passim) that there is no reason to believe that the threat of multiple voting by a credential thief, is any greater for an online election than in the current practices of absentee voting, or voting by mail. We also showed why the large scale use of stolen credentials is very difficult. Each use requires a time consuming log on, and protections exist against automated voting.

Large scale selling of credentials, like large scale coercion, is an unlikely threat. The more publicly visible the commission of a crime is, the more likely it is to be detected and stopped. Online offers to sell or buy would be spotted instantly by law enforcement. The large scale use of bought credentials is as impractical as it is for stolen credentials. Large scale coercion is not a realistic threat. Suppose the boss, or pastor, demands that all his employees or parishioners vote in his office, so he can see they are voting "right." Everyone is a witness to the crime, and the more victims there are, the more likely it is that one or more will alert authorities. Internet voting does not exacerbate the likelihood or the scale of these possible election crimes beyond that of current vote by mail systems.

3. **Auditability**

The four critics of SERVE wrote, in the SSR, that, DREs "have been widely criticized because they are essentially unauditable. First, there is no way that a voter can verify that the vote recorded inside the machine is the same as the vote that he or she entered and saw displayed on the machine's touch screen." And, "there is no independent audit trail of the votes."[185] Their demand for a voter verified paper audit trail (VVPAT), of course, led to the shelving of SERVE, and generally dooms Internet voting. If the online voter's device printed a VVPAT, it could not be deemed official, since anyone could print out anything at any time, and no one would know if it was the actual vote recorded in the website server. If the web server printed out a vote, no voter would be there to verify it. Ergo; the VVPAT requirement kills Internet voting.

On cue, the NIST report concludes with this discouraging observation (as we quoted above):

> it is not clear that remote electronic absentee voting systems can offer a comparable level of auditability to polling place systems. Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution.[186]

Our examination of these points will show their weaknesses.

NIST 7770 sets up the auditability of "polling place systems" as its standard of excellence. However, lacking thoroughness, if not intellectual honesty, the report says nothing about the known problems of auditing those systems in actual practice. Consider some examples.

Using a paper audit trail, such terms as "hanging chads," "pregnant chads," and merely "dimpled chads" were made known during the well publicized audit of the 2000 vote in Florida. Several audits of the paper ballots were required to settle the disputed Minnesota senatorial election held in November 2008. On first count of 2.9 million votes, incumbent Norm Coleman lost to challenger Al Franken by just over 200 votes. A costly and time consuming recount of the paper audit trail brought that up to 225 as of April, 2009. But Coleman found uncounted votes, and sued for a complete recount. Among the uncounted there were over 12,000 absentee ballots that had been rejected for little errors like a slight change in a signature. These had to be re-examined by the lawyers to determine which votes were properly rejected. They found 351 that had been wrongly rejected. But this re-recount did not help Coleman. Instead, it boosted Al Franken's lead by 87 votes, to a grand total of 312 ahead. Finally, Franken was declared the winner on June 30, 2009 – more than six months after the election, and at the cost of hundreds of thousand of dollars.[187]

The problems of auditing votes on millions of pieces of paper can also include boxes of lost, misplaced, or stolen ballots. Errors in counting, made by bleary eyed clerks, are inevitable, too. Inefficiencies like those in Minnesota and Florida seem to illustrate that auditing paper based systems of voting leave something to be desired. The NIST report is remiss in not explaining why those systems are to be preferred to the well known rapid and accurate electronic counting technology, which has been tried and proven over many years of e-commerce.

The report's conception of "auditability" includes "validating and verifying software on remote electronic voting system servers *and personal computers*." Because these tasks are "difficult," the report gives them as reasons to forego the implementation of Internet voting. But by including "personal computers" as a component of the online voting system to be audited, the report makes another *sub rosa* attempt to doom Internet voting. This ruse assumes that the government is responsible for auditing the integrity of the software on the voter's equipment. NIST's own integrity is questionable for failing to defend this novel theory of election official responsibility. We explained above why we reject that theory as an unneeded government intrusion.

