



1 of 1 DOCUMENT

Copyright 2010 The Washington Post  
All Rights Reserved

**The Washington Post**  
**washingtonpost.com**

The Washington Post

April 21, 2010 Wednesday  
Suburban Edition

**SECTION:** A-SECTION; Pg. A15

**DISTRIBUTION:** Maryland

**LENGTH:** 692 words

**HEADLINE:** Google hackers duped company personnel to penetrate networks;  
Cyberattacks growing more sophisticated, experts say

**BYLINE:** Ellen Nakashima

**BODY:**

The hackers who penetrated the computer networks of Google and more than 30 other large companies used an increasingly common means of attack: duping system administrators and other executives who have access to passwords, intellectual property and other information, according to cybersecurity experts familiar with the cases.

"Once you gain access to the directory of user names and passwords, in minutes you can take over a network," said George Kurtz, worldwide chief technology officer for McAfee, a Silicon Valley computer security firm that has been working with more than half a dozen of the targeted companies.

Kurtz and others said hackers are mounting ever more sophisticated and effective attacks that often begin with a ruse familiar to many computer users -- a seemingly innocuous link or attachment that admits malicious software.

The attacks were publicized in January when Google, one of the world's most advanced tech firms, announced that intruders had penetrated its network and compromised valuable intellectual property. Google asserted that the attacks originated in China; Chinese officials say they are investigating.

The New York Times reported on its Web site Monday that the Google theft included source code for a password system that controls access to almost all of the company's Web services.

But the cyber-espionage campaign went far beyond Google, targeting companies with apparently strong intrusion-detection systems, including Adobe, Northrop Grumman and Yahoo, industry sources said.

A decade ago "it was the bad guys burrowing in, breaking through a firewall from the outside," Kurtz said. "Now, in essence, what they're doing is having good people on the inside unwittingly connect out to a malicious Web site where their machines can be infected."

Google hackers duped company personnel to penetrate networks; Cyberattacks growing more sophisticated, experts say  
The Washington Post April 21, 2010 Wednesday

Once a hacker can impersonate a system administrator or a senior executive, it becomes difficult to identify the attackers. "Many of these other companies don't know if source code has been stolen because the hackers have assumed the identities of people whose passwords have been stolen," Kurtz said.

The hackers' goal, industry officials and analysts said, is to obtain information that benefits China in strategic industries and in areas where the country seeks an advantage over U.S. firms.

"The bottom line here is if your company has any business dealings with China or has extremely valuable technology or intellectual property, you have a high likelihood of being a target," said Rob Lee, a director with Mandiant, a security firm that is working with some of the targeted companies.

He said he believes the same group or groups that have targeted Google and the other companies have penetrated "hundreds if not thousands" more firms. They target not only system administrators but anyone with privileged access to a company's network, he said.

Figuring out whom to target and how is the result of research, said Shawn Carpenter, a principal forensics analyst at the security firm NetWitness whose former job involved trying to hack into government agencies' Web sites to help them find their weak spots. "One of the first things we do is build up a dossier," he said. "What conferences has this person spoken at? What people do they know? Are they likely to open up this type of e-mail attachment if I spoof it as coming from a person who has sat on a panel with them?"

The essence of the attack is "exploiting those human tendencies of curiosity and trust," Carpenter said.

The targeting of personnel is only one aspect of a larger, more sophisticated operation that involves planning the mode of attack, reconnaissance inside a company's network, deciding what type of data to go after, and harvesting and analyzing the data, experts said.

"There's a life cycle of activities that occurs, involving many steps, both with human intelligence and electronic intelligence, to ultimately penetrate these organizations," said Eddie Schwartz, NetWitness's chief security officer. "When you're combining all of these techniques, this is the work of a highly organized group or groups that has specific targets in mind."

Staff researcher Julie Tate contributed to this report.

**LOAD-DATE:** April 21, 2010

**Project**

**E V E R E S T**

**Evaluation and Validation of Election Related Equipment,  
Standards and Testing**

*REPORT OF FINDINGS*

OHIO SECRETARY OF STATE  
JENNIFER L. BRUNNER

COLUMBUS, OHIO  
DECEMBER 14, 2007



**Project EVEREST (Evaluation & Validation of Election-Related  
Equipment, Standards, & Testing)**

**Risk Assessment Study of Ohio Voting Systems**

**Executive Report  
Ohio Secretary of State Jennifer Brunner  
December 14, 2007**

## Table of Contents

<b>INTRODUCTION.....</b>	<b>5</b>
<b>OBJECTIVES.....</b>	<b>6</b>
<b>HISTORY .....</b>	<b>7</b>
OHIO'S PURCHASE OF ELECTRONIC VOTING MACHINES .....	7
PUBLIC CONFIDENCE IN ELECTRONIC VOTING.....	7
PROJECT EVEREST .....	8
<b>STRUCTURE OF STUDY .....</b>	<b>12</b>
<b>SECURITY ASSESSMENT .....</b>	<b>14</b>
MICROSOLVED .....	14
Method.....	14
Findings .....	15
Summary.....	15
Penetration Testing: Specific Results .....	16
<i>Premier</i> .....	16
Description of the Premier System.....	16
Physical Access Testing.....	20
Network and Communications Access Testing.....	22
File Systems Access Testing.....	22
Baseline Comparison .....	22
<i>ES&amp;S</i> .....	22
Description of the ES&S Voting System.....	22
Physical Access Testing.....	26
Network and Communications Access Testing.....	27
File Systems Access Testing.....	28
Baseline Comparison .....	28
<i>Hart InterCivic</i> .....	28
Description of the Hart InterCivic Voting System .....	28
Physical Access Testing.....	31
Network and Communications Access Testing.....	32
File Systems Access Testing.....	32
Baseline Comparison .....	32
Suggested Improvements: All Voting Systems.....	32
Summary of Boards of Elections Officials' Review of MicroSolved's Findings on the Security Assessment of the State's Voting Systems .....	33
UNIVERSITY RESEARCH TEAMS .....	35
Method.....	35
Findings .....	37
Summary.....	37
Specific Results: Source Code Analysis and Red Team (Penetration) Testing ....	38
<i>ES&amp;S</i> .....	38
Failure to Protect Election Data and Software.....	38
Failure to Effectively Control Access to Election Operations.....	39
Failure to Correctly Implement Security Mechanisms.....	40
Failure to Follow Standard Software and Security Engineering Practices ...	40

<i>Premier</i> .....	40
Failure To Effectively Protect Vote Integrity and Privacy/Failure to Protect Elections From Malicious Insiders.....	41
Failure to Validate and Protect Software / Failure to Follow Standard Software and Security Engineering Practices .....	42
Failure to Provide Trustworthy Auditing .....	42
<i>Hart</i> .....	42
Failure To Effectively Protect Election Data Integrity.....	43
Failure To Eliminate Or Document Unsafe Functionality .....	44
Failure To Protect Election From “Malicious Insiders” .....	44
Failure To Provide Trustworthy Auditing .....	44
Summary of Boards of Elections Officials’ Review of the Academic Research Teams’ Findings on the Security Assessment of the State’s Voting Systems.....	44
<b>CONFIGURATION MANAGEMENT ASSESSMENT.....</b>	<b>48</b>
SYSTEST .....	48
Method.....	48
Findings .....	49
Summary.....	49
Configuration Management Assessment: .....	49
Specific Results and Suggested Improvements.....	49
<i>Hart InterCivic</i> .....	49
<i>ES&amp;S</i> .....	50
<i>Premier</i> .....	51
Summary of Board of Elections Officials’ Review of SysTest’s Findings on Configuration Management of the State’s Voting Systems.....	52
<b>PERFORMANCE TESTING.....</b>	<b>54</b>
SYSTEST .....	54
Method.....	54
Findings .....	55
Summary.....	55
Performance Assessment: .....	56
Specific Results and Suggested Improvements.....	56
<i>Premier</i> .....	56
<i>ES&amp;S</i> .....	57
<i>Hart InterCivic</i> .....	60
Summary of Board of Elections Officials’ Review of SysTest’s Findings on Performance Testing of the State’s Voting Systems.....	61
Average Performance Report Quality Ratings by Election Officials .....	62
<b>ELECTIONS OPERATIONS AND INTERNAL CONTROL ASSESSMENT .....</b>	<b>63</b>
SYSTEST .....	63
Method.....	63
Findings .....	63
Summary.....	63
Specific Results and Suggested Improvements.....	64
Documentation.....	64
Threat Analysis.....	65
Vulnerability Analysis .....	66

Election Management Software (EMS) and Firmware Version Control Updates .....68

Summary of Boards of Elections Officials’ Review of SysTest’s Findings on the  
Elections Operations and Internal Controls Assessment of the State’s Voting  
Systems ..... 71

Average Operational Controls Report Quality Ratings by Election Officials.... 72

**SECRETARY OF STATE RECOMMENDATIONS ..... 73**

GENERAL CONCLUSIONS AND BACKGROUND ..... 73

RECOMMENDATIONS ..... 76

CONCLUSION .....84

## **Introduction**

Project EVEREST (Evaluation and Validation of Election Related Equipment, Standards and Testing) is a risk assessment of Ohio's current voting system, examining the integrity, handling, and securing of voting machines and systems before, during and after an election. The Ohio secretary of state has conducted this assessment in an effort to provide to the citizens of Ohio a comprehensive, independent, balanced and objective assessment of the accuracy, reliability and security associated with Ohio's voting systems.

The following is a summary of the Executive Report's sections:

- **Objectives** - The Objectives Section describes the overall objectives of the risk assessment study.
- **History** – The History Section summarizes the history of electronic voting in Ohio, and the impetus for and history of Project EVEREST.
- **Structure of Study** – The Structure of Study section describes the parallel testing design used in the study, which allows different parties to test the voting systems using multiple methods. This section summarizes the four tasks used to evaluate each system: security assessment, configuration management, performance testing, and operational controls.
- **Methods/Findings** – The Methods/Findings Section summarizes the methods used by each assessment team, and includes evaluation of the testing reports by a bi-partisan group of election officials, along with the findings reached using each method of assessment. This section is organized by the four tasks used to evaluate each system: security assessment, configuration management, performance testing, and operational controls.
- **Recommendations** – The Recommendations Section contains Secretary of State Jennifer Brunner's recommendations for how Ohio should best proceed in response to the declared findings, including long-term goals, short-term fixes, desired legislation and necessary secretary of state directives.
- **Appendices** – The Appendices Section includes the original Request for Proposals (RFP), State Controlling Board request, information regarding the boards of elections participants, all final testing reports, and a glossary of relevant technical terms.



## **Objectives**

The ultimate objective of Project EVEREST is to improve the integrity of Ohio elections for federal office, and state and local offices and issues, and provide the citizenry with increased confidence and trust in our elections system.

Project EVEREST has sought to accomplish these goals by attempting to provide a comprehensive, independent, balanced and objective assessment of the risks to election integrity associated with Ohio's voting systems, which will in turn be used to make improvements in laws and instructions governing Ohio elections with a focus on the use, handling, and securing of voting machines before, during and after elections.

In order to achieve these objectives, the following questions will be specifically addressed:

1. What are the significant risks of inaccuracy of election results, if any, due to error or fraud, including vulnerability to an "attack"<sup>1</sup>?
2. What are the significant risks of accidental or intentional catastrophic machine failure or unrecoverable error, if any?
3. Do risks exist that cannot be sufficiently mitigated, indicating inherent system inadequacies?

---

<sup>1</sup> An "attack" is a common term used when evaluating the security of a system and generally means an outside influence that may affect the operational integrity of the system.

## **History**

### Ohio's Purchase of Electronic Voting Machines

In 2002, the United States Congress adopted the Help America Vote Act of 2002 (HAVA), which aimed to improve the administration of elections in the United States. With the enactment of HAVA, new voting system requirements were established, and a national program was implemented to provide states with the funds necessary to replace punch card and lever voting systems with new, qualifying systems.

HAVA also created the U.S. Election Assistance Commission (EAC) and transferred the responsibility of developing voting system standards from the Federal Election Commission (FEC) to the EAC. Through HAVA, the EAC was also tasked with establishing the federal government's first voting system certification program.

Before the implementation of HAVA, the vast majority of counties in Ohio used punch card voting systems. With the advent of HAVA, voting machine manufacturers whose new systems met the applicable federal standards and whose equipment was approved for use in Ohio by the state's Board of Voting Machine Examiners<sup>2</sup>, submitted bids for consideration to the Ohio secretary of state. The secretary of state, in turn, worked with each county's board of elections (BOE) to purchase an approved system — either a direct recording electronic (DRE) or an optical scan system manufactured by Diebold (now Premier Elections Solutions), Hart InterCivic, or Election Systems and Software (ES&S) — that best-suited each particular county.

In May 2004, the General Assembly enacted Substitute House Bill 262, which required all DRE voting machines to provide a voter verified paper audit trail (VVPAT). The approved systems, with VVPAT, were subjected to an Independent Verification and Validation (IV&V) test and a security assessment performed by CompuWare. (The 2004 CompuWare study report may be found in Appendix A.)

Approximately half of Ohio's 88 counties used their new voting systems in the November 2005 general election; the other half used their new systems for the first time in the May 2006 primary election.

### Public Confidence in Electronic Voting

The response to the new voting systems has been varied, but overall, public confidence in the new machines and trust in Ohio's elections system have suffered. Individuals, election officials, non-partisan voting rights advocacy groups, and expert researchers both in Ohio and throughout the United States have expressed concerns regarding election integrity, security, accuracy, vote verification, and recounts using the various voting system technologies. Numerous documented malfunctions with elections systems and software, both statewide and nationally, have fueled public concern and contributed to the overall uncertainty of voters.

---

<sup>2</sup> See, R.C. 3506.05 *et.seq.* consisting of three persons appointed by the secretary of state, one of whom is a competent and experienced election official and the other two of whom are knowledgeable about the operation of voting equipment.

Other factors have contributed to the atmosphere of public uncertainty. Potential conflicts of interest in voting system certification, by which vendors select and pay testing labs to certify that their voting systems meet the system standards, have drawn much public scrutiny, as have questions surrounding the adequacy and timeliness of the federal certification and testing process. Another occurrence that has contributed to public unease is the failure of Ciber, Inc. to achieve accreditation by the U.S. Election Assistance Commission, long after Ciber's labs contributed to the certification of more than half of all nationally qualified voting systems. The EAC first temporarily barred Ciber from testing new machines in the summer of 2006 for failure to follow appropriate quality-control procedures and an inability to document that it was conducting all required tests.<sup>3</sup> More recently, the EAC voted to reject altogether Ciber's application to be a security test laboratory for electronic voting machines.<sup>4</sup>

Additionally, voting systems have recently been tested in several other states including California, Florida, New Jersey and Connecticut, all exposing serious flaws in the security of voting systems used in these jurisdictions, several of which are used in Ohio. California's testing resulted in the de-certification on a conditional basis of several components of its various voting systems. For these and other reasons, there is at least some doubt about the integrity of the state's election process and voting systems, and hence Project EVEREST was conceived, developed and implemented.

All public doubt and concern aside, technology is constantly evolving. Even if a voting system was certified under the most rigorous of certification standards, it is reasonable for the public to expect continued testing measures to ensure that voting systems safely, securely and accurately count their votes. Additionally, according to R.C. 3506.05(E), the secretary of state is statutorily required to "periodically examine, test, and inspect certified equipment to determine continued compliance."

### Project EVEREST

Project EVEREST was initiated by the secretary of state of Ohio to provide a comprehensive, independent, balanced, and objective assessment of the risks to election integrity associated with Ohio's voting systems, election-related equipment, testing, standards, and associated internal controls, including the extent to which integrity violations are possible, preventable, detectable, and correctable. The analysis was designed to assess the adequacy of institutional mechanisms of control and accountability as well as the ability to identify sources of error or potential fraud. Project EVEREST is designed as a risk assessment study of Ohio's voting systems' vulnerabilities and potential to mitigate them, providing a comprehensive analysis of the state's voting system as a whole.

Project EVEREST builds on other states' testing, by not only performing a wider range of testing in a secure laboratory environment, but by attempting to incorporate operational procedures used by election officials that could potentially mitigate security threats.

---

<sup>3</sup> Christopher Drew, "U.S. Bars Lab From Testing Electronic Voting," *The New York Times*, January 4, 2007.

<sup>4</sup> U.S. Election Assistance Commission, "Rejected Applications," Election Assistance Commission, <http://www.eac.gov/voting%20systems/test-lab-accreditation/interim-accreditation/pending-applications/?searchterm=ciber>

Project EVEREST's concept is unique in that it integrates the involvement of a bi-partisan group of election officials from a diverse selection of Ohio counties and voting machine environments to review the security assessments' applications to "real world" Election Day experiences.

After several months of research and planning, on June 18, 2007, the Ohio secretary of state issued a Request for Proposals (RFP) for consulting and testing services to perform the Risk Assessment Study of Ohio Voting Systems. The RFP outlines tasks to be performed and permitted proposers to submit proposals to perform one, some or all tasks. (The RFP may be found in Appendix B.) This allowed the secretary of state to select a combination of proposals to ensure all necessary tasks were performed to an optimal level and to facilitate a model of "parallel independent testing" of the state's voting equipment. Several entities representing corporate, professional and academic backgrounds were selected to execute the various tasks for accomplishing the project's objectives, and to provide unbiased, expert work from a diversity of corporate and academic environments.

On September 24, 2007, the State of Ohio Controlling Board approved the Ohio secretary of state's request to waive competitive selection, permitting these contracts to be awarded to SysTest Labs and MicroSolved, Inc. (The Controlling Board materials may be found in Appendix C.)

SysTest Labs, of Denver, Colorado, was selected to assess configuration management, operational controls and performance testing on each of the three certified voting systems in Ohio. SysTest is an approved test lab by the National Institute of Standards and Testing (NIST), and is an EAC federally approved Voting System Testing Lab (VSTL), offering Independent Verification and Validation (IV&V), Software Test Engineering, Quality Assurance (QA), and Compliance Testing services.

MicroSolved, Inc., of Columbus, Ohio, was selected to complete a security assessment of each voting system, evaluating vulnerabilities of each system by performing penetration testing. MicroSolved has performed past vulnerability assessments on sensitive networks found in the private sector and in state and federal government.

The project's academic teams were subcontracted through SysTest, to perform a variety of assessments in addition to and independently parallel to those mentioned above. The academics retained many individual researchers who are considered national and international experts in electronic security, with experience in evaluating security at the state and federal levels, as well as for the private sector, including highly sensitive federal and private sector projects. In addition to performing penetration testing, the project's academic teams performed a source code review of all three voting systems.

The Pennsylvania State University team was selected to perform penetration testing and source code analysis for the Hart InterCivic and Premier Election Solutions systems. In addition, the Penn State team was permitted by Premier to review unredacted reports of the state of California's "top-to-bottom" review of the Premier system to assist in its testing and analysis activities for the study.

The University of Pennsylvania team was selected to focus on the source code evaluation of the ES&S systems, with the potential to include penetration exercises or other security evaluation methods as deemed appropriate. In contrast, the University of California-

Santa Barbara WebWise team was chosen to focus on the penetration evaluation of the ES&S systems, with the potential to include source code analysis or other security evaluation methods as deemed appropriate.

Additionally, a project manager was engaged from Battelle Memorial Institute to provide project management services to the secretary of state's office for scientific oversight of the study schedule, contractor status, issue reporting and general project management.

All three voting machine manufacturers were actively involved in the voting system review. High-level executives from each manufacturer met with secretary of state staff at the beginning of the review to understand the project's operations and goals. All manufacturers pledged their support and cooperation at the outset of the project.

Each manufacturer sent at least one key staff person to conduct orientation on their respective systems. This orientation educated testers on machine operations, set-up, and breakdown.

The testing took place from October 5, 2007 through December 7, 2007. SysTest and MicroSolved's testing was performed under secure conditions at the State of Ohio Computer Center (SOCC) facility, and the three academic teams' testing was performed under secure conditions<sup>5</sup> at their respective universities.

To enable a real-world testing environment of voting equipment actually used in elections, several county boards of elections provided standardized and configured voting system equipment and software to the voting system review. Each voting machine manufacturer provided equipment to those respective county boards of elections to replace the equipment being tested. Additionally, each manufacturer supplied equipment that was unavailable from the county boards of elections. The manufacturers shipped the equipment free of charge.

The voting machine manufacturers also provided essential information to the voting system review. Computers were purchased for analysis of the "back office" for the voting system review to configure and tabulate ballots. The manufacturers configured and installed the necessary software on those computers and sent them to the SOCC to complete the test environments. They also provided the source codes necessary to analyze the voting system and critical confidential and proprietary documentation.

Additionally, the manufacturers provided ongoing support throughout the project. They answered technical questions and supplied documentation, equipment, and supplies such as VVPAT paper, ballots, and ballot stock. Throughout the project, manufacturers provided access to their high-level executives to answer questions and provide responses to testers' needs.

Upon the completion of the testing, SysTest, MicroSolved and the three academic teams provided to the Ohio secretary of state on or before December 7, 2007, their findings in various written reports. On December 9, 2007, the secretary, representatives from her administration, and the bi-partisan group of election officials convened to review and evaluate the various reports and used those findings to reach conclusions for the recommendations contained in this report.

---

<sup>5</sup> These secure conditions are based on industry standards according to uniform guidelines.

This Executive Report documents the cumulative results of the EVEREST assessment, and accordingly provides recommendations to the Ohio General Assembly and Governor Ted Strickland for improvements in laws and instructions governing Ohio elections with a focus on the use, handling, and securing of voting machines before, during and after elections. Both legislative and fiscal needs are detailed for the recommendations included in this report.

## **Structure of Study**

The Ohio Risk Assessment was designed to evaluate Ohio's voting systems along a multidimensional, layered approach so that independent perspectives could be compared for consistency. All voting systems approved for use in Ohio were evaluated under the four "tasks" of the project: (1) a security assessment; (2) a configuration management review; (3) performance testing; and (4) an analysis of the internal controls and operations associated with the voting systems. Upon conclusion of the review, all testing entities were required to submit both summary and detailed reports of their findings to the secretary of state. The secretary of state requested and received the assistance of a bipartisan group of county boards of elections officials who reviewed these reports and vetted and analyzed the recommendations made as a result of this study.

### **The Four Tasks of the Risk Assessment**

MicroSolved and the academic research teams were selected to conduct security assessments of each of Ohio's certified voting systems. Although the two testing entities utilized different methods, the goal of the parallel testing was to examine the security of the electronic voting systems in use in Ohio and identify procedures that may eliminate or mitigate discovered issues.

SysTest was selected to conduct the configuration management review, performance testing, and the analysis of operations and internal controls. Under the configuration management review, the goal was to evaluate the secretary of state's ability to independently verify whether the configuration of each voting system as approved for use by county boards of elections was consistent with, and unchanged from, the configuration certified by the state of Ohio, including, whether the certified configuration remained unchanged during all parts of the election process, including tabulation, during which results potentially could be affected. The purpose of the performance testing was to further determine if there were risks to the integrity of the election and accuracy of vote counts during simple use of each of the certified voting systems. Finally, the purpose of the elections operations and internal control assessment was to determine whether existing or proposed policies, procedures, and internal controls established in manufacturer documentation and administratively by and for county boards of elections are sufficient to ensure secure and accurate elections that may be affected by software, hardware, and operational susceptibilities.

### **Boards of Elections Officials' Review**

Along with the work of the testing entities, the Ohio Risk Assessment had the benefit of the efforts of an advisory group of Ohio boards of elections officials from twelve counties representing both major political parties in equal numbers. (A list of the boards of elections participants may be found at Appendix D.) During the testing of Ohio's voting systems, this group toured the secure testing facility and examined the machines tested and conferred during a weekly conference call with secretary of state team members to monitor project status. Upon conclusion of the testing, the group of election officials met for four days – from December 9, 2007 through December 12, 2007 – at the State of Ohio Computing Center in Columbus to review final reports and discuss with the secretary recommendations to be made as a result of the study.

While in Columbus, the boards of elections officials were first divided into five study groups, with each group tasked to review reports specific to a stated task of the study: (1) security assessment (MicroSolved); (2) security assessment (Academic research teams); (3) configuration management (SysTest); (4) performance testing (SysTest); and (5) internal controls and operations (SysTest). Each study group included at least two boards of elections officials (evenly distributed by party affiliation, except when there were three board officials to a team, and one team had one Republican and two Democrats, while the other had two Republicans and one Democrat) with each team staffed by three secretary of state employees — a “facilitator” to lead the group’s discussion, a “scribe” to document the group’s observations and conclusions, and an attorney for legal issues.

Each review team completed a questionnaire rating the testing entities’ reports in the following areas:

- The clarity of the problem and solution statements;
- The use of data to substantiate problems and solution statements;
- The logic and justifications used to argue from data to problems and solutions;
- The organization and readability of materials; and
- The overall quality of the work on a five-point scale of failing to excellent.

Reviewers were also encouraged to record relevant observations to support their ratings. Upon conclusion of the group’s review, the “scribe” created a “Capsule Summary Statement” of the group’s observations. This report contains those Capsule Summaries and a table of standardized findings according the criteria outlined above.



## Security Assessment

### MicroSolved

MicroSolved performed “red team” penetration tests of the Premier, ES&S and Hart InterCivic voting systems. MicroSolved attempted to “attack” the systems under a range of conditions – from that of a casual voter at a polling location to the skilled attacker with more direct access to the voting system. Unlike the Academic teams, MicroSolved was not given access to the voting machine manufacturers’ source code.

On all three voting systems, MicroSolved discovered “serious vulnerabilities in the systems and many of their components.” (Project Executive Summary Report at 2.) MicroSolved concluded: “[a]ll three vendor systems reviewed have serious gaps in compliance with even the most basic set of information security guidelines used by systems in industries such as finance, insurance, medical care, manufacturing, logistics and other global commerce. Given the extremely valuable data that these systems process and the fact that our very democracy and nation depend on the security of that data, much work remains to be done by all three vendors.” (Project Executive Summary Report at 12.)

MicroSolved created three reports for each voting system: (1) an Executive Summary Report; (2) a Technical Manager’s Report; and (3) a Technical Details Report. MicroSolved also created a Project Executive Summary Report. This Secretary’s Report briefly explains MicroSolved’s methods and findings. (The complete MicroSolved reports are attached at Appendix E.)

### Method

MicroSolved’s methodology followed a “traditional application assessment process,” which consisted of the following testing “phases”:

- **Attack surface mapping:** In the first phase, MicroSolved created a graphical representation of each voting system to determine the areas that were most likely available for assault by an “attacker.”
- **Threat modeling:** In the second phase, MicroSolved developed a model group of potential “attackers” – ranging from the casual external attacker to the focused/resourced internal attacker – and attempted to measure the extent to which these attackers could affect the confidentiality, integrity, and availability of any election or to simply introduce enough issues into the election process that the general public would fail to have confidence in an election.
- **Poor trust/cascading failure analysis:** In the third phase, MicroSolved examined the surface map of each voting system to identify areas where exploitation of vulnerabilities in the attack surfaces of components could lead to the introduction of malicious programming (malware) into the system – that is, where a security compromise could be spread from one component to another or from an external component to the core system.

- **Vulnerability assessment:** After identifying the potential attack surfaces in the previous phases, MicroSolved performed systemic testing of the voting systems to identify the presence of any security vulnerabilities. The vulnerability assessment emulated the “attackers” by performing testing appropriate for each group of “attackers” based on the various levels of access and capability.
- **Penetration testing and reporting:** The penetration phase – the most important of MicroSolved’s phases – explored the damage of exploiting the vulnerabilities identified in the vulnerability assessment. The penetration phase tested three types of access to each of the voting systems:
  - **Physical Access:** MicroSolved tested the system components for vulnerabilities through physical access, including probing the lock mechanisms, the accessible ports of the devices, and the input/output subsystems.
  - **Network and Communications Access:** MicroSolved tested the system components for networking and communications vulnerabilities, using network scanners, serial port probes, sniffing tools and exploit codes.
  - **File System Access:** MicroSolved tested the system components for vulnerabilities in the processing of elections data – that is, the way that the underlying operating system or applications interact with the file system.
- **Baseline comparison:** In order to compare the three voting systems against each other, the final phase of MicroSolved’s testing established a twelve-step framework of industry standard security best practices to “baseline” each system. MicroSolved assigned a “pass” or “fail” grade for each of the twelve requirements in the framework. “Passing” a category means that the voting system meets the best practices requirements for that area, and “failing” a category means that the system does not meet industry standard best practices.

## Findings

### Summary

MicroSolved’s review of the Premier, ES&S, and Hart voting systems identified three key weaknesses in each system.

- **First,** MicroSolved stated that the voting machine companies have “failed to adopt, implement and follow industry standard best practices in the development of the system.” Although basic best security practices have emerged over the previous ten years to assist organizations with the development, configuration, deployment, and management of IT infrastructures in a secure fashion, the three voting systems have failed to comply with these standards. (Project Executive Summary Report at 11.)
- **Second,** MicroSolved concluded there was a “lack of integrity controls” that have been applied to the voting systems. MicroSolved was able to identify

vulnerabilities in all three voting systems that could allow attackers to introduce an infection or malicious programming (malware) into the voting system. (*Id.*)

- **Third**, MicroSolved concluded that Ohio election officials have failed to establish or implement clear and effective security policies and processes, and because many county boards of elections face staff and budget shortfalls, the boards are prevented from having the resources to seek out security solutions on their own. (*Id.*)

### Penetration Testing: Specific Results

#### **Premier**

MicroSolved concluded that the Premier voting system performed “poorly” in the physical access and file system access penetration tests. However, the Premier system performed “well” in the network and communications access penetration test. (Technical Manager’s Report, Premier, at 10-11.)

#### Description of the Premier System

Premier voting systems are used in 48 Ohio counties – 47 counties utilize the Premier DRE as the primary voting machine, while one county uses Premier’s precinct count optical scanner as the primary voting system. To better understand the findings included in this report, the relevant components of the Premier system are described below.<sup>6</sup>

#### ***Components at County Boards of Elections Offices***

The following components reside at county boards of elections offices. The photographs are courtesy of the Academic research teams.

- **Global Election Management System (GEMS):** The GEMS server is responsible for running all election processes. Election officials use the GEMS server to create ballot definitions, program memory cards, and tally all votes after an election.

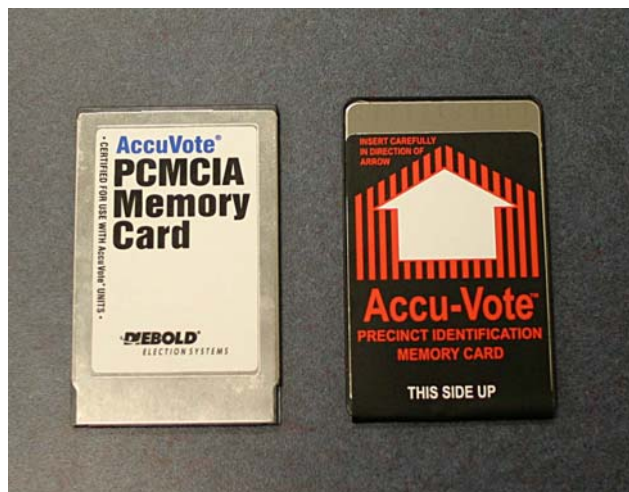
---

<sup>6</sup> Please refer to EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, Final Report (hereinafter “Academic Final Report”) at Chapter 11, attached at Appendix F, for more detailed descriptions.



Premier GEMS Server

- Memory cards:** The Premier system relies on memory cards as the major avenue of communication between the GEMS server and the polling places. In counties using either DREs or optical scan machines, memory cards are encoded with ballot types at a board of elections office and sent to each polling place in the county for poll workers to configure the machines at the polling place. In some less populated counties, the DREs are delivered to the polling place with memory cards installed and with tamper-evident tape placed over each memory card to prevent its removal until the DRE is returned to the board or until the closing of the polling place. After polling places are closed, the ballots cast on either the DRE or optical scan voting machine are stored on the memory card, which is returned to the board of elections office and from which the GEMS server tallies the votes.



PCMCIA and AccuVote-OS Memory Cards used with the Premier Voting System

- **Election Media Processor (EMP):** The EMP is hardware and software used to communicate with GEMS and to interface with memory cards. Premier offers the EMP to efficiently encode and read memory cards. This device can read multiple memory cards in parallel.



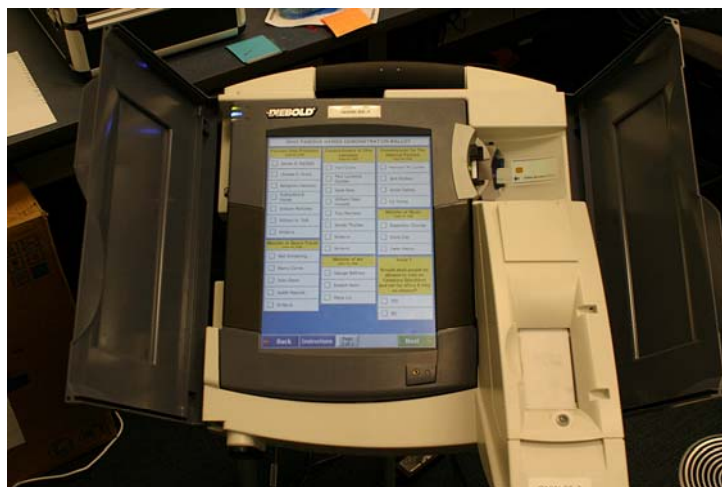
Election Media Processor (EMP) used with the Premier Voting System

- **Verdasys Digital Guardian:** Digital Guardian is additional third party software intended to enhance the security of the GEMS server. Because of previous security studies on the Premier voting system, the State of Ohio requires Premier to include the Digital Guardian software.

### ***Components at Polling Places***

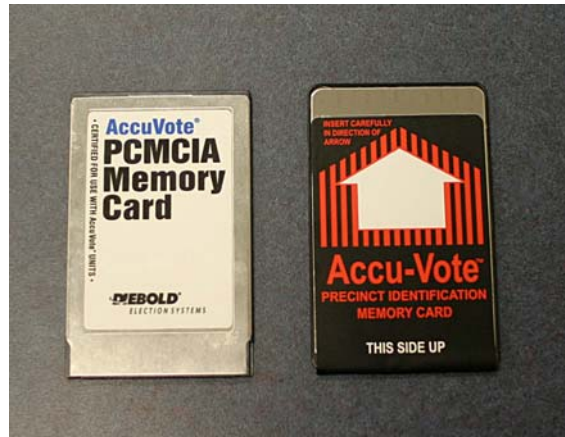
The following components are used at polling locations on Election Day.

- **AccuVote-TSX:** The TSX is a touchscreen DRE, which includes a VVPAT printer unit to create a verifiable paper record of the voter's selections.



Premier's AccuVote TSX DRE Voting Machine

- **PCMCIA Memory Cards:** See previous description of memory cards above.



PCMCIA Memory Card and AccuVote OS Memory Cards used with the Premier Voting System

- **Voter Access Cards and Supervisor Cards:** In counties using the TSX DRE machines, when a voter appears at a polling location to vote, the voter receives a Voter Access Card, which allows the voter to cast a single ballot. Upon reaching the TSX, the voter inserts the card into the machine and follows the on-screen instructions to cast a ballot. After the ballot has been cast and stored on the TSX and memory card, the TSX re-programs the Voter Access Card so that it cannot be used until re-encoded. Supervisor cards are given to the poll workers and are used to open and close the voting machines on Election Day.



Voter Access and Supervisor Cards used with the Premier DRE Voting System

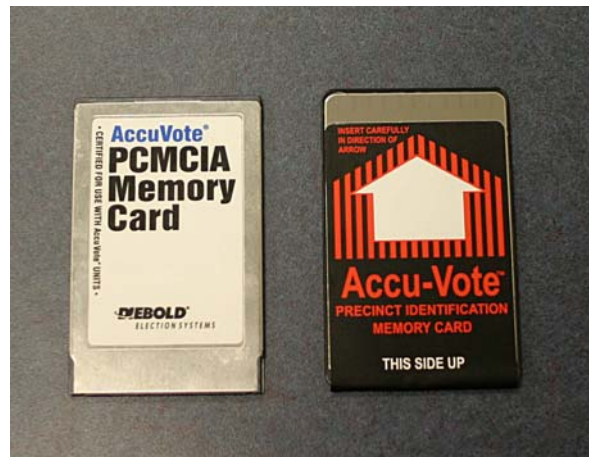
- **AccuVote OS:** The AV-OS Precinct Count is Premier's precinct optical scanner for use in each polling place or at a board of elections office. When a voter arrives at a polling place to vote, he or she marks an optical scan ballot with a marking device, such as a pen or pencil. When finished, the voter inserts the ballot into the AV-OS optical scan machine. The voter is given the chance to reject and retrieve the ballot (such as in the case of an overvote) or to accept the ballot as

voted. The ballots move from the scanner to a locked box in the base of the scanner. After the polling place closes, poll workers print an election summary off of the AV-OS. Poll workers transfer the AV-OS memory card, defined below, to the board of elections office for vote tabulating using EMPs and/or the GEMS server.



Premier's AccuVote Optical Scanner (AV-OS)

- AccuVote OS Memory Card:** On Election Day, AV-OS machines are configured by inserting memory cards that were encoded at the board of elections office. The AV-OS memory card stores the ballot images of the optical scan ballots scanned by the AV-OS on Election Day. After the polling place closes, poll workers transfer the AV-OS memory card to the board of elections office for vote tabulation.



PCMCIA Memory Card and AccuVote OS Memory Cards used with the Premier Voting System

### Physical Access Testing

Premier performed “poorly” in the physical access testing because MicroSolved was able to introduce malware into the system by various methods. MicroSolved concluded: “for devices whose intended deployments are to be public-facing and whose purpose is to



serve a critical function such as government elections, the systems seemed woefully inadequate from physical attacks.” (Technical Manager’s Report, Premier, at 12.)

MicroSolved described the following security vulnerabilities resulting from its physical access penetration testing:

- At the precinct level, locks on the optical scanners and ballot storage/sorting bins were “easily circumvented” using common lock picking tools. (*Id.* at 12.)
- The keys to the physical locks of several devices, including keys to DREs, are not unique and easily obtainable, which could expose many systems to tampering. (*Id.*)
- Physical attacks on the DRE unit were identified that would cause the unit to boot into administrative mode, in which an unauthorized individual could gain access to reconfigure the DRE device, change election settings, and delete electronic ballot results previously cast on the voting machine under the individual’s control. Additionally, security protections on the power button and primary memory slot could be “easily circumvented.” (*Id.*)
- The tamper seals on the DRE unit could be manipulated to make it appear as if tampering has occurred, even if tampering has not occurred. Threat agents working in teams could therefore create general chaos in the election process and disrupt public confidence in an election. (*Id.*)
- The GEMS server and connected EMP workstations that were operated at the board of elections’ offices were discovered to be “poorly configured” and “poorly protected against physical access attacks,” which could allow unauthorized individuals to deploy malware or other malicious code if given access to the system, even for a short period of time. (*Id.* at 13.) For example, the EMP workstations tested did not have anti-virus software installed, and the anti-virus software installed on the GEMS server had not been updated in approximately two years.
- The protections offered by the Digital Guardian security tool, a security program developed specifically for the GEMS server in Ohio and which is installed to overcome already known weaknesses publicly identified in other tests, are “easily circumvented.” (*Id.* at 13.) The Digital Guardian application is not configured to enforce many of the rules for which it is programmed. For example, instead of actually blocking user actions recognized as malicious, Digital Guardian simply alerts the user that the actions have been detected but allows the actions to occur.
- Password policies on the EMP workstations and GEMS server are not in compliance with industry standards and are vulnerable to simple attacks by deciphering the password. (*Id.* at 13-14.)
- Because the Premier system does not serialize optical scan ballots, the ballots are not unique, and optical scan ballots could be re-processed through the optical scanner a second time without notice. (*Id.* at 14.)



### **Network and Communications Access Testing**

The Premier system performed “well” in the network and communication access testing. Manipulation of the communications streams and network traffic failed to discover any significant vulnerabilities. (Technical Manager’s Report, Premier, at 11.) However, MicroSolved did discover weaknesses in the protection mechanisms installed on the GEMS server. For example, MicroSolved identified a vulnerability in the firewall software used to protect the GEMS that allows unauthorized individuals to exploit the GEMS server. As in the physical access testing, MicroSolved also identified poor password policies. These weaknesses expose the GEMS server to network compromise from the EMP workstation or other network devices by an unauthorized individual or malware. (*Id.* at 11, 14-15.)

### **File Systems Access Testing**

The Premier system performed “poorly” in the file systems testing. Several components were found to be vulnerable to input manipulation attacks that could introduce arbitrary code into the system. (Technical Manager’s Report, Premier, at 11, 15.) For example, MicroSolved was able to boot a DRE voting machine into administrative mode based on the data on a memory card inserted into the machine. MicroSolved also identified a “plethora” of buffer overflow exploits. (*Id.* at 15.) Buffer overflow occurs by writing outside the bounds of a block of allocated memory and can corrupt data, crash the program, or cause the execution of malicious code. (*Id.* at 21.) Finally, MicroSolved found ways that unauthorized individuals could manipulate files processed by the EMP workstations connected to the GEMS server at a board of elections to cause the server tabulating votes to report precincts having been counted but the votes from the precinct were not actually added to the tally of the results. (*Id.* at 16.)

### **Baseline Comparison**

Premier scored a “zero” on its twelve-step baseline comparison framework – that is, the Premier voting system failed to meet any of the twelve basic best practices requirements. (Technical Manager’s Report, Premier, at 17-19.)

### **ES&S**

MicroSolved concluded that the ES&S voting system performed “poorly” in the physical access and file system access testing. However, ES&S performed “medium” in the network and communications access testing. (Technical Manager’s Report, ES&S, at 9-10.)

### **Description of the ES&S Voting System**

ES&S voting systems are used in 39 Ohio counties – 11 counties utilize the ES&S DRE as the primary voting machine, while 28 counties use ES&S’s precinct count optical scanner as the primary voting machine. To better understand the findings included in this report, the relevant components of the ES&S system are described below.<sup>7</sup> The photographs are courtesy of the Academic research teams.

---

<sup>7</sup> Please refer to the Academic Final Report at Chapter 5, attached at Appendix F, for more detailed descriptions.

### ***Components at the Boards of Elections Offices***

The following components reside at county boards of elections offices.

- **Unity:** Unity is the election management software for the ES&S system and is responsible for running all elections processes. Unity is a suite of software that creates ballot definitions, programs memory cards, and tallies votes after an election.
- **Model 650:** The M650 is a centralized high-speed optical ballot scanner and counter intended for use at boards of elections offices.



ES&S Model 650 Central Count Optical Scanner

### ***Components at Polling Places***

The following components are used at polling locations on Election Day.

- **iVotronic:** The iVotronic is the DRE touchscreen voting machine. All iVotronic machines used in Ohio include a VVPAT printer unit, which creates a physical copy of a cast ballot on thermal paper. The VVPAT records individual touches on the screen, including changes in a vote but does not create a summary of a voter's ballot at the end of the voting process like the Premier TSX DRE does. Voter verification must occur as the voter votes on each selection.



ES&S iVotronic DRE Voting Machine

- Personalized Electronic Ballot (PEB):** The PEB is a palm-sized hardware token that also stores ballot definitions for and records election results from an iVotronic DRE voting machine. In counties using the iVotronic DRE as the primary voting machine, boards of elections load each PEB with ballot types. One PEB for each precinct is chosen as the master PEB, and the others are referred to as supervisor PEBs. On Election Day, the master PEB opens and closes each iVotronic DRE. When a voter arrives at a polling location to vote, a poll worker inserts his or her supervisor PEB containing the ballot images into the iVotronic. The poll worker then removes the supervisor PEB, and the voter votes. The vote is recorded internally in the iVotronic and in a compact flash memory card contained in each machine. When the polling place closes, a poll worker inserts the master PEB into each of the iVotronic DREs in the precinct so that the single master PEB can collect and store the votes for all DREs in the precinct. The flash cards from each machine and the master PEB from each precinct are then returned to the board of elections office for tabulating the votes.



ES&S Personalized Electronic Ballot (PEB) for the iVotronic DRE Voting Machine  
(compared to the size of a quarter coin)

- **Flash Memory Cards:** The flash memory cards are used for various iVotronic DRE election functions, including updating its software and recording votes. Before each election, a flash card is programmed and inserted into each iVotronic. After an election, the memory cards provide an additional way to tally votes.



Flash Memory Card for iVotronic DRE Voting Machine  
(compared to the size of a quarter coin)

- **Model 100:** The M100 is the ES&S precinct-based optical ballot scanner. Before an election, the M100 is programmed by a prepared PCMCIA memory card to allow the machine to read the polling location's ballots. When a voter arrives at the polling location to vote, the voter is given an optical scan ballot. After marking his or her selections on the optical scan ballot, the voter inserts the ballot into the M100 optical scanner. The voter is given the chance to reject and retrieve the ballot (such as in the case of an overvote) or accept the ballot as voted. The M100 keeps a running tally of votes internally and on a PCMCIA memory card. After the polling place closes, the PCMCIA card is removed and the locked ballot box contained in the base of the scanner is removed. The PCMCIA cards and the ballot boxes are transported to the board of elections office for tabulating the vote.



