Internet Voting: Structural Governance Principles for Election Cyber Security in Democratic Nations

Candice Hoke
School of Law
Cleveland State University
Cleveland, OH, USA
shoke@me.com

ABSTRACT

In Europe, the U.S., and Asia, political and market forces seek expanded use of the Internet for voting and election administrative functions. Governmental responses have differed, but commonly governments omit qualified computer security experts from exercising decisive weight in policy decisions. Given its current architecture and engineering, however, the Internet generally provides neither high assurance data security and integrity, nor reliable information transmission protected from denial of service and other attacks. Nevertheless, pressures to expand Internet-based election functions have intensified. This paper explores the foundational questions and features of a governance system that has the capacity to safeguard democratic elections where Internet-facing technologies will be deployed. The paper recommends that each nation include a policy board with appropriate computer and network security expertise, election administrative knowledge, and public accountability and transparency structures that mandate end-to-end auditability. It further recommends that the national regulatory apparatus not rely predominantly on issuance of rules and technical standards to be met, or particular product design. Owing to dynamic cyber threat environments, the board—whose majority should consist of computer and network security professionals—should issue particularized decisions. They should assess whether an election office proposal for using Internet transmissions for a specified election task is prudent in light of all factors relevant to security based on layered defense. Democratic nations should collaborate in alerting one other to election information system threats and attacks, for mutual aid and maximally robust mitigations.

Keywords

Internet, voting, elections, governance, transparency, security, assurance, integrity, cybersecurity, mitigations, threats

This paper was presented at ISGIG 2009.

GTIP 2010 Dec. 7, 2010, Austin, Texas USA

1. INTRODUCTION

The citizens of democratic republics select their core representatives through periodic public elections. While the specific governmental offices subject to election and the frequency of conducting elections vary among nation-states, a change in elected governmental officers often affects business opportunities, individual and business wealth, the use of military power, and a broad range of other governmental policies. A national election in the most populous nations worldwide often affects vast wealth and the course of domestic and international events.

The potentially high stakes of elections, and the history of intentional electoral disruptions and fraud in numerous countries worldwide, counsel governmental officials to engage in careful planning in order to protect election information and processes from deliberate attacks. Security and contingency planning for elections differs among and within nations, with some significant variations in both the physical contexts for conducting elections and in human factors such as poll staffing. For those nations that use electronic voting technologies, election security has become increasingly comp licated.

The paper proceeds from the baseline premise that the Internet as currently architected and engineered provides neither high assurance data security and integrity, nor information transmission reliably impervious to deliberate targeted attacks and ubiquitous malware. While these factors pose dangers for many entities and activities, public governmental elections are especially vulnerable. That voting occurs using anonymized data presents major hurdles to utilizing the Internet in a secure manner for casting ballots, though careful analysis and appropriate mitigations might permit other election tasks to be securely conducted.

Despite the security community's broad agreement on Internet risks and available mitigations, and the essential role security plays in whether other electoral goals can be met—specifically voter access and the accuracy of the count—these scientific perspectives have largely been diluted by the decisional structures for election policy The paper argues that election policy decisions are affected by an information gap regarding both Internet security risks and the absence of effective mitigations and controls that can achieve assured election data and system integrity. It recommends revised national governance structures based on four fun-

damental principles: **expertise** (in computer and network engineering and security, and in election administration); **transparency and public accountability**, including end-to-end auditability (in order that the election system and reported results have legitimacy and be worthy of public trust); particularized decision making based on defense in depth and other security assessments (so that secure voting technology is not undermined by situational factors), and **transnational cooperation** among democratic republics (to facilitate prompt mitigations and criminal prosecutions of electoral cybercrime).

2. PERVASIVE AND INCREASING ELECTORAL USE OF INTERNET TECHNOLOGIES

The pace of election administrative computerization appears to be rapidly increasing. In the wake of the notorious U.S. presidential election of 2000, passage of the Help America Vote Act [1] stimulated vast computerization of elections. The Act has spurred not only of electronic voting machines but also an array of new options in computer-based and networked equipment. In other nations, both market and "modernization" pressures have led to wide use of computers for election functions. Manufacturers of business automation systems have accelerated development of product adaptations for elections. Many European and Asian nations have joined the U.S. in using or planning transitions to electronic voting devices, tabulation systems, and a broad range of other equipment.

Electronic equipment is now available that permits automation of most election functions, ranging from the creation of voter registration lists to the presentation of an electronic ballot to voters, to recording votes, and to tabulation and reporting election results. Electronic databases often substitute for paper-based systems for retaining the lists of eligible voters and their personal information such as address, birth date, unique identifying number, and political party. Voters may register to vote by visiting a website or by sending a registration document by email attachment or fax. Software is increasingly used to design ballots, including automating the task of rotating candidates into the favored top position on different ballots so no one candidate holds that advantage. Many voting machines use electronic ballots that humans have created on servers using complex election management software.

Electronic voting devices may offer voters the option of ballot error correction where the ballot contains marks for too many candidates in a race ("overvoting"). Vote data may be recorded on removable digital memory media as well as on internal components such as flash memory in order to produce "redundant" vote data records.[1] Voting devices may incorporate hardware and firmware for network transmission of election information, including for sending vote data electronically from remote polling locations. These transmissions may occur using any of a variety of digital transmissions (e.g., the Internet, T1, common telephone lines, satellite) instead of physically transporting memory devices (e.g., thumb drives and memory cards). From security and data integrity standpoints, however, arguably the most problematic electronic voting initiatives are efforts to permit remote voting from personal computers that use operating systems documented to have serious security flaws. These deficiencies are then compounded by the security issues of current Internet architecture. [2]

[1]Independent "red team" or penetration studies of voting systems have demonstrated that the supposed redundant memory systems may be subject to deliberate attacks that can cause the various locations to hold discrepant rather than redundant vote totals. [6], [7].