NIST is also disingenuous by claiming, in absolute terms, that there are "no current or proposed technologies offering a viable solution" to the problem of "validating and verifying software on … servers." Independent Testing Agencies (ITAs) can validate that the software on a server is what it is supposed to be by using "mathematical proofs" to test a system's algorithms. This is widely done commercially, and is regularly done by states prior to certifying DREs. It can be done for Internet voting system servers as well. But NIST gives a very flimsy and specious excuse for dismissing this well known technology: "Because of its considerable *cost,* formal verification of software or designs is likely not well-suited to mitigating risks of software defects or vulnerabilities in remote electronic voting systems."[188] Thus, when the report definitively states there is "no … viable solution," to the problem, it really means there is none within what it considers to be an affordable price range for the states. Hence, "cost," not capability, make "formal verification of software … likely not well-suited" to testing the software in online voting servers. But suppose states pooled resources, or Congress allocated testing funds through the EAC? Would that make such testing better "suited"?

Trust

The report also defines "auditability" as the capacity of a system to "provide evidence to auditors that the system functioned in the way it was supposed to. … In addition, the voting system and its supporting election procedures must provide assurances that the evidence provided by the system is trustworthy."[189] The word "trustworthy" is at the heart of the auditability problem. While server technology can be tested for integrity and proper operation, the fundamental issue is whether the humans who are responsible for constructing and operating the online voting system can be trusted to do so honestly and competently.

Indeed, exercising such judgment is precisely what an elected official is elected to do. Our Constitution establishes a system of representative government. Thus, at least in some measure, that document assumes that citizens will trust their representatives to execute their duties with honesty and competence. Frequent and regular elections, plus the powers of impeachment, are ways for the citizenry to remove officials who violate that public trust. But without some measure of trust, representative government would not be possible.

To put a human face on this political theorizing, in 2011, West Virginia Secretary of State, Natalie Tennant, was invited to participate on a panel, which, as we mentioned above, turned out to be very one-sided. She was the only defender of Internet voting, while there were several high profile anti-Internet voting activists on the other side. The issues of trust and official responsibility soon came up. When a panelist demanded to know how her office vetted the companies that provided her state's Internet voting service, she replied that the vendors had to agree to several conditions. One of these was that third party experts be allowed to inspect the equipment and operating codes the vendors used. She said the companies not only agreed to these conditions, but offered to do the whole job for free, as a demonstration project. Given that situation, the Secretary decided not to exercise the right to bring in a third party inspector. She said she trusted the companies.

Another panelist insisted that the vendors could be corrupt and she wouldn't know it. She replied that election officials have to exercise their professional judgment as to when such trust is reasonable. When pressed by the moderator about possible insider wrongdoing as well as software rigging, Ms. Tennant stated that she trusted the workers in her department because it was like a small community in which everyone knew each other. She trusted the system because it used military grade encryption, had an intrusion detection function, and other security checks. She also pointed out that it was a serious felony to tamper with elections, and this law is a part of the security system.[190]

In a large and complex political system like the US, if election officials could not be trusted to carry out their responsibilities well, public elections would risk descending into anarchy, and the entire political order fall into ruin. Imagine the chaos if mobs of "election integrity" enthusiasts demanded to observe and perhaps photograph or film all voters, the voted ballots, and the officials as they sorted through high piles of paper trying to tally the vote. At least since the discovery of agriculture, the division of labor has made modern civilization possible. Having some trust in the other fellow to do his part has made the division of labor possible; for, if everyone felt that he or she could not depend on anyone else, nothing would get done, and humanity would have to live, like primates, as foragers. As Secretary Tennant understood, the formula for Internet voting success, then, is to combine the ancient, and Constitutional, principle of reasonable trust in other people with 21st Century technology. From that, the further advancement of democracy will follow.