ES&S Model 100 Precinct Count Optical Scan Voting Machine

- **PCMCIA memory cards:** The M100 optical scan voting machines use PCMCIA flash storage memory cards encoded with ballot types from the Unity software operated at the board of elections office. Before an election, appropriately-encoded PCMCIA cards are inserted into an M100 to be used at a polling location. The M100 reads proper election definitions from the prepared

PCMCIA card when the ballot is scanned into the machine. After an election, the PCMCIA card is removed from the M100 at the precinct and transported to the board of elections office for tabulating the votes.



PCMCIA Memory Card for M100 Optical Scanner (compared to the size of a quarter)

- AutoMARK:** The AutoMARK is a combination scanner/printer used by a voter – typically a voter with disabilities. The AutoMark allows touchscreen voting but uses a pre-printed ballot that contains a bar code. When an unvoted ballot is inserted into an AutoMARK machine, the machine reads the ballot’s bar code and identifies the ballot type, allowing the voter to vote by touching the screen and marking the voter’s selections onto the blank ballot. When a voter finishes voting, the ballot is ejected as marked for the voter to place the ballot into a ballot box or to insert the voted ballot into an optical scan machine.

### Physical Access Testing

The ES&S system performed “poorly” in the physical access testing because physical access to many of the system components could be used to “cause availability issues,” making voting machines inoperable to “attack the integrity of the elections data and process and introduce chaos in the elections process.” (Technical Manager’s Report, ES&S, at 9.)

MicroSolved described the following security vulnerabilities resulting from its physical access penetration testing:

- At the precinct level, the Automark – an ES&S electronic ballot printing device that does not tabulate votes, but rather prints voter’s decisions on a pre-printed optical scan ballot – could be easily compromised to allow an unauthorized individual to introduce malware into the system and affect how ballots are marked. The effects of this attack, however, may be minimal, as a voter is able to visually detect any errors on the ballot prior to inserting the ballot in the optical scanner or submitting it for counting. Nonetheless, an attacker could introduce malware into the Automark that is transferred to a memory card that at some point is reloaded into the Unity server operated at the board of elections. (*Id.* at 10-11.)

- ES&S precinct optical scanner, the M100, is susceptible to attacks at the polling location that could affect election integrity. First, a simple physical manipulation of the machine could result in it performing its poll closing function. As a result, an unauthorized individual could delete records of votes by zeroing out the vote totals. Second, an unauthorized individual with physical access to memory cards could prevent some or all scanned ballots from being recorded to the memory card for an M100 optical scan machine. MicroSolved determined it “likely” that unless there is close scrutiny or a recount of the precinct using the paper tapes and the actual ballots for a machine, the attack would go undetected. (*Id.* at 11.)
- Physical battering of a DRE by a voter at the precinct could easily cause the voting machine to have to be rebooted, causing delays and confusion during the voting process. (*Id.* at 11.)
- At the board of elections level, there are “critical weaknesses” in the security configurations of the computers running the Unity software. (*Id.* at 11.) MicroSolved concluded: “the computers hosting the software failed to be secured from physical attack in even the basic ways,” and unauthorized individuals could leverage these security weaknesses to introduce malware or compromise elections data. (*Id.* at 11.)
- The server and workstation lacked proper password policies, anti-virus software, and basic mechanisms for managing the integrity and security of the system. (*Id.* at 11-12.)

### **Network and Communications Access Testing**

ES&S performed “slightly better” in the network and communications access phase of the penetration testing by scoring a “medium.” (*Id.* at 10, 12.) However, problems remained in the equipment used in the precincts and at boards of elections. MicroSolved identified the following security vulnerabilities in its network and communications access phase:

- The DRE units showed a vulnerability in the printer connection where unauthorized individuals could easily connect their own device to the VVPAT printer and print their own results or rewind the paper tape to print over the existing voter records. (*Id.* at 12.)
- At the board of elections office, network attacks against the Unity server’s Windows 2003 storage server and the Windows XP workstation proved possible, which would allow an unauthorized individual access to the server’s network to compromise election data. Lack of firewalls on the PC devices, poor password and configuration policies, and the availability of unneeded services contribute to the identified risk. MicroSolved concluded: “It would be easy for an attacker who gains network access to compromise one or both of the computers and introduce malware to the system to alter voting data over time or outright destroy the software.” (*Id.* at 12.)

### **File Systems Access Testing**

The ES&S system performed “poorly” under the file systems testing. Several vulnerabilities on system components used at precincts and boards of elections could be used to introduce malware to the components. (Technical Manager’s Report, ES&S, at 10, 12.) MicroSolved identified the following security weaknesses in the file system testing:

- At the precinct level, the interaction of the DRE units with their memory cards proved to be “extremely vulnerable.” (*Id.* at 12-13) MicroSolved was able to cause a DRE to crash by tampering with a memory card, which could cause an unauthorized individual to introduce malware into the DRE component or its memory card and transfer illicit code to the Unity server. While access to memory cards is protected with tamper seals, MicroSolved found the seals were “easily circumvented.” (*Id.* at 13.)
- At the board of elections level, more “critical vulnerabilities” were identified. (*Id.*) For example, “fuzzing” – a software testing technique that consists of finding implementation bugs using malformed data injection in an automated fashion – of a certain file of ES&S’s central count optical scan machine, the m650, caused errors in the tabulation mechanism, which could be used to manipulate the vote count in the tabulation process. The Unity software also showed several areas of exposure to file fuzzing and input formatting attacks. According to MicroSolved, “[b]y leveraging these vulnerabilities through either direct access or through malware, an attacker is likely to be able to damage the software or influence its proper operation and handling of vote data.” (*Id.*)
- By using simple network applications, MicroSolved was able to reveal sensitive data hard coded in the software. Unauthorized individuals could use this information to design malware or compromise the software. (*Id.*)
- A mechanism exists in the Unity software for a user to arbitrarily edit vote totals. (*Id.*)

### **Baseline Comparison**

ES&S scored a “one” on the twelve-step baseline comparison framework – that is, the ES&S voting system failed to meet eleven of the twelve basic best practices requirements. (*Id.* at 15-16.)

### **Hart InterCivic**

The Hart InterCivic voting system performed “poorly” in the physical access testing and the file system access testing. The system performed “intermediate” in the network and communications access testing. (Technical Manager’s Report, Hart, at 9-10.)

### **Description of the Hart InterCivic Voting System**

The Hart voting system used in Ohio is a combination of DRE and optical scan components and is used in 2 Ohio counties. To better understand the findings included

in this report, the relevant components of the Hart system are described below.<sup>8</sup> The photographs are courtesy of the Academic research teams.

### ***Components at County Boards of Elections Offices***

The following components reside at county board of elections offices.

- **BOSS:** The Ballot Origination Software Systems is the Hart software used to set up an election, including defining the ballot for each precinct. BOSS exports election data to MBBs, described below, which transport the ballot definitions to each polling location.
- **Tally:** Tally is the Hart software that tabulates the votes in an election. After polling places close, MBBs from each precinct are delivered to the board office and loaded into the server for Tally to tabulate and generate reports of the election results.



Hart Software

### ***Components at Polling Places***

The following components are used at polling locations on Election Day.

- **MBB:** A Mobile Ballot Box is a PCMCIA card that stores ballot definitions and vote results. MBBs are the primary means of transmitting election data between a polling place and the board of elections. Before an election, ballot definitions are transmitted from BOSS to an MBB. MBBs are then installed into the JBC, described below, and also into eScan devices, described below, and tamper-sealed into these machines. The MBBs may also be transported to the polling locations for installation onsite at each precinct. After polling places close, MBBs from the JBC and eScan units are transported back to the board of elections for tabulating votes.

---

<sup>8</sup>Please refer to the Academic Final Report at Chapter 17, attached at Appendix F, for more detailed descriptions.

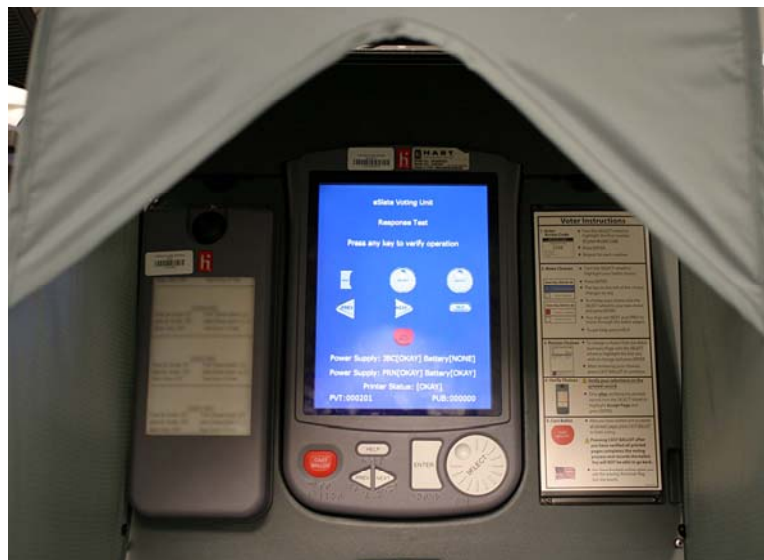


- JBC:** The Judge's Booth Controller is a console that controls access to all the Hart DREs (eSlates, described below) at a polling location. The JBC can be connected to up to twelve Hart DRE voting machines. The JBC generates voter access codes, distributes ballot configuration to the eSlates, records votes, and stores eSlate ballots to internal memory. MBBs are also inserted into a JBC to store ballots. On Election Day, poll workers start the JBC by entering a password. After an election, the MBBs from the JBC are transported to the board of elections for tabulating votes.



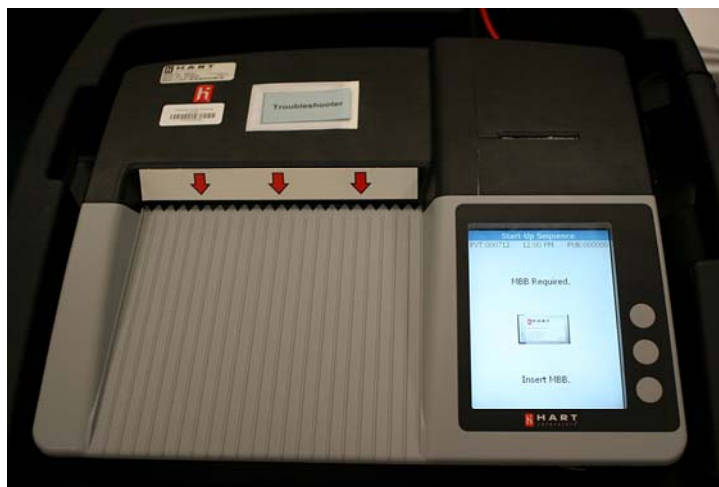
Judges Booth Controller for DRE eSlate Voting Machines

- eSlate:** The eSlate is a DRE voting unit used in a Hart-run precinct – typically for voters with disabilities. When a voter arrives at a polling location to vote on the eSlate, the voter proceeds to the poll worker staffing the JBC. Each voter receives a 4-digit access code. The voter proceeds to the eSlate where he or she enters the code and votes according to the instructions. At the close of the election, poll workers enter a password into the JBC to close the polls and the eSlate machines. The MBB from each JBC is transported to the board of elections for vote tabulation.



## Hart eSlate DRE Voting Machine

- eScan:** The eScan is Hart's precinct-based optical ballot scanner. The eScan scans and tabulates optical scan ballots and contains an MBB used to store tabulated vote results. Before an election, ballot definitions are transmitted to the eScan through an MBB. On Election Day, poll workers activate the eScan by entering a password. During an election, voters complete an optical scan ballot and insert it into the eScan machine. The voter is given the chance to reject and retrieve the ballot (such as in the case of an overvote) or accept the ballot as voted. After the polling places close, poll workers enter a password into the eScan to close the machines and prevent further voting. The MBB from the unit is transported to the board of elections for vote tabulation.



Hart eScan

### Physical Access Testing

The Hart system performed “poorly” in the physical access testing because physical access to the optical scanner device and the two computer systems hosting the Hart software was “tantamount to complete compromise of the system.” (Technical Manager’s Report, Hart, at 9.) MicroSolved identified the following security issues in the physical access testing:

- At the precinct level, the DRE voting units and Judges Booth Controller unit at the precinct level are “quite resistant to physical attack. . . . The team could not identify a way to circumvent the operating modes of these units or achieve access to their underlying operating systems.” (*Id.* at 11.)
- Physical attacks against the Judges Booth Controller led to the discovery of a potential problem with the generation of voter access cards, which could allow an unauthorized individual to vote multiple times using the DRE device. (*Id.*)
- Compromise of the precinct optical scanner can be “easily gained.” An unauthorized individual with sufficient knowledge could “easily overcome the tamper seals and either modify or replace the operating system files or memory card.” (*Id.*) Highly resourced individuals could then introduce malware that could affect the integrity of the election.

- The ballot box on the optical scanner was easily unlocked using common lock picking techniques, which would allow unauthorized individuals to access voted ballots. (*Id.* at 12.)
- The security of the PCMCIA memory cards used to carry the elections data between the precincts and the board of elections is “inadequate.” (*Id.* at 12.) Unauthorized individuals who gain access to the memory cards can easily tamper with the data and affect election integrity.
- At the board of elections level, both computers used with the Hart voting system were “easily compromised.” (*Id.*) Unauthorized individuals could “easily circumvent” any existing protections. (*Id.*)

### **Network and Communications Access Testing**

The Hart system performed “intermediate” during these tests because exploitation of the optical scanner was not proven possible. (*Id.* at 10.) However, MicroSolved identified the optical scanner as running insecure services. In addition, the network connection used to transfer elections data between software components was found to be improperly transferring data in text without encryption, and the computers hosting the software were found to be “easily compromised” through deciphering passwords. (*Id.*)

### **File Systems Access Testing**

The Hart system performed “poorly” in the file systems access testing because unauthorized individuals could gain access to the memory cards and “easily tamper” core voting data. (*Id.* at 10.) MicroSolved identified two critical risks:

- The database storing election data is unencrypted. Unauthorized individuals could therefore gain access to election data. Unless auditing is performed against the paper tapes, this would likely go undetected. (*Id.* at 13.)
- System software allows editing of election results. While editing is logged, the logs could be missed or deleted by an unauthorized individual. (*Id.*)

### **Baseline Comparison**

Hart scored a “zero” on the twelve-step baseline comparison framework – that is, the Hart InterCivic voting system failed to meet any of the twelve basic best practices requirements. (*Id.* at 14-16.)

### **Suggested Improvements: All Voting Systems**

MicroSolved reported three suggestions for improvement:

- **First**, all parties, including voting machine manufacturers, must “embrace industry standard best practices” and election officials must “enforce them through technology, policy and process and education.” (Project Executive Summary Report at 11.)

- **Second**, the voting manufacturers must proceed to “deploy proper integrity controls such as anti-virus software, firewalls, encryption and deeper techniques such as proper bounds checking on inputs and other security programming standards.” (*Id.*) Additionally, the secretary of state must implement use of the Digital Guardian security tool on all voting systems and ensure that the tool is correctly configured.
- **Third**, the voting machine manufacturers must “undertake a systemic approach to mitigating the identified vulnerabilities in the system.” (*Id.*) MicroSolved concluded: “Each issue mitigated by the vendor greatly reduces the amount of risk management that must be transferred to the counties by policy and process controls. Given the lack of resources many of the counties face, this is likely to have significant impact on the entire election process.” (Technical Manager’s Report, Premier, at 17.) The specific security vulnerabilities identified by MicroSolved are listed in its Technical Details Report for each system, which is attached at Appendix E.

### **Summary of Boards of Elections Officials’ Review of MicroSolved’s Findings on the Security Assessment of the State’s Voting Systems**

Two Republicans and one Democrat boards of elections officials reviewed MicroSolved’s findings on the security of Ohio’s three voting systems. All three of these officials utilize the Premier DRE voting system in their respective counties. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a “scribe.” A “Capsule Summary Statement” of the elections officials’ review is provided below, basically as prepared by the “scribe,” along with a table summarizing this boards of elections review team’s standardized evaluation of MicroSolved’s findings.

#### **Capsule Summary Statement by Boards of Elections Teams Reviewing MicroSolved’s Findings**

##### **Executive Summary (All Systems): Group Summary Statement**

- The report is useful, but the summary table is vague. The report is useful in that it can start the conversation, but one does not know if the poll worker or any other unauthorized individual could emulate one of the security attacks. As election officials, we can now go back and re-evaluate what is being done in our office. However, we can see where some of these security attacks could happen — for instance, we can see where the use of generic log accounts allow unidentified users to access the Premier GEMS server.

##### **Premier Report: Summary Statement**

- The overriding theme in all of the MicroSolved reports is that Ohio needs to have statewide written procedures for security. Basic updates to Windows, such as patches certified from Windows, must be allowed without having to go through the Board of Voting Machine Examiners. The voting machine manufacturers must update the software or hardware for the voting systems.

While written procedures are needed in all 88 counties, the state needs to take into consideration that every board of elections is different. Statewide procedures should take into account that in one county there may be two employees, and only one may work on voting equipment or the server. In other counties, however, there may be many employees, and neither the Director or Deputy Director operates the voting equipment or server.

While gaining access to change vote totals is necessary and provided for in Ohio election law, there should be an audit log demonstrating when and if this occurs. Server software should not allow its databases to be opened through a Windows program without having the server software open.

The reports were very thorough, and brought up new topics to start the conversation.

### **ES&S Reports: Group Summary Statement**

- The boards of elections officials could relate to this report more than the Hart report. MicroSolved found more problems with the ES&S machines but clarified their statements and gave good explanations. The findings in the reports are “scary,” but the report is “very good.”

### **Hart Reports: Group Summary Statement**

- The group felt that the report gave good, quality answers, but the group did not feel that every hypothetical security attack was possible. However, the report presented a problem and a corresponding solution, which is what the boards of election officials were seeking.

### **Summary Table of Standardized Evaluations**

#### **Average Commercial Security Report Quality Ratings by Election Officials**

Quality	Scale	Executive Summary	ES&S	Hart	Premier
Data	1-3	2.3	2.7	2.3	3.0
Claims	1-3	2.3	2.7	2.3	2.3
Warrants	1-4	3.0	3.0	3.0	3.7
Coherence	1-4	3.7	4.0	3.7	4.0
Overall	1-5	4.3	4.7	4.3	4.3

Note. This table represents the average ratings of three election officials.

#### **Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent

## University Research Teams

The Academic researchers performed source code analysis and “red-team” testing of the Premier, ES&S, and Hart voting systems. Because the ES&S voting system has not yet been the subject of a detailed security review, a team of faculty and graduate students at the University of Pennsylvania focused on a source code analysis of the ES&S voting system, and a collection of security consultants at Webwise Security, Inc., supported by two experts from the University of California at Santa Barbara, focused on the red-teaming exercises on the ES&S voting equipment. A team of faculty, graduate students, and one consultant at the Pennsylvania State University focused on the source code analysis and red team testing of the Hart and Premier voting systems. The Hart and Premier voting systems have been the subjects of previous security reviews conducted outside of the State of Ohio.

Parallel to MicroSolved’s review, the Academic research teams attempted to assess the security of the voting systems used in Ohio and identify procedures that may eliminate or mitigate discovered issues. The Academic teams concluded: “All of the studied systems possess critical security failures that render their technical controls insufficient to guarantee a trustworthy election.” (EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, Final Report (hereinafter “Academic Final Report”) at 3.) Further, the researchers found that “such flaws mandate fundamental and broad reengineering before the technical protections can approach the goal of guaranteeing trustworthy elections.” (*Id.* at 4.)

The Academic teams created one Academic Final Report – consisting of 316 pages – outlining the methods and results of their review. The Academic Final Report is divided into five parts. Part I provides an executive overview of findings, a broad description of the evaluation structure – including a “threat model” used to structure the evaluation of voting machine security for all three systems – activities, and limitations, and it identifies the security features of the three voting systems. Parts 2 through 4 detail each voting systems’ evaluation. Part 5 contains reference appendices providing supporting technical and testing procedure information. Much of Part 5 is redacted in the Appendix to protect voting systems currently in use from being abused or penetrated. This Secretary’s Report briefly explains the Academic teams’ methods and findings. The complete Academic Report is attached at Appendix F.

### Method

The first step in the Academic security analysis was to define the “threat model.” Similar to that used by MicroSolved, the research teams’ threat model describes (1) the goals an “attacker” might have, (2) the types of attackers that might attempt to attack the system, and (3) the capabilities available to each type of attacker. (*Id.* at 11.)

- **Attacker Goals:** The researchers first identified the possible “attacker” goals:
  - Producing incorrect vote counts
  - Blocking some or all voters from voting
  - Casting doubt on the legitimacy of the election results

- Delaying the results of the election from becoming known, or
- Violating the secrecy of the ballot.
- **Potential Attackers:** The researchers' model then considered the following broad classes of attackers:
  - **Outsiders:** Outsiders have no special access to any voting equipment, other than attacks based on equipment connected to the internet or breaking into storage facilities to tamper with voting equipment.
  - **Voters:** Voters have limited and partially supervised access to voting systems during the process of casting their votes.
  - **Poll workers:** Poll workers have extensive access to polling place equipment, including management of the voting equipment, before, during, and after voting.
  - **Election officials:** Election officials have extensive access to the election management systems and the voting equipment. If election officials have unsupervised access to the systems, the integrity of those systems is provided purely by the integrity and honesty of the election officials.
  - **Vendor employees:** Vendor employees have access to the hardware and source code of the system during development and also assist election officials. Some vendors use third-party maintenance and Election Day support whose employees are not tightly regulated.
- **Types of Attacks:** The researchers categorized the severity of attacks along the following dimensions:
  - **Detectable vs. Undetectable:** Some attacks are undetectable, while others are detected in principle but unlikely to be detected unless certain election processes or procedures are routinely followed. An undetectable threat is especially severe and high priority, as the public could never be certain that the election results were not corrupted by undetected tampering.
  - **Recoverable vs. Unrecoverable:** If an attack is detected, there is often a way to recover. In contrast, some attacks can be detected, but there may be no good recovery strategy. Attacks that are detectable but not recoverable are serious, although not as serious as undetectable attacks. The researchers presumed that most elections will not be subject to attack, and the ability to verify that any particular election was not attacked is valuable.
  - **Prevention vs. Detection:** The researchers presumed that voting systems are designed as a tradeoff between prevention and detection of security attacks. Designing a voting system to prevent attack entirely may not be possible so an attractive alternative is to design mechanisms to detect attacks and recover from them.

- **Wholesale vs. Retail:** The researchers attempted to distinguish attacks that attempt to tamper with many votes (a “wholesale” attack) from attacks that attempt to tamper with only a few votes (a “retail” attack).
- **Casual vs. Sophisticated:** The researchers presumed that some attacks require little technical knowledge or sophistication, and, in contrast, other attacks require deep technical knowledge, specialized skill, or advance planning. The researchers studied both sophisticated attacks and casual, low-tech attacks.

Judgments about the probability of an attack or the impact on the election were specified in the report as outside the scope of the researchers’ review.

After creating the threat model, the Academic researchers reviewed Ohio’s election *procedures*. Election procedures are best practices, typically mandated by a county board of elections or the secretary of state to ensure that an election is carried out securely and correctly. Procedures are often as important as the technical security features of the election system. However, the researchers also presumed that given the human involvement in procedures, any procedure, no matter how well-crafted should be viewed as an “imperfect mitigation.” (*Id.* at 23.) Therefore, those setting procedures should carefully consider what happens when procedures are not followed.

## Findings

### Summary

The Academic researchers identified four “critical failures in design and implementation” of all three voting systems. (*Id.* at 3.)

- **Insufficient Security:** The voting systems uniformly “failed to adequately address important threats against election data and processes,” including a “failure to adequately defend an election from insiders, to prevent virally infected software . . . and to ensure cast votes are appropriately protected and accurately counted.” (*Id.*)
- **Security Technology:** The voting systems allow the “pervasive mis-application of security technology,” including failure to follow “standard and well-known practices for the use of cryptography, key and password management, and security hardware.” (*Id.*)
- **Auditing:** The voting systems exhibit “a visible lack of trustworthy auditing capability,” resulting in difficulty discovering when a security attack occurs or how to isolate or recover from an attack when detected. (*Id.*)
- **Software Maintenance:** The voting systems’ software maintenance practices are “deeply flawed,” leading to “fragile software in which exploitable crashes, lockups, and failures are common in normal use.” (*Id.*)

The Academic teams were able to provide a number of procedures that may mitigate or completely address identified security issues. However, in many cases, the teams could



not identify any practical procedures that will adequately address the security limitations. (*Id.*)

### **Specific Results: Source Code Analysis and Red Team (Penetration) Testing**

#### **ES&S**

The Academic researchers concluded that the central server and software and the precinct-based components, both DRE and optical scan voting machines (*i.e.*, the ES&S Unity Election Management System (EMS), iVotronic DRE and M100 optical scan systems) “lack the fundamental technical controls necessary to guarantee a trustworthy election under operational conditions.” (*Id.* at 29.) The researchers discovered “exploitable vulnerabilities” that allowed even persons with limited access – such as voters or poll workers – to compromise voting machines and election results, or to inject and spread software viruses into the central election management system. (*Id.*) Academic researchers concluded that these vulnerabilities arise from the following “pervasive, critical failures”:

- Failure to protect election data and software
- Failure to effectively control access to election operations
- Failure to correctly implement security mechanisms
- Failure to follow standard software and security engineering practices

(*Id.*)

Given that this was the first in-depth security analysis of the ES&S system, the Academic researchers concluded:

We believe the issues reported in this study represent practical threats to ES&S-based elections as they are conducted in Ohio. It may in some cases be possible to construct procedural safeguards that partially mitigate some of the individual vulnerabilities reported here. However, taken as a whole, the security failures in the ES&S system are of a magnitude and depth that, absent a substantial re-engineering of the software itself, renders procedural changes alone unlikely to meaningfully improve security.

(*Id.* at 30.)

Because the security failures of the ES&S system are “severe and pervasive,” the Academic research teams listed a voting system that uses only a centrally-counted optical scan hardware as an alternative system that may eliminate many of the precinct-based security attacks. (*Id.*)

#### **Failure to Protect Election Data and Software**

The researchers concluded that the firmware and configuration of the ES&S precinct hardware can be “easily tampered with” at the polling place. (*Id.* at 29.) Virtually every piece of precinct hardware could be compromised without knowledge of passwords and

without the use of any specialized proprietary hardware. (*Id.*) Some of the identified vulnerabilities included:

- Poll workers or voters can re-calibrate the screen of an iVotronic to prevent voting for certain candidates or to cause voter input for one candidate to be recorded for another. The procedure for re-calibrating required about one minute and is “largely indistinguishable from normal voter behavior.” (*Id.* at 50.)
- Access to certain PEBs could allow unauthorized individuals to alter poll-closing functions, such as the precinct’s reported vote tallies, and inject malicious code that could be transferred from memory cards to other DREs and memory cards to the board of elections’ central system or server. (*Id.* at 51.)
- The basic physical security features that protect precinct hardware – such as locks and seals – are “ineffective” or “easily defeated.” (*Id.* at 52.) For example, a primary mechanism for logging events on the iVotronic terminal is the RTAL printer. However, the cable connecting the printer is readily accessible to a voter and can be easily removed without tools or suspicious activity. (*Id.*)
- The Unity tallying system and the iVotronic terminal have “buffer overflow software bugs” that allow unauthorized individuals who can provide input on a removable storage media device, such as a PEB or memory card, to effectively take control over the system. A buffer overflow in input processing is a common type of programming error (that is, placing too much code in a memory-limited space) that has been responsible for many security failures in modern computing. (*Id.* at 53.) For example, the researchers experimentally proved that malicious code could be injected at the precinct level to change the votes of both inattentive voters and attentive voters monitoring the VVPAT. The researchers crafted a malicious PEB that overflowed the memory buffer and introduced it into the voting system. (*Id.* at 93-94.)
- Other identified vulnerabilities can be found in Chapters 7 and 9 of Appendix F.

### **Failure to Effectively Control Access to Election Operations**

The researchers concluded that access to administrative and voter functions are protected with “ineffective security mechanisms.” (*Id.* at 29.) Some of the identified vulnerabilities include:

- The iVotronic’s security mechanisms – such as passwords or firmware update functions – are “ineffective,” as the researchers found several practical ways to bypass each security mechanism and successfully replace or alter the iVotronic firmware, without knowledge of passwords or breaking any seals, such as when the polls are open. Any attack that compromises firmware is extremely serious, as the firmware controls every aspect of the ballot presented to the voters, the recorded votes, and the tally system. (*Id.* at 55.) For example, a firewall alteration was experimentally proved to fake a voter into believing that his or her vote was cast, although it was not. Seconds after the voter left the voting machine, the machine returned to the confirmation page, which resulted in a “fleeing voter” scenario, and the vote did not count. (*Id.* at 95-96.)

- The Unity software runs on an off-the-shelf operating system and therefore is “heavily dependent” on the local computing environment for its security. (*Id.* at 56.)
- Any person can load firmware into the M100 precinct optical scan with access to a PCMCIA card slot. Tamper seals may protect the slot, but researchers found that the seal may be bypassed. (*Id.* at 56.)
- The software or firmware of almost every major component can be altered or replaced by input from the other components with which it communicates. (*Id.* at 56.)

### **Failure to Correctly Implement Security Mechanisms**

The researchers concluded that many of the most serious vulnerabilities in the ES&S system arise from the incorrect use of security technologies such as cryptography. This effectively neutralizes several basic security features, exposing the system and its data to misuse or manipulation. (*Id.* at 29.) Some of the identified vulnerabilities include:

- The data on the M100 PCMCIA cards – the removable storage devices used to load ballot definitions and firmware into the M100 and to report vote tallies back to the Unity system at the board of elections office – are not cryptographically protected. Therefore, an unauthorized individual can “easily” forge or modify election results. (*Id.* at 57.)
- The iVotronic DRE uses cryptography to protect data on its removable storage devices – the PEB and the CF card. However, errors in its implementation render the protection “completely ineffective.” (*Id.*)

### **Failure to Follow Standard Software and Security Engineering Practices**

The researchers concluded that a root cause of the security and reliability issues present in the system is the “visible lack of sound software and security engineering practices.” (*Id.* at 29.) Examples include poor or unsafe coding practices, unclear or undefined security goals, technology misuse, and poor maintenance. This general lack of quality leads to a “buggy, unstable, and exploitable system.” (*Id.*)

### **Premier**

The Academic review concluded that the Premier system “lacks the technical protections necessary to guarantee a trustworthy election under operational conditions.” (*Id.* at 103.) Flaws in the system’s design, development, and processes lead a “broad spectrum of issues that undermine the voting system’s security and reliability.” (*Id.*) These vulnerabilities result in the following failures of Premier’s voting system:

- Failure to effectively protect vote integrity and privacy
- Failure to protect election from malicious insiders
- Failure to validate and protect software
- Failure to provide trustworthy auditing
- Failure to follow standard software and security engineering practices.

The researchers' findings were consistent with previous studies identifying vulnerabilities with the Premier system, which were conducted as early as 2001. After numerous reviews and new software and hardware upgrades, the researchers not only discovered the same problems as reported earlier but uncovered new serious issues as well. The researchers concluded: "[t]he review teams feel strongly that the continued issues of security and quality are the result of deep systemic flaws. Thus, we agree with previous analysis and observe that the safest avenue to trustworthy elections is to re-engineer the Premier system to be secure by design." (*Id.* at 104.)

### **Failure To Effectively Protect Vote Integrity and Privacy/Failure to Protect Elections From Malicious Insiders**

The researchers identified numerous vulnerabilities that could allow an unauthorized individual to "modify or replace ballot definitions, to change, miscount, or discard completed votes, or to corrupt the tally processes." (*Id.* at 103.) Furthermore, the Premier system does not provide adequate protections to prevent that election officials or vendor representatives do not manipulate the system or its data. (*Id.*) Some of the identified vulnerabilities include:

- The methods used to protect the integrity and privacy of important election data are circumventable. For example, the security protections on the memory cards – which are the central device for storing and communicating election data – are "ineffective" at preventing an unauthorized individual from viewing or modifying the data held on the card. (*Id.* at 114.) The memory cards for the precinct optical scan machine are completely "unprotected," and the memory cards for the DRE, the AV-TSX, while superficially protected by a "Data Key," are not "adequately protected." (*Id.*) The result is that an unauthorized individual who gains access to a memory card may modify elections results. The researchers experimentally proved that, because the memory cards for the DRE machines are encrypted using the same data key, a single compromised voting machine renders vulnerable the results on all other memory cards in the county. (*Id.* at 160.)
- The precinct-based optical scan and DRE machines "failed" to meet the goal of voter privacy, as the systems could be used in conjunction with poll books to determine voter choices. (*Id.* at 114.)
- The databases on the Premier GEMS server are "largely unprotected and can be freely accessed." (*Id.*) For example, access to GEMS functionality is governed by passwords that can be cracked using "standard password cracker tools." (*Id.*) Additionally, the audit logs, which provide an evidentiary trail of server usage, are not authenticated and are prone to forgery or alteration. (*Id.* at 162-63.)
- The use of many standard security technologies are "deeply flawed." (*Id.* at 113.) For example, the creation, storage, and use of the cryptographic keys used in the DRE and the GEMS server and connected EMP work stations to preserve the secrecy and integrity of election data are "insufficient to ensure an attacker cannot view or modify election data." (*Id.* at 115.) The Voter Card Encoders, used to allow voters to cast individual ballots, are not protected by a PIN or other security enhancement. Once a Voter Card Encoder is enabled, no additional security layer prevents unauthorized use to cast multiple ballots. (*Id.* at 171.)

- The Digital Guardian software, installed on the GEMS server to address already known security issues, is “circumventable” to render Digital Guardian inoperable and remove its protections. (*Id.* at 120.)
- Other identified vulnerabilities can be found in Chapters 13, 14, and 15 of Appendix F.

### **Failure to Validate and Protect Software / Failure to Follow Standard Software and Security Engineering Practices**

The researchers concluded that the Premier system makes only “limited and ineffective attempts to validate the software running within the system.” (*Id.* at 103.) As a result, an unauthorized individual may “exploit software and replace it with their own with little fear of detection.” (*Id.*) For example, because the components of the Premier system trust one another, a malicious GEMS server or DRE could crash an EMP. (*Id.* at 166.)

Additionally, errors in coding and design are concluded to be “widespread” in the Premier system. (*Id.* at 117.) These issues could lead to “serious vulnerabilities” that can affect the processes and accuracy of an election. (*Id.*) The researchers concluded that errors in the coding of the Premier system can be attributed to: complexity of the system components; lack of basic mechanisms to ensure integrity of the software; lack of security practices appropriate for its system; and over-reliance on commercial off-the-shelf software. (*Id.*)

### **Failure to Provide Trustworthy Auditing**

The researchers concluded that the auditing capabilities of the Premier system are “limited.” (*Id.* at 103.) The current auditing features are “vulnerable to a broad range of attacks that can corrupt or erase logs of election activities,” resulting in a severe limitation of election officials’ ability to detect and diagnose attacks. Moreover, because the auditing features are generally unreliable, recovery from attack may in practice be “enormously difficult or impossible.” (*Id.*)

### ***Hart***

The Academic researchers concluded that the Hart system “lacks the technical protections necessary to guarantee a trustworthy election under operational conditions.” (*Id.* at 197.) The vulnerabilities and features of the system work in concert to provide “numerous opportunities to manipulate election outcomes or cast doubt on legitimate election activities.” (*Id.*) These vulnerabilities result in the following failures of Hart’s voting system:

- Failure to effectively protect election data integrity
- Failure to eliminate or document unsafe functionality
- Failure to protect election from malicious insiders
- Failure to provide trustworthy auditing.

The researchers concluded that their findings are consistent with those of previous studies of the Hart voting system:

The lack of protections leaves the system vulnerable. Thus, the security of an election is almost entirely reliant on the physical practices. The technical limitations of its design further show that when those practices are not uniformly followed, it will be difficult to determine if attacks happened and what they were. Even when such attacks are identified, it is unlikely that the resulting damage can be contained and the public's confidence in the accuracy and fairness of the election restored.

(*Id.* at 198.)

### **Failure To Effectively Protect Election Data Integrity**

The researchers concluded that virtually every ballot, vote, election result, and audit log is “forgeable or otherwise manipulatable by an attacker with even brief access to the voting systems.” (*Id.* at 197.) The reason is that the mechanisms that Hart uses to protect data and software is frequently based on absent or flawed security models. The researchers concluded that “in most cases these issues cannot be addressed via software upgrades, but call for rethinking of both technical design and procedural practices.” (*Id.* at 208.) Some of the identified vulnerabilities include:

- Much of the data security in the Hart system flows from the single 32-byte key. The design of the Hart voting system therefore violates a basic isolation tenet of security engineering: compromise of a single precinct provides materials to compromise any precinct and election headquarters. If such compromise occurs, it will be impossible to identify which precinct is responsible for the attack. (*Id.* at 208.)
- Hart’s back-end or board office devices are networked to each other; however, Hart provides no device-to-device communication security, exposing critical data to an unauthorized individual who could generate voter codes, upload firmware, or erase voting or audit data. (*Id.* at 208-209.)
- The Hart software and firmware internal validity checks, where present, are “ineffective” at detecting compromises. (*Id.* at 209.) For example, in the case of the eScan (the precinct-based optical scanner), an unauthorized individual can replace the entire firmware with unobserved access to the eScan for 60 seconds, which would allow an unauthorized individual to completely alter election results on the Mobile Ballot Box (MBB) and the PCMCIA card. (*Id.*)
- Every authentication mechanism in the Hart system is “circumventable,” including the hardware tokens, passwords, PIN numbers, and voter codes. (*Id.*)
- Other identified vulnerabilities can be found in Chapters 19, 20, and 21 of Appendix F.

### **Failure To Eliminate Or Document Unsafe Functionality**

The researchers identified a number of largely undocumented features in the Hart system that are “highly dangerous” in an election system. (*Id.* at 197.) The Hart system consists of thousands of lines of code distributed over a large number of applications and developed over a decade by various developers. A byproduct of this process is a “large number of old, unused, and otherwise ‘orphaned’ features built into the software.” (*Id.* at 210.) The researchers concluded that these features present a source of security issues.

### **Failure To Protect Election From “Malicious Insiders”**

The researchers concluded that the protections in the Hart system that are intended to prevent election officials and vendor representatives from using dangerous features or modifying election data are “circumventable.” (*Id.* at 197.) Individuals with access to the voting system can quickly recover critical system passwords, extract cryptographic keys, and reproduce security hardware, which can ultimately “forge election data and compromise nearly all of the Hart election equipment.” (*Id.*)

### **Failure To Provide Trustworthy Auditing**

The researchers concluded the auditing capabilities of the Hart system are “limited.” (*Id.* at 197.) The auditing features provided are “vulnerable to a broad range of attacks that can corrupt or erase logs of election activities.” (*Id.*) This severely limits the ability of election officials to detect and diagnose attacks.

## **Summary of Boards of Elections Officials’ Review of the Academic Research Teams’ Findings on the Security Assessment of the State’s Voting Systems**

Two Democrats and one Republican boards of elections officials reviewed the Academic research teams’ findings on the security of Ohio’s three voting systems. Two of these officials utilize the Premier DRE voting system in their counties, while the third utilizes the ES&S DRE voting system in his or her county. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a “scribe.” A “Capsule Summary Statement” of the elections officials’ review is provided below, basically as prepared by the “scribe,” along with a table summarizing this boards of elections review team’s standardized evaluation of the Academic teams’ findings.

### **Capsule Summary Statement by Boards of Elections (BOE) Team Reviewing the Academic Teams’ Findings**

#### **Part 1 of the Academic Report: Group Summary Statement**

Part 1 was well written and organized with a clear focus that generates an opinion. The report is created within a logical framework. At this introductory stage, the BOE officials posited that the report is generally based on pure supposition and bias. The BOE officials stated that the information in the Executive Summary, Overview and Threat Model was based on a variety of data intertwined with personal experience, finding that a large amount of information was unsubstantiated and biased and that the report

supported the biases of the authors in order to substantiate their claims. The BOE officials agreed that the claims are presented in a specific manner with a consistent point of view. Nonetheless, after reviewing Part 1, the BOE officials did not initially agree with the report or the conclusions contained within the report.

There was concern about the following statement contained in the report: “Doubt is often difficult to dispel. Lingering concerns often have a chilling effect on voters, and tend to color unrelated legitimate activities as well. Such concerns may continue for future elections.” (Academic Final Report at 16.) The BOE officials are concerned that the authors of the study could be placed in the position to be an “attacker” of voting systems. Therefore, they could have the ability to cast doubt on the election process, which would have a devastating effect on the election process. One BOE official expressed concern that the Academic reviewers appeared not to trust that election officials would make every effort to conduct a fair and honest election.

### **Part 2 of the Academic Report on ES&S: Group Summary Statement**

The BOE officials next reviewed the chapters of the Final Academic Report devoted to ES&S. The BOE officials agreed that this information was extensive and well developed but highly technical. The report contained numerous examples of security issues with the ES&S system and their impact on the system and the election process. However, the BOE officials believed they would have been able to gain a more accurate assessment if the report included a peer review. The BOE officials discovered some discrepancies in the use of footnotes. Additionally, the BOE officials’ most notable concern about the report was that solutions to these security issues were not presented.

The BOE officials described the language in the report as “over-hyped.” For example, the BOE officials highlighted the follow sentence: “additionally, the key blanks for a scanner and ballot box key are easily duplicated, so a compromise of either key could affect machines nation-wide.” (Academic Final Report at 73.) The BOE reviewers believed this language illustrated a biased view of the authors. The BOE officials concluded that a probability scale with a rating system of likely, unlikely and highly unlikely would have been a useful tool for those reviewing the report. Overall, the BOE officials agreed the report on ES&S rated between good and excellent, but the information was voluminous in nature and difficult for a layperson to comprehend. After a review of the ES&S section, the BOE officials did not agree with the information as presented in the report.

### **Part 3 of the Academic Report on Premier: Group Summary Statement**

The BOE officials next reviewed and evaluated the sections of the Academic Final Report devoted to the Premier voting system. The BOE officials concluded that these sections lacked sufficient evidence relating to real-life situations in which an attacker could circumvent the security of the voting system. Because the testing was completed in a controlled-academic setting, the BOE officials gave some areas of the report less weight and validity. The lack of performing these tests in real-life settings provided enough skepticism to cause the BOE officials to question the outcomes as fact-based realities. There was also a concern that the review team had a slightly higher bias toward Premier than other systems. The BOE officials were unclear whether the prior reports on Premier could be attributed to be the cause of this bias, or whether the review team simply replicated experiments within the prior study with a few minor adjustments. For example, the Academic researchers tested voter privacy by stacking ten ballots in the ballot box. The BOE officials agreed that a proper sample for real-life application would



be a test of 350 ballots.

The BOE officials believed the report had a clear and consistent point of view. However, there were several inconsistencies within the report, as well as mechanical errors. For example, there were incorrect statements about the supervisor smart card. The BOE officials agreed that the terminology created a mistrust of election officials by using the term "malicious election officials." The BOE officials felt this reference "planted seeds" in the mind of the public to mistrust those who oversee elections. The report also minimizes mitigation, allowing the problems with the voting systems to seem larger and more complex. The lack of procedural mitigations offered was a disappointment for the group. The BOE officials found the report gave more credibility to the problems than the solution. Generally speaking, the BOE officials found that the report supports a certain political spectrum that believes that all electronic voting equipment is unsafe and evil.

The amount of mechanical errors contained within the report caused the BOE officials to question the validity of certain assertions, but it was not sufficient to compromise the credibility of the report. The study is based on clinical testing with a limited view.

#### **Part 4 of the Academic Report on Hart: Group Summary Statement**

The BOE officials next reviewed and evaluated the sections of the Academic Final Report devoted to the Hart voting system. The BOE officials concluded that the report was written in a coherent fashion with scenarios that could be understood. The report presented various problems that could affect any election with any voting system. The problems stated throughout the report were not unique to the Hart system. The BOE officials believe there were several test assessments that could have been performed with punch cards and lever machines. There were some claims that BOE officials believed to be outside the scope of real-world applications, and there were instances where the BOE officials found that the data contradicted the researchers' claims. The BOE officials suggested that some logical conclusions were not presented as solutions. The flaws in logic found by these BOE officials led them to conclude that these flaws created a lingering doubt over the previously reviewed sections of the report relating to ES&S and Premier.

However, the sections devoted to the Hart voting system suggested more evidence of mitigation. In general, the BOE officials found this section of the report did offer solutions that were feasible and reasonable. The BOE officials believed that the review team could confirm their findings, because the source code was detectable. It was the general consensus that the material presented could have harsh ramifications in an elections context. The group suggested that many of the problems in the report could also happen with a simple desktop computer system. Further, the BOE officials found that some of the conclusions required leaps in logic that could not be related to real-world situations. There were questions of practicality and poor reasoning within the report. Specifically, the BOE officials found that the report itself could be viewed as an attack on the election system. The BOE officials found that the context of the situations needs further clarification in order to be clearly stated and supported.