2.1 Supporting Voters with Internet-Facing Technologies

When the voter will be physically absent on Election Day, many jurisdictions allow voters to file an advance request or application for permission to vote an "absentee" ballot. Others permit "no-fault" or convenience voting from home, regardless of the reason. Until recently, when filing such requests, jurisdictions often required voters to file via paper documents sent through traditional mails or delivered by hand. Depending on the jurisdiction, technological options for filing absentee applications may include applying at a website, by email, by fax, or by telephone.

Electronic automation processes have also been adapted for the voter authentication steps in absentee ballot processing. Originally developed for financial institutions that process bank cheques, by using a digital or optical scanner connected to a computer, these systems compare the voter's two signatures as part of the voter and ballot verification process. High volume urban election offices have often been first to adopt this technology. The machines must be calibrated, however, allowing discretionary human decision in the degree of deviation between the signatures on record and the absentee ballot materials.

Greater speed, fewer administrative costs and barriers, and higher voter convenience are often mentioned as justifications for deploying Internet-facing systems for processing absentee ballot requests. By 2009, a number of U.S. election offices had been using the Internet to transmit a blank ballot to the absent overseas voter. The most aggressive pressures in the U.S., however, can be traced to efforts to ensure that those in overseas military service are not inadvertently disenfranchised by delays in ballot transmissions. [3], [4] Congress's passage of the MOVE Act, [39] illustrates this trend by requiring State governments to provide overseas voters electronic registration services, absentee ballot applications, and blank ballots, should the voters prefer these technologies over hard copy mailings. [40] In the U.S., a 2008 pilot project in Okaloosa, Florida [5] used hardened kiosks while other States have experimented with emailed and faxed ballots. [51]

A number of nations ranging from Estonia [4] to Canada [49] to France [50] have experimented with casting ballots—voting in an actual election—on a website described as "secure." Typically voting occurs by using an encrypted emailed ballot or by using telephones and telephonic networks. These options theoretically permit almost instantaneous delivery of both balloting materials and the return voted ballots to the absentee voter in remote locations, shortening the transmission time by over 98% from that required by traditional mailing of paper.

2.2 Other Electronic Networks

Networks used within the elections process may encompass more than the Internet, however. Some tabulation systems and transmissions of ballot tallies may depend upon

complex internal data networks involving wireless or wired components. These internal devices or networks may also be linked to T1 lines or other external networks.

2.3 Additional Electoral Uses of the Internet

Increasingly, election offices in the U.S utilize the Internet for a broad range of tasks that formerly were handled manually or through traditional mails. Like other software manufacturers, election vendors may choose to send election "management" software patches over the Internet for uploading into the local election servers. These software systems would normally be classified as mission-critical, as they are deployed for the core functions of ballot configuration and for tabulations and reporting of vote totals.

Vendors may also send software patches via the Internet for updating the voter registration databases. Depending upon brand and configuration, the functionality of electronic poll-books may be dependent upon the Internet, for it is the means by which the poll workers connect to the voter registration database in order to verify the voter's eligibility to vote.

Ballot proofing may also occur via the Internet, with jurisdictions posting copies of electronic ballots that will be used for electronic voting machines and for printing paper ballots. These posts provide access by political parties and the candidates for proofing the ballots. If paper ballots are to be ordered, the jurisdiction may transmit the ballot styles and configurations over the Internet to the ballot printer so the printing order may be filled.

Intermediate and final electoral tallies produced by election management software from raw database values are often uploaded to the Internet for public access. Posting these totals may occur via network connectivity or memory media such as thumb or flash drives.

2.4 Disaggregating Election Tasks for Security Assessments

Established precepts of information security assessment direct that each task or function to be conducted using computer or network technologies must be separately evaluated in a threat assessment. [19], [20] Such disaggregation may result in identifying election administrative tasks to which the Internet presents low risks and compensating efficiencies. Examples include the Internet posting of voter information regarding the candidates, ballot issues, and location and timing of voting. Web-based additional "voter services," such as the posting of absentee ballot applications and voter registration forms, are also potentially low-risk. In a dynamically changing risk environment, however, even arguably low-risk functions may become high value targets. [52]

3. THE ELECTION EQUIPMENT MARKETPLACE MEETS INTERNET SECURITY SCIENCE

In both private and public sectors, cybercrime has become sufficiently costly that security has become a primary focus for information system administrators in financial institutions and other businesses. [42], [43], [45], [47] The popular press has covered major intrusions into supposedly "secure" networks that have compromised credit card and other personal financial data, telephone billing records, and the U.S. government's witness protection program. These reports underscore that the Internet generates significant vulnerabilities at the same time as benign opportunities for unprecedented communication. [21] Current Internet, PC and software engineering cumulatively have neglected risks to personal privacy, intellectual property, and financial security, and more, which the technologies have placed in grave jeopardy. [16], [17], [22] [23] [24] To manage these risks, the firm or enterprise an Information Technology (IT) security governance decisions must include types of access controls, authentication systems, and planning for life cycle security.

In market-based nations, private sector, for-profit firms design, manufacture, and market specialized software and hardware components for election administration. Many of these firms have been shown to overstate their voting system products' compliance with fundamental tenets of an IT security program and misrepresent the scope of on-site practices and protocols needed to achieve defense in depth.[2] In independent studies, computer and security scientists have documented profound risks to election data integrity and equipment reliability owing to insecure equipment and flawed managerial security policies. [6], [7], [11], [12], [13], [14], [15].