Conclusion

Article One, section 4, of the US Constitution states, in part, “The times, places, and manner of holding elections … shall be prescribed in each state by the legislature thereof.” Thus, EAC guidelines for voting technology are voluntary. Every state is free to write its own legislation establishing website based Internet voting for both its overseas and domestic voters. However, as long as the existing irrational taboo on Internet voting is being enforced by strong armed extremists, there is little chance that any state will go it alone. But there is one institution in this country that can expose the irrational bases of that taboo, and thus free the states to choose 21st Century technology without fear of public relations reprisals. If only the election technology division of NIST would fulfill its duties as responsibly as have the other departments of that distinguished agency, the prospects for Internet voting in the USA would be excellent.

[1] Edison was issued U. S. Patent 90,646 on 1 June 1869. Rutgers University http://edison.rutgers.edu/vote.htm

[2] One mention of this idea can be found in, *No More Secondhand God: And Other Writings* R. Buckminster Fuller Southern Illinois University Press. April 1, 1967.

[3] Chu, David S. C. "Expanding the Use of Electronic Voting Technology for UOCAVA Citizens." Federal Voting Assistance Program. May 2007 www.fvap.gov/resources/media/ivas2007.pdf (hereinafter "Chu") page 25. At the time, Chu was the Under Secretary of Defense for Personnel and Readiness.

[4] See http://en.wikipedia.org/wiki/Electronic_voting_in_Canada

[5] "A Threat Analysis on UOCAVA Voting Systems." www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf page 4 (hereinafter "NIST 7551"); Cf. "DoD to Test Online Absentee Voting" by Paul Stone http://www.defenselink.mil/news/newsarticle.aspx?id=42801

[6] Election Assistance Commission "A Survey of Internet Voting" http://www.eac.gov/testing_and_certification/eacs_work_with_military_and_overseas_voting.aspx (hereinafter "EAC"), page 13. The EAC credits the Reform Party with offering online balloting in its 1996 presidential primary, but gives no other information. One announcement made before the Party's convention claimed that the Reform Party's "1.3 million … members will submit their votes for the Reform Party's presidential nominee by computer linkups, telephone, or the U.S. mail." But reports of what actually happened could not be readily found. http://archives.obs-us.com/obs/english/books/yellow/food/reformp1_00.htm

[7] EAC, page 14.

[8] EAC, page 15.

[9] NIST 7551, page 4 f. n21.

[10] NIST 7551, page 4.

[11] EAC, page 34; NIST 7551, page 5.

[12] EAC, page 38.

[13] "Voting Over the Internet Pilot Project Assessment Report." Federal Voting Assistance Program 2001 www.fvap.gov/resources/media/voi.pdf The following paragraph cites page numbers from section four of the Assessment.

[14] Chu, page 11.

[15] Chu, pages 10-11. RE: the similar security measures taken for the 2000 online primary vote in Arizona; see Mohen, Joe and Glidden, Julia. (2001) "The Case for Internet Voting," *Communications of the ACM,* 44:1, pp72-85. Made available to me from one of the authors at: http://www.21cconsultancy.com.

[16] See http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107EEmu4A:e876932

[17] EAC, page 29.

[18] EAC, page 30.

[19] EAC, pages 15-16.

[20] EAC, page 30.

[21] EAC, page 29-30.

[22] EAC, pages 30-31.

[23] EAC, pages 31-32.

[24] EAC, page 32.

[25] Chu, page 12.

[26] EAC, page 30.

[27] EAC, page 32.

[28] For more on SPRG see R. Michael Alvarez and Thad E. Hall, *Electronic Elections.* 2008 Princeton University Press, New Jersey, page 83 passim.

[29] Gillmor, Dan. "Paperless E-voting is a Threat." Computer World. February 9, 2004, "Four members of a team looking into the Internet voting idea became so alarmed at the prospect that they jumped the scheduling gun and issued an early report of their own." http://www.computerworld.com/s/article/89910/Paperless_E_voting_Is_a_Threat
This information probably came from Glenn Flood, DoD/FVAP spokesperson. But Rubin claims that "the FVAP agreed to our terms … to issue an independent report … to the public," page 164, "as a condition of

our [the four] joining the group," page 173. Rubin, Aviel. *Brave New Ballot*. 2006 Morgan Road, New York.