**Summary Table of Standardized Evaluations by Boards of Elections Team  
Reviewing the Academic Teams' Findings**

**Average Academic Security Report Quality Ratings by Election Officials**

Quality	Scale	Executive Summary	ES&S	Hart	Premier
Data	1-3	2.3	3.0	2.7	2.7
Claims	1-3	3.0	3.0	3.0	2.7
Warrants	1-4	2.5	3.0	2.7	3.0
Coherence	1-4	3.7	4.0	4.0	3.3
Overall	1-5	4.3	4.7	4.3	4.3

Note. This table represents the average ratings of three election officials.

**Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent

## **Configuration Management Assessment**

### **SysTEST**

The SysTest Risk Assessment Team performed a configuration management assessment of Premier, ES&S, and Hart InterCivic voting systems. The purpose of SysTest's assessment was to evaluate the secretary of state's ability to independently verify that the configuration of each voting system as approved for use by respective jurisdictions was consistent with, and unchanged from, the configuration certified by the State of Ohio, and that the certified configuration remained unchanged during all parts of the election process, including tabulation, during which results potentially could be affected. As part of its assessment, SysTest examined the processes and procedures used by the State of Ohio to manage the equipment configuration in the field, with particular interest given to how upgrades are managed and controlled. SysTest also examined whether the logic and accuracy (L&A) procedures in use by counties include steps for the verification of the hardware, firmware, and software versions in use.

SysTest created two reports: (1) an Executive Summary report and (2) a Final Technical Report. This Secretary's Report briefly explains SysTest's methods and findings. The complete SysTest reports are attached at Appendix G.

### **Method**

- **Physical Configuration Audit:** Initially, SysTest verified and recorded the revision levels (essentially the extent to which something is revised through updates, upgrades, etc.) of the hardware, firmware, and software of each voting system. SysTest then compared this information against documented revision levels of state-certified voting systems to verify if the systems in use by the sample of counties were versions certified by the State of Ohio.
- **Processes and Procedures:** SysTest assessed the processes and procedures used by the State of Ohio to manage the configuration of equipment in the field. This assessment was intended to determine if the successful operation of the equipment in an election is at risk due to incompatible hardware or inadequate processes designed to control and manage the configuration of the equipment.
- **Logic and Accuracy:** Additionally, SysTest conducted a review of L&A testing procedures used by a set of 11 counties specifically chosen by the secretary of state to ensure diverse representation. The purpose was to examine the level of consistency across Ohio's certified and deployed voting equipment, and whether the L&A procedures in place included appropriate steps for the verification of hardware, firmware, and software.

## **Findings**

### **Summary**

The physical configuration audit and assessment of configuration management procedures identified risks to be addressed. Summaries of the risks from a configuration management perspective are as follows:

1. The use of materials (specific memory storage devices, printer paper, etc.) that have not been certified by the manufacturers, but that are readily available on the open market, could “create significant risks.” (Final Technical Report at 58.)
2. To verify that the firmware/software installed on voting machines in use in the various counties is actually the certified version, any such possible procedure used before or after an election would be “impractical for current ES&S and Premier systems.” These systems require “disassembly of the unit, physical extraction of the memory device, and utilization of specialized equipment to read the data.” (*Id.* at 58, 59.)
3. Dissemination of technical specifications, standards and information to the counties, including those for L&A testing procedures to ensure a voting machine will accurately count votes, is not standardized, and therefore, L&A procedures throughout the state are inconsistent. (*Id.* at 59.)
4. Revisions to voting system software of all systems from county-to-county are unknown and not documented or tracked. (*Id.* at 59.)

### **Configuration Management Assessment: Specific Results and Suggested Improvements**

#### **Hart InterCivic**

SysTest concluded that “the installed and as-built configuration (defined by hardware, firmware, and software revision levels) of the Hart InterCivic voting system equipment in Ohio counties is unknown.” (*Id.* at 59.) To address this, SysTest suggests providing “a means for creating and maintaining a centralized database of the field inventory by county containing manufacturer, model, serial number, and revision level information. The database shall be readily accessible by county BOE personnel for verifying the revision levels of their equipment.” (*Id.*)

Further, SysTest determined that the Hart InterCivic SERVO software system provided to SysTest for analysis “was missing a file necessary for verifying the hash codes of the operating software,” thus indicating that the software installed in the counties’ voting system equipment “may not be equivalent to the certified version.” (*Id.* at 60.) As a possible mitigating factor, SysTest suggests that the secretary of state’s office “produce and distribute media containing a complete binary image of the certified version of

software to be installed on a voting machine,” and subsequently use the Hart InterCivic utility to verify that the loaded software is authentic, reloading the image from the supplied media should the software be found not to be the equivalent of the certified version. (*Id.* at 60.)

Additionally, SysTest determined “there is no evidence to indicate that the county BOE personnel utilize the Hart InterCivic code verification procedure for ensuring that the firmware and/or software installed in the voting system equipment has not been compromised before or after an election.” (*Id.* at 60.) SysTest recommends verifying that the procedure provided by Hart is “disseminated to all counties that have Hart InterCivic equipment,” and that BOE personnel are properly educated on the use of the procedure. SysTest also recommends this procedure should be utilized every time the equipment is prepared for use, documenting the results of the verification. (*Id.* at 60.)

SysTest concluded that L&A procedures are not consistent throughout the counties using the Hart InterCivic voting system or have not been provided to the county boards of elections by the secretary of state’s office by directive. (*Id.* at 59.) SysTest recommends the secretary of state “provide a centralized source” for disseminating such information. (*Id.* at 59.)

Finally, Hart InterCivic has certified specific consumables and storage devices for use with its voting system, but uncertified forms of these materials are readily available on the open market. SysTest concluded that the use of uncertified consumables and storage devices present the most severe risk, in terms of configuration management, to the Hart InterCivic voting system, and could result in “significant failures during an election.” (*Id.* at 59.) This risk appears magnified by the fact that safeguards cannot be built into the system to ensure storage cards, thermal printer paper, ballot paper, and ballot fonts are the types certified for use. (*Id.* at 59.) SysTest recommends that the secretary of state “provide a centralized source of information accessible by county BOE personnel that clearly specifies any consumables or storage devices that are to be used with the system,” and “clearly communicate to the BOE personnel that using something other than the specified materials may result in failures during an election.” (*Id.* at 59.)

### **ES&S**

Because SysTest “encountered an ES&S iVotronic unit that had down level software installed,” SysTest concluded that “the installed and as-built configuration (defined by hardware, firmware, and software revision levels) of the ES&S voting system equipment in Ohio counties is unknown.” (*Id.* at 61.) To address this, SysTest suggests providing “a means for creating and maintaining a centralized database of the field inventory by county containing manufacturer, model, serial number, and revision level information. The database shall be readily accessible by county BOE personnel for verifying the revision levels of their equipment.” (*Id.* at 61.)

Further, SysTest determined that the ES&S election management software system provided to SysTest for analysis “was missing files,” thus indicating that the software

installed in other voting system equipment in the counties “may not be equivalent to the certified version.” (*Id.* at 61, 62.) As a possible mitigating factor, SysTest suggests that the secretary of state’s office “produce and distribute media containing a complete binary image of the certified version of software to be installed on a voting machine,” verify that the loaded software is authentic, and reload the image from the supplied media should the software be found not to be the equivalent of the certified version. (*Id.*)

Additionally, SysTest analyzed the ES&S system for the purpose of recommending a procedure that could be used to verify that the software and firmware loaded in a unit was equivalent to the certified version before and after an election. SysTest concluded that “the procedure would be impractical to perform on all units in the field,” because it “requires disassembly of the unit, physical extraction of the non-volatile memory device and use of special equipment to read the binary data for comparison.” (*Id.* at 62.) SysTest further states that this process is “possible” but “cumbersome,” and “can only be performed by qualified personnel.” (*Id.*) SysTest further asserted that not practically being able to perform such a procedure on each machine presents severe risks to election integrity, as the firmware in the iVotronic voting machine could be “compromised and modified without detection,” conceivably occurring “before, during or after an election.” (*Id.*) SysTest suggests that the State of Ohio, as a mitigating factor, “require all manufacturers to implement an automated software routine,” for comparing the configuration of each machine in use with the certified configuration, and further suggests that the secretary of state should include such a process in state certification requirements. (*Id.*)

SysTest concluded that L&A procedures are not consistent throughout the counties using the ES&S voting system or have not been provided to the county boards of elections by the secretary of state’s office by directive. (*Id.* at 61.) SysTest recommends the secretary of state “provide a centralized source” for disseminating such information. (*Id.*)

Finally, ES&S has certified specific consumables and storage devices for use with its voting system, but uncertified forms of these materials are readily available on the open market. SysTest concluded that the use of uncertified consumables and storage devices present a severe risk to the ES&S voting system, and could result in “significant failures during an election.” (*Id.*) This risk appears magnified by the fact that safeguards cannot be built into the system to ensure storage cards, thermal printer paper, ballot paper, and ballot fonts are the types certified for use. (*Id.*) SysTest recommends that the secretary of state “provide a centralized source of information accessible by county BOE personnel that clearly specifies any consumables or storage devices that are to be used with the system,” and “clearly communicate to the BOE personnel that using something other than the specified materials may result in failures during an election.” (*Id.*)

### **Premier**

SysTest concluded that “the installed and as-built configuration (defined by hardware, firmware, and software revision levels) of the Premier voting system equipment in Ohio counties is unknown.” (*Id.* at 62, 63.) To address this, SysTest suggests providing “a means for creating and maintaining a centralized database of the field inventory by county containing manufacturer, model, serial number, and revision level information.

The database shall be readily accessible by county BOE personnel for verifying the revision levels of their equipment.” (*Id.*)

Additionally, SysTest analyzed the Premier system for the purpose of recommending a procedure that could be used to verify that the software and firmware loaded in a unit was equivalent to the certified version before and after an election. SysTest concluded that “the procedure would be impractical to perform on all units in the field,” because it “requires disassembly of the unit, physical extraction of the non-volatile memory device and use of special equipment to read the binary data for comparison.” (*Id.* at 63.)

SysTest further states that this process is “possible” but “cumbersome,” and “can only be performed by qualified personnel.” (*Id.*) SysTest suggests that the State of Ohio, as a mitigating factor, “require all manufacturers to implement an automated software routine,” for comparing the configuration of each machine in use with the certified configuration, and further suggests that the secretary of state should include such a process in state certification requirements. (*Id.*)

SysTest concluded that L&A procedures are not consistent throughout the counties using the Premier voting system or have not been provided to the county boards of elections by the secretary of state’s office by directive. (*Id.* at 61.) SysTest recommends the secretary of state “provide a centralized source” for disseminating such information. (*Id.* at 63.)

Finally, Premier has certified specific thermal printer paper and certain storage devices for use with its voting system. SysTest concluded that the use of materials other than those specified could result in “significant problems.” (*Id.* at 58.) This risk appears magnified by the fact that safeguards cannot be built into the system to ensure only certified consumables and storage cards are used in a Premier voting system. (*Id.* at 63.) SysTest recommends that the secretary of state “provide a centralized source of information accessible by county BOE personnel that clearly specifies any consumables or storage devices that are to be used with the system,” and “clearly communicate to the BOE personnel that using something other than the specified materials may result in failures during an election.” (*Id.*)

### **Summary of Board of Elections Officials’ Review of SysTest’s Findings on Configuration Management of the State’s Voting Systems**

One Republican and one Democrat boards of elections official each reviewed SysTest’s findings on the configuration management of Ohio’s three voting systems. Both of these officials utilize the ES&S Optical Scan voting system in their respective counties. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a “scribe.” A “Capsule Summary Statement” of the elections officials’ review is provided below, basically as prepared by the “scribe,” along with a table summarizing this boards of elections review team’s standardized evaluation of SysTest’s findings.

**Capsule Summary Statement by Boards of Elections Team Reviewing  
SysTest's Findings on Configuration Management**

Although the purpose of the project and testing undertaken were clear and the findings credible, board of elections reviewers had to make assumptions as to how the testers arrived at their conclusions. Board officials found that the contractor did a good job of identifying the inadequacies of vendor products; however, there was not enough detail in the method, logic, or failure modes reported in the test results.

The board officials found that SysTest's recommendations to advertise the need for vendor-required supplies and the need for a common reference database of certified software and hardware versions of county equipment are good ones. However, this report needs to be revised to address:

- Inaccuracies in detail of some findings related to the use of the required thermal paper, ballot stock and fonts;
- The readability and annotations of tabular findings, the addition of footnotes, and consistent labels; and
- An important clarification regarding the specifics of the 2006 secretary of state directive regarding logic and accuracy testing; specifically, the availability of a procedure for logic and accuracy testing. [No such directive has been located in the secretary of state's office since the new administration took over in 2007.]

**Summary Table of Standardized Evaluations by Board of Elections Team  
Reviewing SysTest's Findings on Configuration Management**

**Average Configuration Management Report Quality Ratings by Election Officials**

Quality	Scale	Executive Summary	ES&S	Hart	Premier
Data	1-3	2.0	2.0	2.0	2.0
Claims	1-3	2.0	2.0	2.0	2.0
Warrants	1-4	2.0	2.0	2.0	2.0
Coherence	1-4	2.5	2.5	2.5	2.5
Overall	1-5	3.0	3.5	3.5	3.5

Note. This table represents the average ratings of two election officials.

**Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent



## Performance Testing

### SysTEST

SysTest executed “performance testing” to assess if there were risks to the integrity of the election and accuracy of the vote counts during simple use of each of the certified voting systems. SysTest created test cases to observe the result of any possible deficiencies in an election process. SysTest’s performance testing emphasized preparing for an election, the accuracy and integrity of the voting process, and the accuracy of audit logs.

SysTest created two reports: (1) an Executive Summary report and (2) a Final Technical Report. This Secretary’s Report briefly explains SysTest’s methods and findings. The complete SysTest reports are attached at Appendix G.

### Method

SysTest developed a performance test plan and associated test cases that defined its approach in executing performance testing on the ES&S Unity server software, Premier GEMS server software, and Hart InterCivic Ballot Origination, Tally, Rally, and SERVO election management software components. The purpose of this plan was to provide a clear and precise outline of the test elements required to ensure effective performance testing. The test plan:

- Identified items that needed to be tested;
- Defined the test approach;
- Identified required hardware, support software, and tools to be used for testing; and
- Identified the types of tests to be performed.

The following is a summary of each test case:

- **Election Creation** – The object of this test case is to observe the difficulty or ease of creating an election.
- **Set-up and Closure of Polling Place** – The object of this test case is to observe the difficulty or ease of setting up the election system at board of elections office and polling locations, loading the election, and opening and closing the polls.
- **Configuration Management** – The object of this test case is to verify the versions of software and hardware used in the election system.
- **DRE Functionality** – The object of this test case is to verify the functionality of the DRE in performing administrative duties.
- **Election Vote Consolidation (Primary and General)** – The object of this test case is to verify that the vote totals obtained from each type of supported

voting device (optical scan or DRE) can be accurately consolidated into a central count vote total and that all required reports and audit records can be viewed and/or produced.

- **Voter Verified Paper Audit Trail (VVPAT) Accuracy** – The object of this test case is to test and verify both the functionality and accuracy of a VVPAT printer device associated with a DRE polling location, confirming whether all votes are accurately captured on the paper trail, that they are readable, that they can be cancelled and changed by the voter, and that the VVPAT accurately reflects the correct changes.
- **Load Test Early Voting** – The object of this test case is to verify that votes are not lost due to memory leak while casting ballots on a DRE in Early Voting Mode when its memory capacity is exceeded, to verify that in such cases a warning message is given to a user, and to verify the accuracy and integrity of the tally.
- **Load Test DRE** – The object of this test case is to verify that votes are not lost due to insufficient memory capacity while casting ballots on a DRE in Election Day Mode.
- **Load Test Optical Scan** – The object of this test case is to verify that votes are not lost due to insufficient memory capacity while casting ballots on an Optical Scan device in Election Day Mode.
- **Load Test Storage Components** – The object of this test case is to verify a warning message is given to the user when the user attempts to load an election definition that exceeds the memory capacity of the external memory device.
- **Security** – The object of this test case is to verify the election system will log any unknown external devices that were inserted in any open port of the election system.
- **PCMCIA Card Batch Testing** – The object of this test case is to verify all PCMCIA cards (memory cards or devices) provided for testing will function according to system specifications.
- **Audit Tape** – The object of this test case is to verify the election system will log all activities on each component (server, DRE, scanner, etc.) of the system.

(Final Technical Report, at 14, 15.)

## **Findings**

### **Summary**

SysTest’s risk assessment process “uses a combination of the probability of occurrence and the impact of the occurrence, should it occur.” (Final Technical Report at 16.) SysTest’s performance testing of the Premier, ES&S, and Hart InterCivic voting systems identified numerous risks to election integrity, ranging from minor to severe. Most significantly, SysTest found one severe risk with each the Premier and ES&S system.

(Executive Summary Final Report at 16.) This report focuses on summarizing the moderate and severe risks identified by SysTest for all systems, categorized in their table of results as “yellow” and “red.” (Final Technical Report at 68-73)

**Performance Assessment:**  
**Specific Results and Suggested Improvements**

**Premier**

SysTest identified several moderate risks, and one severe risk to election integrity when testing the Premier GEMS voting system, TSX DRE voting machines (used at the precinct level), and the AccuVote optical scanners (used at both the precinct level and at the board of elections for central count), as summarized below.

Several of the moderate risks identified were in relation to proper documentation provided to boards of elections staff for installing the voting system. Specifically, SysTest found that Premier’s user manuals or guides lacked sufficient information for configuring the AccuVote central count operating system, which could result in delays or improper set-up of equipment. (*Id.* at 65, 66, 68, 69.)

SysTest also identified documentation issues relating to the use of the VVPAT for the TSX DRE printer. VVPAT thermal paper can easily be installed backwards, which would cause no votes to be recorded on the thermal paper used for the VVPAT. Premier’s documentation does not address these issues, and its Poll Workers Guide states that in the event that a VVPAT does not write, it should be taken out of service, which may be a needless measure (and decrease the number of available machines in times of heavy voter turnout). (*Id.* at 65, 66, 69, 70.) SysTest additionally indicated that the TSX did not initially recognize the memory card that contained the election to be loaded unless the memory card was removed and reinserted. This could potentially lead a poll worker to believe the memory card is defective. (*Id.* at 71.)

As a mitigating factor relating to the above documentation issues, SysTest recommends supplemental documentation and/or training be provided to election administrators. (*Id.* at 69, 71.)

Additionally, SysTest identified that Premier’s GEMS Server Configuration Guide may mislead an election administrator to disable a particular service, which in turn, could result in insufficient performance or procedural delays on Election Day. (*Id.* at 66, 69.) To mitigate these risks, SysTest recommends that the server administrator perform a full configuration check before the election. (*Id.* at 69.)

When SysTest performed further testing on the Premier TSX DRE, the VVPAT did not list the entire final ballot for the voter’s verification, which could lead to “voter discontent.” (*Id.* at 70.) Additionally, if a candidate has an unusually long name, the VVPAT will cut off the name at 20 characters, potentially leading to voter confusion. (*Id.* at 66, 67, 70.) SysTest suggests conducting logic and accuracy (L&A) testing on the

VVPAT prior to opening the polls, and if problems occur, recalibrating the VVPAT. (*Id.* at 70.)

SysTest identified that changing the ballot style of paper ballots in the Premier GEMS system at the “last minute,” caused “AccuVote OS [optical scan] (1.96.6) to ignore one race.” (*Id.* at 71.) SysTest suggests “a complete L&A needs to be conducted on absentee ballots with every single race being voted.” (*Id.* at 71.)

Finally, the most severe risk identified in performance testing of the Premier voting system was during a load test on the TSX DRE. SysTest discovered that the TSX DRE erases vote data on the memory card during the voting process when memory capacity is exceeded on the memory card. (*Id.* at 69.) If failure occurs, the official ballot count would have to be conducted by hand using the VVPAT records, which would be tedious and laborious. (*Id.* at 69.) To mitigate this risk, SysTest suggests limiting the number of voters that can vote on a TSX, which can be calculated by establishing the amount of free space that exists on the card and how much space is consumed by each ballot cast.

### **ES&S**

SysTest identified numerous moderate risks and two severe risks to election integrity when testing the ES&S Unity voting system, which includes the iVotronic DRE (used at the precinct level), M100 optical scanner (used at the precinct level), and M650 optical scanner (used at the board of elections for central count). The various risks are summarized below.

SysTest identified that the Unity voting system does not mandate the need to change usernames and passwords (used to access voting equipment during an election) from the default passwords supplied from ES&S documentation. The iVotronic machines tested were accessed by default common and identical usernames and passwords. (*Id.* at 82, 84, 89.) SysTest indicates that this could result in unauthorized personnel changing settings on voting equipment and suggests that the state “mandate that all passwords be changed and only revealed to necessary personnel,” and that “election officials should change the passwords occasionally for security purposes.” (*Id.* at 82, 84, 89.)

SysTest identified that the physical stability of the iVotronic DRE is “fragile,” and the use of these machines over several election cycles makes them susceptible to tipping over and becoming damaged. If damage to a machine occurred on Election Day, a polling location could experience a shortage of DREs. (*Id.* at 88, 89.)

The iVotronic DRE exists in 12-inch and 15-inch versions. SysTest identified that on the 12-inch iVotronic DRE, write-in instructions are not fully displayed on the write-in screen, which could create an obstacle in casting a write-in vote and cause “voter discontent.” (*Id.* at 84, 89.)

SysTest identified that the power supply of iVotronic’s Real Time Audit Log (RTAL), which is ES&S’s version of a VVPAT, is concealed and not readily apparent to poll workers. (*Id.* at 89.) SysTest discovered that if the power supply is not switched to “on”

before the iVotronic screen is locked into position, the RTAL does not work, even though the iVotronic machine itself will operate on battery power and display a message describing the “lack of its RTAL printer.” (*Id.* at 83.) These issues could lead to a poll worker believing that the entire unit is defective, taking it out of service and thereby a shortage of available machines. (*Id.* at 89.) As a mitigating factor to the above risks, SysTest suggests that poll workers fully inspect each DRE as part of their pre-election procedures. (*Id.* at 89.)

Additionally, SysTest identified connectivity issues with the iVotronic RTAL printer, which is located inside the voting machine but connected externally, and the Seiko report printer, which is a separate unit that must be connected via the same external serial port as the RTAL printer. SysTest states, “the connector between the iVotronic and the RTAL printer does not screw into place and may be removed by any voter and left in a position that its removal may not be obvious.” (*Id.* at 83.) If such a disconnection occurs, the iVotronic will not accept any additional votes until the RTAL printer connector is properly reattached. (*Id.* at 83.) If a poll worker wishes to print specific reports, he or she must disconnect the RTAL printer, and connect the separate Seiko report printer. If the poll worker attempts to print specific reports on the iVotronic but fails to physically change the printer, the reports will be temporarily lost. (*Id.* at 89.) Additionally, the iVotronic does not detect when the report printer is disconnected or turned off during printing, so the user must be aware of what he or she expects to be printed and be “cognizant of the printer’s status.” (*Id.* at 84.)

SysTest also states that a routine change from the RTAL printer to the report printer may result in a bent serial connector pin. In the case of a damaged pin, the serial cable and subsequently the RTAL and voting machine may become unusable. SysTest suggests updating training materials to emphasize the risks associated with changing the printer and keeping extra serial cables on hand to mitigate these risks. (*Id.* at 83, 89.)

SysTest identified moderate risks associated with the AutoMARK Voter Assist Terminal (VAT), an ADA-compliant ballot marking and reading device<sup>1</sup> not manufactured by ES&S, but made compatible with the ES&S Unity voting system. Specifically, SysTest found that the AutoMARK does not always recognize the inserted ballot, and when this occurs, the user must eject and reinsert the ballot as many as three times. (*Id.* at 82, 83, 90.) SysTest states, “This will cause voter discontent, confusion, and loss of confidence.” (*Id.* at 90.) SysTest suggests supplemental instructions be provided at the polling location, and increased awareness to this issue in poll worker education. (*Id.* at 90.)

Additionally, SysTest identified the character sets available for use for write-in votes on the AutoMARK differ from those available on the iVotronic DRE, specifically that the iVotronic DRE’s write-in display includes comma (,) and period (.) characters. SysTest states, “The difference in the available character sets may result in vote consolidation errors,” (*Id.* at 83.) and “This will delay reporting results.” (*Id.* at 90.)

SysTest further discovered that when the brail caption button was used, the AutoMARK’s display scrolling sometimes becomes “erratic,” which at times makes it “impossible to completely see the contents of a race’s display box.” (*Id.* at 82, 90.) SysTest states this

---

<sup>1</sup> This device reads a barcode on a pre-printed optical scan ballot that is inserted into the device, which is designed to recognize the ballot style. The device allows the voter to utilize its touch screen to mark the ballot but not tabulate it. Once marked, the ballot is ejected by the device to be read by an optical scanner. This device is frequently used by voters with disabilities.

will result in a “loss of voter confidence” and voter “confusion” and “discontent.” (*Id.* at 90.) As a mitigating factor, SysTest suggests supplemental instructions be provided at polling locations and increasing voter education. (*Id.* at 90.)

SysTest’s performance testing on the ES&S M100 and M650 optical scanners (used at both the precinct level and at boards of elections for central count) identified the following concerns. The M100 optical scanner has an attached metal ballot box, which should contain a diverter for the purpose of separating write-in ballots from normal ballots. Of the three M100 ballot boxes tested, only one contained the required write-in diverter. Without such a diverter, finding and tallying write-in votes “could be a difficult task,” and could result in a “delay tallying the write-ins.” (*Id.* at 87, 89.) SysTest suggests boards of elections conduct a full inspection as part of their pre-election process. (*Id.* at 89.)

SysTest identified that the M100 (precinct-based optical scanner) “does not scan incomplete marks reliably or consistently.” (*Id.* at 86.) SysTest found that incomplete marks are inconsistently recognized – sometimes recognized as votes, sometimes generating an “unreadable marks” message, and sometimes described as undervotes. SysTest states, “It is possible that clearly indicated votes may not be recognized by the scanner, and if the election is not configured to warn of undervotes, those votes will be lost. It’s also possible that overvotes may not be recognized as such and warned about if made with marks that the scanner does not recognize.” (*Id.* at 86.) SysTest suggests several mitigating factors in relation to the M100’s inconsistency relating to incomplete marks, including first ensuring that the M100 is properly configured to reject “unreadable marks,” so the voter receives warnings that his or her marks are unreadable by the scanner. Additionally, SysTest suggests that it is important to educate voters on how to properly fill in ballot ovals, and also suggests that instructions be posted at polling sites for voters to completely darken intended ballot ovals. (*Id.* at 86, 87, 89.)

Additionally, SysTest identified that while printing reports, the M100 does not detect when printer paper runs out, rather it continues printing to nothing and the “print output is lost.” (*Id.* at 86, 90.) SysTest recommends that poll worker training be updated to note this, to verify there is adequate paper prior to printing, and for poll workers to increase their awareness of what is being printed to determine whether something is lost due to insufficient paper. (*Id.* at 86, 90.)

In testing the M650 (high-speed optical scanner), SysTest discovered that the scanner only reads ballot ovals in the either right or left column, depending on how the election administrator configures the ballot definition of the machine. SysTest states, “There is a risk that ballots with ovals on the wrong side could be printed and therefore be unreadable by an M650.” (*Id.* at 85, 90.) Therefore, it is imperative that boards of elections employees create ballots in the correct template, or else votes may not be read correctly. (*Id.* at 85, 90.)

The most severe risk SysTest identified with the M650 is that in order for vote data to be written to its internal hard drive, the user is required to manually save it from the internal RAM to the hard drive. If a power failure occurs, the scanned ballots in the RAM are lost and it becomes necessary to re-scan all ballots processed since the last prior save. “If such ballots are not reprocessed, then those votes will not be counted.” (*Id.* at 88.) SysTest concludes, “It is critical that batches be processed in their entirety,

with very methodical saves performed, or there is a real danger of duplicate scanning of ballots, or of omitting some ballots from the scan process entirely.” (*Id.* at 85, 90.)

SysTest also identified a severe risk inherent in both the M100 and M650 optical scanners. The M100 and M650 scanners do not mark ballots as having been processed. Because of this, “paper ballots can be scanned more than once,” and “a person with malicious intent can skew the election results.” (*Id.* at 89, 90.) SysTest suggests that all batches should be processed in their entirety, and the handling procedures in place must include a political balance of staff handling them. (*Id.* at 89.)

Additionally, SysTest identified a risk inherent to the Election Reporting Manager application, specifically regarding the handling and importing of vote results from the M100 and M650 memory devices to the reporting application. SysTest states, “There are no safeguards inherent in the system to prevent a user from importing vote results from the same memory devices multiple times. System operators should store processed memory devices in a secure location physically segregated from unprocessed media devices immediately after processing them.” (*Id.* at 88.)

### **Hart InterCivic**

SysTest identified two moderate risks to election integrity when testing the Hart InterCivic voting system, which includes the Ballot Origination, Tally, Rally, and SERVO election management software components, the eSlate DRE, and the eScan optical scanner (used at the precinct level).

Initially, SysTest identified through their performance testing that the Hart InterCivic system is “not as feature rich a voting solution as the ES&S and Premier,” and does not offer “the flexibility in election definition and ballot design capabilities.” (*Id.* at 91.) Because of this, the Hart system is “far less complex,” and has “fewer potentials for risks.” (*Id.* at 91.) The two moderate risks identified by SysTest are summarized below.

Both moderate risks with the Hart InterCivic system, as identified by SysTest, involve a console called the Judge’s Booth Controller (JBC). The JBC is a single console that attaches to and can control as many as 12 eSlate DREs for the purpose of generating voter access codes and delivering ballot configurations to the DREs, recording records of votes cast, storing ballots to its internal memory, and is capable of accumulating and reporting vote results.

SysTest identified that “one JBC cannot be used for early voting and Election Day processing,” which would force small counties to purchase two units. (*Id.* at 93.) Additionally, when an audit log was created, the log failed to record when the JBC was powered down and powered up. Because of this, an audit log would not be able to determine how long a JBC unit was powered down. “This could hamper any inquiries if a re-creation of Election Day events needs to be created.” (*Id.* at 93, 94.) As a mitigating factor, SysTest suggests requiring constant monitoring of JBC units. (*Id.* at 94.)

## **Summary of Board of Elections Officials' Review of SysTest's Findings on Performance Testing of the State's Voting Systems**

One Republican and one Democrat boards of elections officials reviewed SysTest's findings on the performance testing of Ohio's three voting systems. One of these officials utilizes the Premier DRE voting system and the other utilizes the ES&S optical scan voting system in their respective counties. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a "scribe." A "Capsule Summary Statement" of the elections officials' review is provided below, basically as prepared by the "scribe," along with a table summarizing this boards of elections review team's standardized evaluation of SysTest's findings.

### **Capsule Summary Statement by Boards of Elections Team Reviewing SysTest's Findings on Performance Testing**

Board of elections officials found the SysTest performance testing report to be complete and thorough. The problems SysTest identified did not come as a surprise to any of the election officials, as the election officials have already encountered such problems. The suggestions offered by SysTest for risk mitigation were found to be realistic and sufficient; however, the officials believed that boards of elections have already taken many of the suggested steps.

The election officials believe that the biggest threat to elections is the complexity of the voting systems in concert with human error, and SysTest's report successfully reflects that. The election officials did not identify glaring deficiencies regarding the subjects the report covered and solutions the report offered.

Overall, the election officials felt the SysTest report was very good, identifying as the report's only shortfall the lack of information and data on the Hart InterCivic system. The election officials agreed that the report could not be accused of being inflammatory or alarmist, especially because mitigating factors were offered for the equipment performance risks SysTest identified.

The election officials believe voting machine manufacturers can take the information in this report and use it as a good working tool to fix some of the faulty elements present in voting systems. The election officials also believe the secretary of state can issue advisories and directives to help alleviate some of the issues documented in this report.

The main point the election officials took from this report is that the systems *perform*, but they can perform more *efficiently* and *securely* if some of the suggestions offered in the report are implemented.



**Summary Table of Standardized Evaluations by Board of Elections Team  
Reviewing SysTest's Findings on Performance Testing**

**Average Performance Report Quality Ratings by Election Officials**

Quality	Scale	ES&S	Hart	Premier
Data	1-3	3.0	2.0	3.0
Claims	1-3	3.0	1.5	2.0
Warrants	1-4	4.0	2.5	4.0
Coherence	1-4	4.0	3.0	4.0
Overall	1-5	4.0	3.0	4.5

Note. This table represents the average ratings of two election officials

**Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent

## **Elections Operations and Internal Control Assessment**

### **SysTest**

The SysTest Risk Assessment Team performed an elections operations and internal control assessment of existing or proposed policies, procedures, and internal controls established in manufacturer documentation and county boards of elections (“BOE”). The purpose of SysTest’s assessment was to determine whether these policies, procedures and internal controls are sufficient to ensure secure and accurate elections based upon software, hardware, and operational susceptibilities. This Secretary’s Report briefly explains SysTest’s methods and findings. The complete SysTest reports are attached at Appendix G.

### **Method**

- **Representative Sample of Ohio Counties:** The SysTest team reviewed specific procedures in eleven counties (one-eighth of Ohio’s 88 counties) (Allen, Belmont, Cuyahoga, Fairfield, Franklin, Hamilton, Jackson, Licking, Lorain, Montgomery and Warren) as a representative sample of Ohio jurisdictions. These counties were chosen based on size, demographics, and voting systems.
- **Surveys:** Each participating county received written surveys, instructions, and an introductory letter from the secretary of state via hand delivery. Every participating county returned the surveys, and their responses were incorporated into SysTest’s analysis.
- **On-site Interviews and Assessments:** The SysTest team visited each participating county. They assessed each participating county’s facilities, access controls and physical security. They also reviewed election setup, and programming and testing methods for paper and electronic voting systems. The SysTest team discussed Election Day procedures for detecting and resolving machine security and operational issues and the corresponding poll worker training and procedures in each county.
- **Review Vendor Documentation:** The SysTest team also reviewed each participating county’s documentation from its voting system manufacturer. This helped SysTest to assess the level of thoroughness and usability of the documents, particularly as they pertain to security and election accuracy. SysTest also evaluated whether each county’s policies, procedures, and processes implement the vendor’s recommendations.

### **Findings**

#### **Summary**

SysTest concluded that solutions to election administration issues lay not only in technology, but also in management practices, training, and documentation. Summaries of the risks from an elections operations and internal controls perspective are as follows:

1. BOE facilities are not equipped to provide adequate security, storage and access controls for ballots, voting machines, and election systems. This is particularly true after business hours.
2. Oftentimes BOEs do not have written policies and procedures that outline how elections are conducted, voting systems used, and sensitive items secured.
3. Statutes, regulations, and directives do not provide sufficient guidance or they mandate unreasonable or unnecessary timelines. Some of the statutes and regulations are based on outdated voting technology and methods.
4. The bi-partisan system at boards of elections creates inefficient staffing, organizational, and management configurations.

### **Elections Operations and Internal Controls Assessment: Specific Results and Suggested Improvements**

#### **Documentation**

SysTest found common problems among all three manufacturers' documentation. First, SysTest concluded that the level of detail provided in manufacturer documentation was often on a very high level that assumed higher than average technical expertise than BOE employees may have (Final Technical Report at 18.) Second, SysTest found that some of the information provided in the documentation was too complex and did not provide step-by-step procedures. (*Id.*) Therefore, a straightforward task may unnecessarily be turned into a very complex one. As discussed later in this summary, documents should be created for BOE use that contain step-by-step instructions and can be used as a resource guide.

#### **ES&S Documentation**

SysTest found that the ES&S documentation was difficult for boards of elections to use. (*Id.* at 19.) Among the most important findings in the ES&S review was that the documentation could not be used as a quick reference guide. (*Id.*) Specifically, ES&S's Poll Worker Election Day Procedures document is very thorough but includes extraneous and unnecessary information that adds to the level of complexity and confusion. (*Id.*) The ES&S documentation is more oriented toward initial installation and setup rather than ongoing operations. (*Id.* at 20) The emphasis on installation and setup adds to the complexity of the documentation. (*Id.*)

#### **Premier Documentation**

SysTest determined that the Premier documentation is much more structured. (*Id.*) However, the Premier documents also assume a high level of technical knowledge and are organized around technical abilities rather than election functions. (*Id.*) No single document exists for the Premier system that can be used to quickly, efficiently and effectively construct policies, procedures, and processes. (*Id.*) Thus, local election policies, procedures, and processes are pieced from multiple documentation sources.

### Hart InterCivic Documentation

The Hart InterCivic documentation was the most structured according to the SysTest study. (*Id.*) It is broken into various system components and accommodates the nature of election cycles. (*Id.*) It also provides a variety of useful check sheets. (*Id.*) Nonetheless, it is very voluminous and difficult to use quickly. (*Id.*) The documents are not meant to be county-specific. Customizing these documents presupposes a level of technical knowledge that may not be available. (*Id.*)

### **Threat Analysis**

SysTest used a threat model to assess the effectiveness of operational procedures and controls for voting systems in a potentially high-risk environment. (*Id.* at 21.) SysTest also analyzed the types of human threats and their potential actions (*Id.* at 22.) ranging from a nuisance level (level 1) to an inadvertent level (level 2) to a malicious level (level 3). (*Id.* at 29.) SysTest used the concepts of threat deterrence, delay, detection, and denial as its basis for identifying and recommending mitigating measures for the vulnerabilities it identified. (*Id.*) Of those concepts, detection is the most powerful, because it enables state and local election officials to identify, isolate and recover.

Nuisance/level 1 threats are characterized by threats emanating from situations of limited time, access and knowledge. These threats pose a minimal risk and are easily deterred, detected, and isolated. If they occur, they are usually isolated to a single machine or precinct. Mitigation factors are easy, inexpensive and not difficult to implement by local election officials and voting system manufacturers. (*Id.*) Nuisance threats include those initiated by foreign governments, activists, political campaigns, political action committees and organizations, and voters. (*Id.*)

Inadvertent/level 2 threats are the most frequent and likely to occur. They are characterized by lack of training, human error, inadequate quality controls, poor management, and operational, budget, and staffing constraints along with outdated, incomplete or contradictory regulation. (*Id.*) Mitigation strategies for this threat level are typically not technical in nature but require complex action from state and local legislative bodies, elected officials, election officials, and voting system manufacturers. (*Id.*) Inadvertent threats include those from voting system manufacturers, boards of elections staff, poll workers, election-related vendors, and legislation, regulations, and directives, along with election administration and management practices. (*Id.*)

Malicious/level 3 threats are potentially the most disturbing, most intricate to find, and difficult from which to recover. These threats are characterized by authorized access and a high level of technical knowledge. (*Id.* at 30.) Malicious level threats include threats by rogue voting system programmers. Mitigation factors are pointed, expensive, and difficult to implement because the threats are difficult to detect and “global in scale.” (*Id.*) Nonetheless, a parallel testing program of randomly selected voting machines by local election officials and voting system manufacturers could address this situation. (*Id.*)

SysTest notes that it is unrealistic to attempt mitigation strategies that would completely eliminate any and all possible risks without requiring very costly and severe limitations on the right to vote. (*Id.*)

### **Vulnerability Analysis**

SysTest identified eight potential times during the election cycle where threats and threat sources exist in the voting system. (*Id.* at 31.) These times encompass the entire election cycle from pre-election storage, Election Day, and election results and post election storage. (*Id.*) SysTest found that significant internal controls, security measures and operational procedures are in place in the representative counties sampled. (*Id.*) However, the risk potential manifests itself in the absence of formal documentation.

SysTest notes that there are many differences among Ohio counties regarding capabilities, approaches, and resources that disallow uniformity in and among Ohio counties. (*Id.* at 32.)

SysTest identified several potential risk areas in more than one single county independent of voting system, county size and political philosophy. These include:

#### **County Documentation**

SysTest observed that more than one county lacked written documentation of election procedures and security plans. (*Id.* at 34.) Instead of written procedures or staff training, those counties relied upon a single person's knowledge. (*Id.*) This reliance could result in overlooking important practices, inconsistent procedures, and lack of continuity during re-organization or staff turnover. In the event of an election contest court action, this could also raise questions about the staff's personal judgment and decisions. This risk could be mitigated by a comprehensive document developed at the state level covering all elections procedures. (*Id.* at 48.) Counties could then develop county-specific documents.

#### **Physical Security**

SysTest discovered that existing facilities do not provide adequate ballot and voting system protection against unauthorized access. (*Id.* at 34.) SysTest recommends that a physical security and crime prevention assessment be conducted. (*Id.* at 49.) It also recommends that the state develop standard practices for equipment and supplies during transport and storage when equipment is not in control of boards of elections staff members. (*Id.* at 54.) Finally, SysTest opines that contractors that deliver or store equipment should be required to be bonded and insured. (*Id.*)

#### **After Hours Access**

The SysTest report states that while many boards of elections are adequately secured during business hours, most of them are not protected against unauthorized access after business hours because of inadequate key controls, glass paned doors, and ground level windows that are not reinforced. (*Id.* at 35.) However, in some cases, the board of elections has no control over some county facilities where maintenance crews enter at

will. Installing an electronic lock system, a visitor and employee badge system, a video surveillance system or an intrusion detection system could mitigate this risk according to the SysTest report. (*Id.* at 35, 49, 50.)

### Secure Storage

Secure storage areas are inhibited by the facility in which the board of elections is located. Items requiring segregation, secure storage, and inventory controls are co-mingled with less sensitive items. SysTest recommends that a physical security and crime prevention assessment be conducted. (*Id.* at 49.) SysTest also points out that installing an intrusion detection system or video surveillance system could help with this problem. (*Id.* at 49, 50.)

### Two Key/Password Systems

SysTest concluded that the two-key and split password approach regarding access to sensitive areas “provides a false sense of security and may even undermine security for several key reasons.” (*Id.* at 35.) The two key system does not allow anyone to detect someone who accesses the facilities without authorization. (*Id.*) The two key system's effectiveness is also compromised by the ability to duplicate keys, lack of control of the keys, and the ability to leave one of the locks unlocked. The split password system's effectiveness is compromised by the ability and/or inclination to share the password with others for convenience. SysTest suggests that installing an electronic lock system could remedy this issue. (*Id.* at 49.)

### Job Classifications and Hiring Practices/Partisanship

SysTest concluded that partisanship requirements in the Ohio election system imply a mistrust of the opposite party and the expectation that the opposite party is pursuing an advantage for its party. (*Id.* at 36.)

The focus on partisanship requirements may impact whether qualified people are hired that meet the boards' operational and administrative needs. (*Id.*) These requirements also impact the ability to hire and fire, thereby inhibiting management's ability to effectively administer elections and set performance standards. (*Id.*) SysTest further found that political parties control the entire hiring process in some cases. (*Id.*) This could be remedied by a comprehensive document covering all elections procedures developed at the state level (*Id.* at 48) as well as standardized job descriptions that outline minimum job qualifications such as Secretary of State Directive 2007-01, setting qualifications for the hiring of directors and deputy directors of BOEs, and merit based hiring and firing practices (*Id.* at 50.)

### Background Checks

Participating counties reported that, due to partisan requirements, they were unable to perform any type of screening, reference checks, or criminal background checks. (*Id.* at 37.) This subjects boards to the possibility of corrupt insiders or similar accusations. SysTest proposes background checks for permanent employees and temporary employees that handle sensitive information. (*Id.*) Note, the secretary of state obtains criminal background checks and performs a search of any campaign finance law violations before appointing members of boards of elections.

### Systems Integration

Participating counties using the Premier system do not connect their voter registration and election management systems. Such a connection is not available for ES&S or Hart users. Consequently, boards of elections maintain multiple databases requiring double data entry and proofing and synchronization of parallel databases. Election systems not “talking” to each other increases the risk of error. (*Id.*) According to SysTest, manufacturers should “create and/or automate data interfaces that support election management systems and require counties to use them.” (*Id.* at 51.)

## **Election Management Software (EMS) and Firmware Version Control Updates**

### Installation

Participating counties change election management software and voting system firmware using very different methods. Larger counties tend to receive updates and improvements directly from their respective vendors. (*Id.*) Smaller counties, on the other hand, receive updates and improvements through the secretary of state’s field staff personnel. (*Id.*) The SysTest report advises that “standardized and centralized software and firmware” should be installed and a “version protocol” created. (*Id.*) In addition, there should be standardized recordkeeping of current software and firmware versions. (*Id.*)

### Software Chain of Custody and Recordkeeping

The SysTest team did not find any consistent statewide processes regarding how boards of elections should handle introducing, delivering, installing, verifying, testing, controlling and documenting software or firmware changes. (*Id.* at 38.) This is a concern since many opportunities to compromise voting involve unauthorized software and/or firmware. Because there is no local record keeping regarding authorized changes or post-change installation testing, board of elections personnel rely completely on their vendors to validate any changes or updates. (*Id.*) SysTest recommends that the State take over that responsibility. (*Id.*)

### Certification of the Ballot

Many time-sensitive tasks are dependent upon ballot finalization and certification. The Ohio Revised Code requires the secretary of state to certify ballots 60 days before Election Day. SysTest recommends that the secretary of state strictly adhere to this timeline to prevent down-stream implications as well as review and seek or implement changes to statutes, regulations, and directives so that they conform to new technology, time constraints, and timelines. (*Id.*)

### Marking of Test Ballots

Logic and accuracy testing (“L&A” testing) is designed to ensure that all ballot layouts can be accurately read, that all ballot positions can be accurately and reliably voted, and

that the ballots will be read correctly. However, the approach toward L&A testing is apparently still based on out-of-date punch card testing and is not designed to catch mistakes unique to optical scan or electronic voting. (*Id.* at 39.) SysTest proposes conducting L&A testing using hand marked ballots and counting a representative sample of test ballots. (*Id.*) Moreover, standardized L&A testing should be conducted at the state level to “include a complete end to end battery of tests of individual machines, and central count systems.” (*Id.*)

### Testing Scenarios

Boards of election have relied upon oral history regarding testing practices rather than developing system-specific documents that outline proofing/testing timelines, criteria, and methodology. (*Id.*) Such documents would avoid chaos when staff turns over and increase the counties’ ability to detect and correct errors.