Internet-based software systems for voter authentication, blank ballot delivery and return of votes or "voted ballots" are no longer fanciful speculations. In May 2009, one Internet voting marketing executive argued:

> The introduction of technology to any process is scary. But the time has come. We have been banking online and shopping online for over a decade, and conducting important business by phone for a century. *Digital technology, while no panacea, is the best method ever invented for securely delivering information and decisions.* [25]

For over a decade, for profit vendors have promoted their new wares for "secure" Internet voting, replete with resuscitation of the false but previously persuasive analogy of voting to banking via automatic tellers and personal computers. Newer Internet voting vendors, including Scytl [41] and Everyone Counts, have followed suit, actively solicit election officials and legislators to purchase their software products.

3.1 Vendor Claims

An example from international vendor Scytl's marketing presentation reflects some major claims of Internet voting vendors. Internet voting:

> the potential to increase voter turnout rates ... offers many advantages over the conventional paper-based electoral systems, including mobility and convenience for voters, greater speed and accuracy in the counting process, prevention of involuntary voting errors, better accessibility, lower costs, support of multiple languages, greater flexibility, etc. ... [It] guarantees the same level of

[2]Documentation reviews of three commercially produced voting systems formed a part of the California Secretary of State's Top to Bottom Review of Voting Systems. All evaluators reported critical omissions in security documentation and risk mitigation.[8],[9],[10]. Principles for achieving defense in depth in election information systems are not qualitatively different from those established for IT systems for other facing significant threats. [6]

> trust, security and privacy that exist in conventional paper-based elections without having to trust either the administrators of the system or the complex technological systems used. [41]

Elaborating on these claims, vendor literature has claimed a net reduction of the financial costs of conducting elections; an increase in voter participation by making voting more convenient and accessible; has features rendering it as secure and private as personal banking transactions; and, emblematic of social and technological progress, of updating archaic systems to accommodate youthful tastes and expectations (the "cool" factor).

3.2 Two Empirical Baselines

In considering the fitness of the Internet for conducting particular election administrative tasks, and the wisdom of permitting a *caveat emptor* market for Internet voting software in lieu of governmental regulation, two constellations of empirical fact should be kept in view. First, despite the contrary vendors' representations, the profound security deficiencies independent researchers have documented pervading for-profit digital voting equipment[3] undermine the credibility of election vendors' claiming Internet voting products "securely" deliver voted ballots and voting materials over the Internet. Within the voting tech industry, "secure," "private" and "reliable" are self-defined marketing terms rather than reflecting a regulatory standard whose satisfaction must be proven to an independent body. In short, the electronic elections manufacturers have established an industry standard of security that grossly misrepresents the systems' achievements. [8], [9], [10], [11], [13].

The second but perhaps more significant empirical baseline relates to the InternetÕs technical and engineering facts. The Internet lacks the capacity for high assurance information transmission, whether for elections functions, military communications, or other transactions. Specific election objectives include packet transmissions that cannot be delayed, blocked, or modified, because otherwise voter disenfranchisement and possibly a fraudulent election may ensue. [2] Election-related websites, for instance, that are designed for distributing voter information, for enabling voter registration, or for casting ballots, continue to be vulnerable to malware, denial-of-service (DOS) and distributed DOS attacks. [48] By underestimating the volume demands for website access in a major election, election outcomes may be gamed, undermining the election's legitimacy. [52] Mitigations that reduce these Internet-based threats to minute levels of potential impact are not available or foreseeable in the near future.

3.3 Private Vendors, Market Pressures and the Internet Security Information Gap

Without computer security training, policymakers empowered to decide which election functions to automate using Internet-facing IT systems may well lack sufficient knowledge to evaluate the types and impacts of risks that are endemic to such systems, and the types of ancillary staffing, equipment, protocols and training programs that are essential to ongoing security. [15] At least eight core insights are needed by those vested with decisional power concerning when and how the Internet shall be used in election functions.

- **Pervasive software coding deficiencies and their election consequences**. Coding deficiencies have been identified to pose grave security consequences for all IT systems. [16], [17], [18] These coding errors and "bugs" open election software to easy, high impact attacks on election systems and data that may easily escape detection and redress, but the errors can also lead to data inaccuracies and machine unreliability having no basis in deliberate attack.

- **Internet transmitted malware**. Worms, viruses and other ubiquitous malware can impair or completely vitiate election software and hardware functionality.

- **Options to manipulate data speed**. Strategically timed high Internet data volume can cause speed of transmissions to fall precipitously, and thus delay timely transmissions, potentially causing vast numbers of ballots to arrive late.

- **Labeling election technology products and websites as "Secure" and "Reliable"**. In contrast to the labeling requirements for prescription drugs, many food products, and toxic chemicals, governments have generally not restricted voting system vendors from using these quasi-scientific, psychologically seductive terms in their marketing literature and presentations. Even though the terms deceptively suggest compliance with accepted standards for security, governments have permitted their use.

- **Re-transmitters access and consequences for information privacy and security**. Unless security-protective protocols and supervision are used, third-party packet re-transmission sites such as ISPs may permit some ISP employees unfettered access to read electronic message contents. This intrusion does not require sophisticated technical abilities or equipment, but only a text viewer or word processing program. The fundamental insecurity of these transmissions means that email forgery or modification, identity theft, and business transaction interceptions are becoming major types of criminal fraud. Voter privacy is illusory. The SERVE Report continues to stand as a comprehensive typology of Internet voting threat genre, most of which are insoluble with current architecture and engineering. [2]

- **Encryption options do not suffice**. Data encryption is not a complete or effective mitigation for most threats that Internet information transmissions pose for elections. [2] Although encrypted vote data may pose insurmountable barriers against attempts to modify that data, strategies can still be deployed to block encrypted transmissions from reaching their destination. Additionally, unless data is properly encrypted—a step that technically untrained individuals might botch—the encryption effort may be nullified.