[30] Schwartz, John. "Report Says Internet Voting System Is Too Insecure to Use." New York Times. January 21, 2004 (emphasis added). http://www.nytimes.com/2004/01/21/technology/23CND-INTE.html

[31] Garamone, Jim. "Pentagon Decides Against Internet Voting This Year." February 6, 2004. American Forces Press Service. http://www.defense.gov/news/newsarticle.aspx?id=27362

[32] Schwartz, John. "Online Voting Canceled for Americans Overseas." New York Times. February 6, 2004. http://www.nytimes.com/2004/02/06/us/the-2004-campaign-voting-online-ballots-canceled-for-americans-overseas.html

[33] Actually entitled "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)," January 21, 2004; Dr. David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, Dr. David Wagner http://www.servesecurityreport.org/paper.pdf (hereinafter, "SSR").

[34] SSR, pages 2, 4, 20 emphasis added.

[35] SSR, page 3.

[36] SSR, pages 2 and 20 emphasis added.

[37] SSR, page 14 emphasis added.

[38] SSR, page 2.

[39] SSR, page 2 emphasis added.

[40] SSR, page 2.

[41] SSR page 16 emphasis added.

[42] Popper, Karl. Conjecture and Refutation.

[43] See, http://www.lasvegasweekly.com/news/2012/dec/20/end-night-history-false-armageddons/

[44] SSR, pages 3 and 21.

[45] SSR, pages 3 and 21 emphasis added.

[46] SSR, pages 3 and 21.

[47] SSR, pages 3 and 21.

[48] SSR, pages 3 and 21.

[49] This argument is reminiscent of the US Electoral College. In 2000, for example, Gore won the popular vote, but Bush won the Electoral College vote and became president. (Although transparent, does that make the Electoral College a kind of virus?)

[50] SSR, page 31 emphasis added.

[51] SSR, page 14.

[52] SSR, page 16.

[53] RE: the FBI Elections Division, see http://www.fbi.gov/about-us/investigate/corruption/election-crimes

[54] SSR, page 31.

[55] SSR, page 14.

[56] SSR, page 19.

[57] Chu, ibid, page 12.

[58] SSR, page 19.

[59] SSR, page 19 emphasis added.

[60] SSR, page 19.

[61] SSR, page 20 emphasis added.

[62] SSR, page 20.

[63] SSR, page 18.

[64] Zitter, Kim. "Risky E-Vote System to Expand." Wired. January 26, 2004. "It took Election.com only 45 minutes to fix the problem…" http://www.wired.com/politics/security/news/2004/01/62041?currentPage=all

[65] See Munson, James. "NDP cyber attack a warning to stay away from Internet voting." April 14, 2012 http://www.ipolitics.ca/2012/04/14/ndp-cyber-attack-a-warning-to-stay-away-from-internet-voting-expert/

[66] Elections Canada has petitioned Parliament to allow the agency to make Internet voting available for national elections. EC Official Reports are available on-line at www.elections.ca

[67] EAC, page 40; Cf. Scytl report: "It was one of the most complicated Internet elections ever carried out: 230,749 students from 21 different universities were able to cast votes for 376 simultaneous elections with over 100 parties and 2411 candidates." No attack of any kind was mentioned in this report.

http://www.scytl.com/scytls-technology-successfully-used-in-the-first-binding-internet-election-in-austria/index.html. Also the EAC Survey lists "Projects not included in the Report," at page 13. Here are two factual items missing that favor Internet voting: 1) Gujarat, the largest state in India, held that nation's first election offering Internet voting as an option in 2011. Election officials reported that there were no known security breaches or other problems, and that "we fended off 4,000 attempted hackings from Pakistan, Taiwan and even China." Thus, professionals can conduct successful Internet voting operations even in the most hostile of environments. Ajay, Lakshmi. "Gujarat became the first Indian state to experiment with e-voting this April." Business Standard. July 23, 2011 http://www.business-standard.com/india/news/e-voting-for-it-land/443583/. 2) Based on past successes, the Parliament in Norway decided to continue Internet Voting in 2013. See http://internetvotingforall.blogspot.com/2012/12/norway-to-continue-internet-voting-in.html

[68] See Schwartz, note 30, and SSR, page 7.