### Absentee Ballots

Recent changes to Ohio law provide for no-excuse absentee voting, an option that is becoming increasingly popular with each election. SysTest found that the procedures for issuing, handling, tabulating, and reconciling absentee ballots are not in line with legal and voting technology changes. (*Id.* at 40.) SysTest makes several recommendations regarding how to bring these practices up to date, including creating consistent absentee ballot stub number policies, and processing absentee ballots before Election Day to accommodate volume and clear directions regarding the process. (*Id.*) SysTest further recommends prioritizing absentee ballot post election reconciliation and creating consistent procedures regarding exceptions to the handling, ballot duplication, and enhancement processes. (*Id.*) Each exception should be documented. (*Id.*) BOEs should further create procedures for elections personnel and volunteers to vote absentee. (*Id.*) SysTest also encourages that the state review and revise absentee ballot statutes, regulations and directives to make them conform to current technology and voting practices. (*Id.* at 53.)

### Inventories

SysTest survey results and onsite visits showed that counties do not have verified serial number inventories or a method to account for or mark memory cards on an ongoing basis. (*Id.*) Memory cards contain ballots that must be retained according to federal or state record retention schedules. SysTest recommends that the state establish standard inventory controls. (*Id.* at 54.)

### Security seals

Boards of elections’ security seal practices generally provided the requisite security. However, SysTest recommends implementing uniform procedures instructing poll workers to check for the presence of the seals and verify the serial number before machine operation. (*Id.* at 41, 42.)

### Poll Worker Training

Due to recent changes in election law and lawsuits related to these changes, there is a wide-variety of election law interpretations among Ohio’s county boards of elections.



Adding to this challenge is the large amount of poll worker turnover. The SysTest report emphasized the need for uniform policies, procedures, and processes for poll workers that take into account each type of voting system. (*Id.* at 42.) SysTest further recommends that Ohio conduct vigorous poll worker training and test whether each poll worker understands the material and can execute it. (*Id.* at 42, 54.) SysTest states that making all poll workers experts in every area of elections is not practical. (*Id.* at 42.) Instead, SysTest suggests that poll workers be trained on prioritized topics and that class time be reduced. (*Id.* at 42, 54.)

### Second Chance Voting

Optical scan systems notify voters if they have under- or overvoted and give them a second chance to correct the under- or overvote. A voter can use an over-ride function to ignore these warnings. Some counties place these ballots in a bin for processing by poll workers after the voters leave. (*Id.* at 42.) SysTest suggests that the over-ride function be left to each voter. (*Id.* at 42-43.) SysTest also recommends that the state review and revise absentee ballot statutes, regulations and directives to make them conform to current technology and voting practices. (*Id.* at 53.) Standard criteria should be developed for handling second chance voting on precinct count optical scan equipment also. (*Id.* at 42.)

### Multi-Precinct Polling Locations

The majority of counties allocate several precincts to common polling locations for accessibility and efficiency. Usually, each machine in the polling location is programmed with ballots for all precincts assigned to that polling location rather than a voting machine's ballots being precinct specific. This way, voters can use any machine in the polling place. SysTest recommends that statutes and directives should recognize and develop standards for this process. (*Id.* at 55.)

### Issuing Provisional Ballots

Provisional voting sometimes creates long lines, making it difficult to manage lines and the flow of voters. Few boards of elections have processes in place to deal with this issue. (*Id.* at 43.) This issue can be lessened by developing procedures that identify provisional voters early and that take them aside to allow them to vote. (*Id.* at 43-44.)

### Two-Person Rule

On election night the presiding judge returns voted ballots to the board of elections or to a designated drop station. Once the board of elections staffs receives the ballot, the two-person rule dictating that a Republican and Democrat handle ballots at the same time is employed. SysTest notes that there is a greater risk of tampering when the ballots are in the presiding judge's custody alone. (*Id.* at 44.)

### Reconciliation/Canvassing

SysTest observed counties using punch card, paper ballot and single voting system assumptions for canvassing election returns. (*Id.*) These processes do not always sufficiently audit electronic voting for multi-precinct polling locations. Absentee ballots are not audited as robustly as poll ballots and at times are not reconciled at all. (*Id.*) A

lack of understanding of auditing and canvassing principles and the absence of written documentation leads to partial and inadequate post election checks and balances. SysTest recommends establishing standards for canvassing, auditing, and reconciling election returns that consider all voting systems, technologies, and ballot types. (*Id.* at 55.) They further suggest that voted paper ballot security and transportation rules be clarified. (*Id.*)

#### Qualification of Provisional Ballots

Provisional ballots are generally processed just after Election Day. However, SysTest notes that checks for double voting were weak, did not exist, or were done manually. (*Id.* at 44-45.) Absentee ballot checks, in contrast, were more thorough and automated. (*Id.*) Additionally, some counties tally and report provisional ballots in such a way that could compromise voter confidentiality. (*Id.* at 44.) SysTest recommends standardizing requirements and procedures for processing provisional ballots. (*Id.* at 56.)

#### Canvass Discrepancies

None of the counties had formalized written procedures to track, document or report discrepancies discovered during the canvass process. (*Id.* at 45.) This could be resolved with written documentation regarding the canvass process. (*Id.* at 45, 56.) This document, SysTest counsels, should address discrepancies found in the canvass, research conducted to find the root of the discrepancy, corrective actions taken, the impact of unresolved discrepancies, and preventive actions taken. (*Id.* at 45.) This document should be a public record presented to each board member. (*Id.*)

### **Summary of Boards of Elections Officials' Review of SysTest's Findings on the Elections Operations and Internal Controls Assessment of the State's Voting Systems**

One Republican and one Democrat boards of elections official each reviewed SysTest's findings on the election operations and internal controls of Ohio's three voting systems. Both of these officials utilize the Premier DRE voting system in their respective counties. In addition to the elections officials, the review group consisted of three secretary of state employees — a facilitator, an attorney, and a "scribe." A "Capsule Summary Statement" of the elections officials' review is provided below, basically as prepared by the "scribe," along with a table summarizing this boards of elections review team's standardized evaluation of SysTest's findings.

#### **Capsule Summary Statement by Boards of Elections Team Reviewing SysTest's Findings on Elections Operations and Internal Controls**

The election officials found the SysTest assessment of elections operations and internal controls credible. The election officials felt the strongest component of the report's credibility stemmed from its reliance on actual information from 11 of Ohio's boards of elections. The four main areas covered in this report called for stronger training and education, written policies and procedures, documentation, and standardization or

centralization.

While the election officials review team found this report credible, there were disagreements with some the report's conclusions. For example, the review team strongly disagrees with the conclusion that Ohio's bipartisan elections system should be eliminated. The review team also expressed some concerns with the levels of threat or risk indicated without having more quantifiable examples of their incidence.

The election officials agreed with the report that there exists a need for more standardization from the office of the secretary of state. The election officials believe that, regardless of which voting system is used and how reliable it may be, without standard procedures and policies greater risk will continue to exist.

**Summary Table of Standardized Evaluations by Board of Elections Team Reviewing SysTest's Findings on Elections Operations and Internal Controls**

**Average Operational Controls Report Quality Ratings by Election Officials**

Quality	Scale	Overall
Data	1-3	2.0
Claims	1-3	2.0
Warrants	1-4	2.5
Coherence	1-4	3.0
Overall	1-5	4.0

Note. This table represents the average ratings of two election officials

**Report Quality Rating Scales**

Scale	Dimension Measured
Data	Conclusions were based on and supported by data.
Claims	Claims were clear, consistent, feasible, and related to solutions
Warrants	Arguments were reliable, trustworthy, and logical
Coherence	Material was integrated and contained sufficient context
Overall	Overall report quality from failing to excellent

## **Secretary of State Recommendations**

### **General Conclusions and Background**

The findings of the various scientists engaged by Project EVEREST are disturbing. These findings do not lend themselves to sustained or increased confidence in Ohio's voting systems. The findings appearing in the reports necessitate that Ohio's voting process be modified to eliminate as many known risks to voting integrity as possible while keeping voting accessible to Ohio's voters. These changes must be thoughtfully planned with the assistance of the Ohio General Assembly, Governor Strickland and Ohio's election officials. As they are implemented, these changes must be made widely known to the public to facilitate orderly and cost efficient implementation.

As Ohio's voting system is restructured, all equipment and any related software, along with software updates, must be documented in a central registry to ensure that all equipment and software in use has been certified by the state's Board of Voting Machine Examiners. Preparation, use and storage of equipment before, during and after an Election Day must be supported by uniform guidelines, procedures and training supplied by a combination of legislation and secretary of state directives.

It has been said that elections belong to the people. Excessive dependence on any voting machine company to operate the state's elections, when that company's voting system is subject to trade secret or propriety information claims, results in a loss of transparency that should exist to assure election officials and the public that a fair and accurate process has been implemented for democratic self-governance. The information utilized by the scientists in this study included reviews of all three systems' software source codes and related documentation, a thorough orientation to the operation and use of the machines, other system documentation and a review of previous reports of risk assessment of similar voting systems performed by other states and institutions. The information available to the scientists who performed the assessments of this study is some of the most comprehensive information available to date for any such study. This was not accomplished without the assistance and cooperation of the voting machine companies whose equipment and software were studied.

It should be noted that, in cooperative discussions with the voting machine companies, it is already recognized by one or more of them that problems exist with systems now in operation in Ohio and elsewhere in the U.S. Upgraded software and hardware is being tested for federal certification, which could replace equipment and software now in use in Ohio. Originally, two of the voting machine companies—Premier Election Solutions and ES&S—had requested that the secretary of state assess as part of Project EVEREST their “next generation” systems. Unfortunately, testing for federal certification of these proposed system solutions was not completed in time for it to be assessed as a part of this study. It is not known whether the “next generation” systems will diminish the risks found by the scientists in this study. Additional, similar testing is warranted, especially as it relates to server software for ballot design and vote tabulation.

All systems studied in Project EVEREST utilize for each county a central server and software for ballot definition and vote tabulation, and in some instances computer

workstations connected to the central server to extend the number of users of the server in preparing for or tabulating an election. Memory cards are the prime method used to transmit ballot definitions from the server or workstations to precinct-based machines and from the precinct-based machines to the server for vote tabulation. The precinct-based machines are either electronic machines that allow for marking ballot selections by either a touch screen or a dial and ballot optical scanners for scanning hand- or machine-marked votes on paper ballots, such as provisional and absentee ballots and some ballots marked by voters with disabilities. This system of voting is, in simple terms, computer-based voting.

Computers are widely used in our society for communication, financial transactions, complex problem solving and other functions requiring timeliness, accuracy and efficiency. Standards exist in the computer industry for requisite levels of security to protect privacy, integrity of methodology, and accuracy of data. It would follow that computers can be used to enhance the voting experience and should be subject to industry security standards as are other computer-based applications.

Unfortunately, the findings in this study indicate that the computer-based voting systems in use in Ohio do not meet computer industry security standards and are susceptible to breaches of security that may jeopardize the integrity of the voting process. Such safeguards were neither required by federal regulatory authorities, nor voluntarily applied to their systems by voting machine companies, as these products were certified for use in federal and state elections.

With Ohio's historical role in presidential elections and the 2008 presidential election fast approaching, the integrity of the state's voting process is of paramount importance. Ohio's voting system must be reliable and accurate to ensure fair results and voter confidence. It is discouraging that public funds have been spent not just in Ohio, but also nationally, for computer-based voting software that is antiquated, underdeveloped from a security standpoint, and in many cases, unstable. Much of today's current situation has evolved from a combination of 1) the unrealistic expectations of the tide of change following the 2000 presidential election seeking quick solutions for better, more reliable voting systems when the underbelly of the punch card election system was exposed in a close presidential popular vote, 2) the opportunities presented by this tide of change for voting machine companies to sell mass quantities of voting machines to state governments all over the nation, resulting in less than optimum research and design of the security of computer software and system configurations, 3) the failure of Congress and/or its newly established regulatory agency, the Election Assistance Commission, to recognize that computer-based voting, heavily marketed as a panacea, should be subject to stringent security testing to ensure it meets computer security industry standards, and 4) the failure of Congress to fully fund the Help America Vote Act by approximately \$800 million dollars to provide for adequate funding of the Election Assistance Commission and for training and other implementation solutions for the states.

While the advisory group of the state's election officials generally found that many of the scenarios described by corporate and academic security scientists may not be regularly anticipated in a "real-life" setting, the fact that no safeguards have been built into the state's voting systems to ensure that they do not occur is disconcerting and serves to undermine voter confidence. When HAVA was implemented in Ohio, the state provided little or no step-by-step guidance to county boards of elections. This left them

in a “thrown to the wolves” position to work with voting machine companies and their service technicians in implementing the new, computer-based systems or to develop their own procedures for implementing these systems in compliance with federal and state law, the latter of which contains gaps and provisions no longer consistent with the new voting machine technology. Election officials, being resourceful, persistent and adaptable, implemented this new generation of voting equipment and software under these less than optimum conditions and, in many cases, without guidance from the state. Complicating this is the state’s structure for funding elections, with directives coming from state and federal sources, but funding coming from the local board of county commissioners. All of this has resulted in a garden variety of procedures from county-to-county in Ohio, not all of which provide to each Ohioan the same level of ease or protection of the voting franchise.

Conscientious elections officials, who work many hours to prepare for an election and take seriously their role in ensuring a fair and efficient process, were placed in precarious positions, resulting in many of them “throwing in the towel” after many years of service and retiring or leaving the field of election administration. Staff turnover, and often with it, the loss of years of experience and knowledge, coupled with a lack of documentation or documentation no longer applicable to new voting procedures, has contributed to confusion and turmoil in the administration of elections.

The term “elections professional” has emerged, with training conferences and organizations often funded in part by voting machine companies resulting in an inevitable blurring of the distinctions between being an expert at ensuring a competent and responsive election process and being an expert at handling computer-based voting machines. This may account, in part, for the reluctance of some proficient election officials to scrutinize the security or integrity of computer-based voting systems. It has fed the accusations by voting protection activists that elections officials and voting machine companies share a common purpose. Such grassroots voting protection activism developed after a voting machine company chief executive from Ohio expressed in writing his intention to deliver the state for a particular presidential candidate in 2004—an incident that has been described as a “nuclear moment.”

In this environment Project EVEREST was conceived and undertaken in Ohio, a state at the root of election controversy, by a new secretary of state administration, to keep a promise to conduct a top-to-bottom review of its voting systems. The study’s purpose is and has been to gain information about the integrity of Ohio’s voting process and, more specifically, to assess risks associated with the state’s voting systems to ultimately strengthen voter confidence in Ohio and the confidence of the nation in Ohio’s voting process. While the initial reaction may be that the study’s findings do not instill confidence, the recommendations contained in this report will allow Ohio to move forward toward meeting Ohio voter expectations for elections that are safe, reliable and trustworthy and that merit the nation’s confidence in its outcomes.

The results of the study point to the need for great change not just in Ohio, but also in voting systems and procedures used in federal elections in general. The recommendations of this report were developed in consultation with an advisory group of twelve (12) elections officials from throughout Ohio with geographic and voting machine diversity, and whose numbers totaled six (6) Democrats and (6) Republicans, all of whom are directors or deputy directors of boards of elections with collective decades of experience. While not all elections officials have fully embraced all aspects of

these recommendations, all have expressed their willingness to assist in their implementation if Governor Strickland and the Ohio General Assembly agree that they should be implemented in whole or in part. For this, the secretary of state expresses gratefulness and respect.

## **Recommendations**

### ***Introduction***

In reviewing the findings of the various scientists of the study, the secretary of state finds that no system used in Ohio is without significant and serious risks to voting integrity. This appears to be a problem inherent with the products in use throughout the country as supplied by the industry. The Ohio secretary of state is constrained by the existence of available resources and necessarily makes some recommendations that security experts may consider less than optimum but that pose fewer risks than continuing to use the system as currently configured and implemented.

At present, Ohioans vote on Election Day at localized polling locations and, before the election, at boards of elections. Ballots are organized according to precincts comprised of no more than 1400 electors. Voting occurs on Election Day from 6:30 a.m. to 7:30 p.m., while early voting (as an in-person form of absentee voting) takes place during regular hours of boards of elections from thirty-five (35) days before the election through the day before Election Day.

Absentee voting by mail takes place beginning thirty-five (35) days before Election Day, and all ballots must be received no later than Election Day, except for military and overseas absentee ballots, which must be postmarked no later than Election Day and received no later than ten (10) days after the election. Provisional voting generally takes place on Election Day by voters who do not supply the preferred methods of identification (photo ID issued by the state or federal government, utility bill, bank statement, paycheck or government check or other government document) and by voters appearing at a polling location whose address does not match the address recorded in the poll book at that polling location or whose name does not appear in the poll book. Regardless of type of voting system used in a county, provisional ballots are paper ballots by virtue of a recent directive issued by the secretary of state (as a result of limitations of the VVPAT, “voter verified paper audit trail” in identifying provisional ballots ultimately as belonging to a particular voter) to ease the process of recounts and protect ballot secrecy for each voter.

## **Recommendations**

### ***Recommendation #1 – Eliminate points of entry creating unnecessary voting system risk by moving to Central Counting of Ballots***

The computer-based voting systems (all three of them) used in Ohio transmit ballot definition and votes for tabulation on memory cards (and in some cases on peripheral coding devices). These cards and devices are insecure and operated in environments where there are many levels of access to these devices (voters, poll workers, election officials, contractors and vendor representatives). These devices are used in multiple ports of entry to the system and shared between various components of

the system, whose shared data travels to the ultimate destination of the server software used for present and future elections. Accordingly, the prudent course of action is to remove insecure ports of entry to the system from less secure environments such as polling locations.

**Recommendation #2 – Eliminate DREs and Precinct-based Optical Scan Voting Machines that tabulate votes at polling locations**

Simply put, the elimination from polling locations of vote recording and tabulation machines such as DREs and precinct-based optical scan machines (except to use optical scan machines for determining overvotes and undervotes to satisfy HAVA “second chance” requirements) and instead migrating to central counting of ballots, ensures greater stability to the computer-based voting systems, because it eliminates multiple points of entry to a system not adequately secured.

**Recommendation #3 – Utilize the AutoMark for voters with disabilities**

The only computer-based system operated at the precinct level that does not tabulate votes is the AutoMark voting machine. This machine “reads” the bar code on a blank ballot using preprogrammed firmware and acts solely as a ballot marking device, allowing voters, especially those with disabilities, to mark their ballots with little or no assistance, preserving the secrecy of their ballot selections. The marked ballot is ejected once voted, and the voter places the voted ballot into a ballot box or scanner along with all other optical scan ballots. AutoMark voting machines should be used at all polling locations for voters who need assistance marking their ballots and for voters wishing to cast their ballots via a touch screen method.

**Recommendation #4 – Require all ballots be Optical Scan Ballots for central tabulation and effective voter verification**

As noted above, optical scan ballots provide greater opportunities for voter verification and are the only type of paper ballot able to be centrally counted with current technology. They are compatible with the non-tabulating AutoMark voting machine, effective for voters needing assistance. Optical scan voting is currently used in polling locations in approximately twenty-nine (29) counties. Optical scan ballots are consistent with provisional and absentee ballots already in use. Counties currently using DRE technology must still use optical scan ballots for absentee and provisional voting. With a movement to optical scan voting, ballots in a county would be of the same type and counted by high speed optical scanners (or by formerly precinct-based optical scanners centrally located as an interim measure.) Legislation would be needed to allow printing of ballots by printers from outside the State of Ohio to accommodate the increased volume of ballots to be printed.

**Recommendation #5 – Maintain “no fault” absentee voting while establishing Early (15 days prior to the election) and Election Day Vote Centers (of the size of 5 to 10 precincts), eliminating voting at individual precincts or polling places of less than 5 precincts**

“No fault” absentee voting (voting absentee without a stated reason), adopted in 2005, should be maintained to encourage participation while thinning Election Day voting. “Early voting” currently occurs as an “in-person” form of absentee voting,



requiring the voter to complete an absentee ballot application onsite when he or she appears at a board of elections to vote during the absentee balloting period. Voting at boards of elections by in-person absentee ballot would begin at the inception of the 35-day absentee voting period prior to an election, but at the 15-day point, additional voter centers would open for continuous voting seven (7) days per week through Election Day. On Election Day, vote centers would be open during traditional voting hours—6:30 a.m. through 7:30 p.m. On the days during the 15-day early voting period, vote centers (including boards of elections) would be open from 7:00 a.m. through 7:00 p.m. Monday through Saturday and from 12:00 noon through 7:00 p.m. on Sundays, staffed by two shifts of seven (7) hours each with an hour overlap during the period of 12:30 p.m. to 1:30 p.m. on Mondays through Saturdays. Voters would be assigned to a particular vote center as their polling location. Examples of vote centers would include libraries, community centers, senior centers, shopping centers or other accessible public buildings with adequate parking. Precincts would be maintained in the board's records, but vote centers would be created for 5 to 10 precincts, with extra staffing and materials planned for Election Day, especially in the first few years.

Ballots would be pre-printed optical scan ballots, and each polling place would maintain a separate ballot box for each election precinct. Voted ballots would be placed in the appropriate precinct box and returned in the box unopened or sealed for secrecy at the end of each day to the board of elections. Procedures would be prescribed by directive and/or statute for daily ballot reconciliations and with daily poll lists and poll books transported to the voter center each day. On Election Day, a mid-day pickup of ballots by board personnel would need to be authorized by legislation to permit scanning (not tabulation) before 7:30 p.m. on Election Day. Vote centers would also be equipped with two AutoMark ballot marking devices for voters with disabilities or needing assistance or who wished to use touchscreen and with two precinct-based optical scan machines for voters who wish to check their ballots for overvotes or undervotes by scanning them (with no tabulation occurring, but some firmware needed to read ballots to detect overvotes or undervotes). Voters would be able to drop off absentee ballots at vote centers for return to boards of elections. Early voting at vote centers may reduce the number of provisional ballots and provide more time to verify information for provisional ballots. Adequate signage and voter education would also need to be conducted to inform voters of 1) the availability of early voting in multiple locations, 2) the change to vote centers on Election Day, and 3) the need to carefully check ballots to ensure they have been correctly voted, avoiding overvotes or undervotes.

Other equipment needed for polling places would include privacy booths with surfaces for voting optical scan ballots, marking devices such as pens or pencils, extension cords for AutoMark machines, and optional storage for election related equipment and supplies. Any ballots stored at vote centers would need to meet standardized security requirements set by directive or statute. Otherwise, ballots would be delivered to vote centers daily. All ballots would be serialized for reconciliation purposes and all voted ballots would be returned to the board of elections at the end of each voting day.

After piloting the vote center/early voting concept in 2 or 3 counties at the March 2008 primary election (see Recommendation #7 below), vote centers and centralized optical scan voting would be implemented in the November 2008 election, as long as funding is available by mid-April 2008. Funding would be for the 2008 general election only and would include the following:

1. Funding for vote center workers exceeding what is already budgeted for paying poll workers in the November 2008 election (per county). Suggested minimum rate of pay is the state minimum wage of \$6.85 per hour, allowing counties to adjust upward for differing wage rates around the state;
2. Funding for printing optical scan ballots above what is already budgeted for November 2008 election (per county). Note some counties already have budgeted the printing of optical scan ballots for the entire county, since they are already using optical scan ballots;
3. Funding for high-speed optical scan machines (at present only one voting machine company has a certified high-speed optical scan machine, but several other vendors are awaiting certification of high speed optical scan machines, which would likely be available for certification by the Board of Voting Machine Examiners and for sale in Ohio by April 2008). Some counties already have high-speed optical scan machines, and the secretary of state has an inventory record of what is already on hand;
4. Funding for voting booths for use with voting optical scan ballots. Some counties retained their voting booths for punch card voting, and some of these may be converted for optical scan voting for a cost less than purchasing new ones. Other counties currently using optical scan that moved from precinct based voting to vote center voting would have extra voting booths. Those purchased with federal HAVA dollars could be redistributed, and those purchased with county funds could be purchased at resale cost;
5. Funding for purchase of ballot boxes for daily transport of voted ballots from vote centers to the board of elections;
6. Funding for leases of space for vote centers in excess of what is already budgeted for leases for polling places for November 2008;
7. AutoMark precinct-based ballot marking devices purchased with federal HAVA dollars could be redistributed among vote centers from counties using them in each precinct or polling location, with funding necessary to pay only for machines or accessories purchased with county funds, but at resale cost;
8. Already existing precinct-based optical scan machines purchased with federal HAVA dollars could be redistributed among vote centers (to satisfy second-chance voting requirements) from counties using them in each precinct or polling location, with funding necessary to pay only for machines or accessories purchased with county funds, but at resale cost;
9. Funding for software and/or servers compatible with high speed scanners purchased for central tabulation of optical scan ballots; and

10. Funding for public education about the changes to vote centers and second chance voting where precinct-based optical scanners may not be in use to scan for overvotes and undervotes.

***Recommendation #6 – require all Special Elections (issues only) held in August 2008 to be voted by mail (no in-person voting, except at the board of elections, for issue-only elections held in August 2008)***

Adopt either Sen. Cates' bill (S.B. 182) or similar legislation to require all-absentee voting for special elections (issues-only) as an interim step to all-mail special elections (issues-only). Eventually eliminate the required step of applying for an absentee ballot and simply mail ballots to all electors eligible to vote on the issue(s) submitted to the electorate.

***Recommendation #7 – implement Pilot Programs for vote centers at the March 2008 election in 2 to 3 counties already using optical scan voting***

Allow 2 to 3 counties already utilizing optical scan voting to voluntarily implement Pilot Programs for Vote Centers in the March 2008 presidential primary election and evaluate specific features and practices for improved future implementation, however, being poised to implement them statewide for the November 2008 election.

***Recommendation #8 – adopt legislation to allow a county to vote on whether it desires to vote by mail for a temporary or permanent period of time (see, R.C. 3506.02 for amendment).***

Such an election could take place on a pilot basis at the August 2008 special election. Voters in a county could specify if they wanted mail-in voting and whether it would be solely by absentee vote or by regular ballots mailed to all registered electors in the county. The mail-in voting could be for a specific trial period or indefinitely, depending on legislative preference.

***Recommendation #9 – for the March 2008 primary election permit county boards of elections using precinct-based optical scan machines to move the machines to a central location to implement centralized counting of optical scan ballots***

Counties exercising this option could opt to move to high speed optical scanners for the November 2008 election with available funding.

***Recommendation #10 – for the March 2008 primary election require counties utilizing DREs to offer paper ballots to voters who do not want to vote on DREs***

At the date of this report, it would be extremely difficult for all Ohio counties currently using DREs (a total of 58 counties) to move to a central count optical scan system before the March 2008 primary election. For counties that find themselves in a position of needing to conduct the March 2008 primary election utilizing DREs for voting, electors should be provided the option to vote a paper optical scan ballot at their

polling places. This may be accomplished by legislation. The secretary of state should provide by directive (as opposed to legislation) a temporary determination (specific to the March 2008 election) of the number of optical scan ballots counties should print for distribution upon request in voting precincts where DREs are still in use. The secretary of state is willing to confer with legislative leaders, the Ohio Association of Election Officials and the Ohio Association of County Commissioners on appropriate levels of these substitute paper ballots for the March 2008 primary election. Ballot boxes and secrecy envelopes would also need to be purchased, in addition to voting booths for marking optical scan ballots. These could be used in the fall election for vote centers.

### **Other Options**

The advisory group of 12 election officials discussed earlier assisted in the development of the recommendations listed above. Not all were enthusiastic about eliminating DREs but all expressed willingness to assist at every stage of planning and implementation of any or all of these recommendations.

Other options explored but deemed to be more costly include the following:

#### ***Central Count Optical Scan Voting at Regular Precinct/Polling Locations using AutoMark for Voters with Disabilities***

1. Continue with precinct or polling place based voting using central count optical scan machines, with second chance provided by advertising as permitted by HAVA and utilizing AutoMark ballot marking devices for voters with disabilities. Potential problems with this option include the perennial challenge of recruiting enough poll workers, although training is simpler without DREs or precinct based optical scan machines. In addition, more AutoMark machines would need to be purchased at a per-unit price of approximately \$5400, and this adds significantly to the cost.

#### ***Vote by Mail***

2. Eliminate in-person voting, except in case of voters with disabilities using AutoMark machines. All registered electors would receive a regular ballot by mail. Potential problems with this option include ensuring the integrity of county voter databases that should avoid (but do not always avoid) duplications. Voter ID requirements would more likely ensure honesty in voted ballots (i.e. actually voted by the named voter). This is a more expensive option, especially if the ballot is several pages. It is anticipated that return postage would need to be paid, but "drop off boxes" at specific locations could be utilized to avoid return postage. The State of Oregon successfully utilizes this method, along with nearly all counties in the State of Washington. Voter participation is shown to be higher with this method. This could be piloted at the November 2008 election at a county's option (see Recommendation #8 and R.C. 3506.02 and potential to amend this section).

#### ***Move back the 2008 Primary Election Date to Implement More Recommendations Sooner***

3. This option may allow for the implementation of more recommendations sooner; for more pilot experiments before the November 2008 general election; and for some counties to discontinue DRE use and move to optical scan for the primary. However, delays in funding past, for instance, a first Tuesday after the first Monday in May date could make November implementation difficult if only pilot programs are attempted in May or if funding for changes in November is not determined until after a May primary. Moreover, political and primary election logistical problems could arise in moving back the primary election date, because candidate planning, petition circulation and even filing may already have begun. This would appear to be an option of lesser attraction for all of these reasons.

### ***Cuyahoga County Primary Election Remedy***

4. Software problems associated with Cuyahoga County's GEMS server for its DRE-based voting system occurred at the November 2007 election. Because that election involved a turnout of approximately 15%, and turnout is expected to be substantially higher in March 2008, great concern exists for continued use of this voting system in Cuyahoga County in the March 2008 primary. With the state's funding assistance, Cuyahoga County could move to a central-count optical scan system for the March 2008 primary election by utilizing leased DREs for precinct based voting by persons with disabilities and purchasing high speed optical scanners (with compatible server and software and voting booths) for optical scan voting. This option has been estimated to cost between \$2 million and \$2.5 million dollars. All purchased equipment could transfer to a vote center voting system for use in November 2008, and extra voting booths not needed for vote centers could be redistributed to other counties migrating from DRE to optical scan central count vote centers. The county would be responsible for printing a sufficient number of ballots for the March primary election. If this option is approved, purchases would need to be made immediately, with reimbursement applied for by the secretary of state to the Ohio General Assembly to reimburse the Cuyahoga County Commissioners for equipment purchases.

### **Other Legislation and/or Directives or Rules to be Implemented as a Result of Findings**

Following is a list of other legislation and/or directives or rules not specifically mentioned in the Recommendations above but that are recommended to be implemented as a result of the study's findings. This list is not exhaustive, especially as to directives that will be needed to implement some or all of the above Recommendations:

1. Clarify the law to ensure that vendors and boards of elections notify the secretary of state when "enhancements" and "significant adjustments" are made to the hardware and software. Also, include "firmware" as part of the identified items. (LEGISLATION);
2. Adequately and more frequently train poll workers and presiding judges. (Requires changes to R.C. 3501.27) (LEGISLATION);

3. Require a standard quality of paper and method of handling for the Voter Verified Paper Audit Trail (VVPAT) as a temporary measure for the 2008 primary election. (DIRECTIVE);
4. Reduce the amount of necessary information required on the official ballot to decrease the number of pages of a ballot, including exploring using a “key-type ballot” for voting on issues, with a less expensively printed explanation of the issues. (Requires changes to R.C. 3513.052 & 3513.30) (LEGISLATION);
5. Establish set procedures for the distribution of electronic voting machines. This proposal would allow the secretary of state to define, using specified variables, how many machines should be allocated for each precinct for the March 2008 primary election. (R.C. 3501.11 (I)) (LEGISLATION OR DIRECTIVE);
6. Expand the “Youth at the Booth” program to allow up to 2 high school seniors to serve as poll workers (for early voting at vote centers and) on Election Day and to allow college students to serve in the county where they attend school. (Requires change to R.C. 3501.22(C)) See also, H.B. 350. (LEGISLATION);
7. Change or remove sections of the Ohio Revised Code that are out-dated and/or inconsistent with technology and related procedures. (Ohio Association of Election Officials has been compiling a list.) (LEGISLATION);
8. Permit absentee ballots that are postmarked on or before Election Day to be counted if received by the board of elections within 10 days of Election Day (see Rep. Dyer’s bill, H.B. 336). (LEGISLATION);
9. Permit absentee ballots to be counted if the identification envelope is missing information that was supplied on the absentee ballot application that does not prevent the board of elections from identifying the voter. (LEGISLATION);
10. Permit boards of elections to accept faxed absentee ballot applications. (R.C. 3509.03) (LEGISLATION);
11. Permit permanent absentee status for stated situations, e.g. permanently disabled, no longer have a driver’s license or of a certain age. (LEGISLATION);
12. Make absentee ballot return envelopes significantly distinguishable from regular mail so as to make it easily identifiable by United States Postal Service workers. (DIRECTIVE OR RULE);
13. Permit and require the certification of electronic poll books. (R.C. 3505.05) (LEGISLATION);
14. Establish security protocols for election servers and software. (DIRECTIVE OR RULE);

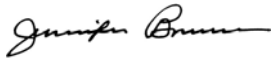
15. Specify standards for Logic and Accuracy (L&A) testing of tabulating machines. (DIRECTIVE OR RULE, POSSIBLY LEGISLATION); and
16. Establish standardized security procedures based on specified levels of risk for components of voting systems. (DIRECTIVE OR RULE).

## **Conclusion**

The implications of this report are serious. Swift and specific changes are needed to improve the quality of Ohio elections so that Ohio is prepared to successfully execute next year's presidential election. Ohio election officials have shown an eagerness to participate in the planning and implementation of these needed changes, and the secretary of state looks forward to working with them and the Ohio legislature in achieving these needed improvements.

The secretary of state is grateful for the stated intentions of Governor Strickland and leaders of the Ohio General Assembly to work in a bipartisan fashion to resolve issues affecting election integrity and to make Ohio a model for other states in implementing election reform.

Sincerely,



Jennifer Brunner  
Ohio Secretary of State



**JENNIFER BRUNNER**  
**OHIO SECRETARY OF STATE**

180 EAST BROAD STREET  
COLUMBUS, OHIO 43215  
TELEPHONE: 614-466-3613  
TOLL-FREE: 877-767-3453  
[WWW.SOS.STATE.OH.US](http://WWW.SOS.STATE.OH.US)  
[JBRUNNER@SOS.STATE.OH.US](mailto:JBRUNNER@SOS.STATE.OH.US)





CALIFORNIA

Secretary of State **DEBRA BOWEN**
[HOME](#) ▶  
[SITE SEARCH](#) ▶  
[CONTACT US](#) ▶
[SECRETARY OF STATE](#)[ELECTIONS & VOTER INFO](#)[POLITICAL REFORM](#)[BUSINESS PROGRAMS](#)[ARCHIVES & MUSEUM](#)[OTHER SERVICES](#)
**ELECTIONS  
& VOTER  
INFORMATION**


## Top-to-Bottom Review

---

[About Elections](#)
[Division](#) ▶

[Election Results and  
Election Dates](#) ▶

[Register to Vote](#) ▶

[Voter Registration  
Statistics](#) ▶

[Voter Information](#) ▶

[Initiatives](#) ▶

[Voter Education](#) ▶

[Political Parties](#) ▶

[Candidate  
Information](#) ▶

[Resources](#) ▶

[Site Map](#) ▶

Secretary of State Debra Bowen conducted a top-to-bottom review in 2007 of many of the voting systems certified for use in California. The review, led by computer scientists from the University of California, was designed to restore the public's confidence in the integrity of the electoral process and to ensure that California voters cast their ballots on machines that are secure, accurate, reliable, and accessible. Following the top-to-bottom review, on August 3, 2007, Secretary Bowen strengthened the security requirements and use conditions for certain systems. The following documents detail Secretary Bowen's decisions and the independent experts' findings in the review.

### Withdrawal of Approval and Reapproval Decisions Issued by Secretary of State Debra Bowen

#### Premier Election Solutions (formerly Diebold Election Systems)

- [Withdrawal of Approval/Conditional Reapproval - October 25, 2007 Revision \(.pdf, 9,903KB\)](#)
- [Withdrawal of Approval/Conditional Reapproval - October 25, 2007 Redline Version \(.pdf, 64KB\)](#)
- [Post-Election Manual Tally Regulations](#)

#### Hart InterCivic

- [Withdrawal of Approval/Conditional Reapproval - December 6, 2007 Revision \(.pdf, 5,886KB\)](#)
- [Withdrawal of Approval/Conditional Reapproval - December 6, 2007 Red Line Version \(.pdf, 5,886KB\)](#)
- [Post-Election Manual Tally Regulations](#)

#### Sequoia Voting Systems

- [Withdrawal of Approval/Conditional Reapproval - October](#)

- [1, 2009 Revision \(.pdf, 14MB\)](#)
- [Withdrawal of Approval/Conditional Reapproval - October 1, 2009 Redline Version \(.pdf, 58KB\)](#)
- [Withdrawal of Approval/Conditional Reapproval - October 25, 2007 Revision \(.pdf, 10,356KB\)](#)
- [Withdrawal of Approval/Conditional Reapproval - October 25, 2007 Redline Version \(.pdf, 67KB\)](#)
- [Post-Election Manual Tally Regulations](#)
- [Letter to Riverside County - October 2, 2007 \(.pdf, 114KB\)](#)

## **Election Systems and Software**

- [ES&S Inkavote Plus Conditional Approval - January 2, 2008 \(.pdf, 12.4MB\)](#)
- [InkaVote Plus Source Code Report - October 2, 2007 \(.pdf, 172KB\)](#)
- [InkaVote Plus Red Team Report - October 2, 2007 \(.pdf, 123KB\)](#)
- [InkaVote Plus Voting System Accessibility Review - January 2, 2008 \(.pdf, 697KB\)](#)
- [InkaVote Plus - November 26, 2007 Public Hearing Notice \(.pdf, 48KB\)](#)
- [InkaVote Plus - November 26, 2007 Hearing Transcript \(.pdf, 169KB\)](#)
- [Rescission and Withdrawal of Approval - August 3, 2007 \(.pdf, 303KB\)](#)
- [Post-Election Manual Tally Regulations](#)

---

## **UC Final Reports**

Following are the final reports from the University of California scientists detailing their findings from the top-to-bottom review. The red, source code, and documentation review team reports are separated by voting system. The accessibility report contains findings on all of the voting systems that were reviewed.

## **UC Source Code Team Reports**

- [UC Principal Investigator David Wagner's Statement on Protection of Security-Sensitive Information \(.pdf, 13.9KB\)](#)
- [Premier Election Solutions \(formerly Diebold\) \(.pdf, 561KB\)](#)
- [Hart InterCivic \(.pdf, 573KB\)](#)
- [Sequoia Voting Systems \(.pdf, 831KB\)](#)

## UC Red Team Reports

- [Overview by UC Principal Investigator Matt Bishop](#) (.pdf, 303KB)
- [Red Team Test Protocol](#) (.pdf, 134KB)
- [Premier Election Solutions \(formerly Diebold\)](#) (.pdf, 498KB)
- [Hart InterCivic](#) (.pdf, 376KB)
- [Sequoia Voting Systems](#) (.pdf, 108KB)

## UC Documentation Review Reports

- [Premier Election Solutions, Inc. \(formerly Diebold\)](#) (.pdf, 402KB)
- [Hart InterCivic](#) (.pdf, 1,028KB)
- [Sequoia Voting Systems](#) (.pdf, 368KB)

## UC Accessibility Report

- [Accessibility Report](#) (.pdf, 1.07MB)
- [Accessibility Report](#) (HTML)

## Public Hearing

- [Webcast of the July 30, 2007, Public Hearing Transcript](#) (.pdf, 48KB)
- [Public Notice](#) (.pdf, 58KB)
- [Agenda](#) (.pdf, 48KB)
- [Written Public Comment and Testimony](#)

## Press Releases

- [Video of Secretary of State Bowen's August 3, 2007, Announcement](#)
- [August 3, 2007](#) (.pdf, 152KB)
- [July 27, 2007](#) (.pdf, 152KB)
- [June 21, 2007](#) (.pdf, 138KB)
- [May 10, 2007](#) (.pdf, 165KB)
- [May 9, 2007](#) (.pdf, 144KB)

## Testing Security Plans

- [Secretary of State Testing Security Plan](#) (.pdf, 51KB)
- [Source Code Review Security Plan](#) (.pdf, 78KB)
- [Red Team Security Plan](#) (.pdf, 128KB)

- [Documentation Review Security Plan \(.pdf, 68KB\)](#)

## Additional Information

Following are a number of documents related to the review, including a "Frequently Asked Questions" document to help people understand how the review was designed.

- [One-Page Summary - May 9, 2007 \(.pdf, 148KB\)](#)
- [Frequently Asked Questions - Revised August 15, 2007 \(.pdf, 242KB\)](#)
- [Frequently Asked Questions - Revised July 2, 2007 \(.pdf 232KB\)](#)
- [Frequently Asked Questions - Revised June 13, 2007 \(.pdf, 232KB\)](#)
- [Frequently Asked Questions - Revised May 11, 2007 \(.pdf, 257KB\)](#)
- [Frequently Asked Questions - Revised May 9, 2007 \(.pdf, 248KB\)](#)
- [Contract Between Secretary of State and University of California Regents \(.pdf, 186KB\)](#)
  
- [Public Observation Guidelines \(.pdf, 56KB\)](#)

---

## Professional Qualifications of the Top-to-Bottom Review Teams

### Documentation Review Team Members

*The reviewers were responsible for analyzing voting system security, accessibility, usability, reliability, accuracy and protection of ballot secrecy based on relevant documentation. The reviewers had access to documents such as reports from Independent Testing Authorities (ITAs), reports and data from state certification testing, and documentation related to how the systems are designed to be used in an actual election. The reviewers were split into three teams of two or three members to review each voting system subject to the top-to-bottom review.*

[David Wagner \(.pdf, 455KB\)](#) Principal Investigator

[Aaron Burstein \(.pdf, 57KB\)](#)

[Nathan Good \(.pdf, 311KB\)](#)

[Joseph Hall \(.pdf, 229KB\)](#)

[Candice Hoke](#) (.pdf, 404KB)

[Dave Kettyle](#) (.pdf, 167KB)

[Deirdre Mulligan](#) (.pdf, 460KB)

[Laura Quilter](#) (.pdf, 55KB)

[Tom Ryan](#) (.pdf, 125KB)

### **Source Code Review Team Members**

*Source code is the computer language that effectively controls how electronic voting systems operate. The source code reviewers were split into three teams of six or seven members to review each voting system subject to the top-to-bottom review. Here is a more detailed description of [source code review](#).*

[David Wagner](#) (.pdf, 455KB) Principal Investigator

[Matt Blaze](#) (.pdf, 72KB)

[Joseph Calandrino](#) (.pdf, 62KB)

[Arel Cordero](#) (.pdf, 52KB)

[Sophie Engle](#) (.pdf, 145KB)

[Ariel Feldman](#) (.pdf, 47KB)

[J. Alex Halderman](#) (.pdf, 60KB)

[Srinivas Inguva](#) (.pdf, 174KB)

[Chris Karlof](#) (.pdf, 70KB)

[Eric Rescorla](#) (.pdf, 78KB)

[Naveen Sastry](#) (.pdf, 138KB)

[Hovav Shacham](#) (.pdf, 164KB)

[Micah Sherr](#) (.pdf, 108KB)

[Till Stegers](#) (.pdf, 62KB)

[Dan Wallach](#) (.pdf, 634KB)

[Ka-Ping Yee](#) (.pdf, 173KB)

[Harlan Yu](#) (.pdf, 54KB)

[William Zeller](#) (.pdf, 65KB)

### **Red Team Members**

*Red team members were responsible for testing the functions and performance of the voting systems and identifying security or accuracy vulnerabilities. The red team members were split into three teams to review each voting system subject to the top-to-bottom review. Here is an explanation of [red team testing in general and the preliminary protocols](#) that were used in the red team testing.*

[Matthew Bishop](#) (.pdf, 934KB) Principal Investigator

[Robert Abbott](#) (.pdf 203KB)  
[Elliot Proebstel](#) (.pdf 124KB)  
[Sujeet Sheno](#)i (.pdf 37KB)  
[Davide Balzarotti](#) (.pdf 66KB)  
[Greg Banks](#) (.pdf 12KB)  
[Marco Cova](#) (.pdf 61KB)  
[Mark Davis](#) (.pdf 33KB)  
[Viktoria Felmetsger](#) (.pdf 59KB)  
[Richard Kemmerer](#) (.pdf 49KB)  
[William Robertson](#) (.pdf 69KB)  
[Jacob Stauffer](#) (.pdf 32KB)  
[Fredrik Valeur](#) (.pdf 74KB)  
[Giovanni Vigna](#) (.pdf 111KB)

### **Accessibility Team Members**

*The accessibility reviewers examined the voting systems subject to the top-to-bottom review to determine whether they were accessible to voters with disabilities and voters with alternative language needs.*

[Noel Runyan](#) (.pdf 13KB)  
[James Tobias](#) (.pdf 20KB)

---

### **Draft Criteria**

The draft criteria for the top-to-bottom review of voting systems certified for use in California were released for public comment on March 22, 2007. The final criteria for the review can be found in the [Contract Between Secretary of State and University of California Regents](#).