[3] In the "red team" overview report on California voting systems, Dr. Matt Bishop stated: "the security mechanisms provided for all systems were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results." [6] With only minor differences, these same systems are used in many other States.

- **Concealed, untraceable attacks may accord the false appearance of information security**. Attacks that disrupt election processes, or result in fraudulent election totals, may be completely hidden and untraceable. [2]
- **Security mitigations and Internet re-engineering solutions that will achieve high assurance are not imminent**. Funding entities such as the U.S. National Science Foundation are underwriting major research efforts to re-envision the Internet. [26] As a result of this multi-faceted research, potentially radical revisions to Internet architecture, engineering, and communication protocols may occur. The transformations may, for instance, include multiple "Internets" with controlled network access and other enhanced technical security features. But these will not be available in the near future, and probably not for more than a decade.

3.4 Security in a Dynamic Electoral World

Even if high assurance security architecture and engineering is generated that is largely impervious to the then-current Internet, the risk environment is not static nor merely a technical property of a IT system. Computer security science teaches that these do not comprise the entirety of factors relevant to evaluating information security risks. Computer and network security are not an output of merely technological attributes. Rather, physical security (such as locks on doors and surveillance cameras), staff expertise, staff continuing education and values commitment to security compliance, and other factors play as significant a role in the security quotient as the technological features. [6], [44] Further, the physical, managerial, and staffing contexts within which the election technologies are deployed will not be static. Thus, threat analysis and policy formation must occur in a dynamic manner, a task that an effective elections cybersecurity agency should undertake.

Computer security principles and their relation to other core election values remain misunderstood, however. Yet in an electronic electoral world, both voter participation and election result accuracy depend on security features. In this manner, security can be understood as a precondition for other core election values.

4. A GOVERNANCE SYSTEM FOR INTERNET-BASED ELECTION TASKS?

Unquestionably, the Internet offers profound democratization and communicative benefits that should not be impeded[4] without a sound basis in other fundamental democratic elections values. The Internet need not be placed off-limits to deployment in elections. However, the rapid commercialization of the Internet and World Wide Web in ways incompatible with individual and the larger public interest raises concerns that election processes could be similarly skewed. As Peter Neumann and others have noted, such incompatibilities have surfaced in domain name policy, spam, security, encryption, freedom of speech issues, privacy, content rating and filtering, intellectual property and copyright issues, and many other areas. [24], [25] The governance systems that determine how to use the Internet in election administration must have the capacity to evaluate the risks soberly without becoming enmeshed in overly rosy technological utopianism or subject to regulatory capture by for-profit vendors. The structure should require, and the governance culture embrace, the duty to protect the integrity of elections processes.

The proposal outlined here recommends a national regulatory apparatus that will not rely predominantly on issuance of rules and technical standards to be met, or particular product design. Rather, it should review and issue particularized decisions on whether an election office proposal for using Internet transmissions for a specified election task is permissible in light of all factors relevant to security based on layered defense. Thus, governance personnel would need to remain abreast of technical and security developments, and obtain information on staff education and security physical contexts, in order to decide the question before it.

The analogue in the Anglo-American legal system would be courts of chancery, where equitable review employed principles to guide wise decisions in light of all the facts, rather than use mandatory common law precedents to compel certain outcomes.

Recognizing that information security is one objective among many, the agency will need to be structured to maintain personnel with election administrative knowledge and not only those with technical and security training. The range of expertise would facilitate balancing the competing objectives of speed of transmission, low administrative costs; auditability; reliability; environmental impact; and voter convenience/access as against data security.

4.1 Regulatory Scope and Definitions

Elections cybersecurity[5]recognizes that the election information systems hold valuable information that both outsiders and insiders may seek to compromise.

The underlying policy objectives are to prevent or to neutralize potential negative consequences for voters and the election process because computers, networks, and information technology systems transmissions were used. The negative impact to be avoided may arise from deliberate attack, such as disruptions of electoral processes via DOS or viral attacks, and undesired intrusions that can produce fraudulent election records, such as by malware or unauthorized access to databases for manipulating voter registries or vote totals. Election cybersecurity also seeks to protect the personal and other data held within the election administrative system, where unauthorized access can lead to identity theft.

Increasingly, courts and commentators are urging that election law include as fundamental rights principles of transparency and public accountability for election processes. [29], [30] Germany's high court invalidated certain uses of computers in elections, resting its decision on the core require-

[4]Michael Froomkin reviews strategies for achieving the communicative and democratizing opportunities the Internet offers as a part of his overall assessment of Internet governance structures. [21]

[5]"*Election cybersecurity*" encompasses the objectives of information and system security, reliability, and data integrity with regard to the computers and networks used to record, process, and report election-related information at all points in the electoral process. The term encompasses all electronic and electromagnetic communications including telephony, fax, and Internet, in each case inclusive of wired and wireless, analog and digital systems. The term reflects one facet of the more comprehensive systemic governmental duty to achieve election integrity.

ment of election transparency to the public. The Court emphasized the "principle of the public ... which prescribes that all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception." [30] In the Court's view, the voters themselves must be able to understand without detailed knowledge of computer technology whether their votes cast are recorded in an unadulterated manner as the basis of vote counting, or at any rate as the basis of a later recount. If the election result is determined through computer-controlled processing of the votes stored in an electronic memory, it is not sufficient if merely the result of the calculation process carried out in the voting machine can be taken note of by means of a summarizing printout or an electronic display.