[69] SSR, page 7.

[70] SSR, page 12.

[71] Sanger, David et al. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." The New York Times. February 18, 2013 http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=1& Google sought to increase its profits by going into the Chinese market. As a condition, they allowed Chinese engineers to censor searches on democracy and religion. Meanwhile, the engineers were sending all they knew to two Chinese universities, which reversed engineered Google's email security codes. That was not a cold hack, but poetic justice.

[72] New York Times, ibid, February 6, 2004.

[73] Hall and Alvarez, ibid, 2008, page 84f.

[74] Garamone, Jim. "Pentagon Decides Against Internet Voting This Year." American Forces Press Service February 6, 2004. http://www.defense.gov/news/newsarticle.aspx?id=27362

[75] See note 30

[76] Rubin, Avi. *Brave New Ballot.* Morgan Road Books, NY. 2006

[77] See http://ballotpedia.org/wiki/index.php/Help_America_Vote_Act

[78] Rubin Ibid, page 41.

[79] Ibid, page 28.

[80] Ibid, page 28.

[81] Ibid, page 45.

[82] Ibid, page 45.

[83] Ibid, page 45.

[84] Ibid, page 30.

[85] Ibid, page 41.

[86] Ibid, page 41.

[87] Ibid, page 41.

[88] Ibid, page 107. His wife said he "seemed more excited about being on The Daily Show than about getting tenure," page 234.

[89] Ibid, page 104.

[90] Ibid, page 46.

[91] Ibid, page 156.

[92] Ibid, page 156 emphasis added.

[93] Ibid, page 42.

[94] Ibid, page 42.

[95] SCHADE vs. LAMONE. Opinion available in pdf from Michael Shamos at euro.ecom.cmu.edu/people/faculty/mshamos/schade.pdf

[96] Ibid, page 6.

[97] Ibid, page 7.

[98] Ibid, page 7.

[99] Ibid, page 3.

[100] Ibid, page 7; September 2004, no date for the day available.

[101] Rubin, ibid, page 160.

[102] Ibid, page 158.