- [Press Release - March 22, 2007](#)
- [Draft Criteria Released for Public Comment - March 22, 2007](#)

### **Public Comment**

#### **Counties**

[California Association of Clerks and Election Officials \(CACEO\)](#)  
[California State Association of Counties \(CSAC\)](#)

[Butte](#)  
[Contra Costa](#)  
[Kern](#)  
[Los Angeles](#)  
[Madera](#)  
[Mariposa](#)  
[Mendocino](#)  
[San Joaquin](#)  
[San Luis Obispo](#)  
[San Mateo](#)  
[Santa Clara](#)  
[Santa Cruz](#)  
[Shasta](#)  
[Solano](#)  
[Sonoma](#)  
[Yolo](#)  
[Yuba](#)

## **Voting System Vendors**

[Avante](#)  
[Premier Election Solutions \*\(formerly Diebold\)\*](#)  
[Equalivote and VotePAD](#)  
[ES&S](#)  
[Hart InterCivic](#)  
[Sequoia Voting Systems](#)

## **Organizations**

[Black Box Voting](#)  
[California Council of the Blind](#)  
[California Foundation for Independent Living Centers](#)  
[Coloradoans for Voting Integrity](#)  
[Open Voting Consortium](#)  
[Protection and Advocacy, Inc.](#)  
[Secure Accurate Elections](#)  
[Townsend and Associates](#)  
[VerifiedVoting.org](#)  
[Wellstone Democratic Renewal Club](#)

## **Individuals**

[Comments from Individuals](#)

All personal information has been removed from comments submitted by individuals.



Copyright ©2008 California Secretary of State. [Privacy Statement](#)



## **Pentagon cancels Internet voting test**

Too many concerns about ballot security, official says

**The Associated Press**

updated 7:07 p.m. ET, Mon., May 17, 2004

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.

The official said alternative voting systems will now be considered, possibly using the Internet as well. The official could not say when, if ever, such a system would be ready.

### **Debate will continue**

Accenture eDemocracy Services, the vendor that built the system, issued a statement indicating testing will continue.

"This is now an opportunity to demonstrate that the Internet is viable, valuable and secure enough to use for filing absentee ballots," said Meg McLaughlin, the Accenture unit's president. "We are confident that sending absentee ballots via the Internet is just as secure and reliable as sending them by mail."

The skeptics were elated.

"We certainly share their desire to make sure that our military people have the opportunity to vote in the national election, but it's always been our contention that we're not doing them any favor by providing them an insecure system on which to vote," said Barbara Simons, one of four co-authors of the critical Pentagon voting report and a former president of the Association for Computing Machinery.

### **Aimed at aiding overseas citizens**

The \$22 million Secure Electronic Registration and Voting Experiment, or [SERVE](#), was designed to help overseas citizens vote in U.S. elections. Nearly one in three overseas soldiers registered to vote in the 2000 presidential election didn't receive ballots in time.

In a smaller Internet voting trial conducted that same year by the Pentagon's Federal Voting

Assistance Program, 84 citizens submitted online ballots to Florida, South Carolina, Texas and Utah.

This year's \$22 million trial, also overseen by the Pentagon agency, was to have covered 50 counties in Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah and Washington. It would have been open to nonmilitary Americans abroad and military personnel stationed at U.S. and foreign bases. Any Internet-connected computer running Windows operating systems, including at a cybercafe, could have been used for voting.

The system was to be ready for the general elections and possibly later primary states, though it had not been certified in time for use in Tuesday's South Carolina primary.

About 6 million U.S. voters live overseas, most of them members of the military or their relatives.

### **Risks tallied**

The report from Simons and three other experts on a 10-member Pentagon peer-review panel said Internet voting could not be made secure — at least using today's technology — primarily because the Internet and personal computers are inherently vulnerable to hackers and viruses.

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.

Doug Lewis, executive director of the Houston-based Election Center research group, said the Pentagon decision will likely set back Internet voting. Many states had been awaiting the results of the trial before committing to widespread online voting.

Michigan Democrats already have begun online voting leading up to Saturday's caucuses, which are run by the party and are thus not subject to election certification requirements.

*© 2009 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.*

URL: [http://www.msnbc.msn.com/id/4184803/ns/politics-voting\\_problems/](http://www.msnbc.msn.com/id/4184803/ns/politics-voting_problems/)

[MSN Privacy](#) . [Legal](#)

© 2010 MSNBC.com

## Computer Technologists' Statement on Internet Voting

Election results must be verifiably accurate -- that is, auditable with a permanent, voter-verified record that is independent of hardware or software. Several serious, potentially insurmountable, technical challenges must be met if elections conducted by transmitting votes over the internet are to be verifiable. There are also many less technical questions about internet voting, including whether voters have equal access to internet technology and whether ballot secrecy can be adequately preserved.

*Internet voting should only be adopted after these technical challenges have been overcome, and after extensive and fully informed public discussion of the technical and non-technical issues has established that the people of the U.S. are comfortable embracing this radically new form of voting.*

A partial list of technical challenges includes:

- **The voting system as a whole must be verifiably accurate in spite of the fact that client systems can never be guaranteed** to be free of malicious logic. Malicious software, firmware, or hardware could change, fabricate, or delete votes, deceive the user in myriad ways including modifying the ballot presentation, leaking information about votes to enable voter coercion, preventing or discouraging voting, or performing online electioneering. Existing methods to “lock-down” systems have often been flawed; and even without that problem, there is no guaranteed method for preventing or detecting attacks by insiders such as the designers of the system.
- **There must be a satisfactory way to prevent large-scale or selective disruption** of vote transmission over the internet. Threats include “denial of service” attacks from networks of compromised computers (called “botnets”), causing messages to be mis-routed, and many other kinds of attacks, some of which are still being discovered. Such attacks could disrupt an entire election or selectively disenfranchise a segment of the voting population.
- **There must be strong mechanisms to prevent undetected changes to votes**, not only by outsiders but also by insiders such as equipment manufacturers, technicians, system administrators, and election officials who have legitimate access to election software and/or data.
- **There must be reliable, unforgeable, unchangeable voter-verified records** of votes that are at least as effective for auditing as paper ballots, without compromising ballot secrecy. Achieving such auditability with a secret ballot transmitted over the internet but without paper is an unsolved problem.
- **The entire system must be reliable and verifiable** even though internet-based attacks can be mounted by anyone, anywhere in the world. Potential attackers could include individual hackers, political parties, international criminal organizations, hostile foreign governments, or even terrorists. The current internet architecture makes such attacks difficult or impossible to trace back to their sources.

Given this list of problems, there is ample reason to be skeptical of internet voting proposals. Therefore, the principles of operation of any internet voting scheme should be publicly disclosed in sufficient detail so that anyone with the necessary qualifications and skills can verify that election results from that system can reasonably be trusted. Before these conditions are met, “pilot studies” of internet voting in government elections should be avoided, because the apparent “success” of such a study absolutely cannot show the absence of problems that, by their nature, may go undetected. Furthermore, potential attackers may choose only to attack full-scale elections, not pilot projects.

The internet has the potential to transform democracy in many ways, but permitting it to be used for public elections without assurance that the results are verifiably accurate is an extraordinary and unnecessary risk to democracy.

## Endorsements

The computer technology experts below endorse this statement. Affiliations are for identification only, and do not imply that employers have a position on the statement.

Alex Aiken  
Professor of Computer Science, Stanford University  
<http://cs.stanford.edu/~aiken>

Andrew W. Appel  
Professor of Computer Science, Princeton University  
<http://www.cs.princeton.edu/~appel/>

Ben Bederson  
Associate Professor, Computer Science Department, University of Maryland  
<http://www.cs.umd.edu/~bederson>

L. Jean Camp  
Associate Professor, School of Informatics, Indiana University  
<http://www.ljean.com/>

David L. Dill  
Professor of Computer Science, Stanford University and Founder of VerifiedVoting.org  
<http://verify.stanford.edu/dill>

Jeremy Epstein  
Software AG and Co-Founder, Verifiable Voting Coalition of Virginia  
<http://www.visualcv.com/jepstein>

David J. Farber  
Distinguished Career Professor of Computer Science and Public Policy, Carnegie Mellon University  
<http://www.epp.cmu.edu/httpdocs/people/bios/farber.html>

Edward W. Felten  
Professor of Computer Science and Public Affairs, Princeton University  
<http://www.cs.princeton.edu/~felten>

Michael J. Fischer  
Professor of Computer Science, Yale University, and President, TrueVoteCT.org  
<http://www.cs.yale.edu/people/fischer.html>

Don Gotterbarn  
Director, Software Engineering Ethics Research Institute, Computer and Information Sciences,  
East Tennessee State University  
<http://csciwww.etsu.edu/gotterbarn>

Joseph Lorenzo Hall  
UC Berkeley School of Information  
<http://josephhall.org/>

Harry Hochheiser  
Assistant Professor, Computer and Information Sciences, Towson University  
<http://triton.towson.edu/~hhochhei>

Jim Horning  
Chief Scientist, SPARTA, Inc., Information Systems Security Operation  
<http://www.horning.net/pro-home.html>

David Jefferson  
Lawrence Livermore National Laboratory  
<http://people.llnl.gov/jefferson6>

Bo Lipari  
Retired Software Engineer, Executive Director New Yorkers for Verified Voting  
<http://www.nyvv.org/bolipari.shtml>

Douglas W. Jones  
Professor of Computer Science, University of Iowa  
<http://www.cs.uiowa.edu/~jones/vita.html>

Robert Kibrick  
Director of Scientific Computing, University of California Observatories / Lick Observatory  
<http://www.ucolick.org/~kibrick>

Scott Klemmer  
Assistant Professor of Computer Science, Stanford University  
<http://hci.stanford.edu/srk/bio.html>

Vincent J. Lipsio  
<http://www.lipsio.com/~vince/resume.pdf>

Peter Neumann  
Principal Scientist, SRI International  
<http://www.csl.sri.com/users/neumann>

Eric S. Roberts  
Professor of Computer Science, Stanford University  
<http://cs.stanford.edu/~eroberts/bio.html>

Avi Rubin  
Professor, Computer Science, Johns Hopkins University  
<http://avi-rubin.blogspot.com/>

Bruce Schneier  
Chief Security Technology Officer, BT Global Services  
<http://www.schneier.com/>

John Sebes  
Co-Director, Open Source Digital Voting Foundation  
Chief Technology Officer, TrustTheVote Project  
<http://www.osdv.org/who>

Yoav Shoham  
Professor of Computer Science, Stanford University  
<http://cs.stanford.edu/~shoham>

Barbara Simons  
IBM Research (retired)  
<http://www.verifiedvoting.org/article.php?id=2074>

Eugene H. Spafford  
Professor and Executive Director of CERIAS, Purdue University  
<http://spaf.cerias.purdue.edu/narrate.html>

Michael Walfish  
Assistant Professor of Computer Science, University of Texas, Austin  
<http://nms.csail.mit.edu/~mwalfish>

Dan S. Wallach  
Associate Professor, Department of Computer Science, Rice University  
<http://www.cs.rice.edu/~dwallach/>

Luther Weeks  
Retired Software Engineer and Computer Scientist  
[http://www.ctvoterscount.org/?page\\_id=2](http://www.ctvoterscount.org/?page_id=2)

Jennifer Widom  
Professor of Computer Science, Stanford University  
<http://infolab.stanford.edu/~widom/>

David S. Wise  
Computer Science Dept., Indiana University  
<http://www.cs.indiana.edu/~dswise/>

## Questions and Answers on the "Computer Technologists' Statement on Internet Voting"

We hope these questions and answers clarify the intention of the statement.

**Q:** Who is behind this statement?

**A:** The primary author is David Dill, Professor of Computer Science at Stanford, with extensive input and editing from a number of others. This is also the position of VerifiedVoting.org on internet voting, and VerifiedVoting.org will help to publicize it.

**Q:** Why this statement at this time?

**A:** Serious proposals to use internet voting keep coming up. There have been several internet primaries in the last few years, including a primary conducted by Democrats Abroad in 2008. Furthermore, internet voting schemes are being promoted for the general election in 2008, including a proposal by Okaloosa County, Florida, and the State of Alabama.

In many cases, these schemes have been deployed without due consideration of the technical challenges, based on unsupported assertions by vendors that the systems are "secure". Independent experts need to speak out.

**Q:** Is this an anti-internet voting statement?

**A:** No. Some of the people who have endorsed it are working on internet voting methods. The statement is intended to be a warning: internet voting is not as easy to do safely as some people seem to think. Before we move to it, we need an informed public debate so the people know what they're getting into.

**Q:** What explains the enthusiasm for internet voting?

**A:** Currently, most of the momentum seems to be coming from the difficulties that Americans overseas, especially in the military, have voting. The mails are inefficient, so absentee ballots take a long time to reach the voter and a long time to return.

We understand this problem, but it seems clear that the situation can be made a lot better for overseas voters without internet voting. First, a system could be set up where any voter can print a ballot obtained over the internet (or obtain a remotely printed ballot at a military facility or embassy), which would eliminate half the mail problems, and difficulties with local elections offices that mail ballots late. Second, marked ballots could be returned by express mail or (better) by military transport or in diplomatic pouches, after being appropriately signed and sealed. This year, Federal Express is offering discounts to overseas voters for returning ballots. Finally, laws in some states could be modified to make the time constraints on ballot arrival less stringent, to reduce the risk that ballots will not be counted. In voting, there has been a tendency to look for technical solutions to problems that are mostly non-technical. We believe that is happening again with internet voting.

Alternatively, someone could come up with an internet voting scheme that is at least as safe as current overseas ballots, and convince the rest of us that it actually is secure and doesn't have other harmful effects.

We do not feel that it is appropriate to "enfranchise" voters by providing them with a system that may allow their votes to be lost or stolen undetectably.

**Q:** The statement asks that the "principles of operation" of the system need to be disclosed. What does that mean? Does it require open source?

**A:** We're going by analogy with low-tech voting systems. For example, to understand why a fully manual paper ballot voting system can be trusted, people have to know how the ballots are handled, how polling places are run, etc. For example, if there are multiple poll workers present in each polling place at all times, it's harder for someone to "stuff" the ballot box. If hand counts are conducted in public view, it's less likely that the counts are erroneous.

We don't need to know everything about a system to know whether it is trustworthy. For example, most people would not feel that they need to know how computerized typesetting works before they marked a paper ballot. In fact, if you have to know a lot of complex details to understand whether a system can be trusted, that system probably can't be trusted.

The statement asks that the things we need to know to trust a proposed internet voting scheme be revealed. This is a problem because many schemes are being proposed where the details of operation are secret.

Some of us think "open source", or, more precisely, public disclosure of source code is a good idea. However, source code disclosure is neither necessary nor sufficient for trustworthy voting. Even when source code has been carefully inspected, it is very easy to overlook program bugs or malicious behavior in the system. It is also very difficult to make sure that the program running on a particular voting system matches the source code that was reviewed (vs. "acting the same" for certain test cases). Finally, errors and malicious changes can exist in parts of the system that are not in the source code, including low-level firmware and the hardware itself.

In a nutshell, if the security of a system depends on source code review, the system is not secure.

**Q:** Are you implying vendors or election officials are dishonest?

**A:** No, not any more than wanting bank statements implies that my bank is dishonest. Almost all trust in modern society is based on checks and balances (e.g., auditing requirements). Without the accountability that follows from checks and balances, systems become inaccurate and often dishonest. Classical election procedures are based on checks and balances, with the knowledge that elections are important and that unscrupulous people may seek to commit fraud. The same principles need to be maintained in new election systems.

**Q:** As someone without a strong technical background, why should I have to rely on a bunch of computer scientists to tell me whether I can trust my elections?

**A:** Maybe you shouldn't (however, the statement at least insists that there should be enough disclosure so that a technical person you trust can review the scheme and tell you what he or she thinks about it). If you have non-technical concerns about internet voting, this would be a good time to speak up. As the statement notes, we are NOT saying that the decision whether to use internet voting is a purely technical decision -- just that it needs to be a technically INFORMED decision. The technical challenges of internet voting are currently being minimized, often by people who simply don't understand them.

We're calling for an in-depth, public debate on the technical and NON-TECHNICAL issues in internet voting before adopting it. It's very possible that a technically sound internet voting scheme could be rejected for non-technical reasons, including other issues such as whether internet voting might disenfranchise legal voters who cannot easily access the internet.

**Q:** Isn't this statement at odds with the position of some of the people involved that only "voter verified paper ballots" should be used in elections?



**A:** The statement is a floor, not a ceiling. Endorsing it is definitely NOT an endorsement of internet voting or voting that uses electronic ballots. It says that internet voting should NOT be deployed unless certain minimum conditions -- with which we believe most technologists would agree -- are met. It does not imply the internet voting or electronic ballots can be used safely, or ever should be used.

**Q:** Why doesn't the statement demand (my favorite requirement)?

**A:** The statement is focused on the technical problems of internet voting, and sets out minimal conditions that represent a consensus of those endorsing it. The decision about whether or not internet voting should be used depends on many issues, including whether it has (your favorite requirement).

The main goal of the statement is to prevent deployment of internet voting without due consideration of the risks. It also calls for the ability of the general public to participate in the decision of whether or not to use internet voting -- including you, should you choose to argue for (your favorite requirement).

**Q:** Why “internet” and not “Internet”?

**A:** The early endorsers who objected to my earlier capitalization of “internet” were more passionate and spoke earlier than those who objected to spelling it in lower-case. Also, see <http://www.wired.com/culture/lifestyle/news/2004/08/64596>



# The Uniformed and Overseas Citizens Absentee Voting Act: Overview and Issues

**Kevin J. Coleman**  
Analyst in Elections

November 4, 2009

**Congressional Research Service**

7-5700

[www.crs.gov](http://www.crs.gov)

RS20764

## Summary

Members of the military and U.S. citizens who live abroad are eligible to register and vote absentee in federal elections under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986. The law was enacted to improve absentee registration and voting for this group of voters and to consolidate existing laws. Since 1942, a number of federal laws have been enacted to assist these voters: the Soldier Voting Act of 1942 (amended in 1944), the Federal Voting Assistance Act of 1955, the Overseas Citizens Voting Rights Act of 1975 (both the 1955 and 1975 laws were amended in 1978 to improve procedures), and the Uniformed and Overseas Citizens Absentee Voting Act of 1986. The law is administered by the Secretary of Defense, who delegates that responsibility to the Director of the Federal Voting Assistance Program at the Department of Defense (DOD).

Improvements to UOCAVA (P.L. 99-410) were necessary as the result of controversy surrounding ballots received in Florida from military and overseas voters in the 2000 presidential election. The National Defense Authorization Act for FY2002 (P.L. 107-107; S. 1438) and the Help America Vote Act (P.L. 107-252; H.R. 3295) both included provisions concerning military and overseas voting. The President signed P.L. 107-107 on December 28, 2001, and P.L. 107-252 on October 29, 2002. The Defense Authorization Act for FY2005 (P.L. 108-375) amended UOCAVA as well, to ease the rules for use of the federal write-in ballot in place of state absentee ballots, and the Defense Authorization Act for FY2007 (P.L. 109-364) extended a DoD program to assist military and overseas voters.

In the 111<sup>th</sup> Congress, a major overhaul of UOCAVA was accomplished when the President signed the National Defense Authorization Act for FY2010 (P.L. 111-84) on October 28. It included an amendment (S.Amdt. 1764) that contained the provisions of S. 1415, the Military and Overseas Voter Empowerment Act. The Senate had approved the conference committee report (H.Rept. 111-288) on the defense authorization act (H.R. 2647) on October 22 and the House had done so on October 8. Also on the House side, the Committee on House Administration reported H.R. 2393, which would require the collection and express delivery of ballots from overseas military voters before the polls close on election day. A similar provision was included in the defense authorization act as enacted.

This report will be updated periodically to reflect new developments.

## **Contents**

Historical Overview .....	1
Summary of the Law .....	1
The Federal Voting Assistance Program.....	3
SERVE Internet Voting Program .....	4
Legislation .....	4
111 <sup>th</sup> Congress .....	4
110 <sup>th</sup> Congress .....	5
Current Issues and Developments.....	6

## **Contacts**

Author Contact Information .....	7
----------------------------------	---

## Historical Overview

Several federal laws have been enacted since 1942 to enable those in the military and U.S. citizens abroad to vote in federal elections. The original law, the Soldier Voting Act of 1942 (P.L. 712-561), was enacted to guarantee federal voting rights for members of the armed forces during wartime. The law allowed members of the armed forces to vote for presidential electors, and candidates for the U.S. Senate and House, whether or not they were previously registered and regardless of poll tax requirements. The law provided for the use of a postage-free, federal post card application to request an absentee ballot; it also instructed secretaries of state to prepare an appropriate number of “official war ballots,” which listed federal office candidates, as well as candidates for state and local office if authorized by the state legislature. The law “had almost no impact at all” as it was enacted on September 16, only weeks before the November general election.<sup>1</sup>

Congressional authority to regulate state voting procedures expired once the war ended, as the law noted that its provisions applied “in time of war.”<sup>2</sup> The Soldier Voting Act of 1942 was amended in 1944. Under congressional war powers, the 1942 law *mandated* procedures for the states to permit service members to vote, but the amended law of 1944 *recommended* that states follow such procedures. The law was amended again in 1946 to include technical changes.

In 1951, President Truman asked the American Political Science Association (APSA) to study the military voting problem and make recommendations. APSA completed its study in 1952 and the President endorsed the association’s legislative recommendations, which were sent to Congress. The Federal Voting Assistance Act was subsequently enacted in 1955; it recommended, but did not guarantee, absentee registration and voting for members of the military, federal employees who lived outside the United States, and members of civilian service organizations affiliated with the armed forces. The law was amended in 1968 to include a more general provision for U.S. citizens temporarily residing outside the United States, expanding the number of civilians covered under the law. The Overseas Citizens Voting Rights Act of 1975 guaranteed absentee registration and voting rights for citizens outside the United States, whether or not they maintained a U.S. residence or address and their intention to return was uncertain.

## Summary of the Law

The current law, the Uniformed and Overseas Citizens Absentee Voting Act (P.L. 99-410), was signed into law by President Reagan on August 28, 1986.<sup>3</sup> It was amended in 2002 by the Help America Vote Act (P.L. 107-252), the National Defense Authorization Act of 2002 (P.L. 107-107), the Defense Authorization Act for FY2005 (P.L. 108-375), and the Defense Authorization Act for FY2007 (P.L. 109-364). The main provisions of the law require states to do the following:

- Permit absent uniformed services voters, their spouses and dependents, and overseas voters who no longer maintain a residence in the United States to

---

<sup>1</sup> U.S. Department of Defense, *The Federal Voting Assistance Program*, 11<sup>th</sup> Report (Washington: December 1977), p. 2.

<sup>2</sup> P.L. 56-393, Sec. 1.

<sup>3</sup> 42 U.S.C. §1973ff-ff-6.

register absentee (overseas voters are eligible to register absentee in the jurisdiction of their last residence) and to vote by absentee ballot in all elections for federal office (including general, primary, special, and runoff elections).<sup>4</sup> The National Defense Authorization Act of 2002 amended UOCAVA to permit a voter to submit a single absentee application in order to receive an absentee ballot for each federal election in the state during the year. The Help America Vote Act subsequently amended that section of the law to extend the period covered by a single absentee ballot application to the next two regularly scheduled general elections for federal office. The Help America Vote Act also added a new section that prohibits a state from refusing to accept a valid voter registration application on the grounds that it was submitted prior to the first date on which the state processes applications for the year.<sup>5</sup>

- Accept and process any valid voter registration application from an absent uniformed services voter or overseas voter if the application is received not less than 30 days before the election. The Help America Vote Act amended that section of the law to require a state to provide to a voter the reasons for rejecting a registration application or an absentee ballot request.<sup>6</sup>
- Furthermore, the law recommends that states accept the federal write-in absentee ballot for general elections for federal office (provided the voter is registered, has made a timely request for a state absentee ballot, the absentee ballot has not arrived with sufficient time to return it, and the ballot is submitted from outside the United States or its territories).<sup>7</sup>
- The law also stipulates that voting materials be carried “expeditiously and free of postage.”<sup>8</sup> It recommends that states accept the Federal Post Card Application (FPCA) from uniformed services voters, their spouses and dependents, and overseas voters to allow for simultaneous absentee registration and to request an absentee ballot. While all states and territories accept the FPCA, some require that a voter submit the state registration form separately in order to be permanently registered. Other recommendations in the law suggest that states:<sup>9</sup>
  - waive registration requirements for military and overseas voters who do not have an opportunity to register because of service or residence;
  - send registration materials, along with an absentee ballot to be returned simultaneously, if the FPCA is not sufficient for absentee registration;

---

<sup>4</sup> Sec. 107 (1). An absent uniformed services voter is defined as follows: a member of a uniformed service on active duty or a member of the merchant marine who, by reason of such active duty or service in the merchant marine, is absent from the place of residence where the member is otherwise qualified to vote; and a spouse or dependent of a member of a uniformed service or a member of the merchant marine who is absent from his or her place of residence where he or she is otherwise qualified to vote, because of the active duty or service of the member.

<sup>5</sup> 42 U.S.C. §1973ff-1(1), as amended by section 1606 (b) of the National Defense Authorization Act of 2002, and subsequently, by section 704 of the Help America Vote Act of 2002.

<sup>6</sup> 42 U.S.C. §1973ff-1(2), as amended by section 707 of the Help America Vote Act of 2002.

<sup>7</sup> 42 U.S.C. §1973ff-1(3).

<sup>8</sup> The United States Postal Service domestic mail manual notes that “To be mailable without prepayment of postage, the balloting materials must be deposited at a U.S. post office, an overseas U.S. military post office, or an American Embassy or American Consulate.”

<sup>9</sup> 42 U.S.C. §1973ff-3.

- expedite the processing of voting materials;
- permit any required oath to be administered by a commissioned officer in the military or by any official authorized to administer oaths under federal law or the law of the state where the oath is administered;
- assure mailing absentee ballots to military and overseas voters at the earliest opportunity; and
- provide for late registration for persons recently separated from the military.

In addition to the amendments to UOCAVA mentioned above, the Help America Vote Act of 2002 does the following:

- requires the Secretary of Defense to establish procedures to provide time and resources for voting action officers to perform voting assistance duties; establish procedures to ensure a postmark or proof of mailing date on absentee ballots; requires secretaries of the armed forces to notify members of the last day for which ballots mailed at the facility can be expected to reach state or local officials in a timely fashion; requires that members of the military and their dependents have access to information on registration and voting requirements and deadlines; and requires that each person who enlists receives the national voter registration form;
- amends UOCAVA to require each state to designate a single office to provide information to all absent uniformed services voters and overseas voters who wish to register in the state;
- amends UOCAVA to require states to report the number of ballots sent to uniformed services and overseas voters and the number returned and cast in the election; and
- amends UOCAVA to require the Secretary of Defense to ensure that state officials are aware of the requirements of the law and to prescribe a standard oath for voting materials to be used in states that require such an oath.

The Defense Authorization Act for FY2002 also included provisions that (1) required an annual review of the voting assistance program and a report to Congress; (2) guaranteed state residency for military personnel who are absent because of military duty; (3) continued the online voting pilot project begun for the 2000 elections; and (4) permitted the use of DOD facilities as polling places if they had previously been used for that purpose since 1996 or were designated for use by December 2000.

## **The Federal Voting Assistance Program**

The Federal Voting Assistance Act of 1955 called for the President to designate the head of an executive department to be responsible for and coordinate the federal functions described in the law. President Eisenhower designated the Secretary of Defense, who delegated the responsibility to the Assistant Secretary of Defense for Public Affairs, as coordinator of the Federal Voting Assistance Program (FVAP). Under the current law, the Director of the Federal Voting Assistance Program administers the FVAP for citizens covered by the Uniformed and Overseas Citizens Absentee Voting Act. This office publishes the *Voting Assistance Guide*, a compilation of state

requirements and practices with respect to the federal law (including information on possible tax liability incurred in some states based on residence, as determined by voter registration). The FVAP office also maintains a toll free phone number to provide assistance to voters and to military and federal government personnel who are responsible for implementing the law; the office also maintains a website <http://www.fvap.gov>.

## **SERVE Internet Voting Program**

The FVAP administered an experimental internet voting program, the Secure Electronic Registration and Voting Experiment (SERVE), for military and overseas citizens in the November 2000 election. Those eligible to cast ballots via the Internet were voters whose legal residence was in one of fourteen participating counties in Florida, South Carolina, Texas, and Utah. The pilot project was limited to a total of 350 voters, of whom 84 cast absentee ballots over the Internet. The FVAP issued a June 2001 report evaluating the program. An expanded version was in place in seven states for the 2004 elections, but it was cancelled after a report reviewing the program raised Internet security concerns. Among other conclusions, the report noted that because fundamental vulnerabilities exist with Internet voting, a successful cyber attack on the SERVE program could undermine the November election.<sup>10</sup>

## **Legislation**

### **111<sup>th</sup> Congress**

A number of bills that focus specifically on military and overseas voting have been introduced in the 111<sup>th</sup> Congress. The Senate Rules Committee reported S. 1415, as amended, on July 15. The text of the bill was subsequently added as an amendment to the National Defense Authorization Act for Fiscal Year 2010 (H.R. 2647), which was passed by the Senate on July 23. The House voted in favor of the conference report to the bill (H.Rept. 111-288) on October 8 and the Senate approved it on October 22; President Obama signed the bill on October 28 (P.L. 111-84). It establishes procedures for the use of email and facsimile transmittal for registration and absentee ballot applications, establishes procedures for the collection of marked absentee ballots from overseas uniformed services voters for delivery to the appropriate state election officials, and establishes additional procedures and requirements to improve UOCAVA voting. The House Administration Committee also reported H.R. 2393, the Military Voting Protection Act, on June 10, 2009. The bill would require the Secretary of Defense to establish procedures for the collection of marked absentee ballots from overseas uniformed services voters for delivery to the appropriate state election officials.

Both the Senate Rules and Administration and House Administration Committees had previously held hearings on UOCAVA voting. The hearings were convened on May 13 in the Senate and May 21 in the House.<sup>11</sup> Among the bills introduced thus far in the 111<sup>th</sup> Congress are two sponsored by Representative Maloney, H.R. 1659 and H.R. 1739. The first would amend

---

<sup>10</sup> The report may be found at <http://www.servesecurityreport.org/>.

<sup>11</sup> An archived version of the webcast for the Senate hearing can be found at [http://rules.senate.gov/public/index.cfm?FuseAction=CommitteeSchedule.Hearing&Hearing\\_id=4bbeb7a-f4b9-487b-a1e6-47065a293ccf](http://rules.senate.gov/public/index.cfm?FuseAction=CommitteeSchedule.Hearing&Hearing_id=4bbeb7a-f4b9-487b-a1e6-47065a293ccf); an archived version of the House hearing webcast can be found here: [http://cha.house.gov/view\\_hearing.aspx?r=50](http://cha.house.gov/view_hearing.aspx?r=50).



UOCAVA to require that the presidential designee have experience in election administration that includes oversight of voter registration and absentee ballot distribution and it would establish an Overseas Voting Advisory Board. H.R. 1739 is a more far-reaching proposal that would amend UOCAVA to make a series of adjustments concerning balloting materials and related election administration procedures in the states, and would establish a grant program for voter outreach. H.R. 2082 (Holt) would amend UOCAVA to require states to accept ballots submitted by overseas voters using a provider of express mail service, so long as the ballot was submitted the day before, and received within 10 days after, the election. The bill would also require the presidential designee to reimburse the voter for the express mail cost. As noted above, H.R. 2393 (McCarthy), would amend UOCAVA to require the presidential designee to collect marked general election ballots from overseas uniformed services voters for delivery to the appropriate election officials before the polls close, using U.S. Postal Service express mail delivery. The bill would also require a tracking system so the voter could determine whether the ballot was delivered. It was reported by the House Administration Committee on June 10. A companion measure, S. 1026 (Cornyn), was introduced in the Senate.

## **110<sup>th</sup> Congress**

Several relevant election reform bills were introduced in the 110<sup>th</sup> Congress and two received action. On October 1, the Senate passed S. 3073 (Cornyn), which would have required the Secretary of Defense to collect ballots from overseas military voters and ensure their delivery to election officials using express mail services. On the House side, H.R. 6625 was passed on September 17; it would have allowed state election officials to designate facilities of the Department of Veterans Affairs as voter registration agencies under the National Voter Registration Act (P.L. 103-31, the “motor-voter” law). Other bills that were not acted on included H.R. 2835, H.R. 4173, H.R. 4237, H.R. 5673, and S. 1487. H.R. 2835 (Faleomavaega) would have extended UOCAVA law’s provisions to cover legislative and gubernatorial elections in American Samoa. H.R. 4173 (Honda) would have prohibited states from requiring notarization of absentee ballots, broadened the use of the federal write-in ballot, established a grant program to inform overseas citizens about absentee voting, and required that overseas federal employees be informed about UOCAVA and information about the law included in U.S. passports. H.R. 4237 (Maloney) would have prohibited states from refusing to accept registration or ballot applications because they do not meet nonessential requirements, clarified postage markings on balloting materials, and would have amended the law concerning individuals who never lived in the United States, notification of the rejection of registration or ballot applications, and the use of the diplomatic pouch to transmit absentee ballots. H.R. 5673 (McCarthy) would have required the Secretary of Defense to collect marked absentee ballots from overseas uniformed services voters and to guarantee their delivery to the appropriate election officials before the polls close. The bill would also have encouraged the use of private providers of air transportation to deliver ballots, which would allow individual voters to track the progress of their voted ballot. S. 1487 (Feinstein) would have prohibited states from refusing to accept registration or ballot applications because they do not meet nonessential requirements and would have permitted accepting a federal write-in ballot from an overseas voter if it is submitted from a location in the United States. No action was taken on any of these measures.

## Current Issues and Developments

The Overseas Vote Foundation published a report in February 2009 based on survey responses from approximately 24,000 UOCAVA voters and 1,000 local election officials. The report noted that there is “some evidence of overall progress” with respect to voting under UOCAVA, but that “progress is uneven, and the surveys point to numerous areas ripe for reform.”<sup>12</sup> For example, one in four respondents did not receive their requested absentee ballot; 8% of these voters used the federal write-in absentee ballot to vote, but 14% did not participate in the election (not all voters are aware that they may use the federal write-in ballot if they have requested a regular state ballot that does not arrive). Furthermore, more than half (52%) of those who tried to vote but failed to do so either received a late ballot or never received one at all.<sup>13</sup>

The Pew Center on the States issued a January 2009 report that examined the variety of state practices that can make casting a ballot difficult for UOCAVA voters and made recommendations for improving the voting process.<sup>14</sup> Among its findings, the report noted that “25 states and Washington, D.C., need to improve their absentee balloting rules for military voters abroad,” and “the other 25 states would better serve these voters by giving them additional time to request and return their ballots as well.”<sup>15</sup> The report recommended eliminating notarization requirements, expanding electronic transmission of election materials, expanding the use of the federal blank ballot if a regular ballot does not arrive in time, and providing for a period of at least 45 days to receive and return a ballot.

In October 2007, the Overseas Vote Foundation (OVF) launched a website to assist UOCAVA voters by providing a means to electronically register and request a ballot.<sup>16</sup> The OVF, a nonpartisan, non-governmental entity, offers the necessary information to complete the application process for each of the states, including a database of local election officials to whom the applications must be delivered.

Reports on military and overseas voting in the 2006 election highlighted continuing challenges faced by these voters, despite the efforts of the past several years to improve voting rates. The GAO issued an evaluation of federal efforts to facilitate electronic absentee voting in June 2007<sup>17</sup> and the EAC reported in September 2007 the results of its survey of military and overseas voters after the 2006 election.<sup>18</sup> According to the EAC report, 33% of ballots requested by these voters were cast or counted in the election; of those that were not counted, nearly 70% were returned to election officials as undeliverable. GAO estimated that there were six million UOCAVA voters

---

<sup>12</sup> The Overseas Vote Foundation, 2008 OVF Post Election UOCAVA Survey Report and Analysis: A Detailed Look at How Overseas and Military Voters and Election Officials Fared in the 2008 General Election and What To Do About It, February 2009; it may be found at [https://www.overseasvotefoundation.org/files/OVF\\_2009\\_PostElectionSurvey\\_Report.pdf](https://www.overseasvotefoundation.org/files/OVF_2009_PostElectionSurvey_Report.pdf).

<sup>13</sup> *Ibid.*, p. 5.

<sup>14</sup> The Pew Center on the States, *No Time to Vote: Challenges Facing America's Overseas Military Voters*, January, 2009; the report may be found at [http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Election\\_reform/NTTV\\_Report\\_Web.pdf](http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Election_reform/NTTV_Report_Web.pdf).

<sup>15</sup> *Ibid.*

<sup>16</sup> The OVF website can be found at <https://www.overseasvotefoundation.org/overseas/home.htm>.

<sup>17</sup> The GAO report may be found at <http://www.gao.gov/new.items/d07774.pdf>.

<sup>18</sup> The EAC report may be found at <http://www.eac.gov/clearinghouse/2006-uniformed-and-overseas-citizens-voting-act-survey-and-conference-materials/>.

and its report outlined a series of recommendations to DoD (the FVAP) and the EAC for electronic solutions to overcome the obstacles posed by time and distance.

The Defense Authorization Act for FY2007, signed into law on October 17, 2006, as P.L. 109-364, included a number of provisions on military and overseas voting. It continued the Integrated Voting Assistance System (IVAS) for military voters and employees of the Department of Defense through the 2006 elections and required reports from the Comptroller General on IVAS and other efforts to utilize electronic mail, facsimile transmission, and the Internet to facilitate registration and voting. The Government Accountability Office (GAO) issued a report in September 2006, which noted that two major challenges remained with respect to (1) simplifying and standardizing absentee voting across the states, and (2) developing a secure electronic registration and voting system.<sup>19</sup>

## **Author Contact Information**

Kevin J. Coleman  
Analyst in Elections  
kcoleman@crs.loc.gov, 7-7878

---

<sup>19</sup> The GAO report can be found at <http://www.gao.gov/htext/d061134t.html>.

# Testimony of Ellen Theisen on H.B.1624, February 6, 2009

The National Institute of Standards and Technology (NIST), the U.S. Government Accountability Office, and dozens of professional computer security experts warn that the safe use of the Internet for voting is essentially impossible, given the technology available today.

- ◆ **In 2004, a panel of experts commissioned by the U.S. Department of Defense** concluded that it was not possible to ensure the privacy, security, or accuracy of votes cast over the Internet with its current architecture. They said the attempt to provide secure, all-electronic Internet voting was “an essentially impossible task.”<sup>1</sup>
- ◆ **In 2007, the U.S. Government Accountability Office (GAO)** found that email and Internet voting is “more vulnerable to privacy and security compromises than the conventional methods now in use” and that “available safeguards may not adequately reduce the risks of compromise.”<sup>2</sup>
- ◆ **In 2008, the National Institute of Standards and Technology (NIST)** wrote, “Technology that is widely deployed today is not able to mitigate many of the threats to casting ballots via the web.”<sup>3</sup>
- ◆ **In 2008, thirty leading computer science experts and professors at major universities** signed a statement asserting that until “serious, potentially insurmountable, technical challenges” are overcome, permitting the Internet to be used for public elections “is an extraordinary and unnecessary risk to democracy.”<sup>4</sup>

In their 2004 report, the panel of experts commissioned by the Department of Defense to evaluate the DoD’s Internet voting project addressed a commonly asked question in the section entitled “Why security for Internet voting is far more difficult than for e-Commerce.” They said:

Many people mistakenly assume that since they can safely conduct commercial transactions over the Internet, that they also can safely vote over the Internet. First, they usually underestimate the hazards of online financial transactions, and are unaware of many of the risks they take even if they are careful to deal only with “secure” web sites through the SSL protocol. But they also assume that voting is comparable somehow to an online financial transaction, whereas in fact security for Internet voting is far more difficult than security for e-commerce. There are three reasons for this: the high stakes, the inability to recover from failures, and important structural differences between the requirements for elections and e-commerce.

---

<sup>1</sup> “A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE).” January 20, 2004. By Dr. David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, Dr. David Wagner.  
<http://www.servesecurityreport.org/>

<sup>2</sup> “Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens,” June 2007, p. 30. [GAO Report 07-774]  
<http://www.gao.gov/new.items/d07774.pdf>

<sup>3</sup> “A Threat Analysis on UOCAVA Voting Systems.” [NISTIR 7551] <http://vote.nist.gov/uocava-threatanalysis-final.pdf>

<sup>4</sup> “Computer Technologists’ statement on internet voting.” September 11th, 2008.  
<http://www.verifiedvoting.org/article.php?id=5867>

They explain the structural differences these three reasons require, and they conclude.

There are no such requirements for e-commerce systems. In general, designing an Internet voting system that can detect and correct any kind of vote fraud, without issuing voters receipts for how they voted, and without risking vote privacy by associating voters with their votes, is a deep and complex security problem that has no analog in the e-commerce world. For these reasons, the existence of technology to provide adequate security for Internet commerce does not imply that Internet voting can be made safe.

The NIST report provides a detailed list of threat to the various types of electronic and Internet voting, assessing the aspect of an election that is threatened, the risk level of each, and the difficulty level of threat. The report summarizes its threat analysis of the three electronic methods of transmitting election materials – fax, email, and Web-based Internet voting – and concludes that the threats to returning voted ballots by fax can be mitigated by proper procedures. But regarding the return of ballots via the Internet, NIST says,

“The security challenges associated with e-mail return of voted ballots are difficult to overcome using technology widely deployed today.” and

“Technology that is widely deployed today is not able to mitigate many of the threats to casting ballots via the web.”

In its suggested next steps, NIST says:

“The threat analysis documented in this paper identifies blank ballot distribution methods as a potential area to immediately improve UOCAVA voting without threatening the security of elections. Fax, e-mail and web-based systems could distribute blank ballots quickly and reliably to voters, significantly reducing the ballot delivery times faced by mailing ballots to voters and improving the UOCAVA voting experience for citizens overseas. In addition, registration and ballot requests can also take advantage of these distribution methods, but there are more threats when handling personal information from voters.”

A report from the Pew Center on the States, released last month found that Washington State was one of 25 states where military and overseas voters had time to vote. The Pew report points out that Washington State has already implemented the next steps that NIST suggests, and that the state already provides the 45 days transit time recommended by the DoD’s Federal Voting Assistance Program (FVAP). In other words, Washington State is already providing well for its UOCAVA voters, without taking the severe risks associated with returning voted ballots through the Internet.

**H.B. 1624 is a solution in search of a problem, and the solution it proposes would put at risk the privacy and votes of the very voters it is seeking to protect.**

It is important to point out that the federal government has not been able to protect its own networks from cyber attacks. The Department of Homeland Security spent \$6.6 billion dollars in 2008 on programs to secure the Internet networks of the Pentagon and other military computers, many of which house classified or sensitive information.<sup>5</sup>

---

<sup>5</sup> [http://www.dhs.gov:80/xnews/releases/pr\\_1207684277498.shtm](http://www.dhs.gov:80/xnews/releases/pr_1207684277498.shtm)

However in November 2008, a serious attack on the Pentagon was successful: <sup>6 7</sup>

The Pentagon has suffered from a cyber attack so alarming that it has taken the unprecedented step of banning the use of external hardware devices, such as flash drives and DVD's.

The attack came in the form of a global virus or worm that is spreading rapidly throughout a number of military networks.

A Navy rear admiral outside the Pentagon, in a briefing to his staff on Thursday, characterized the virus as a coordinated attack that was strategically timed to hit between the Nov. 4 presidential election and Inauguration Day, Jan. 20.

Furthermore, the federal Department of Defense has been unable to meet Congress's expectation "to establish a secure and private electronic and Internet-based UOCAVA voting environment."<sup>8</sup> The GAO report says that, "the DoD has not developed a secure, Internet-based absentee voting demonstration project, as Congress mandated in the Ronald W. Reagan NDAA [National Defense Authorization Act] for Fiscal Year 2005."<sup>9</sup>

It is unrealistic to expect the Washington Secretary of State - on the State's limited budget - to accomplish something the United States Department of Homeland Security and the Department of Defense have been unable to accomplish with their billion dollar budgets and under the mandate of Congress.