Translating the core principles for trustworthy elections into computer security terminology, in demonstrable ways elections must maintain data integrity at all points in the process; assure the availability of systems for voters to register and to cast valid ballots that will be counted; and, provide accountability systems such as random auditing that will provide public transparency and equipment checks. Election technology security and auditing features can be designed to achieve each of these objectives, but often software vendors do not invest in developing effective security. As one computer security commentator has noted, "the buying public has no way to differentiate real security from bad security." [18] A better regulatory apparatus can facilitate product development that meets higher standards of software security in the elections arena, without the need for expanding use of product liability lawsuits for defective software products.

4.2 Recommendations for the Elections Cybersecurity Regulatory Structure and Powers

4.2.1 Dynamic Decisionmaking

At least two divergent approaches potentially offer sufficient protection for mission critical election information security systems: (1) An aggressive, bright line approach: codification of a legal barrier to any use of digital equipment, of equipment that depends on software and networks, for any mission critical election task within the electoral jurisdiction; or (2) creation or revision of a regulatory apparatus that reviews applications and can authorize election administration to use digital equipment and networks for some election tasks under specified conditions.

While a complete barrier might appear to provide the most substantial election cybersecurity protection, its rigidity and overbreadth would likely render it a controversial and potentially unstable policy approach. It would also invalidate many current practices without any review of the alternatives and their risk factors. Given that risks and technological options change over time, a more dynamic regulatory approach would be more prudent.

An alternative is for the law to invest the regulatory entity (hereafter termed Board) with conducting sophisticated security assessments in light of all relevant factors known when the application is reviewed. This approach would be more consistent with the dynamism of the technologies and risk environments, allow review of the applicantÕs most recent record on security policies implementation, and other facts.

4.2.2 National Supervisory Authority

Where the government must capably respond to external threats that are dynamic rather than static and that present threats at a nationwide scale, it is appropriate for the regulatory entity to be positioned at the national level. Economies of scale and access to the best expertise in the nation can be achieved. Given cybersecurity's dynamic set of serious threats, it is unrealistic to expect that local and Provincial/State governmental authorities will have the resources, the expertise, and the political will to invest in oversight of elections cybersecurity issues.

4.2.3 Structure and Staffing

A regulatory structure that can balance the need for diverse political involvement and public accountability with the need to utilize appropriate expertise is an independent Board with a professional staff. A statute could allocate to national legislative and executive leaders the power of appointment. Nominations of technical and security professionals could be allocated to qualified professional organizations as an extra assurance for appropriate expertise. Legislative leaders of varying major parties could be vested with power to appoint without a nominating intermediary experienced election administrators and public interest advocates on election transparency, privacy and security issues.

Professional associations having expertise in the requisite areas, such as the ACM and the IEEE, could be vested with the power to nominate a short list of experts with statutorily specified credentials.[6] The law could name a high official (e.g., President or Prime Minister) to review nominees and appoint them to office for a specified term of office. Avoiding service at the pleasure of the appointing officials would help to ensure that the Board's decisions are evidence-based and not a matter of political influence.

The BoardÕs cybersecurity work would require a professional staff. In some nations including the U.S., elections administrative processes have often been staffed with political patronage appointees who sometimes lacked the skill set and knowledge base needed to run administratively competent and secure elections. A national elections cybersecurity Board can provide a counterbalance. The permanent staffing expertise could be specified by statute and direct:

- Significant technical expertise be present (including network security, computer security, secure database and database management expertise, software development and testing; IT auditing and computer/voting system forensics);
- Significant election administration expertise, preferably having experience in computer-based election technologies and a record of achievement in implementing election security best practices, achieving a security culture, and establishing effective auditing and accountability systems;
- The Board and staff to engage election officials "in the field"—in their election offices and on-site in actual elections—and with States' chief election officers

[6] If international professional organizations such as the ACM, IEEE, and ISACA were each to develop the capacity for national divisions within specialized expertise, lodging nominating powers there might be less controversial.

to promote informational interchanges about the complexities and risks presented by election technologies and their possible mitigations

- Board and staff executives have both information systems and security expertise plus election administrative experience;

- Satisfaction of high personal and professional ethics standards, which would include a strong conflicts of interest policy, and barriers to the revolving door (moving from the regulated entity to a job with the regulated.

4.2.4 Sophisticated, Nuanced Cybersecurity Assessments

While renowned computer and network security experts appear to agree that security is a series of complicated tradeoffs, [6], [23], [34] not an abstract property of equipment or systems, structuring a regulatory agency to undertake informed, nuanced and voter-protective cybersecurity evaluations is qualitatively different task than training individuals in these skills. Regulatory entities are often subject to political appointee leadership who might lack critical knowledge or capacities for sound judgment. The regulated firms often seek and sometimes achieve "regulatory capture." Flawed personnel decisions can vitiate a sound structural approach that is designed to achieve the nuanced decisions needed for national and election security-sensitive policies.

Despite the risks that the regulatory entity may not be staffed or structured well, the status quo presents too many risks for its continuation. By combining explicit requirements for expertise and public accountability, the regulatory framework may enhance the likelihood that nuanced, sound judgments will issue.

Given that effective computer security is virtually never strictly a property of technical equipment but rather a function of the interaction of people (including security training and practices), equipment features (such as avoidance of software coding errors known to introduce vectors for attack) and physical circumstances (including physical security, such as locks and video surveillance), regulatory systems dedicated to achieving high information and information system security cannot evaluate only the equipment's technical features. In the U.S., for instance, the Voluntary Voting System Guidelines and accompanying federal lab testing program commits precisely this error, among many others. [33] Highly laudable technical and network security features can be negated by human errors and omissions. Conversely, poorly designed software and other technical security deficiencies can be somewhat mitigated by security practices including staff compliance assessments. [6] "Layered defense" security principles prescribe multiple levels and types of security mechanisms, to force an attacker to breach several rather than only one to compromise the system. The Board should be charged to evaluate all defensive layers when determining the acceptability of a proposed use of the Internet in election functions.