[103] Ibid, page 158.
[104] Ibid, page 149.
[105] Ibid, page 267. The National Science Foundation seems to have been in harmony with that opinion, because Rubin happily reports that in 2005 his foundation was "funded to the tune of $7.5 million," page 246.
[106] Zetter, Kim. "Risky E-Vote System to Expand," Wired. January 26, 2004. http://www.wired.com/politics/security/news/2004/01/62041?currentPage=all
[107] SSR, ibid, pages 2 and 20.
[108] Hall and Alvarez, ibid, 2008, page 83.
[109] Rubin, ibid, page 165.
[110] Ibid, page 165.
[111] Ibid, page 170.
[112] Ibid, page 170.
[113] Ibid, page 171.
[114] Ibid, page 170.
[115] Ibid, page 171.
[116] Keating, Dan. "Pentagon's Online Voting Program Deemed Too Risky." Washington Post. January 22, 2004. Archived at http://www.votersunite.org/article.asp?id=1061
[117] CNN.com. "Federal remote voting system called flawed" Thursday, January 22, 2004 http://www.cnn.com/2004/TECH/01/21/internet.voting/index.html
[118] Vijayan, Jaikumar. "Panel members find security flaws in Internet voting system." Computer World. January 22, 2004. http://www.computerworld.com/s/article/89290/Panel_members_find_security_flaws_in_Internet_voting_system?taxonomyId=17&pageNumber=1
According to its website, CW receives "over 3 million unique monthly visitors," http://www.computerworld.com/s/pages/about
[119]"The Perils of Online Voting." New York Times. January 23, 2004. http://www.nytimes.com/2004/01/23/opinion/23FRI1.html
[120] Rubin, ibid, page 175.
[121] Schwartz, John. "Who Hacked the Voting System? The Teacher." New York Times. May 3, 2004 http://www.nytimes.com/2004/05/03/technology/03vote.html
[122] NBC News. "Pentagon cancels Internet voting test - Too many concerns about ballot security, official says" May 17, 2004 http://www.nbcnews.com/id/4184803
[123] Weiss, Todd. "Pentagon Drops Web Voting Plans for Military Personnel." Computer World. February 9, 2004 http://www.computerworld.com/s/article/89950/Pentagon_Drops_Web_Voting_Plans_for_Military_Personnel brackets in original.
[124] The use of Internet voting has had more acceptance in the private sector than it has in the public sector. While there were just three uses of the voting technology in 2000 (Republicans in Alaska, Democrats in Arizona, and the VOI – the only true government use), a January 2000 article in Forbes said that Votation.com claims to have already conducted some 600 elections for clients such as the Sierra Club, the Pennsylvania State Employees Credit Union and the California Bar. Einstein, David. "Internet voting: A touchy issue." January 10, 2000 http://www.forbes.com/2000/01/10/feat.html. There has been little formal study of Internet voting in the private sector.
[125] Dismissing the critics of Internet voters as outliers, only a few months before the New York Times published the claims made in the SSR, Alvarez and Hall declared "Everyone knows that an Internet voting system can be built." *Point, Click, and Vote: The Future of Internet Voting.* Thad Hall and R. Michael Alvarez. Brookings Institute, Washington, D.C. 2004, page 146.
[126] See Hall and Alvarez, ibid, 2008, page 92, turnout page 93. Cf. EAC, ibid, pages 22-23.
[127] Ibid, page 97.
[128] Ibid, page 97.
[129] Ibid, page 97.
[130] NIST 7551, ibid, page 6.
[131] Ibid, page 9.