I urge the legislature to take NIST's suggestion regarding the return of voted ballots via the Internet:

"Voted ballot return remains a more difficult issue to address, however emerging trends and developments in this area should continue to be studied and monitored."

Alter H.B. 1624 to authorize the Secretary of State to form a task force of qualified computer security experts to study and monitor developments in Internet security.

The intent of Congress in passing UOCAVA was that:

"all eligible American voters, regardless of race, ethnicity, disability, the language they speak, or the resources of the community in which they live, should have an equal opportunity to cast a vote and to have that vote counted."<sup>10</sup>

It is unfair to our military and overseas voters to offer them a means of voting that presents such a severe threat to the privacy and integrity of their ballots that NIST, the GAO, and computer security professionals across the country are warning against it. I urge you to defeat this seriously defective bill.

Ellen Theisen  
660 Jefferson Ave.  
Port Ludlow, WA 08365  
360-437-9922

---

<sup>6</sup> "Pentagon Hit by Unprecedented Cyber Attack." FOXNews.com. November 20, 2008.

<http://www.foxnews.com/politics/2008/11/20/pentagon-cyber-siege-unprecedented-attack/>

<sup>7</sup> "Military Looking Abroad for Source of Cyber Attack on Pentagon." FOXNews.com. November 21, 2008.

<http://www.foxnews.com/politics/2008/11/21/source-cyber-attack-pentagon-come-china/>

<sup>8</sup> GAO Report 07-774, page 31 (pdf page 35) <http://www.gao.gov/new.items/d07774.pdf>

<sup>9</sup> GAO Report 07-774, page 27 (pdf page 31)

<sup>10</sup> [http://www.usdoj.gov/crt/voting/42usc/subch\\_ig.php](http://www.usdoj.gov/crt/voting/42usc/subch_ig.php)



## Hackers attacked Colombian vote count

Wed Mar 17, 12:04 PM

BOGOTA (AFP) - Unidentified hackers struck the computerized system used to transmit voting data in Colombia's legislative elections, disrupting the vote count, the private contractor responsible for the system charged Wednesday.

Ivan Ribon, spokesman for Arolen, a company hired to transmit results of Sunday's voting over the Internet, told local media Wednesday that hackers struck at the moment polls closed at 2100 GMT.

"Early reviews show that there were 75,000 hits a second, which does not happen even on the busiest sites in the world," Ribon told RCN radio.

"That went on all night Sunday into Monday, which forced us ... in order to safeguard the integrity and confidentiality of the data, to downgrade service on Internet results," he explained.

Three days after the polls, final results still have not been released.

The National Electoral Board has blamed companies contracted to assist in releasing results. The companies have claimed there were problems with some results gathering at some polling stations.

President Alvaro Uribe has complained that while the armed forces risk their lives to protect Colombia's democracy, the electoral board has "serious" trouble simply reporting on it.

Conservatives were on track to keep their majority in Colombia's congress, early results showed Monday, as US ally Uribe's government complained the count's slow pace undercut the vote's credibility.

---

Copyright © 2010 Agence France Presse. All rights reserved. The information contained in the AFP News report may not be published, broadcast, rewritten or redistributed without the prior written authority of Agence France Presse.

Copyright © 2010 Yahoo! Canada Co. All Rights Reserved. [Privacy Policy](#) - [Terms of Service](#)

[Community Guidelines](#) - [Privacy Guidelines](#)

Need [help](#)? Want to send [feedback](#)?

.



1 of 1 DOCUMENT

Copyright 2008 Los Angeles Times  
All Rights Reserved  
Los Angeles Times

November 28, 2008 Friday  
Home Edition

**SECTION:** MAIN NEWS; National Desk; Part A; Pg. 1

**LENGTH:** 1021 words

**HEADLINE:** Pentagon computer networks attacked;  
The cyber-strike on key sites is thought to be from inside Russia.

**BYLINE:** Julian E. Barnes, Barnes is a writer in our Washington bureau.

**DATELINE:** WASHINGTON

**BODY:**

Senior military leaders took the exceptional step of briefing President Bush this week on a severe and widespread electronic attack on Defense Department computers that may have originated in Russia -- an incursion that posed unusual concern among commanders and raised potential implications for national security.

Defense officials would not describe the extent of damage inflicted on military networks. But they said that the attack struck hard at networks within U.S. Central Command, the headquarters that oversees U.S. involvement in Iraq and Afghanistan, and affected computers in combat zones. The attack also penetrated at least one highly protected classified network.

Military computers are regularly beset by outside hackers, computer viruses and worms. But defense officials said the most recent attack involved an intrusive piece of malicious software, or "malware," apparently designed specifically to target military networks.

"This one was significant; this one got our attention," said one defense official, speaking on condition of anonymity when discussing internal assessments.

Although officials are withholding many details, the attack underscores the increasing danger and potential significance of computer warfare, which defense experts say could one day be used by combatants to undermine even a militarily superior adversary.

Bush was briefed on the threat by Navy Adm. Michael G. Mullen, chairman of the Joint Chiefs of Staff. Mullen also briefed Defense Secretary Robert M. Gates.

Military electronics experts have not pinpointed the source or motive of the attack and could not say whether the destructive program was created by an individual hacker or whether the Russian government may have had some involvement. Defense experts may never be able to answer such questions, officials said.

The defense official said the military also had not learned whether the software's designers may have been specifically targeting computers used by troops in Afghanistan and Iraq.



Pentagon computer networks attacked; The cyber-strike on key sites is thought to be from inside Russia. Los Angeles Times November 28, 2008 Friday

However, suspicions of Russian involvement come at an especially delicate time because of sagging relations between Washington and Moscow and growing tension over U.S. plans to develop a missile defense system in Eastern Europe. The two governments also have traded charges of regional meddling after U.S. support for democratic elections in former Soviet states and recent Russian overtures in Latin America.

U.S. officials have worried in recent years about the possibility of cyber-attacks from other countries, especially China and Russia, whether sponsored by governments of those countries or launched by individual computer experts.

An electronic attack from Russia shut down government computers in Estonia in 2007. And officials believe that a series of electronic attacks were launched against Georgia at the same time that hostilities erupted between Moscow and Tbilisi last summer. Russia has denied official involvement in the Georgia attacks.

The first indication that the Pentagon was dealing with a computer problem came last week, when officials banned the use of external computer flash drives. At the time, officials did not indicate the extent of the attack or the fact that it may have targeted defense systems or posed national security concerns.

The invasive software, known as agent.btz, has circulated among nongovernmental U.S. computers for months. But only recently has it affected the Pentagon's networks. It is not clear whether the version responsible for the cyber-intrusion of classified networks is the same as the one affecting other computer systems.

The malware is able to spread to any flash drive plugged into an infected computer. The risk of spreading the malware to other networks prompted the military to ban the drives.

Defense officials acknowledged that the worldwide ban on external drives was a drastic move. Flash drives are used constantly in Iraq and Afghanistan, and many officers keep them loaded with crucial information on lanyards around their necks.

Banning their use made sharing information in the war theaters more difficult and reflected the severity of the intrusion and the threat from agent.btz, a second official said.

Officials would not describe the exact threat from agent.btz, or say whether it could shut down computers or steal information. Some computer experts have reported that agent.btz can allow an attacker to take control of a computer remotely and to take files and other information from it.

In response to the attack, the U.S. Strategic Command, which oversees the military's cyberspace defenses, has raised the security level for its so-called information operations condition, or "INFOCON," initiating enhanced security measures on military networks.

The growing possibility of future electronic conflicts has touched off debates among U.S. defense experts over how to train and utilize American computer warfare specialists. Some have advocated creating offensive capabilities, allowing the U.S. to develop the ability to intrude into the networks of other countries.

But most top leaders believe the U.S. emphasis in cyberspace should be on improving defenses and gathering intelligence, particularly about potential threats.

On Tuesday, Gen. Norton A. Schwartz, Air Force chief of staff, received a specialized briefing about the malware attack. Officers from the Air Force Network Operations Center at Barksdale Air Force Base in Louisiana outlined their efforts to halt the spread of the malware and to protect military computers from further attack.

Schwartz, praising those efforts, said that the attack and the military's response were being closely monitored by senior military leaders.

The offending program has been cleansed from a number of military networks. But officials said they did not believe they had removed every bit of infection from all Defense Department computers.

"There are lots of people working hard to remove the threat and put in preventive measures to protect the grid," said the defense official. "We have taken a number of corrective measures, but I would be overstating it if I said we were through this."

--

julian.barnes@latimes.com

Pentagon computer networks attacked; The cyber-strike on key sites is thought to be from inside Russia. Los Angeles Times November 28, 2008 Friday

**LOAD-DATE:** November 28, 2008

 Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit [www.djreprints.com](http://www.djreprints.com)

[See a sample reprint in PDF format.](#) [Order a reprint of this article now](#)

**THE WALL STREET JOURNAL**  
WSJ.com

• TECHNOLOGY

| • NOVEMBER 19, 2009

## FBI Suspects Terrorists Are Exploring Cyber Attacks

By [SIOBHAN GORMAN](#)

The Federal Bureau of Investigation is looking at people with suspected links to al Qaeda who have shown an interest in mounting an attack on computer systems that control critical U.S. infrastructure, a senior official told Congress Tuesday.

While there is no evidence that terrorist groups have developed sophisticated cyber-attack capabilities, a lack of security protections in U.S. computer software increases the likelihood that terrorists could execute attacks in the future, the official warned.

If terrorists were to amass such capabilities, they would be wielded with "destructive and deadly intent," Steven Chabinsky, deputy assistant director of the FBI's Cyber Division, told the Senate Judiciary Committee Tuesday.

"The FBI is aware of and investigating individuals who are affiliated with or sympathetic to al Qaeda who have recognized and discussed the vulnerabilities of the U.S. infrastructure to cyber-attack," Mr. Chabinsky told the committee, without providing details.

Such infrastructure could include power grids and transportation systems.

The control systems of U.S. infrastructure as well as money transfers are now connected directly or indirectly to the Internet. Hackers have been able to penetrate computer systems running components of the U.S. electric grid as well as divert bank transfers.

In an interview Tuesday, former Homeland Security Secretary Michael Chertoff said al Qaeda already has some cyber-attack capability. "I don't think they're the most capable in the world, but they have some capability," he said.

Mr. Chertoff said he expects al Qaeda to develop more cyber-attack skills that would allow them to attack infrastructure that is less well protected, perhaps in the transportation and energy sectors. "It's only a matter of time," he said. "They're getting the capability to do some damage."

These descriptions reinforced concerns that former Director of National Intelligence Mike McConnell raised publicly last month about the potential for a terrorist attack on the computer systems and data underpinning the U.S. financial sector.

"I am worried about some terrorist group [with] the capability to destroy the U.S. money supply," Mr. McConnell said. The impact of such an attack would be "an order of magnitude greater" than the Sept. 11 terrorist attacks, he said.

At the Senate hearing, officials from the Homeland Security and Justice departments also told the panel that the country isn't fully prepared for a cyber-attack and current laws don't provide an adequate framework for the government to fend off such attacks.

"We do need to step up our defensive game," said Philip Reitinger, a Homeland Security deputy undersecretary in charge of cybersecurity. He said U.S. systems are attacked every day by criminals and other adversaries who steal money to fund terrorist or criminal activities, as well as valuable information.

Among the chief areas of concern, Mr. Reitinger said, are vulnerabilities introduced when components of technology systems aren't properly vetted for security gaps before they are assembled into larger systems.

Officials also hinted at an internal battle brewing over whether laws that govern technology and surveillance need to be changed to better fend off cyber-attacks.

Associate Attorney General James Baker said the laws are not adequate, when pressed by Sen. Sheldon Whitehouse, a Rhode Island Democrat.

"We are definitely debating these kinds of issues inside the administration," Mr. Baker added.


Separately, the computer antivirus company [McAfee Inc.](#) issued a report by Paul Kurtz, who led the cyber-security review for the Obama transition team. He concluded that some cyber-attacks in 2007, including Israeli cyber-attacks on Syria and U.S. cyber-weapons employed in Iraq, constitute cyber-warfare.

The report is the first attempt to spell out characteristics of cyber-warfare and analyze how different attacks measure up.

**Write to** [Siobhan Gorman](#) at [siobhan.gorman@wsj.com](mailto:siobhan.gorman@wsj.com)

Printed in The Wall Street Journal, page A9

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit [www.djreprints.com](http://www.djreprints.com)

 **Most Liked on Facebook**



1 of 2 DOCUMENTS

Copyright 2010 The New York Times Company  
The New York Times

April 20, 2010 Tuesday  
Late Edition - Final

**SECTION:** Section A; Column 0; Foreign Desk; Pg. 1

**LENGTH:** 1150 words

**HEADLINE:** Hackers Said to Breach Google Password System

**BYLINE:** By JOHN MARKOFF

**BODY:**

Ever since Google disclosed in January that Internet intruders had stolen information from its computers, the exact nature and extent of the theft has been a closely guarded company secret. But a person with direct knowledge of the investigation now says that the losses included one of Google's crown jewels, a password system that controls access by millions of users worldwide to almost all of the company's Web services, including e-mail and business applications.

The program, code named Gaia for the Greek goddess of the earth, was attacked in a lightning raid taking less than two days last December, the person said. Described publicly only once at a technical conference four years ago, the software is intended to enable users and employees to sign in with their password just once to operate a range of services.

The intruders do not appear to have stolen passwords of Gmail users, and the company quickly started making significant changes to the security of its networks after the intrusions. But the theft leaves open the possibility, however faint, that the intruders may find weaknesses that Google might not even be aware of, independent computer experts said.

The new details seem likely to increase the debate about the security and privacy of vast computing systems such as Google's that now centralize the personal information of millions of individuals and businesses. Because vast amounts of digital information are stored in a cluster of computers, popularly referred to as "cloud" computing, a single breach can lead to disastrous losses.

The theft began with an instant message sent to a Google employee in China who was using Microsoft's Messenger program, according to the person with knowledge of the internal inquiry, who spoke on the condition that he not be identified.

By clicking on a link and connecting to a "poisoned" Web site, the employee inadvertently permitted the intruders to gain access to his (or her) personal computer and then to the computers of a critical group of software developers at Google's headquarters in Mountain View, Calif. Ultimately, the intruders were able to gain control of a software repository used by the development team.

The details surrounding the theft of the software have been a closely guarded secret by the company. Google first publicly disclosed the theft in a Jan. 12 posting on the company's Web site, which stated that the company was changing its policy toward China in the wake of the theft of unidentified "intellectual property" and the apparent compromise of the e-mail accounts of two human rights advocates in China.

## Hackers Said to Breach Google Password System The New York Times April 20, 2010 Tuesday

The accusations became a significant source of tension between the United States and China, leading Secretary of State Hillary Rodham Clinton to urge China to conduct a "transparent" inquiry into the attack. In March, after difficult discussions with the Chinese government, Google said it would move its mainland Chinese-language Web site and begin rerouting search queries to its Hong Kong-based site.

Company executives on Monday declined to comment about the new details of the case, saying they had dealt with the security issues raised by the theft of the company's intellectual property in their initial statement in January.

Google executives have also said privately that the company had been far more transparent about the intrusions than any of the more than two dozen other companies that were compromised, the vast majority of which have not acknowledged the attacks.

Google continues to use the Gaia system, now known as Single Sign-On. Hours after announcing the intrusions, Google said it would activate a new layer of encryption for Gmail service. The company also tightened the security of its data centers and further secured the communications links between its services and the computers of its users.

Several technical experts said that because Google had quickly learned of the theft of the software, it was unclear what the consequences of the theft had been. One of the most alarming possibilities is that the attackers might have intended to insert a Trojan horse -- a secret back door -- into the Gaia program and install it in dozens of Google's global data centers to establish clandestine entry points. But the independent security specialists emphasized that such an undertaking would have been remarkably difficult, particularly because Google's security specialists had been alerted to the theft of the program.

However, having access to the original programmer's instructions, or source code, could also provide technically skilled hackers with knowledge about subtle security vulnerabilities in the Gaia code that may have eluded Google's engineers.

"If you can get to the software repository where the bugs are housed before they are patched, that's the pot of gold at the end of the rainbow," said George Kurtz, chief technology officer for McAfee Inc., a software security company that was one of the companies that analyzed the illicit software used in the intrusions at Google and at other companies last year.

Rodney Joffe, a vice president at Neustar, a developer of Internet infrastructure services, said, "It's obviously a real issue if you can understand how the system works." Understanding the algorithms on which the software is based might be of great value to an attacker looking for weak points in the system, he said.

When Google first announced the thefts, the company said it had evidence that the intrusions had come from China. The attacks have been traced to computers at two campuses in China, but investigators acknowledged that the true origin may have been concealed, a quintessential problem of cyberattacks.

Several people involved in the investigation of break-ins at more than two dozen other technology firms said that while there were similarities between the attacks on the companies, there were also significant differences, like the use of different types of software in intrusions. At one high-profile Silicon Valley company, investigators found evidence of intrusions going back more than two years, according to the person involved in Google's inquiry.

In Google's case, the intruders seemed to have precise intelligence about the names of the Gaia software developers, and they first tried to access their work computers and then used a set of sophisticated techniques to gain access to the repositories where the source code for the program was stored.

They then transferred the stolen software to computers owned by Rackspace, a Texas company that offers Web-hosting services, which had no knowledge of the transaction. It is not known where the software was sent from there. The intruders had access to an internal Google corporate directory known as Moma, which holds information about the work activities of each Google employee, and they may have used it to find specific employees.

**URL:** <http://www.nytimes.com>

**LOAD-DATE:** April 20, 2010

## COVER STORY

Advertisement

# China's Cyber-Militia

**Chinese hackers pose a clear and present danger to U.S. government and private-sector computer networks and may be responsible for two major U.S. power blackouts.**

**Saturday, May 31, 2008**

**by Shane Harris**

Computer hackers in China, including those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of U.S. companies and government agencies, stolen proprietary information from American executives in advance of their business meetings in China, and, in a few cases, gained access to electric power plants in the United States, possibly triggering two recent and widespread blackouts in Florida and the Northeast, according to U.S. government officials and computer-security experts.

One prominent expert told *National Journal* he believes that China's People's Liberation Army played a role in the power outages. Tim Bennett, the former president of the Cyber Security Industry Alliance, a leading trade group, said that U.S. intelligence officials have told him that the PLA in 2003 gained access to a network that controlled electric power systems serving the northeastern United States. The intelligence officials said that forensic analysis had confirmed the source, Bennett said. "They said that, with confidence, it had been traced back to the PLA." These officials believe that the intrusion may have precipitated the largest blackout in North American history, which occurred in August of that year. A 9,300-square-mile area, touching Michigan, Ohio, New York, and parts of Canada, lost power; an estimated 50 million people were affected.

Officially, the blackout was attributed to a variety of factors, none of which involved foreign intervention. Investigators blamed "overgrown trees" that came into contact with strained high-voltage lines near facilities in Ohio owned by FirstEnergy Corp. More than 100 power plants were shut down during the cascading failure. A computer virus, then in wide circulation, disrupted the communications lines that utility companies use to manage the power grid, and this exacerbated the problem. The blackout prompted President Bush to address the nation the day it happened. Power was mostly restored within 24 hours.

There has never been an official U.S. government assertion of Chinese involvement in the outage, but

intelligence and other government officials contacted for this story did not explicitly rule out a Chinese role. One security analyst in the private sector with close ties to the intelligence community said that some senior intelligence officials believe that China played a role in the 2003 blackout that is still not fully understood.

Bennett, whose former trade association includes some of the nation's largest computer-security companies and who has testified before Congress on the vulnerability of information networks, also said that a blackout in February, which affected 3 million customers in South Florida, was precipitated by a cyber-hacker. That outage cut off electricity along Florida's east coast, from Daytona Beach to Monroe County, and affected eight power-generating stations. Bennett said that the chief executive officer of a security firm that belonged to Bennett's trade group told him that federal officials had hired the CEO's company to investigate the blackout for evidence of a network intrusion, and to "reverse engineer" the incident to see if China had played a role.

Bennett, who now works as a private consultant, said he decided to speak publicly about these incidents to point out that security for the nation's critical electronic infrastructures remains intolerably weak and to emphasize that government and company officials haven't sufficiently acknowledged these vulnerabilities.

## The Florida Blackout

A second information-security expert independently corroborated Bennett's account of the Florida blackout. According to this individual, who cited sources with direct knowledge of the investigation, a Chinese PLA hacker attempting to map Florida Power & Light's computer infrastructure apparently made a mistake. "The hacker was probably supposed to be mapping the system for his bosses and just got carried away and had a 'what happens if I pull on this' moment." The hacker triggered a cascade effect, shutting down large portions of the Florida power grid, the security expert said. "I suspect, as the system went down, the PLA hacker said something like, 'Oops, my bad,' in Chinese."

The power company has blamed "human error" for the incident, specifically an engineer who improperly disabled safety backups while working on a faulty switch. But federal officials are still investigating the matter and have not issued a final report, a spokeswoman for the Federal Energy Regulatory Commission said. The industry source, who conducts security research for government and corporate clients, said that hackers in China have devoted considerable time and resources to mapping the technology infrastructure of other U.S. companies. That assertion has been backed up by the current vice chairman of the Joint Chiefs of Staff, who said last year that Chinese sources are probing U.S. government and commercial networks.

Asked whether Washington knew of hacker involvement in the two blackouts, Joel Brenner, the government's senior counterintelligence official, told *National Journal*, "I can't comment on that." But he added, "It's certainly possible that sort of thing could happen. The kinds of network exploitation one does to explore a network and map it and learn one's way around it has to be done whether you are going to ... steal information, bring [the network] down, or corrupt it.... The possible consequences of this behavior are profound."

Brenner, who works for Director of National Intelligence Mike McConnell, looks for vulnerabilities in the government's information networks. He pointed to China as a source of attacks against U.S. interests. "Some [attacks], we have high confidence, are coming from government-sponsored sites," Brenner said. "The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction. It's a kind of cyber-militia.... It's coming in volumes that are just staggering."

The Central Intelligence Agency's chief cyber-security officer, Tom Donahue, said that hackers had breached the computer systems of utility companies outside the United States and that they had even demanded ransom. Donahue spoke at a January gathering in New Orleans of security executives from government agencies and some of the nation's largest utility and energy companies. He said he suspected that some of the hackers had inside knowledge of the utility systems and that in at least one case, an intrusion caused a power outage that affected multiple cities. The CIA didn't know who launched the attacks or why, Donahue said, "but all involved intrusions through the Internet."

Donahue's public remarks, which were unprecedented at the time, prompted questions about whether power plants in the United States had been hacked. Many computer-security experts, including Bennett, believe that his admission about foreign incidents was intended to warn American companies that if intrusions hadn't already happened stateside, they certainly could. A CIA spokesman at the time said that Donahue's comments were "designed to highlight to the audience the challenges posed by potential cyber intrusions." The CIA declined *National Journal's* request to interview Donahue.

## Cyber-Espionage

In addition to disruptive attacks on networks, officials are worried about the Chinese using long-established computer-hacking techniques to steal sensitive information from government agencies and U. S. corporations.

Brenner, the U.S. counterintelligence chief, said he knows of "a large American company" whose strategic information was obtained by its Chinese counterparts in advance of a business negotiation. As Brenner recounted the story, "The delegation gets to China and realizes, 'These guys on the other side of the table know every bottom line on every significant negotiating point.' They had to have got this by hacking into [the company's] systems."

Bennett told a similar story about a large, well-known American company. (Both he and Brenner declined to provide the names of the companies.) According to Bennett, the Chinese based their starting points for negotiation on the Americans' end points.

Two sources also alleged that the hacking extends to high-level administration officials.

During a trip to Beijing in December 2007, spyware programs designed to clandestinely remove information from personal computers and other electronic equipment were discovered on devices used by Commerce Secretary Carlos Gutierrez and possibly other members of a U.S. trade delegation, according to a computer-security expert with firsthand knowledge of the spyware used. Gutierrez was in China with the Joint Commission on Commerce and Trade, a high-level delegation that includes the U.S. trade representative and that meets with Chinese officials to discuss such matters as intellectual-property rights, market access, and consumer product safety. According to the computer-security expert, the spyware programs were designed to open communications channels to an outside system, and to download the contents of the infected devices at regular intervals. The source said that the computer codes were identical to those found in the laptop computers and other devices of several senior executives of U.S. corporations who also had their electronics "slurped" while on business in China. The source said he believes, based on conversations with U.S. officials, that the Gutierrez compromise was a source of considerable concern in the Bush administration. Another source with knowledge of the incident corroborated the computer-security expert's account.

*National Journal* had a series of conversations with Rich Mills, a Commerce Department spokesman. Asked whether spyware or other malicious software code was found on any electronic devices used by Gutierrez or people traveling with him in China in December 2007, Mills said he "could not confirm or



deny” the computer-security expert’s allegations. “I cannot comment on specific [information-technology] issues, but the Department of Commerce is actively working to safeguard sensitive information.” Mills added that the source had provided some inaccurate information, but he did not address the veracity of the source’s claim that the delegation was electronically compromised.

“China is indeed a counterintelligence threat, and specifically a cyber-counterintelligence threat,” said Brenner, who served for four years as inspector general of the National Security Agency, the intelligence organization that electronically steals other countries’ secrets. Brenner said that the American company’s experience “is an example of how hard the Chinese will work at this, and how much more seriously the American corporate sector has to take the information-security issue.” He called economic espionage a national security risk and said that it makes little difference to a foreign power whether it steals sensitive information from a government-operated computer or from one owned by a contractor. “If you travel abroad and are the director of research or the chief executive of a large company, you’re a target,” he said.

“Cyber-networks are the new frontier of counterintelligence,” Brenner emphasized. “If you can steal information or disrupt an organization by attacking its networks remotely, why go to the trouble of running a spy?”

Stephen Spoonamore, CEO of Cybrinth, a cyber-security firm that works for government and corporate clients, said that Chinese hackers attempt to map the IT networks of his clients on a daily basis. He said that executives from three *Fortune* 500 companies, all clients, had document-stealing code planted in their computers while traveling in China, the same fate that befell Gutierrez.

Spoonamore challenged U.S. officials to be more forthcoming about the breaches that have occurred on their systems. “By not talking openly about this, they are making a truly dangerous national security problem worse,” Spoonamore said. “Secrecy in this matter benefits no one. Our nation’s intellectual capital, industrial secrets, and economic security are under daily and withering attack. The oceans that surround us are no protection from sophisticated hackers, working at the speed of light on behalf of nation-states and mafias. We must cease denying the scope, scale, and risks of the issue. I, and a growing number of my peers believe our nation is in grave and growing danger.”

## **A Growing Threat**

Brenner said that Chinese hackers are “very good and getting better all the time.... What makes the Chinese stand out is the pervasive and relentless nature of the attacks that are coming from China.”

The issue has caught Congress’s attention. Rep. Jim Langevin, D-R.I., who chairs the Homeland Security panel’s Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, said that his staff has examined a range of hacker networks, from criminal syndicates to nationally supported groups. “China has been a primary concern,” he said. The deepest penetrations into U.S. systems have been traced back to sources within China, Langevin noted.

(At a hearing last week, Langevin said that the private sector, which owns the vast majority of U.S. information networks, including those that operate power plants, dams, and other critical infrastructure, had taken a “halfhearted approach” to improving security. He cited a new report by the Government Accountability Office, which found that the Tennessee Valley Authority, the nation’s largest power generator, “has not fully implemented appropriate security practices to secure the control systems and networks used to operate its critical infrastructures.” Langevin said that the TVA “risks a disruption of its operations as the result of a cyber-incident, which could impact its customers,” and he expressed “little confidence that industry is taking the appropriate actions.”)

The Chinese make little distinction between hackers who work for the government and those who undertake cyber-adventures on its behalf. "There's a huge pool of Chinese individuals, students, academics, unemployed, whatever it may be, who are, at minimum, not discouraged from trying this out," said Rodger Baker, a senior China analyst for Stratfor, a private intelligence firm. So-called patriotic-hacker groups have launched attacks from inside China, usually aimed at people they think have offended the country or pose a threat to its strategic interests. At a minimum the Chinese government has done little to shut down these groups, which are typically composed of technologically skilled and highly nationalistic young men. Officially, Chinese military and diplomatic officials say they have no policy of attacking other governments' systems.

"This has been a growing wave in recent years," Brenner said, attributing China's cyber-tactics to its global economic and political ambitions. "The Chinese are out to develop a modern economy and society in one generation.... There is much about their determination that is admirable. But they're also willing to steal a lot of proprietary information to do it, and that's not admirable. And we've got to stop it as best we can."

High-profile penetrations of government systems have been occurring for several years. In 2007, an unidentified hacker broke into the e-mail system for Defense Secretary Robert Gates's office, and the Pentagon shut down about 1,500 computers in response. But officials said that the intrusion caused no harm. In 2006, a State Department employee opened an e-mail containing a Trojan horse, a program designed to install itself on a host machine to give a hacker covert access. As a result, officials cut off Internet access to the department's East Asia and Pacific region, but the department suffered no long-term problems.

The Homeland Security Department, which is responsible for protecting civilian computer systems, suffered nearly 850 attacks over a two-year period beginning in 2005, officials have said. In one instance, they found that a program designed to steal passwords had been installed on two of the department's network servers. In these and other incidents, there is considerable debate about whether the intruders stole truly valuable information that could compromise U.S. strategy or ongoing operations.

"The penetrations we've seen are on unclassified systems, which are obviously less protected than classified systems," Brenner said.

## **Private Sector Foot-Dragging**

There is little indication that cyber-intrusions, however menacing, have severely impaired government operations for very long. So why are so many officials increasingly sounding the alarm about network attacks, Chinese hacking and espionage, and the advent of cyberwar?

Part of the answer lies in officials' most recent appraisals of the cyber-threat. They cite evidence that attacks are increasing in volume and appear engineered more to cause real harm than sporadic inconvenience. Without naming China, Robert Jamison, the top cyber-security official at DHS, told reporters at a March briefing, "We're concerned that the intrusions are more frequent, and they're more targeted, and they're more sophisticated."

"In terms of breaches within government systems, it's something that has happened quite a bit over the last six, seven years," says Shannon Kellogg, the director of information-security policy for EMC Corp., which owns RSA, a top cyber-security research firm. "But the scale of these types of breaches and attacks seems to have increased substantially."

Government officials are more concerned now than in recent years about the private sector's inability, or unwillingness, to stop these pervasive attacks. When Donahue, the CIA cyber-security officer, warned

the gathering in New Orleans about foreign hackings of power plants, some saw it as a direct challenge to American companies.

“Donahue wouldn’t have said it publicly if he didn’t think the threat was very large and that companies needed to fix things right now,” Alan Paller, the highly regarded director of research at the SANS Institute, told *The Washington Post* at the time. (SANS, a cyber-security research and education group, sponsored the January meeting in New Orleans.) Another security expert noted that in the previous 18 months, there had been “a huge increase in focused attacks on our national infrastructure networks ... and they have been coming from outside the United States.”

In comments posted on *Wired* magazine’s *Danger Room* blog, which is trafficked by many techno-elites who are skeptical of the administration’s more boisterous public warnings, Donahue’s remarks about power plants drew support. Michael Tanji, a former intelligence officer with the Defense Intelligence Agency, said that the comments weren’t part of a government plot to hype the threat. “Having worked with [Donahue] on these and related issues in the past, I regret to inform conspiracy theorists that he is virulently allergic to hyperbole,” Tanji said. “I’ve long been a skeptic of claims about being able to shut down the world from the Net... But after today, I’m starting to come around to the idea that the ignorance or intransigence of utility system owners just might merit a more robust response than has been undertaken to date.”

Tanji’s remarks pointed to one of the most nettlesome realities of cyber-security policy. Because most of the infrastructure in the United States is privately owned, the government finds it exceptionally difficult to compel utility operators to better monitor their systems. The FBI and DHS have established formal groups where business operators can disclose their known vulnerabilities privately. (Companies fear that public exposure will decrease shareholder confidence or incite more hackings.) But membership in these organizations isn’t compulsory. Furthermore, many of the systems that utility operators use were designed by others. Intelligence officials now worry that software developed overseas poses another layer of risk because malicious codes or backdoors can be embedded in the software at its creation. U.S. officials have singled out software manufacturers in emerging markets such as, not surprisingly, China.

## **Military Response**

The intelligence community’s and private sector’s vocal warnings and dire suspicions of Chinese hackers join a chorus of concern emanating from the Defense Department in recent months. In the most recent annual report on China’s military power, the Defense Department declared publicly for the first time that attacks against government and commercial computer networks in 2007 appear to have emanated from China. “Numerous computer networks around the world, including those owned by the U.S. government, were subject to intrusions that appear to have originated within” the People’s Republic of China. Although not claiming that the attacks were conducted by the Chinese government, or officially endorsed, the declaration built upon the previous year’s warning that the People’s Liberation Army is “building capabilities for information warfare” for possible use in “pre-emptive attacks.”

The military is not waiting for China, or any other nation or hacker group, to strike a lethal cyber-blow. In March, Air Force Gen. Kevin Chilton, the chief of U.S. Strategic Command, said that the Pentagon has its own cyberwar plans. “Our challenge is to define, shape, develop, deliver, and sustain a cyber-force second to none,” Chilton told the Senate Armed Services Committee. He asked appropriators for an “increased emphasis” on the Defense Department’s cyber-capabilities to help train personnel to “conduct network warfare.”

The Air Force is in the process of setting up a Cyberspace Command, headed by a two-star general and comprising about 160 individuals assigned to a handful of bases. As *Wired* noted in a recent profile,

Cyberspace Command “is dedicated to the proposition that the next war will be fought in the electromagnetic spectrum and that computers are military weapons.” The Air Force has launched a TV ad campaign to drum up support for the new command, and to call attention to cyberwar. “You used to need an army to wage a war,” a narrator in the TV spot declares. “Now all you need is an Internet connection.”

“It’s a kind of cyber-militia... It’s coming in volumes that are just staggering.”

--*Joel Brenner*

Defense and intelligence officials have been surprised by China’s cyber-advances, according to the U.S.-China Economic and Security Review Commission. In November, the commission reported that “Chinese military strategists have embraced ... cyberattacks” as a weapon in their military arsenal. Gen. James Cartwright, the former head of U.S. Strategic Command and now the vice chairman of the Joint Chiefs, told the commission that China was engaged in cyber-reconnaissance, probing computer networks of U. S. agencies and corporations. He was particularly concerned about China’s ability to conduct “denial-of-service” attacks, which overwhelm a computer system with massive amounts of automatically generated message traffic. Cartwright provocatively asserted that the consequences of a cyberattack “could, in fact, be in the magnitude of a weapon of mass destruction.”

A former CIA official cast the cyber-threat in a similarly dire terms. “We are currently in a cyberwar, and war is going on today,” Andrew Palowitch, who’s now a consultant to U.S. Strategic Command, told an audience at Georgetown University in November. STRATCOM, headquartered at Offutt Air Force Base in Nebraska, oversees the Defense Department’s Joint Task Force-Global Network Operations, which defends military systems against cyber-attack. Palowitch cited statistics, provided by Cartwright, that 37,000 reported breaches of government and private systems occurred in fiscal 2007. The Defense Department experienced almost 80,000 computer attacks, he said. Some of these assaults “reduced” the military’s “operational capabilities,” Palowitch noted.

## **Presidential Attention**

President Bush has personally devoted more high-level attention to the cyberattack issue in the last year or so than he did in the first six years of his tenure combined. Many security experts are surprised that the administration is only now moving to take dramatic measures to improve the security of government networks, because some Cabinet-level and White House officials have been warning about the threat for years to just about anyone who will listen.

Until McConnell, the national intelligence director, personally drove the point home to Bush in an Oval Office meeting in 2006, there was little top-level support for a comprehensive government cyber-security plan. “They ignored it,” one former senior administration official said flatly. “McConnell has the president’s ear.”

McConnell, a former director of the National Security Agency, whose main job is to intercept foreign communications intelligence but which is also responsible for protecting U.S. classified information and

systems, takes the computer-security issue as seriously as his counter-terrorism mission. After McConnell left the NSA, in 1996, he took over the intelligence practice at Booz Allen Hamilton, where he again turned to security problems, particularly within the nation's financial infrastructure. Working with officials from the New York Stock Exchange, McConnell developed a report for the government on network vulnerabilities; he has said that it was so revealing, the administration decided to classify it.

Lawrence Wright of *The New Yorker* reported earlier this year that McConnell told Bush during the 2006 Oval Office meeting, "If the 9/11 perpetrators had focused on a single U.S. bank through cyberattack and it had been successful, it would have had an order-of-magnitude greater impact on the U.S. economy." According to Wright, the president was disturbed, and then asked Treasury Secretary Henry Paulson Jr., who was at the meeting, if McConnell was correct; Paulson assured the president that he was.

Brenner confirmed Wright's account as "a true story." And separately, a former senior administration official told *National Journal* of another dimension. In that meeting, McConnell also told the president that White House communications systems could be targeted for attack just as other U.S. government systems had been targeted. The intelligence chief was telling the president, "If the capability to exploit a communications device exists, we have to assume that our enemies either have it, or are trying to develop it," the former official said.

This meeting compelled the White House to craft an executive order laying out a broad and ambitious plan to shore up government-network defenses. Known internally as "the cyber-initiative," it was formally issued in January. The details remain classified, but it has been reported that the order authorizes the National Security Agency to monitor federal computer networks. It also requires that the government dramatically scale back the number of points at which federal networks connect to the public Internet. The Office of Management and Budget has directed agencies to limit the total number of Internet "points of presence" to 50 by June.

Limiting connection points is analogous to pulling up drawbridges in order to defend the government's cyber-infrastructure. Security experts interviewed for this story said that it shows how little the government can do, at least for now, to ward off intrusions if the first line of defense is to "unplug."

## Mixed Reactions

Under the president's cyber-initiative, the Homeland Security Department will be responsible for monitoring government agencies apart from the Defense Department. In March, Homeland Security Secretary Michael Chertoff told *National Journal* that the first step is "to survey all the points" of presence. "We have no final number yet."

"The agencies' networks have grown very haphazardly. No one really knows where [the connections to the Internet] are," said Bruce McConnell, who was the chief of information technology and policy in the Office of Management and Budget. He left government in 2000. "Trying to catalogue where things are so you could turn them off is a daunting task in and of itself," said McConnell, who is not related to the intelligence chief.

Bush's cyber-initiative has received mixed reviews. Generally, cyber-experts favor a comprehensive approach, and they are relieved that the issue finally has the president's full attention. But some question how the program is being implemented—under a cloak of secrecy and with a heavy reliance on the intelligence community.

“Our nation’s intellectual capital, industrial secrets, and economic security are under daily and withering attack.”

--*Stephen Spoonamore*

The sharpest criticisms are directed at the NSA, an intelligence agency whose traditional mandate is to collect information coming from outside the United States; it has no customary role monitoring networks inside the country, although this has changed in the years following the 9/11 attacks. It's not clear just how far the government's monitoring of computer networks will extend into the private sector and precisely what role the NSA will play tracking networks inside the United States, but lawmakers have already raised concerns that the cyber-initiative will creep into domestic intelligence-gathering. The same kinds of technologies that are used to monitor networks for viruses and other malicious threats could be used to track domestic communications. On May 2, DHS's top overseers sent a letter to Chertoff questioning “the secrecy of the project.” Sens. Joe Lieberman, ID-Conn., and Susan Collins, R-Maine, the chairman and ranking member of the Homeland Security and Governmental Affairs Committee, respectively, noted that the department had requested an additional \$83 million for its National Cyber Security Division; DHS had already been allocated \$115 million for the cyber-initiative in the 2008 omnibus appropriations bill. “This would be a nearly \$200 million increase, tripling the amount of money spent on cyber-security in DHS since 2007,” the senators wrote. The full cost of implementing the president's cyber-initiative is estimated to be \$30 *billion*. The entire 2009 budget request for the Homeland Security Department is about \$50 billion.

Marc Sachs, who was the director for communication infrastructure protection in the White House Office of Cyberspace Security in 2002, praised the administration for taking a bold initial step. But he said that the level of attention is 10 years overdue. Sachs noted that in 1998, President Clinton issued a directive that set ambitious infrastructure-protection goals. “I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber-systems,” Clinton wrote.

Without pointing to particular policies, Brenner, the counterintelligence chief, said, “We need to take these policy declarations that we've had for 10 years and turn them into practical reality.” He said the job of securing cyberspace is hardly as simple as “put two padlocks on the door.... This is an incredibly open and porous and, in many cases, wireless system. Controlling cyber-security is like controlling the air flow in a large, segmented building complex in a noxious neighborhood. You cannot be sure you are keeping all the noxious stuff out. What you've got to say is, gee, in the infirmary, we've really got to deal differently than we do in the lobby.”

## **False Accusations?**

Given the political fallout that could stem from a proven Chinese attack on power plants or theft of government secrets—not to mention the pressure to launch some sort of military response—skeptics have asked whether the Chinese really are behind so many high-profile incidents.

Brenner affirmed the widely held view that it's technologically difficult to attribute the exact source of any cyberattack and that the government needs better technologies to do so. But despite his assurances that

the government has indeed sourced cyber-intrusions to China, others urge caution.

“We want to find a natural enemy, so we’re looking everywhere,” Sachs said. He noted that some hackers launch their attacks through computers based in other countries, and that China is an easy mask. “I think all of us should remember that not everything you see online is truthful.”

Another former administration official echoed those sentiments. “I think it’s a little bit naive to suggest that everything that says it comes from China comes from China,” said Amit Yoran, the first director of DHS’s National Cyber Security Division, who left the post in 2004.

But there is little to no doubt, including among skeptics, that China is vigorously pursuing offensive cyber-capabilities. Military analysts say that the Chinese know their armed forces cannot match America’s in a head-on confrontation, and they realize their nuclear arsenal pales in comparison. These imbalances have forced Chinese military planners to adopt what the Pentagon calls “asymmetric” techniques—tactics that aim at a foe’s vulnerabilities—in order to counter, or at least deter, U.S. military power.

“There has been much writing on information warfare among China’s military thinkers, who indicate a strong conceptual understanding of its methods and uses,” according to the Pentagon’s annual report on China’s military power. The report stated that “there is no evidence of a formal Chinese ... doctrine” but noted that the People’s Liberation Army has “established information-warfare units to develop viruses to attack enemy computer systems and networks.”

U.S. military officials see cyber-warfare as one arrow in a quiver of asymmetric techniques to disrupt an enemy’s command-and-control systems. The Chinese strategy, according to this line of thinking, is not to defeat U.S. military forces but to make it harder for them to operate.

China’s military history has been defined by asymmetric warfare, said Harry Harding, an expert on Chinese domestic politics and U.S.-China relations, who teaches at George Washington University’s Elliott School of International Affairs. Cyber-warfare is just one of the more recent tactics. If the U.S. government tries to protect its systems, the Chinese will simply attack the private sector; he cited the financial services industry as an obvious target. “I have no doubt that China is doing this,” Harding said.

Bennett, the former head of the Cyber Security Industry Alliance, said that if China has penetrated power plants and the power grid, it serves as a show of force to the United States and is likely meant to deter any U.S. military intervention on behalf of Taiwan. He noted that the Florida blackout occurred only a few days after the Navy shot down a failing U.S. satellite with a missile designed to intercept inbound ballistic missiles. A year earlier, the Chinese had downed one of their own satellites in orbit. The Bush administration has pursued ballistic missile defense systems, and Taiwan has sought that technology from the United States.

## **Cyberwar**

The Chinese are not alone, of course, in their pursuit of cyber-warfare. The Air Force is setting up the Cyberspace Command, the 10th command in the service’s history.

“The next kind of warfare will be asymmetric warfare,” Gen. William Lord, the provisional commander, said during a roundtable discussion at the Council of Foreign Relations in March. “Who is going to take on the United States Army, Marine Corps, U.S. Air Force, and U.S. Navy as probably the most powerful force on the face of the planet?”

Lord didn’t limit his remarks to China. He said that cyber-criminals and other “bad guys” were as much a concern for the military. He also pointed to a massive cyberattack launched last year against computers

in Estonia, in which Russian hackers—perhaps operating at Moscow's behest—tried to take down the country's systems in retaliation for Estonia's decision to move a statue commemorating fallen Soviet troops, a statue that Russians living in Estonia love but that native-born Estonians don't. The attack has been billed as the first "cyberwar" because of the overwhelming electronic force brought to bear on the tiny country of 1.3 million people.

"I had an opportunity to speak with the minister of defense from Estonia," Lord said. "He was attacked by 1 million computers."

The Estonia attack probably shook nerves more than it caused long-term damage. But it served as a potent example of how determined, coordinated hackers could gang up on a foreign government. It has also created profound policy questions about what qualifies as war in cyberspace.

"The problem with this kind of warfare," Lord said, "is determining who is the enemy, what is their intent, and where are they, and then what can you do about it?"

Brenner, the senior U.S. counterintelligence official, said, "Another country knows that if it starts taking out our satellites, that would be an act of war." But "if they were to take out certain parts of our infrastructure, electronically, that could be regarded as an act of war," he said. "It's not my job to say that."

NATO officials are reluctantly struggling with that question, too. At a ministerial meeting last June, Defense Secretary Gates asked the allied members to consider defining cyberattacks in the context of traditional warfare. Cyberwar is still abstract, and there are no international conventions that govern military conduct on a digital battlefield.