4.2.5 Initial Decisions and Burden of Proof

The Board will face threshold decisions concerning which election administrative or voting tasks that are currently using the Internet can continue to do so and under what conditions. The Help America Vote Act of 2002, [35] by contrast, in some respects appears to assume that all election related activities can be securely conducted over the Internet—a seriously flawed assumption—yet in others states an empirically "clean rule" governing numbers of permitted DREs. [36] [2] The law should impose the burden on proof that the on the applicant for permission to utilize the Internet, with a required showing that risks to election data security and integrity are highly remote and very low in potential impact. The risk of nonpersuasion would thereby be legally reposed in the applicant.

Another structural mechanism by which to protect the voting public and election integrity could be to require a specified supermajority of Board members, for instance, 75% or 85% of the members, to approve any proposed elections use of the Internet as sufficiently secure.

4.2.6 Specific Powers and Duties

The Board should be vested with broader statutory authority to protect election security and integrity, including for instance:

- The authority to identify election practices and procedures, such as connecting an election tabulation server to the Internet, or re-connect that present grave security threats, and have the power to require cessation of the practice.

- The power to issue binding technical, operational, and other minimum standards for each discrete election function that is permitted to be conducted over the Internet or other networks, and to bar functions if network involvement presents significant risks to the security, reliability, ballot secrecy, and accuracy of elections.

If a bright line statutory barrier to Internet delivery of voted ballots should be contemplated instead of vesting the power in the Board, three major arguments will be raised that these questions should be subject to a more nuanced agency decision making process. First, in those nations that maintain a two-stage election tally process, where preliminary or unofficial vote tallies are followed by more a more careful thorough canvass (often known as the official or certified results), the claim will be that any intrusion into networked tallies and transmissions of voted ballots can be corrected at the official count. Thus, use of networked communications should not be off limits for transmitting preliminary tallies and voted ballots.

Second, arguments will be lodged that where Internet communications are permitted to be used for delivery of voted ballots and vote tallies, whether for unofficial or official tallying, rigorous auditing will deter attacks and also permit correction of tallies if attacks should occur. While rigorous auditing indeed should be mandatory, its limits must be recognized. While auditing is a commonplace in government and business financial matters, auditing elections remains quite novel with nascent professional standards and protocols. When pressed to audit elections, governments often claim to "audit" without using, for instance, random sampling procedures, auditing every contest, or using statistical auditing models that provide a 98% degree of confidence that the audited races' results were correctly reported. Post-election auditing cannot function as a reliable check on networked election communications as through the Internet, nor can it recover blocked or tampered ballots.

Finally, in some locations, internal election administrative culture urges employees not to disrupt public confidence in the agency or its electoral process by reporting irregularities. Given that some administrators would have decided to use vulnerable networked transmissions, tacit or explicit pressures may be placed to confirm that no mischief occurred in the original transmissions or other discretionary tallying processes, rather than might reveal the flawed planning and ignorance of the serious risks.

Legislation can remove from the arsenal of discretionary local and State decision making the options that imperil election integrity. The legislature need not conclude that voted ballots and vote tallies can never be securely transmitted over networks such as the Internet, but rather recognize that the array of prerequisites and resources required, such as exceptional expertise, contingency planning, ongoing training, and special equipment, to effectively manage and respond to the dynamic development of cyberthreats, does not warrant discretionary authority be placed outside the national Board. Allowing the local governments to be more security conscious than the national Board should remain within the permitted range.

4.2.7 *Contrast with the U.S. EAC*

The election cybersecurity board proposed here stands in sharp contrast to the current EAC. A few reasons include: First, the EAC is not staffed with top drawer computer security experts. Second, the EAC is authorized only to issue voluntary standards for voting systems, which function as a voluntary minimum federal standards Third, as directed by Congress, the EAC, is required to study and discuss, and then recommend static standards for the voting equipment that will last perhaps 5 or 10 years, if the EAC Commissioners approve of the proposed standards. Fourth, the Board conception is staffed with a majority of computer scientist professionals, whose decisions are final on which internet voting technologies should be authorized. These are the core differences but they are not exhaustive.

4.2.8 *Achieving Public Accountability and Effective Cybersecurity Compliance*

To achieve transparency and accountability objectives, [37] the Board must be subject to "sunshine" laws that compel an agency to publicly post its activities, actions and documents, and conduct its decision-making sessions in the public domain. These requirements would necessitate that security clearances and classified information not be presented to the Board.

To achieve the accountability needed for public confidence and legitimate elections, the elections cybersecurity statute should also:

- Authorize the BoardÕs rulemaking powers to encompass procedures to guarantee meaningful end-to-end auditability and accountability for every ballot, including those transmitted electronically or electromagnetically;
- Vest the Board and the national Justice ministry with concurrent authority to commence an investigation into any violation of the elections cybersecurity rules;
- Direct the Agency to initiate a process by which citizens can provide notice to it of alleged violations of elections cybersecurity rules, shield their identity from public disclosure, and provide effective whistleblower protection from adverse employment consequences to those who report possible elections cybersecurity violations.

4.3 Transnational Cooperation

Internet and information security threats are systemic and world-wide. Sharing information on election cybersecurity risks and attempted attacks can augment mitigations and criminal prosecutions. Internationally negotiated procedures will be needed. These objectives of world-wide Internet cybersecurity attention can also be facilitated by treaties, international police cooperation, and other mechanisms.