[132] Ibid, page 9.
[133] See the New York Times, http://www.nytimes.com/2005/01/07/international/middleeast/07military.html
[134] See Strips.com http://www.stripes.com/news/u-s-troop-presence-in-afghanistan-at-17-900-and-expected-to-hold-steady-1.21700 7-9-04
[135] "No Time to Vote." The Pew Center http://www.pewcenteronthestates.org/uploadedFiles/NTTV_Report_Web.pdf
[136] Serbu, Jared. "DoD personnel miss out on absentee ballots." Federal News Radio October 28, 2011. http://www.federalnewsradio.com/?nid=239&sid=2610686
[137] See http://ballotpedia.org/wiki/index.php/Military_and_Overseas_Voter_Empowerment_(MOVE)_Act
[138] "Internet Voting, Still in Beta." The New York Times. January 28, 2010 http://www.nytimes.com/2010/01/28/opinion/28thu4.html emphases added.
[139] Urbina, Ian. "States Move to Allow Overseas and Military Voters to Cast Ballots by Internet." The New York Times. May 7, 2010 http://www.nytimes.com/2010/05/09/us/politics/09voting.html
[140] "How to Trust Electronic Voting." The New York Times. June 21, 2009 http://www.nytimes.com/2009/06/22/opinion/22mon2.html
[141] Chen, David. "City Finally Poised to Give Up Lever Voting Machines." The New York Times. January 4, 2010 http://www.nytimes.com/2010/01/04/nyregion/04machines.html
[142] EAC, ibid, page 23.
[143] Sofge, Erik. "Internet Voting in Florida Raises Security Concerns: Geek the Vote." Popular Mechanics. October 22, 2008 http://www.popularmechanics.com/technology/industry/4288327.html]
[144] "A Bad Experiment in Voting." New York Times. September 5, 2008 http://www.nytimes.com/2008/09/05/opinion/05fri2.html
[145] Sofge, ibid; and, EAC, ibid, pages 23-27. And cf. Carol Paquette, "Response to New York Times Editorial." When Ms. Paquette spoke with the Times editor, he demanded to know why Avi Rubin wasn't on the inspection committee. She said he was invited but declined the invitation. http://www.operationbravo.org/Response%20to%20NYT%20Editorial%20Opinion.pdf
[146] Chapman University. "Military Voting Update: A Bleak Picture in 2012." August 27, 2012 PDF available at, http://mvpproject.org/. This apparent failure of the MOVE Act could be another lesson, like slavery and prohibition, that when irrational thinking is the dominant input into the policy making process, bad law is the inevitable output.
[147] Hall and Alvarez, 2008; see Chapter four, Moveon.org and quote from page 70. RE: Common Cause, see http://internetvotingforall.blogspot.com/2012/08/common-cause-caught-using-junk-science.html. Verified Voting is well funded, and intends to stay that way. It was awarded a $300,000 grant from the MacArthur Foundation on April 19, 2012. http://philanthropy.com/article/article-content/131598/. It appears that the money was used wisely: Hasen, Rick. "Verified Voting Hires Lobbying Powerhouse Patton Boggs." http://electionlawblog.org/?p=38991. Henry, Captain Chas U.S. Marine Corps (Retired) "Lots of Bullets, Not Enough Ballots." US Navel Institute. July 2008. The Overseas Voting Foundation received "a $100,000 grant from the Pew Center for the States." http://www.usni.org/magazines/proceedings/story.asp?STORY_ID=1525. And, cf. https://www.overseasvotefoundation.org/alliances-sponsors-and-supporters.
[148] The discussion about Secretary Tennant comes from the West Virginia Secretary of State website at http://www.sos.wv.gov; and http://internetvotingforall.blogspot.com/2011/08/natalie-e-tennant-internet-voting.html; http://internetvotingforall.blogspot.com/2011/11/cyber-bullying-in-connecticut.html; and, http://internetvotingforall.blogspot.com/2012/02/news-hour-internet-voting-story.html. Also see EAC, ibid, page 32f.
[149] See Tennant, Natalie E. "Making the Case for Online Voting." Government Technology. June 29, 2012 http://www.govtech.com/e-government/Making-the-Case-for-Online-Voting.html
[150] See http://internetvotingforall.blogspot.com/2011/11/cyber-bullying-in-connecticut.html. After the private contractors requested a fee for their services, in 2012 the state legislature declined to renew West Virginia's Internet voting program. Reports stated the decision was due to budgetary consraints.
[151] Roberts, Sam. "Parent Voting for School Councils Is Moving Online." The New York Times. March 15, 2009 http://www.nytimes.com/2009/03/15/nyregion/15voting.html

[152] EAC, ibid, page 21; and, http://www.dkosopedia.com/wiki/City_and_County_of_Honolulu_Neighborhood_Board_System

[153] See http://www.scytl.com/eng/news.php

[154] Pictures and full report by the UM hackers at http://www.washingtonpost.com/blogs/mike-debonis/post/dc-vote-hackers-publish-their-vote-hacking-exploits/2012/03/06/gIQArbG4uR_blog.html. Putting his new fame to good use, Professor Halderman went on a mission to India to spread his anti-e-voting gospel. But authorities wisely detained him at the airport, and held his plane while they did the paperwork for deportation. He narrowly avoided deportation by wilily promising to stay in India for tourism only and not for propaganda, or "educational," purposes. Williams, Kaitlin. "U prof. nearly deported from India for research on electronic voting." The Michigan Daily. January 17, 2011 http://tmd.pub.umich.edu/content/university-assistant-professor-nearly-deported-india-research-flaws-indian-electronic-voting

[155] See the National Institute of Standards and Technology website at http://www.nist.gov

[156] HAVA PDF available at http://www.eac.gov/about_the_eac/help_america_vote_act.aspx. TGDC at Section 221f.]