"The U.S. government doesn't really have a policy on the use of these techniques," said Michael Vatis, a former director of the FBI's National Infrastructure Protection Center. "The closest analogy is to covert actions," he said, meaning spy operations undertaken by intelligence agencies against foreign governments. "They take place, and people have strong suspicions about [who's responsible]. But as long as they're not able to prove it, there's very little that they can do about it. And so there's often not as much outrage expressed."

*Staff Correspondent Bruce Stokes contributed to this article. The author can be reached at [sharris@nationaljournal.com](mailto:sharris@nationaljournal.com)*

Copyright ©2010 by National Journal Group Inc. The Watergate 600 New Hampshire Ave., NW Washington, DC 20037  
202-739-8400 • fax 202-833-8069 NationalJournal.com is an Atlantic Media publication.



## HOW CHINA WILL USE CYBER WARFARE TO LEAPFROG IN MILITARY COMPETITIVENESS

by Jason Fritz BS (St. Cloud), MIR (Bond)

### *Introduction*

*The People's Republic of China (PRC) may be a global power economically but its military lacks force projection beyond the Asia Pacific region. Its traditional military hardware is one to three generations behind the US and Russia. In light of these deficiencies it is probable that cyber warfare will provide China with an asymmetric advantage to deter aggression from stronger military powers as they catch up in traditional military capabilities. Cyber warfare would also allow China to leapfrog by means of technology transfer and exploiting adversary weaknesses. This investigation will address three primary questions: What is China's current military capability? How would cyber warfare allow China to seriously advance its strategic abilities? And what is the evidence that China is headed in a cyber warfare direction?*

### **1. Traditional Military Power of the PLA**

In order to see how the Chinese military will 'leapfrog' in military competitiveness, it is necessary to establish its current capabilities. The Chinese People's Liberation Army (PLA) is composed of five main service branches, the PLA Ground Force, PLA Navy, PLA Air Force, Second Artillery Corps, and the PLA Reserved Force. China has one of the world's largest military forces, with 2.3 million active members, a reserve force of 800,000, and a paramilitary force of 3.9 million, for a grand total of approximately 7 million members. The PLA has tried to transform itself from a land based power, to a smaller, mobile, high tech power that is capable of reaching beyond its borders (Annual Report to Congress 2007; China's National Defense in 2006).

During the 1980's paramount leader Deng Xiaoping pushed for quality over quantity, and the military was reduced by one million members. In 1993, President Jiang Zemin officially announced a Revolution in Military Affairs (RMA) a part of the national military strategy for modernization. RMA is a theory about the future of warfare, often connected to technological and organizational recommendations for change in the United States military and others. RMA is tied to modern information, communications, space technology, and total systems integration. Careful observation of US involvement in the Kosovo, Afghanistan, and Iraqi wars, furthered China's interest in network-centric warfare and asymmetric warfare, the former successfully used by the US, and the latter successfully used against the US. At the turn of the century, the bulk of China's traditional military force remained 1950s to 1970s era technology imported and reverse engineered from Russia. China is seeking to modernize this force. The size of China's traditional force will shrink, as fewer numbers are needed when new technology is introduced (Cordesman and Kleiber 2006; Corpus 2006; Moore 2000).

China's defence budget has increased dramatically over the last 15 years. The official military budget of China was US\$57 billion in 2008, making it the second largest military budget in the world. By contrast, the largest is the US with \$623 billion, and the third largest is Russia with \$50 billion. Japan, South Korea, and India are the next largest spenders in the Asia Pacific region with \$41 billion, \$21 billion, and \$19 billion, respectively (World Wide Military Expenditures 2007). China's annual defence budget increases at approximately the same rate as its annual GDP, with an average increase of 9% per year since 1996 (Pike 2008; China's National Defense in 2006). However, China's total military spending may be far greater than the official figures reported. Foreign acquisitions, research and development of dual use science and technology, national security, construction, and emergency response and disaster relief, are a few examples of expenditures which may fall under non-military headings but directly relate to the advancement of the military. The US Department of Defence estimates China's total military-related spending for 2007 could be between \$97 billion and \$139 billion. Think tanks and academic institutions report a wide range of estimates for China's defence budget, using varying methodologies and sources, however most arrive at the same conclusion: China significantly under-reports its defence expenditures (Annual Report to Congress 2008; International Assessment and Strategy Center 2005).

### **Ground Force**

The PLA Ground Force (PLAGF) is the world's largest, with 1.25 million personnel, or about 70% of the PLA's total manpower (Annual Report to Congress 2008). Approximately 400,000 of these troops are based in the three military regions (MRs) opposite Taiwan. According to the 2008 Military Balance of the International Institute for Strategic Studies (IISS), the PLAGF comprises 18 group armies which include 9 armoured divisions, 3 mechanised infantry divisions, 24 motorised infantry divisions, 15 infantry divisions, two amphibious assault divisions, one mechanised infantry brigade, 22 motorised infantry brigades, 12 armoured brigades, 7 artillery divisions, 14 artillery brigades, and nine anti-aircraft artillery missile brigades. China's military doctrine places an emphasis on electronic and information warfare, long-range precision strikes, surface-to-air missiles, special operations forces, army aviation helicopters, and satellite communications. The PLAGF continues to reduce its overall size, opting for a more high tech and mobile force (China's National Defense in 2006).

While much of the equipment remains antiquated, China is continually upgrading. This includes approximately 200 Type 98 and Type 99 main battle tanks now deployed to units in the Beijing and Shenyang MRs. As many as 6,000 tanks were produced by China in the 1960's. From the early 1970's to 2000, China's tank inventory remained around 10,000. This was mostly composed of old Soviet tanks and Chinese versions of old Soviet designs. China continually upgraded over the decades, but was always one step behind the current Soviet models. The Chinese-produced versions of the Soviet T-54A (Type 59 and Type 69) account for over two-thirds of the total PLA tank inventory. While retiring some of the older Type 59/69 series and replacing them with the second generation Type 88 and Type 96, the PLA is also upgrading the remaining Type 59/69 series tanks with new technologies including improved communication and fire-control systems, night vision equipment, explosive reactive armour, improved power plant, and gun-fired anti-tank missiles so that they can remain in service as mobile fire-support platforms. China's newest tank, the Type 99, entered PLA service in 2001. Maintenance of such a massive force becomes a problem, and many of China's tanks may have fallen into disrepair. This may also be a push for modernizing to a smaller but more effective force (Armoured Fighting Vehicles 2008).

The PLAGF's hand guns further illustrate China's attempts to modernize and catch up by means of foreign acquisition and reverse engineering. Most of China's weapons are derived from Soviet models acquired before the Sino-Soviet split in late 1950s and early 1960s. Examples include Soviet or Russian small arms like the Mosin-Nagant series rifles and carbines, the SKS carbine, the AK-47 assault rifle, the RPD light-machine gun, the Tokarev TT33 pistol, and the DShK heavy machine gun. The PLA's main infantry rifle, the QBZ-95 is derived from the Russian AK-47, and the Chinese Type 56 Assault Rifle is a direct copy, albeit locally produced and with a permanently attached bayonet with a more sword-like, stiletto style. The Chinese Type 56 Assault Rifle, a locally produced version of the SKS, also differs from its Russian counterpart by having a permanently attached bayonet. The Chinese Type 56 was mass produced from the 1960's to 1980's and was exported to many states around the world (Small Arms 2008).

## **Navy**

The People's Liberation Army Navy (PLAN) is composed of 250,000 personnel divided into three major fleets, the North Sea Fleet, East Sea Fleet, and South Sea Fleet, each containing surface ships, submarines, naval air force, coastal defence, and marine units. China's naval force includes 57 attack submarines, 55 medium and heavy amphibious ships, and 49 coastal missile patrol craft. A priority has been placed on anti-air capabilities with improvements in over-the-horizon targeting, range, and accuracy in surface-to-air missiles. "Taking informationization as the goal and strategic focus in its modernization drive, the Navy gives high priority to the development of maritime information systems, and new-generation weaponry and equipment" (China's National Defense in 2006). As a part of PLAN's modernization program, PLAN has been developing blue water navy capabilities.

PLAN does not currently have an aircraft carrier. However, evidence suggests they are pursuing such technology and have the capability to construct one. Renovation to a former Soviet Kuznetsov-class aircraft carrier may be used for training purposes, and the Chinese have expressed interest in acquiring Russian Su-33 carrier-borne fighters. The ex-Australian carrier Melbourne also provided research for the PLAN as it was towed to China for scrap. Russian assistance, coupled with an already capable ship building infrastructure, could allow PLAN to rapidly develop an aircraft carrier. The PLAN's ambitions include operating out to the first and second island chains, extending operations to the South Pacific near Australia, north to the Aleutian Islands, and west to the Strait of Malacca towards the Indian Ocean (Annual Report to Congress 2008).

China's submarine fleet is derived from outdated Russian technology and is seeking to become a more modern and smaller force. Early Chinese submarines were domestically produced versions of the Soviet Romeo class submarine, which were only capable of coastal patrols with deployment to sea limited to a few days per year. One Romeo was modified to carry six YJ-1 (C-801) anti-ship missiles, but it had to surface to fire them. The Chinese Ming class submarines produced in the 1970s were not much better, other than being of newer construction. This was followed by the Song class submarine, which had a streamlined hull and can be fitted with anti-ship missiles capable of being fired while submerged. China returned to purchasing subs in the late 1990s with the Russian Kilo class submarine. The Type 041 Yuan Class is the newest diesel-electric submarine in the PLAN. Its design incorporates parts of the Song class and Russian Kilo class submarines. The Yuan class has five torpedo tubes capable of launching indigenous torpedos as well as Russian

designed torpedos, and it is believed to have anti-ship missiles. This ship was designed to replace the aging Romeo and Ming class submarines which currently form the backbone of the PLAN's submarine fleet (Chinese Submarines 2008; see also China's Navy 2007).

Chinese produced Han class nuclear submarines were plagued with problems. A follow-on Type 093 nuclear submarine was developed with experience from the Han class and further assistance from Russian submarine builders, such as advanced welding and construction techniques. Despite being armed with new Chinese wire-guided torpedoes; the Type 093's overall capability remains comparable to Russian technology of the late 1970s. Nevertheless, China continues to make progress and the true level of Russian assistance lacks transparency (Smith 2001). Further, the Type 093 may have benefited from German fuel cell technology and French design, which could allow for two to three weeks of submerged operations without having to surface to recharge batteries. Internet-source photos of Type 039s under construction also show Chinese mastery of advanced multi-layer rubber/polymer hull coatings that greatly reduce hull-radiated noise while limiting the effectiveness of active-sonar detection (Chinese Submarines 2008).

China maintains a fleet of approximately 28 destroyers, 48 frigates, and 30 ocean-capable fast attack craft. The frigates were designed for anti-surface warfare, and lacking significant self-defence. Chinese-built destroyers include the Luhai class, the Luhai class, and the Luda I/II/III, from oldest to newest, respectively. The Luhai and Luda class are armed with a battery of guns, torpedos, mortars, optional helicopter pads, and domestically built Crotales SAMs which were built from designs provided by France in the 1980s. Construction of the Luhai class was delayed from the mid 1980s to the mid 1990s due to construction of frigates for the Thai Navy. The most powerful addition to the PLAN is the Russian-built Sovremenny class destroyers. These include MOSKIT anti-ship missiles and KASHTAN combined gun/missile ship defence systems. While these designs are non-stealth 1970s Russian technology, outdated by current designs, they provided the PLAN with modern anti-ship, anti-air, and anti-submarine systems. The most recent Sovremenny acquisitions carry 8 Sunburn supersonic sea-skimming ASM and the SA-N-7 Gadfly, which will give PLAN limited naval air-defence capability. Up to this point, China only possessed short-range SAMs of French or domestic design (Surface Combatants 2008; IISS 2008).

Improvements in stealth design of the PLAN's ships further the notion that China seeks to modernize by purchasing or clandestinely obtaining technology from other states, reverse engineering that technology, and then attempting to make upgraded domestically produced versions. According to Frank Moore of the Institute for Defence and Disarmament Studies:

The PLA developed new stealthy warships benefiting from Russian or Ukrainian design advice, weapons, electronics and other systems, plus new computer aided design methods which speeded their development. By 2002 it was possible to observe the construction of three new classes of warships via Chinese internet sources ... the No. 168 class, which armed with Russian SHTIL SAMs, Russian radar, Kamov Ka-28 ASW helicopters and Chinese C-802/803 anti-ship missiles, and powered by Ukrainian gas turbine engines. Soon after two No. 170 class destroyers were launched. These featured large phased array radar similar in appearance to the U.S. AEGIS system... Most likely the new "AEGIS" radar comes from the Ukrainian KVANT bureau and is a newly-developed active phased array radar with a broad search range of about 150km ... In 2003 [PLAN] launched two Type 054 stealthy frigates. Some sources indicate production was halted at two ships pending the completion of a new Russian SAM... In early 2004 internet-source pictures of a model of this new variant, apparently from a Chinese shipbuilding exhibition, confirmed that it will feature a new vertical-launched SAM and be outfitted with Russian radar and missile guidance systems. The Type 054 is also powered by co-produced French-designed SEMT Pielstick marine diesel engines.

A fourth stealthy warship emerged in April 2004: a new fast-attack craft (FAC). Now being produced at two or three shipyards, this new FAC utilizes a wave-piercing catamaran (twin) hull design, which improves stability at high speeds even in rough seas. It is based on a design obtained from the Australian fast-ferry firm AMD... [with] radar-absorbing materials applied to the hull. (Moore 2000).

Not only does this illustrate China's use of foreign technology, it also demonstrates the complexity of modern warfare. These are highly sophisticated weapons, weapons pieced together from multiple sources, the existence of which was leaked onto the internet.

## **Air Force**

The People's Liberation Army Air Force (PLAAF) is the third largest air force in the world behind the United States and Russia. The PLAAF employs 250,000 personnel and 1,762 combat aircraft (IISS 2008). The Soviet Union helped found the PLAAF in 1949, providing aircraft in 1951, and production technology and pilot training in 1953. China gained limited air combat experience during the Korean War. In 1956 China began assembling its own aircraft based on Soviet design, such as the J-2, J-5, and J-6, copies of the MiG-15, Mig-17, and Mig-19 respectively. The Sino-Soviet split was a significant setback to the PLAAF as was resource competition with the missile and nuclear divisions of the military. China's aircraft industry received a boost during the Vietnam War by providing aircraft for North Vietnam.

During the 1980s, the PLAAF underwent significant restructuring, opting for a more streamlined force and increased training. Due to the Sino-Soviet Split, the PLAAF turned to Western states for military expertise. Western states saw China as a counterbalance to the Soviet Union; however support dissolved following the 1989 Tiananmen Square incident. Reverse engineering of Soviet weaponry continued with the Chinese aircraft F-7 being an illegitimate copy of the MiG-21, and the F-8 incorporating various Soviet designs. Gorbachev's 1989 visit to China marked an end to the Sino-Soviet split. The newborn and economically struggling state of Russia used the transfer of military technology and expertise to China as a way to sustain its own aerospace industry (Moore 2000).

The collapse of The Soviet Union, and concerns over a Taiwan conflict that could draw in the United States, reinvigorated the PLAAF's modernization program. In the 1990s, China began development of fourth generation fighters, including the J-10 and a collaboration with Pakistan on the JF-17. China continued focusing on improved pilot training and retiring obsolete aircraft, preferring quality over quantity. The PLAAF is currently developing its own fifth generation stealth craft and increasing Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems for all its fighters.

In addition to jet fighter aircraft, "China is upgrading its B-6 bomber fleet (originally adapted from the Russian Tu-16) with a new variant which, when operational, will be armed with a new long-range cruise missile" (Annual Report to Congress 2008). China is also developing Airborne Early Warning and Control (AEW&C) aircraft utilizing Russian and possibly Israeli technology; and is making progress in tanker aircraft used for in-flight refuelling and airlift planes. These are important steps in obtaining the capability to conduct operations beyond China's borders (China's National Defense in 2006; Allen 2005).

Production of indigenous Chinese aircraft has been lacklustre. Most of the designs require foreign expertise which is then reverse engineered. The technology obtained is often one generation old at the time of acquisition, as states do not want to give up their advantage. Further, to reverse engineer they not only need the aircraft itself, but also high-precision and technologically advanced machine tools, electronics and components, skilled personnel, and facilities. By the time the technology is fully understood, and indigenous versions produced, the aircraft may be two or three generations behind the latest models of the world's advanced military forces. China is not alone in this difficulty. Except for the five largest industrial arms producers (France, Germany, Russia, the UK, and the US), other countries that have attempted to produce indigenously designed combat aircraft, such as Israel, South Africa, India, Taiwan, and South Korea, have abandoned their efforts and returned to importing systems from one of the five main producers. One reason is the economy of scale involved with financing research, development, and production of all of the systems and sub-systems that compose modern combat aircraft (Moore 2000; see also Allen, Krumel and Pollack 1995). Despite these difficulties, China remains committed to producing indigenous aircraft. Continued purchase of foreign technology demonstrates that the Chinese believe reverse engineering and then upgrading is the best approach to establish themselves as a self-sufficient producer in the future. In other words, the PRC aspires to become one of the elite weapons producers, but it does not want to wait for the infrastructure to evolve; it wants to leapfrog these capabilities.

## **Space**

The PLA is responsible for the Chinese space program. China was the fifth nation in the world to place a satellite in orbit, the third nation to put a human into space, and the third nation to successfully test an anti-satellite weapon (ASAT) capable of destroying an enemy satellite in low earth orbit. China's manned space activities have received substantial support from Russia. This can be seen in the design of the Shenzhou spacecraft, which closely resembles the Russian Soyuz spacecraft. Although China's commercial space program has utility for non-military research, it also demonstrates space launch and control capabilities that have direct military application. All taikonauts have been selected from members of the PLAAF, and the PLA has deployed space-based systems for military purposes. These include imagery intelligence satellite systems such as the ZiYan series and JianBing series, synthetic aperture satellites (SAR) such as JianBing-5, the BeiDou satellite navigation network, and secured communication satellites such as FengHuo-1. China launched its 100th Long March series rocket in 2007, and continues to put more sophisticated and diverse satellites into orbit. The PRC is developing the Long March 5, an improved heavy-lift rocket that will be able to lift larger reconnaissance satellites into low-earth orbit or communications satellites into geosynchronous orbits by 2012. It expects to replace all foreign-produced satellites in its inventory with indigenously produced sun-synchronous and geo-stationary models by 2010 (Annual Report to Congress 2008; Center for Strategic and International Studies 2003).

Many of China's space assets are dual use, having financial and prestige benefits in addition to military applications. The Ziyuan-2 series, the Yaogan-1 and -2, the Haiyang-1B, the CBERS-1 and -2 satellites, and the Huanjing satellites, offer ocean surveillance, disaster and environmental monitoring, and high resolution imaging in the visible, infrared, and radar spectrums. New electro-optical satellites are capable of penetrating night and weather with a 1/10 meter resolution, providing near continuous targeting data for the PLA forces. In the arena of navigation and timing, China has five BeiDou satellites with 20 meter accuracy over

the region. The PRC also uses the Russian GLONASS navigation system and is a primary investor in the European Union's Galileo navigation system. China has developed small satellite design and production facilities, and is developing microsattelites, satellites which weigh less than 100 kilograms. These satellites offer remote sensing, imagery, and radar, and could allow China to rapidly replace or expand its satellite force in the event of war or a disruption to the network. The country is also improving its ability to track and identify foreign satellites, which is an essential component in the event of counter-space operations. China's successful test of an ASAT weapon demonstrates an ability to strike enemy assets in low earth orbit. This acts as a deterrent to conflict and demonstrates the PRC's commitment to relatively low-cost asymmetric warfare (International Assessment and Strategy Center 2005).

## **Second Artillery Corps**

The Second Artillery Corps (SAC) controls the PLA's nuclear and conventional missile forces. Weapons from the SAC are subsequently filtered to other branches of the PLA. Items such as the land attack cruise missile (LACM) may be used by the PLAAF on H-6 bombers, or by the PLAN on Type 093 nuclear submarines. China's total nuclear arsenal is estimated to be between 120 and 250. China maintains a "no first use" policy; however, the ambiguous nature of declaratory policies leave open the option for first strike if China's leaders believe their national security or the CPC are under threat.

China began developing nuclear weapons in the late 1950s with the help of Soviet assistance. After the Sino-Soviet split in the late 1950s, China continued its development on its own and made significant progress. The People's Republic detonated its first atomic bomb in 1964, making it the fifth state to do so, following the United States, Russia, the United Kingdom, and France. With the addition of India and Pakistan, and possibly Israel and North Korea, China remains only one of nine states with a nuclear capability. China launched its first nuclear missile in 1966, and detonated its first hydrogen bomb in 1967. Short-range ballistic missile (SRBM) capability was obtained with the development of the Dongfeng-1, medium-range ballistic missile (MRBM) capability with the Dongfeng-2, intermediate-range ballistic missile (IRBM) capability with the Dongfeng-3, and limited intercontinental ballistic missile (ICBM) capability with the Dongfeng-5 (Missile and Space Programme 2008; Second Artillery Corps 2000).

It is estimated that China has 24-36 liquid fuelled ICBMs capable of striking the US and approximately 100-150 IRBMs capable of striking Russia and Eastern Europe. China also possesses approximately 1,000 SRBMs with ranges between 300 and 600 km. Beijing is continually upgrading the range, accuracy, and payload capability of its SRBMs at a rate of 100 new missiles per year. Its most current missile, the Dongfeng-31A is a solid fuel ICBM with a range of 11,200km. It is road mobile, and has multiple independently targetable re-entry vehicles (MIRVs). As noted above, China possesses submarine-launched ballistic missiles (SLBMs) on its SSBN submarines. The PLAAF also has bombers capable of delivering nuclear bombs. However, they would be unlikely to break through the modern air defence systems of advanced military powers. The SAC has sought to improve its retaliatory strike capability by hardening missile silos, developing mobile launchers, and increasing range, accuracy, and response time of its missile system (Annual Report to Congress 2008; see also Wortzel 2007).

China's non-nuclear missile arsenal continues to develop anti-access/area denial capabilities. These include the land attack cruise missile (LACM) DH-10, the Russian SUNBURN anti-ship cruise missile (ASCM), the Russian SIZZLER supersonic ASCM, and indigenous versions of anti-ship missiles based on their own MRBMs. The acquisition of Russian arms demonstrates China's continued commitment to technology transfer and reverse engineering. Thus, "The DH-10 will be similar in size and capability to the U.S. TOMOHAWK, in part because the PLA has been collecting parts of this U.S. cruise missile from Iraq and Afghanistan. The PLA has obtained at least six Russian Kh-55 cruise missiles from the Ukraine, and reportedly, has benefited from Israeli cruise missile technology associated with the DELILAH anti-radar missile" (Moore 2000). Asymmetric warfare, another tendency of the PLA, is shown by its research into manoeuvring re-entry vehicles (MaRV), decoys, chaff, jamming, thermal shielding, and ASAT weapons that will strengthen deterrence and strike capabilities. Many of these technologies can also be used to defeat, deter, or stymie US attempts at a National Missile Defence shield. By examining the weapons and deployment of the SAC, China's perceived primary threats can be identified. The majority of the SAC's SRBMs are opposite Taiwan. DF-11 Mod 1s are capable of carrying thermobaric and cluster munitions as well as high-explosives. In addition, they may carry radio-frequency/electromagnetic pulse (EMP) warheads which, if used in sufficient numbers, could disable electronic communications and electric power networks (Annual Report to Congress 2008).

### **People's Armed Police**

The People's Armed Police (PAP) is no longer the official fifth service branch of the PLA; however it remains an integral part of Chinese defence. The line between military operations against foreign elements and operations of internal security are often blurred. This can be seen all the way down to the PAP uniforms which differ only slightly from PLAGF, often leading foreigners to mistake them as soldiers. In contrast, public security officers wear dark gray or blue uniforms more common among Western police forces. Much of the PAP force was absorbed directly from the PLA. They use a similar rank structure, and they obey the PLA's general regulations. PAP guards are also recruited at the same time and through the same procedures as PLA soldiers. The PAP has a dual command structure including the Central Military Commission (CMC) and the State Council through the Ministry of Public Security. By law the PAP is not part of the PLA; however, their interconnection is unavoidable, and the PAP will play an important role as domestic or non-military issues become intertwined with traditional military issues (People's Armed Police Force Organisation 2007; Tkacik 2007).

The PAP is a paramilitary force primarily responsible for law enforcement. China's National Defence White Paper, published in 2006, lists the total strength of the PAP at 660,000. The IISS Military Balance of 2008 lists an estimated 1.5 million (IISS 2008). The PAP has its origins in the PLA, which was originally tasked with both defending China from foreign threats and providing internal security. While the two share much in common, China eventually decided the differences were greater than the similarities. The PAP's primary mission is internal security. They are responsible for guarding government buildings at all levels, including party and state organisations, foreign embassies, consulates, and airports. The PAP provides personal protection to senior government officials, and performs security functions for major corporations and public events – including its much-publicized role in the 2008 Beijing Olympics (see Paramilitary Olympics 2008). Additionally, the PAP maintains multiple counter-terrorism units, sea and land border security forces, fire fighting units, and



has a role in the protection of forests, gold mines, hydroelectric facilities, and highway infrastructure. The secondary mission of the PAP is external defence, and in times of war PAP internal security units can act as light infantry supporting the PLA in local defence missions. Similarly, the PLA can fill in for the PAP and has done so during the Cultural Revolution, the Tiananmen Square incident, and flooding of the Yellow River (People's Armed Police Force Organisation 2007; China's National Defense in 2006; People's Armed Police 2005).

### **Military Intelligence**

The General Staff Department carries out staff and operational functions for the PLA and is responsible for implementing military modernization plans. It serves as the headquarters for the PLAGF and contains directorates for the PLAN, PLAAF, and SAC, as well as a department for electronic warfare. The General Staff Department also includes sub-departments for artillery, armoured units, communications, engineering, mobilization, operations, politics, training, and surveying. Direct control over the four military branches is sub-divided among the General Staff Department and regional commanders; however the General Staff Department can assume direct operation control at any time. The General Staff Department is under the control of the Central Military Commission (General Staff Department 1997).

The Second Department of the General Staff Headquarters is responsible for collecting military intelligence. This includes military attachés at Chinese embassies abroad, clandestine agents to conduct espionage, and the analysis of publicly available data published by foreign countries. The Second Department oversees military human intelligence (HUMINT), open source intelligence (OSINT), and satellite and aerial imagery intelligence (IMINT) which it disseminates to the Central Military Commission and various branches. The Second Department has increased its focus on scientific and technological military intelligence gathering. The Third Department of the General Staff Headquarters is responsible for monitoring the telecommunications of foreign militaries and producing reports based on the military information gathered. China operates the most extensive signals intelligence (SIGINT) network of all the countries in the Asia-Pacific region. Since the 1950s, the Second and Third Departments have maintained a number of secondary and higher learning institutions for producing recruits, particularly in foreign languages. The Third Department not only intercepts communication of foreign militaries, but also those of the PLA, thereby maintaining control and supervision over the different branches and commanders within all of the military regions (Second Intelligence Department 2005, General Staff Department 1997).

Other branches of the General Staff Department include the Fourth Department and the General Political Department (GPD). The Fourth Department (ECM and Radar) is responsible for electronic intelligence (ELINT) including electronic countermeasures and maintaining databases on electronic signals. The GPD is responsible for overseeing the political education required for advancement within the PLA and controls the PLA's internal prison system. The International Liaison Department, a branch within the GPD, conducts propaganda, psychological operations (PSYOPS), and counter-espionage against foreign intelligence. As with the PAP, many of the departments within the General Staff Department appear to have significant overlap. The structural details are beyond the scope of this study; however, they are worth noting, as they pertain to the discussion below of cyber warfare.

## **Technology Transfer**

China continues to pursue the acquisition of foreign military technology. Beijing is in ongoing negotiations with Moscow to obtain multiple weapons systems, and in 2007 signed arms agreements worth \$150 million. Israel has previously supplied advanced military technology to China. However, under pressure from the US, Israel began to implement strict military export regulations. China is attempting to remove an embargo placed on lethal military export from the EU. This embargo was a response to the Tiananmen Square incident. Opinion on removing the embargo remains divided among EU member states. According to the 2008 Annual Report to Congress on China's Military:

China continues a systematic effort to obtain dual-use and military technologies from abroad through legal and illegal commercial transactions. Many dual-use technologies, such as software, integrated circuits, computers, electronics, semiconductors, telecommunications, and information security systems, are vital for the PLA's transformation into an information-based, network-enabled force.

Between 1995 and 2008, several high profile cases of Chinese espionage against the US surfaced. These attempts targeted aerospace programs, space shuttle design, F-16 design, submarine propulsion, C4ISR data, high-performance computers, nuclear weapons design, cruise missile data, semiconductors, integrated circuit design, and details of US arms sales to Taiwan. Targeted organisations include Northrop Grumman, NASA, Los Alamos Laboratories, Boeing, Lockheed Martin, Sun Microsystems, and various defence installations. The Chinese do not limit themselves to high value targets or an elite group of agents. They obtain any data which may be of value, including legally obtained documents or OSINT, which may help them piece together the larger picture. China utilizes a decentralized network of students, business people, scientists, diplomats, and engineers from within the Chinese Diaspora. The majority of these individuals have legitimate purposes within the host state; however they are recruited at a later date, or asked for small pieces of information or favours which can seem harmless in scope to the individual. Attempts are also made to purchase interests within high technology companies, as well as win political favour with government officials. For example, there have been repeated allegations that President Bill Clinton's decision to sell sophisticated computer and satellite technology to China was influenced by campaign contributions (Appel 2004; Cooper 2006; Grier 2005; Jordan 2008; Warrick and Johnson 2008; Lynch 2007; Cox Report 1999; McLaughlin 1999; PRC Acquisitions of US Technology 1998).

China's use of espionage to obtain foreign military technology is not restricted to the US. In 2007, the head of a Russian rocket and space technology company was sentenced to 11 years for passing sensitive information to China. An alleged agent who defected in Belgium claimed hundreds of Chinese spies were working within Europe's industries. These allegations coincided with an arrest in France for illegal database intrusion of the automotive components manufacturer Valeo, and a guest researcher in Sweden arrested for stealing unpublished and unpatented research. Further, Chinese diplomat Chen Yonglin defected to Australia in 2005, claiming there were over 1,000 Chinese secret agents and informants within Australia (Luard 2005; Isachenkov 2007). Espionage and technology transfer prosper in cyber warfare, where being physically present is not required, and attribution becomes increasingly difficult. It also falls in line with China's strategy of leapfrogging. By acquiring foreign military knowledge, China can quickly catch up and begin working at a comparable level, rather than investing the large amounts of time and effort it would take to acquire this knowledge independently.

## Doctrine/Strategy

Chinese military doctrine and strategy remain focused on modernization. Beijing has not explicitly laid out an official grand strategy. This may be due to disagreement within the government, or done intentionally to hide true motives and avoid being bound by them. Much of the writings published by the PRC are contradictory or ambiguous, using modern and ancient foundations, while being disseminated by varied sources. However, several points which are continually emphasized may point to a general consensus. These include modernization of weapons, equipment and training; accelerating the RMA; improving education and training of the PLA and the CPC; “informationized” (*xinxihua*) warfare; and scientific development. China seeks to maintain domestic and regional stability while developing its economic, military, technologic, scientific, and soft power. It also seeks a balance between military and economic development, believing they are mutually dependant. Beijing maintains its One China Policy in relation to Taiwan, and claims sovereignty over the Parcel and Spratly islands and adjacent waterways (China's National Defense 2006).

Deng Xiaoping, representing second generation leadership after Mao, sought to avoid international responsibilities and limitations, as they could slow down development of the military and economy. The third generation leadership of Jiang Zemin did look outward, promoting a multipolar world in the face of the post-Cold War unipolarity under the US, just as fourth generation leader Hu Jintao promoted the ideology of a Harmonious World (*hexie shijie*) which places more emphasis on international relations (Lam 2004; Zheng and Tok 2007). However the PRC continues to avoid concrete stances through concepts of non-interference, diversity, and equality. It compares itself to other states through Comprehensive National Power (CNP - *zonghe guoli*), using qualitative and quantitative values, and not accepting traditional Western categorizations (see Pillsbury 2000). For example, China includes the economy, soft power, and domestic stability as factors of CNP. This is important, because it shows a correlativity which holds relevance for cyber warfare. Under CNP the economy, soft power, and domestic stability can be seen as military matters. Further, maintaining the status quo in regards to Taiwan and the Spratly islands may not be China's long-term intention, but rather a way to stall efforts while it builds up military strength, strength which can include economic and international influence.

Despite not wanting to become embroiled in concrete commitments to military strategy, Chinese leaders cannot ignore the interconnectedness of the modern world, and they have realized the necessity of international cooperation. For example, the need for resources has fuelled China's global presence. The PRC is the world's second largest importer of petroleum. As the country's economy grows and the middle class expands, the demand for fossil fuel resources will continue to grow. This creates a need for sound international relations with exporting nations and the need for securing transportation routes, such as the Strait of Malacca and the South China Sea. These are intertwined with the politics and military affairs of the states involved. Competition with the US for these resources has often led to China making agreements with nations the US opposes on several points, such as Angola, Chad, Egypt, Indonesia, Iran, Kazakhstan, Nigeria, Oman, Saudi Arabia, Sudan, Venezuela, and Yemen (Hanson 2008; Brookes 2006).

Beijing may be using these countries simply because there is less competition for resource access in the case of these suppliers. However, the result is often international criticism of China as these states may be violating human rights or supporting terrorism. Moreover,

Beijing's methods of befriending these exporters comes into question, especially in regards to arms being traded or availability of finance which may be supporting controversial policies. China currently lacks the power projection to protect critical sea lanes from disruption or to deter international criticism. Crucial to extended power projection is the blue water navy which would benefit from online technology transfer and the further development of C4ISR. Online PSYOPS and media warfare would enhance China's soft power. Beijing believes that economic growth is critical to military development; economic growth creates a greater energy demand, which in turns creates a greater military demand, thus the two form a positive feedback loop (Ikenberry 2008; China's National Defense in 2006).

While Beijing recognizes the need for international cooperation, it remains cautious. The country suffered greatly from foreign incursions within the last century. Colonialism by Western powers, Japanese occupation in World War II, the Korean War, the Vietnam War, and border conflicts with India, the Soviet Union, and Vietnam are all kept fresh through China's historical discourse. Despite China's long history, these events are of special note as they are within living memory, and these events were present during the founding and duration of the CPC's rule.

Ensuring the survival of the CPC shapes China's strategic outlook. In order to bolster domestic support for policies, nationalism has been emphasized over communist ideology. This can be seen with government organised protests against Japan over visits by Japanese leaders to WWII war shrines and protests against the publishing of Japanese school text books which downplay Japan's atrocities against the Chinese. These protests often coincide with other strategic interests, such as territorial disputes in the East China Sea, which are often unbeknownst to the casual observer or participant. The mobilization of nationalism can also be seen during the holding of a US reconnaissance plane in 2001, and the mistaken bombing of the Chinese Embassy in Belgrade in 1999. The 2008 Olympics further demonstrated how China could garner national support in the face of a widening wealth gap, forced relocation, corruption, and environmental degradation. These events demonstrate a strategic value in public manipulation through nationalism; one that is interconnected with military affairs, and one which is increasingly turning to online assets (see Faiola 2005).

Several conclusions can be drawn from the status of the PLA. China is committed to modernizing its military, primarily through the purchase or illicit acquisition of foreign technology and subsequently reverse engineering that technology so it can be produced domestically. The PLA has placed an importance on trimming down its size, favouring quality over quantity. The PLA's weaponry often lags one or two generations behind that of Western military powers. However, the total force base still poses a significant deterrent, and establishes China as a dominant power within the Asia-Pacific Region. China lacks force projection beyond its region, primarily do to the lack of a blue water navy and aircraft carrier fleet, but also due to limits in missile technology and air-defence penetration, and opposition by foreign powers such as the United States. China seeks to become self-sufficient in many of these key capabilities. Once they have leapfrogged and are no longer trying to catch up, the Chinese will no longer need such widescale technology transfer, and they will possess the might to shape the international system, rather than be bound by one that was created by foreign powers.

## **2. A New Era**

History has demonstrated that the advantage often goes to those who develop a technology first. The great naval voyages of Ming admiral Zhang He were unprecedented for their time and helped establish China as a suzerain of the wider Asian region. However, the mid-15th century saw China retreat to xenophobic and isolationist policies that paved the way towards China's decline and opened the door for colonialism (see Dick 2006). This lesson has not been lost among Chinese officials, and it is often used to spur initiatives such as their stated desire to be the first to mine the moon for helium-3 (China's Space Program 2005). The information revolution has given more power to individuals and increased globalization through the interconnectedness of economies, rapid dissemination of news, and improved access to communication and information of all types. Any attempt to compete on a global level without the use of these technologies would place the PRC at a significant military and financial disadvantage. For this reason, the benefits of electronic reliance outweigh the risks involved. Further, it is impossible for a state to develop a defence against cyber warfare without simultaneously learning how to execute attacks themselves.

The US is the sole superpower, making it a benchmark for military competitiveness. Beijing also views the US as a potential adversary, in particular due to perceptions of the US military attempting to encircle China with bases in nearby states and opposition to China's modernization goals, to concerns over any forceful application of the One China Policy, and to concerns over a range of internal affairs issues. China seeks to learn from US mistakes and successes, using American expertise and field-tested military experience to accelerate China's development. The People's Republic also focuses on weaknesses in the US military in order to improve upon the American example and to expose asymmetric advantages. For these reasons it is important to examine where the US is headed in military thinking and development, as China is likely to follow (Derene 2008; Lasker 2005; Liang Xiangsui 1999).

### **Network-Centric Warfare**

The US has viewed the internet as a potential tool of warfare since its inception. Arpanet, a precursor of modern internet, was heavily funded by the US military, with a particular emphasis on its research collaboration benefits. Despite fears of cyber terrorism post 9/11, the US continues to place increasing reliance on the internet as a security tool. This can be seen in the restructuring of US intelligence agencies and the creation of new online exchange such as Intellipedia and A-Space (Shaughnessy 2008; Magnuson 2006). Militarily, the information revolution has given rise to an increasing reliance on situational awareness, weather monitoring, surveillance, communication, and precision strikes. Chinese military strategists have made special note of the US reliance on, and dominance with, electronic means in the Kosovo, Afghanistan, and Iraqi conflicts (Tellis 2007; Center for Strategic and International Studies 2003; Liang and Xiangsui 1999).

Since the 1990s the US has put emphasis on developing network-centric warfare (NCW). NCW seeks to translate an information advantage, enabled in part by information technology, into a military advantage through the networking of well informed, geographically-dispersed forces. Originally described as a system of systems, it includes intelligence sensors, command and control systems, and precision weapons that enable enhanced situational awareness, rapid target assessment, and distributed weapon assignment. In essence, NCW translates to information superiority, which requires the reduction of hard categorization, because compartmentalizing military branches can stem the flow of information. In 2001, the

Pentagon began investing in peer-to-peer software as a means to spread information while supplying redundancy and robustness. The US Department of Defense has sought the creation of the Global Information Grid (GIG) as a backbone of NCW. All advanced weapons platforms, sensor systems, and command and control centres are eventually to be linked via the GIG. Collecting, processing, storing, disseminating, and managing classified security information on demand will be made globally available to soldiers, policymakers, and support personnel to achieve information superiority (Alberts 2002; Alberts, Garstka, and Stein 2000).

Vice President Richard Cheney stated in 2004:

With less than half of the ground forces and two-thirds of the military aircraft used 12 years ago in Desert Storm, we have achieved a far more difficult objective . . . . In Desert Storm, it usually took up to two days for target planners to get a photo of a target, confirm its coordinates, plan the mission, and deliver it to the bomber crew. Now we have near real-time imaging of targets with photos and coordinates transmitted by e-mail to aircraft already in flight. In Desert Storm, battalion, brigade, and division commanders had to rely on maps, grease pencils, and radio reports to track the movements of our forces. Today, our commanders have a real-time display of our armed forces on their computer screen (Raduege 2004).

### **Information Operations**

In 2003, under the direction of former Secretary of Defense Donald Rumsfeld, the US expanded on NCW in a document titled the *Information Operations Roadmap*. Now declassified, it was obtained under the Freedom of Information Act by George Washington University's National Security Archive. Information Operations (IO) calls for NCW to become a core military branch along with the Army, Navy, Air Force, Intelligence, and Space. To accomplish this it requires the development of a comprehensive education program to enlist new recruits, and an overhaul of the organizational structure of current military branches in an attempt to break down barriers that hinder information exchange and progress. IO activities include PSYOPS troops who try to manipulate the adversary's thoughts and beliefs, military deception and disinformation, media warfare, electronic warfare (EW), and computer network operations (CNO). Thus Information Operations Roadmap stands as another example of the US commitment to transform military capabilities to keep pace with emerging threats and to exploit new opportunities afforded by innovation and rapidly developing information technologies.

IO seeks to "dominate the electromagnetic spectrum", in an attempt to "deny, degrade, disrupt, or destroy a broad range of adversary threats, sensors, command and control and critical support infrastructures" (Information Operations Roadmap 2003). The document notes that PSYOPS and manipulating the thoughts of populations through media and internet require constant observation during peacetime, otherwise in the event of conflict, a state would not be sufficiently engrained into the information culture to utilize them fully. This can be seen with the emergence of patriotic hackers, the advancement of social media, and the rapid evolution of memetics, slang, and subcultures, all of which will be discussed further below (List of Internet Phenomenon 2008; Pang 2008; Slashdot Subculture 2008; Slashdot Trolling Phenomenon 2008). IO includes defence, attack, and reconnaissance as vital components (Information Operations Roadmap 2003).

IO seeks to put out a political message in coordination with any traditional military assault. It places an emphasis on finding, and clandestinely promoting, favourable media from third

parties, so as to appear more credible. IO also seeks to establish a legal framework to defend against cyber attacks and cyber reconnaissance, as well as establish rules of engagement for conducting cyber attack. For example, how much certainty is required in identifying the source of an attack before responding? If an attack is being routed through multiple computers, is it acceptable to attack the intermediary computer? This would halt the attack but it would harm or destroy a computer which may have been infected without the owner's knowledge or consent. Additionally, an intangible computer attack can result in significant tangible loss, but does this warrant the use of traditional military weapons as a response?

### **Future Combat Systems**

Another US project that is gaining attention and closely resembles NCW and IO is Future Combat Systems (FCS). FCS places a particular emphasis on advanced robotics, including Unmanned Ground Vehicles (UGVs), Unmanned Aerial Combat Vehicles (UCAVs), Non-Line of Sight Launch Systems, and Unattended Systems. This system of systems seeks to make warfare as networked as the internet, as mobile as a mobile phone, and as intuitive as a video game. The highly interconnected nature of FCS can even be seen in its development, utilizing 550 contractors in 41 US states. While the US has yet to determine a definitive name for this new type of information based, highly networked, and highly technological warfare, it is clear that the US government has spent a significant amount of time and money seeking to make it a reality. US Army officials have already stated that they intent to change FCS's name, because they believe the name is inappropriate, stating 'the future is now' (FCS Watch 2008; Future Combat Systems 2008; Baard 2007; Klein 2007; Gannon 2001).

Some of the complex logistical problems inherent in such an undertaking include: finance allocation, giving the approval for use to commanders, inter-agency cooperation, a common vernacular, rules of engagement, and adhering to the program's stated goals. The US is continually modernizing its cyber force, creating new hacker units, conducting cyber war exercises, and diversifying and limiting the number of access points that could be used for an attack (Waterman 2008; Greenberg 2007). And the US is not alone, 'more than 120 countries already have or are developing such computer attack capabilities' (GOA 1996). Information warfare is being adopted by all modern nations and competition is mounting.

### **Informationization**

China's 2006 white paper on national defence places an emphasis on the informationization of the military. "Informationization" (*xinxihua*) means improving the PLA's ability to use the latest technologies in command, intelligence, training, and weapon systems. New automatic command systems linked by fibre-optic internet, satellite and new high-frequency digital radio systems, allow for more efficient joint-service planning and command, while also enabling a reduction in layers of command. The PLA's move towards information technology can be seen with the use of new space-based surveillance and intelligence gathering systems, ASATs, anti-radar, infrared decoys, and false target generators. PLA soldiers are using decision simulators, a low-light automatic tracking system for helicopters, and a battlefield artillery/mortar fuse jamming system derived from Russian technology. OSINT on China's military continually makes note of informationization and the related, if not identical, fields of cyber warfare, information warfare, CNO, and EW. "Priority is given to R&D of new and high-tech weaponry and equipment, and endeavours to achieve breakthroughs in a number of key technologies and leapfrogging technological progress, thus speeding up weaponry and equipment modernization" (China's National Defense 2006).