4.4 The U.S. Election Assistance Commission

The chief federal agency acting on electoral administrative issues is the U.S. Election Assistance Commission (EAC). An extensive analysis of the EAC's structure, powers, staffing, and record on technical issues in elections leads to the conclusion that a different agency, likely located within the Department of Homeland Security, should be vested with the powers to regulate the electoral functions that could securely utilize the Internet. [38] The EAC has no national security expertise, and the agency record shows that it has lacked both appreciation of the risks that inhere in the Internet and the types of technical expertise requisite to manage complex computer networks when election tasks are concerned.

5. CONCLUSION

Two competing metaphors represent the information gap underlying the paper. As metaphor for the dynamic security environment, consider a swiftly moving river within which information can be trapped or modified with the ease of trout fishing in a well-stocked backwoods stream. Constant vigilance and frequent threat assessments are par.

But through the eyes of elections administrative policy and equipment procurement officers, the Internet appears to be an armored currency delivery truck, protected by security guards who are trained and equipped with weapons befitting paramilitary officers. Thus protected, they mistakenly election officials often gauge cause as an extremely remote possibility the likelihood of intercepted or fraudulent information deliveries.

The risks of Internet connectivity charted warrant a revised approach to IT security issues. The serious Internet security information gap warrants innovative thinking, modified practices, and redesigned governmental structures. Democratic governments must structurally assure that appropriate technical and security expertise plays a decisive role in policy decisions concerning election administrative use of the Internet. It can be structured to manage elections cybersecurity, thus providing far better voter and national security protection than available previously.

Acknowledgements. The author is indebted to Dr. Matt Bishop, Dr. David Jefferson, Dr. Barbara Simons, and Dr. Gene Spafford for suggestions, but of course they shoulder no responsibility for errors and omissions. This project was partially supported by the Cleveland-Marshall Fund. Law librarians Amy Burchfield and Schuyler Cook of the Cleveland-Marshall College of Law, and law student Pleurat Dreshaj provided superb research assistance, for which the author extends great appreciation.

6. REFERENCES

[1] Help America Vote Act (HAVA), 42 U.S.C. §§15301–15545.

[2] Jefferson, D., Rubin, A. D., Simons, B. Wagner, D., *A Security Analysis of the Secure Electronic Registration and Voting Experiment* (SERVE) (2004), http://www.servesecurityreport.org/.

[3] Pew Charitable Trusts, *No Time to Vote: Challenges Facing America's Overseas Military Voters* 6 (2009), http://www.pewtrusts.org/our_work_report_detail.aspx?id=47922&category=488.

[4] Alvarez, R. NM., Hall, T. E., *Electronic Elections: The Perils and Promises of Digital Democracy* (2008).

[5] Operation Bravo Foundation, http://www.operationbravo.org/pilot_projects.html.

[6] Bishop, M., *Overview of Red Team Reports*, Office of the Secretary of State of California, 1500 11th St, Sacramento, CA 95814 (2007), http://www.sos.ca.gov/elections/elections_vsr.htm.

[7] Bishop, M., Blaze, M., Vigna, G., et al., *University of California Red Team Reports on Voting Systems* (2007), http://www.sos.ca.gov/elections/elections_vsr.htm.

[8] Hoke, C. and Kettyle, D., *Documentation Assessment of the Diebold Voting System* (2007), http://www.sos.ca.gov/elections/elections_vsr.htm.

[9] Hall, J. L., Quilter L., *Documentation Review of the Hart Intercivic System 6.2.1 Voting System* (2007), http://www.sos.ca.gov/elections/elections_vsr.htm.

[10] Burstein, A. J., Good, N. S., Mulligan, D.S., *Review of the Documentation of the Sequoia Voting System* (2007), http://www.sos.ca.gov/elections/elections_vsr.htm.

[11] Bishop M., Wagner, D., *Risks of E-Voting*, Communications of the ACM, 50(11), p. 120 (Nov. 2007).

[12] Neumann, P. *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology*, 1.22 Election Problems, http://www.csl.sri.com/users/neumann/illustrative.html#25.

[13] Bishop, M., Graff, M., Hoke, C., Jefferson, D., Peisert, S., *Resolving the Unexpected in Elections: Election Officials' Options*, Appendix 2: Partial List of Voting Systems Studies (Oct. 2008), http://www.electionexcellence.org/.

[14] Commission on Electronic Voting (Ireland), First Report (Dec. 2004), http://www.cev.ie/htm/report/first_report/part2_5.htm.

[15] Hoke, C., *Public Monitor's Memorandum on Possible Legal Noncompliance in the November 2006 General Election*, at www.urban.csuohio.edu/cei.

[16] *Experts Announce Agreement on the 25 Most Dangerous Programming Errors - And How to Fix Them: Agreement Will Change How Organizations Buy Software*, http://www.sans.org/top25errors/.

[17] MITRE, *Common Weakness Enumeration*, www.cwe.mitre.org/top25/.

[18] Schneier, B., *The Process of Security*, Information Security Magazine (April 2000), http://www.schneier.com/essay-062.html.

[19] Regenscheid, A. and Hasting, N., *A Threat Analysis on UOCAVA Voting Systems*, NISTIR 7551, http://vote.nist.gov/.

[20] Bishop, M., *Introduction to Computer Security* (2004).

[21] Froomkin, A. M., *habermas@discourse.net*: *Toward a Critical Theory of Cyberspace*, 116 Harv. L. Rev. 749 (2003).

[22] Schwartz, P. M., *Privacy and Democracy in Cyberspace*, 52 Vanderbilt L. Rev. 1609, 1614 (1999).

[23] Neumann, P. G., *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology*, ACM SIGSOFT Software Engineering Notes 21:1 (1996), http://portal.acm.org/citation.cfm?doid=381790.381797.