[157] Congress displayed a very clear understanding of the potential of the Internet for enhancing democracy in the US. As to Internet voting, Section 245 required NIST (as the research arm of the EAC) to
(1) … conduct a thorough study of issues and challenges, specifically to include the potential for [online] election fraud, in the Federal, State, and local electoral process.
(2) [Other research to include:]
(A) the appropriate security measures required and minimum standards for certification;
(B) the possible methods … to register voters and enable citizens to vote online, and recommendations concerning statutes and rules to be adopted in order to implement an online or Internet system in the electoral process;
(C) the impact … Internet technology … could have on voter participation rates, voter education, public accessibility, potential external influences during the elections process, voter privacy and anonymity, and other issues related to the conduct and administration of elections;
(D) whether … public availability of candidate information and citizen communication with candidates, could benefit from the increased use of online or Internet technologies;
(F) the implementation cost of an online or Internet voting or voter registration system;
(I) the impact of technology on the speed, timeliness, and accuracy of vote counts in Federal, State, and local elections.

[158] "Security Considerations for Remote Electronic UOCAVA Voting," available at http://www.nist.gov/itl/vote/nistir-7770.cfm (Hereinafter NIST 7770)

[159] Listed in NIST 7770, ibid, at page 59. Another outrage that both the SSR and NIST 7770 warn of, and which will shock the democratic conscience in members of Congress, and of the various state legislatures, is the potential for online "vote swapping." First stated in the SSR, at pages 10-11, and repeated, of course, in NIST 7770, at page 18.

[160] SSR, ibid, "The vulnerabilities we describe … are fundamental in the architecture of the Internet and of the PC hardware and software that is ubiquitous today. They cannot all be eliminated for the foreseeable future without some unforeseen radical breakthrough. It is quite possible that they will not be eliminated without a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet," pages 2-3

[161] "Risky E-Vote System to Expand," Kim Zetter, Wired 01-26-04 http://www.wired.com/politics/security/news/2004/01/62041?currentPage=all emphasis added.

[162] NIST 7770, ibid, page 12.

[163] Ibid, page 14.

[164] Ibid, page 14.

[165] Ibid, page 17.

[166] Ibid, page 29.

[167] Ibid, pages 52-53.

[168] Ibid, 50f.

[169] For example, Aristotle, Inc has a "nationwide voter file of over 165 million registered voters," http://www.aristotle.com/

[170] See http://lacounty.gov

[171] "Vote Fraud in Florida." http://ballotpedia.org/wiki/index.php/Vote_fraud_in_Florida
[172] NIST 7770, ibid, page 51.
[173] Ibid, page 23.
[174] SSR, ibid, pages 2, 13, 20.
[175] NIST 7770, ibid, page 29.
[176] Ibid, page 37.
[177] Ibid, page 19.
[178] Search "botnets" at www.fbi.gov; also see http://blog.fireeye.com/research/2012/06/stories-about-botnets-part-1.html
[179] This discussion draws its factual data from, Statement of Vote, November 6, 2012, General Election, California Secretary of State Debra Bowen, www.sos.ca.gov/elections/sov/2012-general/
[180] To see how little election fraud there actually is in the US, search "election fraud" at The Brennan Center for Justice at http://www.brennancenter.org/; and see Hall and Alvarez (eds), *Election Fraud*, Brookings Institute, NY 2008
[181] SSR, ibid, pages 2 and 20.
[182] NIST 7770, ibid, page 37.
[183] The EAC estimates that there could be up "to 10,000 depending on the how the reporting unit is defined. [It had] a jurisdictional count of 4,678 in 2010." See http://www.eac.gov/research/election_administration_and_voting_survey_faqs.aspx
[184] See note 154, and http://ballotpedia.org/wiki/index.php/Help_America_Vote_Act#SVRS-Statewide_Voter_Registration_System.
[185] SSR, ibid, page 9.
[186] See note 157.
[187] "Court Rules Franken has Won." The New York Times. June 30, 2009 http://thecaucus.blogs.nytimes.com/2009/06/30/court-rules-franken-has-won-senate-seat/?scp=3&sq=Al%20Franken%20wins&st=Search; more at http://www.nytimes.com/2009/01/20/us/politics/20minnesota.html?_r=1&fta=y
[188] NIST 7770, ibid, page 34.
[189] Ibid, page 24.
[190] See http://internetvotingforall.blogspot.com/2011/11/cyber-bullying-in-connecticut.html