[24] Neumann, P. G., *Risks in Trusting Untrustworthiness*, CACM 46: 9 (2003), http://portal.acm.org/citation.cfm?id=903893.903924.

[25] Cortorer, A., *America's Newest State Holds America's Newest Election* (May 2009), http://www.huffingtonpost.com/aaron-contorer/americas-newest-state-hol_b_203639.html.

[26] *Workshop on GENI and Security*, January 22—23, 2009, University of California at Davis, Davis, California, USA, http://seclab.cs.ucdavis.edu/meetings/genisec/.

[27] The Carter Center, Democracy Program, Declaration of Principles for International Election Observation, http://www.cartercenter.org/peace/democracy/des.html.

[28] Jones, D., *Developing a Methodology for Observing Electronic Voting*, (Oct. 2007), http://www.cartercenter.org/peace/democracy/des_e_voting.html.

[29] Hoke, C., *Trustworthy Elections? The Way Forward*, (Chautauqua Institution Lecture in the *Restoring Legitimacy to Our Elections* week, July 3, 2008), http://fora.tv/2008/07/03/Candice_Hoke_Restoring_Legitimacy_to_Our_Election.

[30] Federal Constitutional Court (Germany), Press Office, *Use of Voting Computers in 2005 Bundestag Election Unconstitutional*, No. 19/2009, 3 Mar 2009.

[31] Tokaji, D., *The Paperless Chase: Electronic Voting and Democratic Values*, 73 Fordham L.R. 1 (2005).

[32] Pinkerton, J. P., *Will Democrats Become a Permanent Majority Thanks to Internet Voting?*, http://foxforum.blogs.foxnews.com/2009/05/26/pinkerton_democrats_internet/.

[33] U.S. Election Assistance Commission, Voting System Test Laboratory Program Manual (July 2008), http://www.eac.gov/program-areas/voting-systems/.

[34] Schneier, B., *Secrets and Lies: Digital Security in a Networked World* 12, 15 (2000, 2004).

[35] Help America Vote Act, 42 U.S.C. §15385.

[36] National Institute of Standards and Technology, *Initial Project Plan for NIST UOCAVA Efforts*, http://www.eac.gov/program-areas/voting-systems/.

[37] President Obama, *Memorandum For The Heads Of Executive Departments And Agencies* (Jan. 21, 2009), http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/.

[38] Hoke, C. *Evaluating the Federal Voting Technology*

Regulatory Record (forthcoming).

[39] Military and Overseas Voters Empowerment Act (MOVE Act), Pub. L. No. 111-84, Subtitle H, §§575-589, 123 Stat. 2190, 2318-2335 (2009), amending the UOCAVA Act, 42 USC §§1973ff–1973ff-7 (2002).

[40] Hoke, C. and Bishop, M. *Essential Research Needed to Support UOCAVA-MOVE Act Implementation at the State and Local Levels* (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1697848.

[41] Scytl, *Solutions, Remote e-Voting (Internet Voting)*, http://www.scytl.com/en/remote-e-voting-internet-voting-s-5.html.

[42] Kirk, J., *Armenian Botnet Suspect Raked in $140,000 a Month*, http://www.computerworld.com/s/article/9194019/Russian_Armenian_botnet_suspect_raked_in_140_000_a_month?source=CTWNLE_nlt_security_2010-11-01.

[43] Gillibrand, *Cybercrime Costs NY Businesses Approximately $4.6 Billion Each Year* (March 23, 2010) http://gillibrand.senate.gov/newsroom/press/release/?id=91bf0d70-0d13-41fa-b663-733e79c2813f.

[44] Johnston, Roger G., *Security Blunders Dumber than Dog Snot*, http://www.usenix.org/events/sec10/tech/techspeakers.html.

[45] Keizer, *Zeus botnet gang targets Charles Schwab accounts; Attacks vulnerable PCs to steal full access to investments, cash* (October 16, 2010), http://www.computerworld.com/s/article/9191479/Zeus_botnet_gang_targets_Charles_Schwab_accounts.

[46] NIST, *Cybersecurity, Innovation and the Internet Economy* (July 27, 2010), http://www.nist.gov/itl/csd/cybersecurity-noi-072710.cfm.

[47] Arthur, C., *How ATM fraud nearly brought down British banking: Phantoms and rogue banks* (Oct. 21, 2005), http://www.theregister.co.uk/2005/10/21/phantoms_and_rogues/print.html.

[48] AFP, *Myanmar's Internet 'under attack' ahead of election* (Nov. 4, 2010), http://www.google.com/hostednews/afp/article/ALeqM5h9weF3XT4BKWBx3Wp6UEgeFX0Jpw?docId=CNG.b4492f600922f04f062f99cc1bbdbf2d.871.

[49] *Electronic voting creates problems across eastern Ontario*, http://ottawa.ctv.ca/servlet/an/local/CTVNews/20101026/OTT_E_Vote_101026/20101026/?hub=OttawaHome.

[50] Citizens 2.0, *New French experience of e-voting* (July 10, 2009), http://www.edemocracy-forum.com/2009/07/frencevoting2009.html#more.

[51] Verified Voting Foundation, *Internet Voting Map of the U.S.* (Oct. 25, 2010), http://www.verifiedvotingfoundation.org/article.php?list=type&type=27.

[52] Messenger, T., *Secretary of State's voter database has been unavailable all day* (Nov. 2, 2010), http://www.stltoday.com/news/local/govt-and-politics/political-fix/article_bd3a67e0-e6ac-11df-bd36-00127992bc8b.html.

[53] Council of Europe, *Distance Voting*, Doc. 11434, Part II (12 October 2007), http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc07/EDOC11434.htm.