Informationization includes increased education of soldiers in cyber warfare and NCW, a reorganization of military branches and command system, and integrating joint operations. The PLA is improving the information network for military training, and has built more virtual laboratories, digital libraries and digital campuses to provide distance learning and online teaching and training. University courses have emerged for cyber attack and defence, a study of hacker methods, computer virus design and application, and network security protocols (Annual Report to Congress 2008). Following the Russian example, China is engaging in the debate of defining cyber warfare, in part through the Shanghai Cooperation Organization, in order to have a hand in the shaping of a legal framework and rules of engagement related to this new warfare. The PLA is pursuing a comprehensive transformation from a mass army designed for protracted wars of attrition on its territory to one capable of fighting and winning short duration, high intensity conflicts along its periphery against high-tech adversaries (Annual Report to Congress 2008) – an approach that China refers to as preparing for “local wars under conditions of informationization” (China's National Defense 2006).

### **Exponential Growth and Unrestricted Warfare**

One view on twentieth century patterns of unrestricted warfare has noted:

The names Watt and Edison are nearly synonymous with great technical inventions, and using these great technological masters to name their age may be said to be reasonable. However, from then on, the situation changed, and the countless and varied technological discoveries of the past 100 years or so makes it difficult for the appearance of any new technology to take on any self importance in the realm of human life. While it may be said that the formulations of “the age of the steam engine” and “the age of electrification” can be said to be names which reflect the realities of the time, today, with all kinds of new technology continuously beating against the banks of the age so that people scarcely have the time to accord them brief acclaim while being overwhelmed by an even higher and newer wave of technology, the age in which an era could be named for a single new technology or a single inventor has become a thing of the past. This is the reason why, if one calls the current era the “nuclear age” or the “information age,” it will still give people the impression that you are using one aspect to typify the whole situation. (Qiao Liang & Wang Xiangsui 1999).

It is important to stop for a moment and ponder the rapid advancement in military weaponry. New weaponry and concepts are easily dismissed as science fiction, yet the integration of mobile phones and the internet in 2008 would resemble science fiction to someone in the 1980s. Reports of research and development may be noted momentarily before being subsumed in a busy, informationally-competitive world. For the purpose of this study, it is useful to acknowledge them in passing as they show the rapid advancement in science and technology, where military weapons are headed, and the increasing complexity and cooperation involved in their development and use. Current militarily-applicable science and technology, under development or already in use, include: augmented reality (Bonsor 2008); biotechnology; genetics; giving soldiers internal/biologic infrared, night vision, radar, and sonar capability (Block 2006); GPS; force fields (Hershkovitch 1998); invisibility cloaks (Mark 2008; Winkler 2003); microwave guns (Beam It Right There Scotty 2005); nanotechnology; neuroscience; positron bombs (Davidson 2004); robotic exoskeletons (Berkeley Bionics Human Exoskeleton 2007; Yeates 2007); space-based weapons such as ANGELS (Lewis 2005) and Rods from God (Adams 2004); telepathy (Braukus 2004; Put Your Mobile Where Your Mouth Is 2002); thought control of internet surfing and electronic



devices (New Technology Operated by Thought 2007); unmanned ground combat vehicles (Bloom 2008); and unmanned combat aerial vehicles (Pike 2008).

Adding further to this complexity, *Unrestricted Warfare*, a book by two PLA senior colonels, Qiao Liang and Wang Xiangsui, claims that warfare is no longer strictly a military operation, and that the battlefield no longer has boundaries. *Unrestricted Warfare* was published by the PLA Literature and Arts Publishing House in Beijing in February 1999. According to the FBIS translation editor, the book 'was endorsed by at least some elements of the PLA leadership' and an interview with one of the authors was published in the CPC Youth League's official daily newspaper on June 28, 1999. Thus while the book is not entirely backed by the PLA, especially the older generation, like the 'half empty, half full' glass analogy, it does have some official backing and hence a degree of legitimacy as a document assisting analysis as to where the PLA is headed and how asymmetric tactics against a superior hi-tech military might be employed.

Environmental concerns, human rights in regard to weapons of mass destruction, and the increasingly intertwined economies and political structures of globalization all have an impact on modern warfare. Sheer might of weaponry can no longer guarantee victory under these conditions. US extravagance in weaponry has been shown to stymie in the face of guerrilla warfare in Vietnam and Iraq. Under limited warfare, asymmetric warfare has seen a resurgence in use and value. Terrorist groups such as Al Qaeda employ guerrilla tactics and make use of the internet and financial institutions to subvert traditional warfare (Levinson 2008; Yassin 2008). No single weapon can deliver a decisive victory, and weapons have been replaced by weapons systems. For example, the patriot missile relies on multiple technologies working in concert, from satellites to the missile itself, with data being relayed around the world. Modern militaries have become reliant on electronic sophistication. The authors of *Unrestricted Warfare* assert that war has not disappeared, but its appearance has changed and its complexity has increased (Qiao and Wang 1999).

### **Non-Traditional Threats**

Increasing interdependence among states has increased the danger of non-traditional security threats, including the spread of disease, environmental damage, international terrorist groups, international crime, acquisition and transportation of energy and resources, natural disasters, and intertwined economies that can have an impact on social and political issues. For example, modern transportation has made it possible for criminals to traverse the globe with relative ease. The internet allows them to transfer or hide money across the globe and to covertly communicate beyond the jurisdiction of their enemies. Natural disasters or communicable diseases are no longer something which can be kept quiet as information radiates out through global media, causing damage to soft power factors, tourism, business, and international scrutiny (China's National Defense in 2006).

The line between military and non-military, soldier and civilian, is being blurred. Terrorism is the most common example: the 2001 plane hijackings in the US, the Madrid train bombings in 2004, and the London bombings in 2005 to name just a few key examples. These lack an easily identifiable enemy to target, they cross territorial boundaries and use asymmetric attacks. Further blurring the line are the Sarin gas attacks on the Tokyo subway by disciples of the Aum Shinri Kyo, the actions of currency speculators in relation to the East Asian financial crisis, drug cartels, the mafia, media moguls who can influence the opinion of a mass audience, or industrial polluters who affect the economy and health of their

neighbours. These events can cause damage and disruption equal to war, but there is no foreign military or state against which to go to war. The individuals involved may be from multiple states and acting without government sponsorship.

Another form of non-traditional threat comes from hackers. Hackers tend not to have military training, they may or may not have a political agenda, and they are capable of causing massive damage with nothing more than an off-the-shelf computer and an internet connection. For example, two British teenagers were able to access files on ballistic weapons research of the US. They then took control of US air force computers and proceeded to intrude into other military and government installations, making it appear as though the US military was hacking other states (Hacking U.S. Government Computers from Overseas 2001). The rapid advancements in technology and globalization are opening new and complex ways to subvert security. In 2008, a group of 11 people managed to steal 45 million users' bank and credit card details, resulting in a loss of more than \$256 million. The group members were from diverse, yet cyber-advanced, geographical locations, including: Belarus, Estonia, China, Ukraine, and the US. Their unprecedented feat was accomplished by sitting outside of TJX retail stores and hacking into the store's wireless network. This illustrates asymmetry, emerging technology security risks, globalization, and the enhanced vulnerability of commercial targets as opposed to direct military targets (Malone 2008; Almeida 2006).

### **Combination**

To be militarily successful in this new era will require the ability to combine operations. Combining weapons has been used throughout military history. Horses, armour, stirrups, and swords are not as effective when used individually. Their combination can create synergy, where the combined strength is greater than the individual parts. During the Gulf War, the US combined the old A-10 ground attack aircraft with the new Apache helicopter to create a "lethal union" (Qiao and Wang 1999). By dropping leaflets and publicizing video of precision strike weaponry, the US combined PSYOPS and media warfare as well. The US has pursued additional combinations of traditional and non-traditional attack methods. During the 1979 Iran Hostage Crisis, the US initially tried traditional military force, but when this attempt failed they froze Iran's foreign assets, imposed an arms embargo, supported Iraq with weaponry and training, and began diplomatic negotiations. When all these channels were used together, the crisis finally came to an end. The Americans have also employed non-traditional attacks against non-traditional enemies. For example, they used hacking methods to search for and cut off the bank accounts of Osama Bin Laden in various states (Musharbash 2008; Vallence 2008).

China has demonstrated its commitment to such combinations. It seeks to develop military modernization and economic growth in tandem, with an emphasis on science and technology. China's 2006 defence white paper puts forth a goal to "work for close coordination between military struggle and political, economic, diplomatic, cultural and legal endeavours", using "strategies and tactics in a comprehensive way. . ." Also noted is the importance of taking part in international organizations, such as ASEAN+Three, the Shanghai Cooperation Organization, WTO, IMF, and the International Olympic Committee. These open up diplomacy, aid in soft power, and give China a voice in determining the legal framework of a globalized world (Ikenberry 2008; China's National Defense in 2006).

To learn how to conduct cyber security, the Chinese must have a full understanding of how attacks are conducted; therefore they will learn offence along with the defence - the two are

inseparable. China has repeatedly stated its goal of military modernization, and cyber warfare is where modern militaries are headed. However, cyber warfare would unlikely be used alone. It could be used simultaneously with a traditional attack, perhaps as a first blow to take an opponent off guard, or in tandem with multiple non-traditional attacks, such as PSYOPS and economic operations, or variants of each. Additional combined tactics that will be discussed in the following sections include cyber attack, cyber reconnaissance, and market dominance.

### **Internal Security**

As seen with the lack of division between the PLA and PAP, the Chinese defence white paper's stated goal of developing the military and economy in tandem, and with the blurring of lines in Unrestricted Warfare, China cannot ignore the full spectrum of impact that Information Communication Technologies (ICT) will have, including that within its borders. China's internet population has risen to 210 million people (Anick 2008; Bridis 2008). And, as of 2007, China possessed over 500 million mobile phones. China has become a world leader in the communications industry, and 3G and 4G technology are increasing the ability for mobile phones to supplant a personal computer for online activities. On the one hand ICT supports economic, scientific, and technology development; on the other it creates a non-traditional security threat.

Social networking services can be used as a tool to further nationalistic goals. These goals may include the spread of political ideology, propaganda, and disinformation. As seen with the US Information Operations Roadmap, PSYOPS are an integral component of cyber warfare. Operatives can sway audiences by presenting well thought out arguments or by altering opposing views; they may also manipulate democratized news by artificially inflating votes using scripts (Cuban 2008). Recent informationization military courses offered at Wuhan University include "An introduction to US and Taiwanese social information systems" suggesting that China has already recognized the benefits of utilizing social networking externally (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008).

Additionally, online users are increasingly volunteering to enter large amounts of personal data, which can, and has been, used for prosecutions (Use of Social Network Websites in Investigations 2008; WFTV 2008; Layer 8 2007). Users do so to enjoy the social service it provides, either not realizing, or unconcerned, that the government is simultaneously gaining access to a self-imposed Big Brother. Not only can China use this information to its benefit, but also it must secure it from being used by an adversary, such as its use for identifying potential espionage and subversive assets. In terms of stemming anti-government agendas, state agencies censor blogs, bulletin boards, email, and forums. Internet Service Providers (ISPs) often take it upon themselves to censor users, because they are held legally responsible for any customer who violates the law. Internet cafés are required to keep detailed records of their customers. In addition, "every Chinese person who signs up for internet service must register with his or her local police department within 30 days" (China and Internet Censorship 2006).

As China's economy continues to grow, personal electronic devices are becoming more accessible to Chinese citizens. Products such as personal computers, high speed internet connections, mp3 players, large hard drives for storage, gaming systems, and advanced mobile phones fuel a desire for more software and entertainment. This will enhance

international criticism of Chinese copyright infringements *and* it will make it difficult for China to prevent the spread of Western culture (French 2006; People's Daily Online 2006; Pirates of the Orient 2006). Increased connectivity also increases the capability of people to conduct subversive activities that endanger state security. This may include, "Signing online petitions, calling for reform and an end to corruption, planning to set up a pro-democracy party, publishing rumours about SARS, communicating with groups abroad, opposing the persecution of the Falun Gong and calling for a review of the 1989 crackdown on the democracy protests . . ." (Kumar 2006). Other emerging non-traditional threats include mob mentality, consumer price manipulation, domestic hacker groups who can damage and interfere with the Chinese government or drag it into conflict with other states, and the security of the identity and financial details of a growing online consumer market (Delio 2001).

In addition to China's economy being directly linked to military issues, so too are domestic threats, soft power, and the control of information. Readily available free web sources, such as blogs, photo uploading, video uploading, Podcasts, torrents, and RSS feeds, have given powers to individuals that were once restricted to large media outlets. Social networking sites allow for the spread of this information across the globe at speeds exceeding traditional mass media, and they are capable of reaching larger markets. These social networking services, often referred to as Web 2.0, are noted for their ability for people to collaborate and share information online, particularly emphasizing real-time dynamic displays, interconnectedness, and being a part of a larger community. China maintains strict government control over television, newspapers, and radio; therefore these new forms of distribution pose a threat to China's control. Censorship of the internet by China, known as the Great Firewall, can be seen in the banning of foreign sites, such as Blogger and Voice of America, as well as a wide range of search terms and images the government deems a threat to national security or counter-productive to the political party. During the 2007 uprising in Tibet, China blocked access to the video website YouTube (Richards 2008), and on multiple occasions it has been accused of using Photoshop to digitally alter photos in its favour (Pasternack 2008; Yue 2008). With the increasing popularity and economic success of Web 2.0, coupled with China's global presence (prestige and international scrutiny) it is unlikely that the Chinese government will ban these new forms of news distribution on a permanent basis. However, it will seek to understand and entrench itself within the emerging system.

China has struggled to cope with internal and external cyber dissidents. This includes pro-democracy movements and the dissemination of sensitive information such as the spread of SARS and human rights abuses. Pro-democracy activists Li Yibing and Jiang Lijun of Hong Kong used virtual dead drops to secretly pass messages, such as a plot to "disrupt the 16th Communist Party Congress by phoning the police with a false bomb alert" (Reporters Without Borders 2006). Each member knew the user name and password to a single email account. They would save messages as drafts, allowing the other member to log in and read it at a later point. This avoided detection, because no message was ever sent. This represents an asymmetric advantage provided by new technology; however China demonstrated its prowess in using the same technology to combat the cyber-dissidents by using international cooperation, internet laws, and online eavesdropping. Activists can use the internet to build coalitions, create e-petitions, and organize protests, using elements such as maps, lookouts, and live broadcasts. Foreign bloggers using commercially available satellite imagery have compromised Chinese military secrets on numerous occasions. These non-governmental bloggers have uncovered a Chinese site used for developing submarine technology, a training facility used to prepare for a potential conflict with India, and the construction of a fourth

satellite and missile launch facility in Hainan (Reporters Without Borders 2006; Yahoo implicated in third cyberdissident trial 2006).

Determined Chinese internet users are finding ways around The Great Firewall. One popular way is to use proxy relays. A proxy server acts as an intermediate; it allows them to access banned sites through servers that are based abroad. Other techniques include using specifically designed software, circumventors, tunnelling, encryption, and cached pages. Several foreign organizations have voluntarily taken on the task of circumventing China's censorship and making this information public. Among the groups that may have breached The Great Firewall are the University of Cambridge, the University of Toronto, M.I.T., underground hackers (presumably doing it just for the challenge), and groups formed by Chinese defectors. Software such as Dynapass, Ultrasurf, Freegate and Garden Networks are used by approximately 100,000 people in China to gain access to news and information that is blocked by the firewall. With the increasing interconnectivity of modern times, China must actively defend against these internal threats or risk having collateral damage to the military, soft power, economy, and political integrity (China Tightens Vice on Internet 2006).

Despite some drawbacks, it is in China's best interest to promote the growth of the internet as it will boost the economy, improve education, and keep the nation competitive in the 21<sup>st</sup> century. New freedoms for expressing political opinion will be counterbalanced by new means of censorship and means to reduce a widening digital and social divide. The Chinese government must be moderate in its approach to censorship and the digital divide or it runs the risk of widespread dissent resulting from increasing socio-economic/rural-urban disparities. The impact of the internet on China's near future will be one of expanded growth, a complex interaction of balances, and a constant adaptation to evolving technologies from within pre-established ideologies. The following sections will further demonstrate how the average internet user is becoming intertwined with military activity.

### **3. Cyber Reconnaissance and Attack**

NCW, IO, FCS, and Informationization are not identical to cyber attack and cyber reconnaissance; however they significantly overlap. The first four, discussed above, tend to deal with the hi-tech advancement of traditional military assets, PSYOPS, and media warfare – all of which rely on the internet in some form. The lexicon is continuing to develop, having at times included the terms: total dimensional warfare, expeditionary forces, command and control warfare, information warfare, full spectrum dominance, and electronic warfare. Cyber attack may be thought of as hacking with the intent to destroy or disrupt. This could include the physical destruction of a computer, deleting/re-writing of files, or knocking a network or service offline. Cyber reconnaissance is the collection of data, also known as cyber espionage or network intrusion. This may include technology transfer or intelligence, such as troop locations or weaknesses that could be used in an attack. In many cases a hacker goes from reconnaissance to attack at will. Here all six will be addressed – NCW, IO, FCS, Informationization, Cyber Attack, and Cyber Reconnaissance - as components of cyber warfare (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008).

This section will examine cyber reconnaissance with an emphasis on Chinese examples and military applications. In addition to China's stated goal of informationization and the quasi-officially endorsed book, *Unrestricted Warfare*, this section will show that foreign allegations

and widespread network intrusions suggest China is developing a cyber warfare capability. Cyber warfare fits with China's established patterns of asymmetry and technology transfer. In order to grasp why Beijing would pursue cyber warfare as a means of leapfrogging, it is essential to acknowledge the skills of hacking. Hackers utilize a wide range of tools with highly sophisticated techniques, the scope of which is beyond this article; however some basic understanding is necessary. Hacking is capable of causing massive damage with little funding, it is difficult to detect and defend against, it provides a high level of deniability, and it eliminates the problem of geographical distance.

### **Security Hacking**

A common method used in cyber reconnaissance and attack is the security exploit. A security exploit is a prepared application that takes advantage of a known weakness. It is a piece of software, data, or commands that utilize a bug, glitch, or vulnerability to cause an unintended or unanticipated behaviour to occur on computer software, hardware, or electronic devices. This can allow the attacker to take control of the computer, permitting its use for other tactics, such as DDoS discussed below. An exploit may be used to gain low-level entrance to a computer, after which a hacker can search for further exploits to attain high-level access such as system administrator (root). This tactic is known as privilege escalation. Once exploit vulnerability has been identified by security experts, a patch will be issued. For this reason hackers try to keep known exploits secret. These are known as zero day exploits, and hackers may catalogue large numbers of them for their own use or to be sold on the black market (Hines 2008). In 2006, Taiwan was hit with "13 PLA zero-day attacks", for which it took Microsoft 178 days to develop patches (Tkacik 2007).

Vulnerability scanners may be used to identify exploits. One such scanner known as a port scanner automates the process of finding weaknesses of computers on a network. These check to see which ports on a specified computer are 'open', available to access, and sometimes will detect what program or service is listening on that port. Turning from reconnaissance to attack, once an open port is found, large quantities of data can be sent in an attempt to cause a buffer overflow. This can cause exposure of data, memory loss, and/or a crash within the compromised system.

The primary means to identify computers used in cyber warfare is the IP address. An IP address is a numerical identification that network management assigns to devices participating in a computer network utilizing the Internet Protocol (TCP/IP) for communication between nodes. In essence, each computer has its own unique IP address. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for global IP address allocation. ICANN, a non-profit organisation operating in the US, is under contract with US Department of Commerce and previously with US Department of Defense. Despite this identification tool, hackers can mask their identity by using proxy servers. Information is routed through multiple computers, only showing each computer's identity to the next in line. For example, a Chinese hacker could route his or her activity through a computer in Brazil, which routes its activity through Russia. The computer in Russia could be used to attack a computer in the US, and the US would see it as an attack from Russia. Perhaps through painstaking effort the American investigators can identify that the Russian computer was a proxy, but then they are led to Brazil. If they manage to go from Brazil to China, they are still unsure whether China was the originator or simply another link in the chain. Proxy servers can be rented or obtained through compromised systems. Additionally,

free software such as Tor (The Onion Router), encryption, tunnelling protocol, and wireless access points (hotspots) add additional anonymity.

A spoofing attack is when a person or program fools another into thinking it is someone or something else. One example is the man-in-the-middle attack, in which person C gets person A to believe they are person B, and they get person B to believe they are person A, thus gaining access to information sent in both directions. This is accomplished by monitoring packets sent from A to B (often involving a packet sniffer), guessing their sequence and number, knocking them out with a SYN attack, and injecting packets from C. Firewalls may defend against these attacks, if they have been configured to only accept IP addresses from the intended correspondent.

Webpage spoofing, known as phishing, imitates a webpage such as a bank's website. When the user enters their data, such as passwords and usernames, the fake website catalogues their information. Webpage spoofing is often used in conjunction with URL spoofing, using an exploit to display a false URL, and DNS cache poisoning to direct the user away from their intended site and then back again when the data has been collected. As a precaution some websites require a user to arrive at their login page from a specified referrer page, but these referrer pages may also be spoofed. During the 2008 Olympics net users in China received a high volume of email spam offering video highlights of the games. Clicking on the links brought users to spoofed CNN pages which asked them to download a codec to watch the videos; once installed the computer was compromised and become a part of the Rustock botnet, i.e. an automated 'robot' running on the web to generate false headlines that entice people to load harmful code (Miller 2008; Hi-tech Thieves Target Olympics 2008).

Spoofing may also be used defensively. For example, the Recording Industry Association of America (RIAA) has practised spoofing on peer to peer networks. The RIAA floods these communities with fake files of sought-after material. This deters downloaders by means of fear and by wasting their time and bandwidth. This could be employed in the same manner by militaries, or as a source of disinformation. A similar defensive tactic, known as a honey pot, lures criminals in by offering sought-after data or what appears to be a compromised network. The honey pot is designed to collect data on the intruder, while giving away nothing, or giving away something that is perceived as an acceptable loss to gain something greater in return.

Attackers may also compromise a computer or network by using a Trojan horse, often known simply as a Trojan. A Trojan appears to perform a desirable function, while secretly performing malicious functions. Trojans can be used to gain remote access, destroy data, download data, serve as a proxy, falsify records, or shut down the target computer at will. The Pentagon, defence-related think tanks, and defence-related contractors were the target of a combined spoofing and Trojan attack in 2008. Trojans were hidden in email attachments designed to look as if they were sent from a reliable source. The Trojan was designed to bury itself into the system, covertly gather data, and send it to an internet address in China. Due to the ability of hackers to route their activity through foreign computers, security experts were unable to determine if China was the final destination, if it was an attempt at framing China, or if it was a state-sponsored activity (Waterman 2008).

This was not the first time US research facilities received spoofed emails with Trojans purportedly from China. In 2005 the Oak Ridge National Laboratory and Los Alamos National Laboratory became infected. No classified information was believed to have been

obtained; however personal information of visitors from the years 1990 to 2004 was compromised. This included names, date of birth, and social security numbers. These two research facilities were originally constructed for sensitive nuclear weapons research during WWII. Today they are used ‘for research in numerous areas including national security, nanotechnology, advanced materials, and energy’ (Lasker 2005). In general, Cyber reconnaissance may be an attempt to attain victory conditions before battle. These intrusions, if undetected, allow intruders to identify vulnerabilities for future cyber attack. The cost of probing computer networks is low, given the lack of attribution, requiring as few as one hacker, and the ability to work from remote locations using off-the-shelf hardware.

A rootkit is a toolkit hidden on a compromised computer. The rootkit can be a diverse set of programs, but invariably is designed to hide the fact that the computer has been compromised and defending itself once detected. These rootkits often hide themselves as seemingly innocuous drivers or kernel modules, depending on the details of the operating system and its mechanisms. In addition to covering the tracks of an intruder, they can allow easier access in the future by opening backdoors. They may also include an arsenal of sniffers, key loggers, and tools that relay email chat conversations. Rootkits may also serve as a staging ground for email spam distribution and DDoS attacks as a part of a larger botnet. In 2005, it was revealed that Sony BMG included rootkit software on their CDs. This software altered the Windows OS to allow access to the computer by anyone aware of the rootkits existence, presumably to enforce copyright protection. This example shows that corporations, too, can be a part of cyber attack or reconnaissance, furthering China’s desire to create its own software and establish market dominance as opposed to being subjected to the US’s. Numerous source codes for ready-made rootkits can be found on the internet. In 2006, alleged Chinese hackers infiltrated “the Department of Commerce’s Bureau of Industry and Security, which manages export licensing of military-use products and information” using rootkits to allow privilege escalation. The agency spent millions of dollars on new, clean, hardware and software, because they could not restore the integrity of the compromised network (Tkacik 2007).

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. The original virus may modify the copies, known as a metamorphic virus, making its destruction more difficult (similar to genetic diversity). A virus can spread from one computer to another through the internet, email, the network file system, or removable medium such as a USB drive. Damage caused by viruses include deleting files, damaging programs, reformatting the hard drive, and disrupting or debilitating the system completely. Viruses may also be used as PSYOPs or demoralizers by presenting text, video, or audio messages to the computer user. In order to replicate, a virus must be allowed to execute code and write to memory. For this reason, many viruses attach themselves to executable files, such as Word and pdf documents, or html links. Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them. The Panda Burning Incense Virus is an example of cyber warfare posing an internal security threat to China, and it set a legal precedent for pursuing and prosecuting hackers (Lemon 2007).

Like a virus, a worm is also a self-replicating program. A worm is a program or suite of programs that attempts to scan a network for vulnerable systems and automatically exploit those vulnerabilities. Some worms work passively, sniffing for usernames and passwords and using those to compromise accounts, installing copies of themselves into each such account, and typically relaying the compromised account information back to the intruder through a



covert channel. Many worms have been designed only to spread, and do not attempt to alter the systems through which they pass. However, the Morris worm and Mydoom showed that network traffic and other unintended effects can cause major disruption. A 'payload' is code designed to do more than spread the worm - it might delete files on a host system, encrypt files for extortion, send documents via email, or destroy the target computer by rendering it unusable.

The Code Red and Code Red II worms were the most successful worms in internet history, causing nearly \$2 billion in damages and infecting over 600,000 computers. The worms, which may have originated from a university in Guangdong, China (United States General Accounting Office 2001), attacked computers running Microsoft's IIS web server and exploited a buffer overflow. Home computers were largely unaffected; however any attempt at infection caused them to crash. The worms created slow downs in internet speed, knocked websites and networks offline, and defaced websites with the phrase "Hacked by Chinese!" - although Chinese involvement was never confirmed. The attacks may have been state-sponsored, they may have been underground hackers and script kiddies, or they may have been a combination of the two. A script kiddie is not an expert in computer security. They use pre-packaged automated tools written by others and found online, such as WinNuke applications, Back Orifice, NetBus, Sub7, Metasploit, and ProRat. Even though script kiddies lack sophistication, and they are looked down on by the hacker culture, they still pose a significant security risk. When media attention is drawn to internet incidents, it is often followed by individuals seeking to participate without any coordinated effort or instructions to do so. Code Red II had a slightly different payload that could open a backdoor, leaving the computers vulnerable to further exploitation (Schwartz 2007; Cost of 'Code Red' Rising 2001).

The Code Red worms coincided with the collision of a US reconnaissance plane and a Chinese fighter jet, in which the Chinese pilot died, and known as the Hainan or EP-3 Incident. Patriotic Chinese hackers defaced dozens of US military and computer industry websites. Patriotic US hackers responded with inflammatory web page defacements, comment spamming, posting of photoshopped derogatory pictures, and probably were the source of the Code Blue Worm (Delio 2001). Code Blue sought out systems infected by Code Red and reprogrammed them to launch attacks against targets based in mainland China. In particular, it launched DDoS attacks against the Chinese security firm NS Focus. These type of attacks could be used clandestinely against one's own country to spur nationalism. Or cyber attacks could be used by a third party state, or organization, to create conflict between external states to further some masked goal. For example, Iran could benefit by creating tension between the US and China through an attack prior to a US proposed UN resolution, in which China has veto power (Onley and Wait 2006; Delio 2001).

In 2004, the Myfip worm probably originated from IP addresses in the Chinese municipality of Tianjin (Brenner 2005). This worm stole pdf files, with later variants targeting Microsoft Word documents, schematics, and circuit board layouts. Among the victims were Bank of America, BJ's Wholesale Club, and Lexis-Nexis. The worm not only stole intellectual property, such as product designs, but also took customer lists and databases. Identifying the number of companies affected poses difficulties as they do not wish to further damage their business by coming forward. To do so can damage consumer confidence and require the

implementation of costly security measures. Businesses may also be oblivious to the number of previous infections and potential data loss as they simply update their patches and move on (Brenner 2005).

A denial-of-service (DoS) attack or distributed denial-of-service (DDoS) attack is an attempt to make a computer resource unavailable to its intended users. This is accomplished by flooding the target with data requests, so that it cannot respond to legitimate traffic, or so that it responds so slowly that it is rendered useless. DDoS attacks may be conducted by a collective of individuals, often co-ordinating their efforts, or by a network of computers under the control of a single attacker. Such networks are called botnets, with each computer in the botnet being known as a bot, or a zombie. These computers have been taken control of by malicious users without the knowledge of the owner, usually through a rootkit, Trojan, or virus. Sobig and Mydoom are examples of worms which created zombies. A botnet's originator, known as a bot herder, can control the group remotely, usually through a means such as IRC, and usually for nefarious purposes. Infected zombie computers are used to send email spam, to host contraband data such as child pornography, or to engage in distributed denial-of-service attacks as a form of extortion. The services of a bot herder can be rented on the black market. One estimate suggested that Chinese hackers have 750,000 zombie computers in the US alone (Waterman 2007). A similar, but non-malicious, phenomenon involving the banding together of excess computer power can be seen in the Search for Extra-Terrestrial Intelligence (SETI@home), or Stanford University's protein folding simulations (Folding@home).

DoS and DDoS attacks can prevent an internet site or service from functioning temporarily or indefinitely. DOS attacks can also lead to problems in the network branches around the actual computer being attacked. For example, the bandwidth of a router between the internet and a local area network may be consumed by an attack, compromising not only the intended computer, but also the entire network. If the attack is conducted on a sufficiently large scale, entire geographical regions of internet connectivity can be compromised without the attacker's knowledge or intent by incorrectly configured or flimsy network infrastructure equipment. Scripts can be set up to automate the process, and subtle variations of these attacks, such as smurf attacks, fraggle attacks, teardrop attack, ping flood, SYN flood, IRC floods, banana attack, Fork bomb, pulsing zombie, and nuke exemplify their sophistication. Various DoS-causing exploits such as buffer overflow can confuse server-running software and fill the disk space or consume all available memory or CPU time. A permanent denial-of-service (PDoS), also known loosely as phlashing, is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. Unlike the DDoS, a PDoS attack exploits security flaws in the remote management interfaces of the victim's hardware, be it routers, printers, or other networking hardware. These flaws leave the door open for an attacker to remotely 'update' the hardware firmware to a modified, corrupt or defective firmware image, therefore bricking the device and making it permanently unusable for its original purpose. The PDoS is a hardware-targeted attack which can be much faster and requires fewer resources than using a botnet in a DDoS attack.

It is important to note the difference between a DDoS and DoS attack. If an attacker mounts a smurf attack from a single host it would be classified as a DoS attack. In fact, any attack directed against computer availability would be classified as a DoS attack. On the other hand, if an attacker uses a thousand zombie systems to simultaneously launch smurf attacks against a remote host, this would be classified as a DDoS attack. Several botnets have been found and removed from the internet. Dutch police located and disbanded a 1.5 million node

botnet, and the Norwegian ISP Telenor disbanded a 10,000 node botnet (Keizer 2005; Leyden 2004). Large, coordinated international efforts to shut down botnets have also been initiated, such as Operation Spam Zombies, which included agencies from 25 different states (Operation Spam Zombies 2005). It has been estimated that up to one quarter of all personal computers connected to the internet may become part of a botnet. And an estimated 50% of all pirated Windows programs contain pre-installed Trojans. China is renowned for its use of pirated Windows programs. This is a cause for concern for China as it bogs down internet and computer efficiency. It also could make Chinese computers susceptible to international condemnation, if their computers are used via proxy. Further, it demonstrates to China the value of developing its own operating systems for domestic and world markets, either to avoid such problems, or to create them for others (Weber 2007).

There are also hybrids. A worm can install a rootkit, and a rootkit might include copies of one or more worms, packet sniffers, or port scanners. A rootkit or virus may be used to conduct a DoS attack, and compromising the system may include some traditional social engineering (HUMINT). So all of these terms have somewhat overlapping usage and they are often misused by mainstream media. The depth of security hacking goes far beyond the examples given here. These examples serve as an introduction to the level of sophistication with which computers can be compromised, illustrating the difficulty in providing defence. They also demonstrate the high level of damage that can be caused by a small group of individuals who work with little funding. This adds to the lack of attribution as it does not require the funding and support of a military, making state-sponsored hacking easy to deny. In combination with anonymity tools and the ability to hide intrusions, security hacking provides a high level of stealth and asymmetry.

### **Military Applications of Hacking**

The USA's paramount position and its heavy reliance on computers have made it a prime target. For this reason it has some of the most extensive information on cyber attacks. The United States has had millions of computers infected at a cost in the billions of dollars. Hackers may be lone teenagers searching for fun or curiosity or state-sponsored intelligence gathering and technology transfer, the determination of which is highly problematic. Frequently hit targets include the US Department of Defense, the Pentagon, NASA, Los Alamos Laboratories, Boeing, Lockheed Martin, Northrop Grumman, Raytheon, Harvard University, California Institute of Technology, and a wide range of think tanks, defence contractors, military installations, and high profile commercial corporations. The attacks have come from across the globe and identifying and prosecuting those responsible has proven difficult (Greenberg 2007; Hacking U.S. Government Computers from Overseas 2001).

These hackers have been able to steal classified data, such as naval codes, information on missile guidance systems, personnel performance reports, weapons development, and descriptions of the movement of equipment and personnel. Jonathan ("c0mrade") James downloaded \$1.7 million worth of software used to control the International Space Station's life support. Dutch teenagers stole information on the Patriot rocket launching system, and the Navy's Tomahawk cruise missile, and tried to sell it to Iraqi officials during the Gulf War – Iraq thought it was a hoax and declined (Miklaszewski 1999). Hackers have commandeered US commercial, educational, and military computers and used them in attacks against other nations, including Taiwan. Hackers can cause an immense amount of damage to a state, stealing information, deleting and changing files, transferring capital, and

destroying programs or entire networks (Hacking U.S. Government Computers from Overseas 2001; Christensen 1999; Qian and Wang 1999).

In 2001 and 2002 Gary (“Solo”) McKinnon probed US Army, Navy, Air Force, Department of Defence, and NASA computers causing \$700,000 worth of damage, taking down a network of 2,000 computers, accessing classified data, deleting and re-writing files. He accomplished this on his own from his home in London using commercially available software and a dial up connection. McKinnon claims he was searching for proof that the US is hiding information about UFOs and an anti-gravity propulsion system. This illustrates the relative ease with which intrusions can take place, the difficulty of determining whether or not it is a state-sponsored action, and a lack of legal framework for timely response. With such attacks occurring so frequently to vital industries, the US, with the largest military budget in the world, has inevitably developed a means to defend against them, which by association means they have also developed the means to conduct cyber reconnaissance and cyber attacks itself. China, too, is the subject of frequent attacks, albeit less publicized, and it will want to remain competitive with US military capabilities (Boyd 2008; Bruno 2008).

### **Titan Rain**

A coordinated series of attacks against US installations are strong indicators that China is developing a cyber warfare capability. The attacks which ran from 2003 to 2006 were designated ‘Titan Rain’. They targeted US defence and aerospace installations, Sandia National Laboratories, Lockheed Martin, Redstone Arsenal, the Department of Defense, and NASA, gathering sensitive military data. The United Kingdom also reported being attacked by the Titan Rain hackers. Much of the data stolen was not classified; however it was not meant for public or foreign consumption, nor was it meant for unlicensed use. For example, the US military’s classified data is typically not connected to the broader internet, but sensitive information such as logistics support for the armed forces is. This can provide valuable insight into field tested experience, as well as expose possible weaknesses to an adversary (Brenner 2007; Espiner 2005).

In addition to the unauthorized gathering, the US is concerned that enough of this data could be used to piece together a larger picture, one that would be considered classified. Among the information gathered were “a stockpile of aerospace documents with hundreds of detailed schematics about propulsion systems, solar panelling and fuel tanks for the Mars Reconnaissance Orbiter . . . specs for the aviation-mission-planning system for Army helicopters, as well as Falconview 3.2, the flight-planning software used by the Army and Air Force” (Thornburgh 2005). Although the majority of data appears to have been benign, its massive quantity may one day prove to include items that the US deems classified at a later date. These attacks could be a staging ground, testing US defences, for future operations of a more serious nature.

Titan Rain demonstrated how China could use cyber warfare as an asymmetric tactic (Norton Taylor 2007). Apparently, a team of hackers, estimated to number between 6 to 30, would take control of US defence computers, copy everything on the hard drive within 30 minutes, and send that data to zombie computers in South Korea, Hong Kong, or Taiwan, where it was subsequently routed to computers in the Chinese province of Guangdong. The ability to route the data makes it difficult to prove the attacker’s identity. While it is believed China was responsible, there is no certainty that the data was not further routed to another location. Additionally, those computers may have been under remote control by a separate

government, or the hackers may not have been state-sponsored. The attacks themselves were not particularly sophisticated, requiring only minimal training with commercially available products. The instructions on how to conduct such attacks are widely available on the internet itself (Delio 2001). But attempts to identify the attackers would require the burdensome task of sending covert agents to physically identify the source.

By using the virtual world, hackers are able to traverse great distances without leaving their station. On the night of November 1, 2004, Titan Rain members scanned, broke into, and retrieved data from defence installations in Arizona, Virginia, California, and Alabama (in that order) all within a period of six hours. Once attackers gain control of US computers, through methods such as Trojans, they can not only shut down the system, they can also conduct attacks using those computers. This could be used to raise condemnation of the US, as it would appear the US is attacking other states (Graham 2005; Thornburgh 2005). While proof is non-existent, some US officials believe that the PLA was responsible (Norton-Taylor 2007). Chinese military doctrine repeatedly discusses “the importance of penetrating an adversary's military logistics and personnel networks. Furthermore, the multiple intrusions into what nuisance and criminal hackers would regard as boring, mundane networks--networks that do not offer the treasure trove of credit card numbers, bank accounts, and identity data that criminal hackers typically seek-- suggest a military purpose” (Tkacik 2007).

### **Further Evidence of Build-up**

Attacks under the code name Titan Rain have ceased. However, OSINT suggests that cyber attacks from China persist. From 2005 to 2007, the US State Department, Bureau of Industry and Security, DoD, National Nuclear Security Administration, Department of Homeland Security, Boeing, Northrop Grumman, Raytheon, Lockheed Martin, and defence-related think tanks had intrusions from Chinese ISPs (China's Proliferation Practices and the Development of Its Cyber and Space Warfare Capabilities 2008; Leyden 2007, Tkacik 2007, Almeida 2006). Sensitive but non-classified data continues to be harvested; items such as emails and the ‘names and other personal information on more than 1,500 employees’ (Onley and Wait 2006). Attacks from Chinese ISPs have forced entire networks to be taken offline or replaced. In 2005 alone, ‘the Pentagon logged more than 79,000 attempted intrusions’ (Reid 2007). Cyber reconnaissance and attacks from Chinese IP addresses had become so frequent and aggressive that US President George W. Bush raised the subject to Chinese President Hu Jintao at the APEC summit in 2007.

The difficulty of attribution in cyber attacks, such as proxies, botnets, non-state-sponsored hackers, and a lack of legal framework to pursue them, means these attacks may not have come from China; however the accusations alone are evidence that China will want to develop a cyber warfare capability. China now has the world's largest internet population, so in terms of volume, China has the most targets to defend. Chinese officials have stated that they are the victim of ‘massive and shocking losses of state and military secrets via the Internet’ (Leyden 2007). Foreign states wishing to use cyber warfare against the US may recognise the focus being placed on China and use Chinese computers to conduct their own reconnaissance and attacks by using botnets or proxies based there. Further, denouncements by the US may indicate that retaliatory responses are in the works and that the US will use allegations of Chinese incursions to bolster support for increasing US cyber warfare capability, thereby putting China further behind in military competitiveness. Damage to China's soft power, particular in relation to ICT, may affect China's economy by making investors cautious and export controls/legal bureaucracy more stringent. PSYOPS campaigns

and media warfare, of the type outlined by the US Information Operations Roadmap (discussed above), may help China regain its lost credibility. These are elements of cyber warfare, but viewed as less offensive than reconnaissance and direct cyber3 attack.

### **Non-US Foreign Allegations**

The US is not alone in accusing China of using cyber warfare. In 2007 and 2008, China was publicly accused of hacking into government facilities by officials in Australia, France, Germany, India, Japan, New Zealand, South Korea, and the UK (Basu 2008; Goodin 2008; Ha 2008; Leyden 2007; Marquand 2007). The number of countries under Chinese attack could be far greater as some may not know that they are under attack, may not wish to reveal their weakness due to a loss of soft power and consumer confidence, or they do not wish to upset China as a valuable trading partner. Hans Elmar Remberg, Vice President of the German Office for the Protection of the Constitution (Germany's domestic intelligence agency) stated that "across the world the PRC is intensively gathering political, military, corporate-strategic and scientific information in order to bridge their technological gaps as quickly as possible" (Tkacik 2007).

Unlike HUMINT, cyber warfare provides a lack of definitive attribution, makes distance nearly irrelevant, allows for the mass accumulation of data in a short span of time, and at a small cost in comparison to traditional espionage or military activities. Cyber attacks, such as an incident that shut down the UK House of Commons, may only be small scale test runs, probing, or reconnaissance blunders, meaning that the true scope of cyber attack has yet to be seen (Norton-Taylor 2007). Cyber reconnaissance appears to be the most beneficial tool of cyber warfare. Beyond finding exploitation points in the military for future attack, the commercial sector allows China the opportunity to skip generations of research and development efforts, levelling the playing field in science and technology, and by association boosting economic and military might. Chinese hackers have even gone after British parliamentary files on human rights issues, showing a potential interest in relation to soft power, globalization, international condemnation, and the legal apparatus. As *Unrestricted Warfare* has shown, there are no boundaries in relation to such military operations.

### **4. Case Studies: Estonia, Georgia and Chanology**

The 2007 cyber attacks against Estonia, Georgia and Project Chanology are examples of large-scale cyber attacks. The Estonian attacks were the first to show how cyber attack against a state provides a debilitating effect at a low cost, a lack of attribution, a lack of legal framework in defence, world-wide attention, and may point to a new arm of traditional attack. The Russo-Georgian war of August 2008 was even more sophisticated and intense than the Estonian case, showing the maturation of the process. Project Chanology reveals how the collective masses can use online tools to emerge as a powerful force without a central leadership. This can be harnessed by military power through the tactics described in IO (Information Operations, see above). And as a matter of internal security, Chanology-style movements must be carefully observed as they pose a non-traditional threat. Estonia and Chanology are an emerging expression of warfare that is fuelled by new powers afforded by the internet, but spills over into the real world, not only through financial loss and media coverage (soft power), but also in the form of volatile protests, disruption, mob mentality, and the capability of drawing governments and militaries into unwanted actions.

## **Estonia**

In 2007, the Estonian government relocated a Soviet-era war memorial and bronze statue in Tallinn, stating that the memorial symbolised Soviet occupation. The Russian government condemned the relocation, claiming it was a tribute to those who fought in World War II. The relocation sparked protests which resulted in 150 injuries, one death, and a month-long cyber war campaign. Estonian websites including parliament, banks, ministries, schools, and newspaper outlets were attacked with DDoS attacks and web page defacements. Some websites also redirected users to images of Soviet soldiers and quotations from Martin Luther King about resisting evil. Hackers who hit the ruling Reform Party's website left a fake message that the Estonian prime minister and his government were asking for Russian forgiveness and promising to return the statue to its original site (The Cyber Raiders Hitting Estonia 2007).

These attacks garnered world-wide attention. The Russian government was directly accused by media outlets and the Estonian Prime Minister Andrus Ansip. Russia had the motive and the means for such an attack. However, there was no direct evidence to suggest that the attacks were state-sponsored. There was evidence that some of the IP addresses used in the attacks belonged to Russian government officials, and instructions on how to carry out cyber warfare did circulate on Russian websites. However, the source of DDoS attacks could have been masked by using proxies or botnets that are located across the globe. Neither NATO nor European Commission experts were able to find any proof of official Russian government participation. Further, the Russian government denounced Estonia's claims and refused to participate in any type of investigation (Bright 2007; Estonia Fines Man for 'Cyber War' 2008; Estonia Hit by Moscow Cyber War 2007).

### **Debilitating Effect at a Low Cost**

The effects of the cyber attacks were magnified as Estonia is one of the most internet-savvy states in the European Union (The Cyber Raiders Hitting Estonia 2007). The Estonian government has pursued a paperless society, or e-government, and web-based banking. Slowing down, or halting, banking services and newspaper outlets that rely on advertising revenue strains the economy. This happens not only through a direct loss in revenue, but also with a reduction in productivity, lost efficiency, diverting resources, escalating frustration, and lost consumer and investor confidence. Estonia also uses the internet to elect parliamentary officials, file their taxes and, via mobile phone, shop or pay for parking. In some cases, website administrators simply blocked access from foreign states. While this was effective in curbing the attacks, it completely cut off banking services to Estonians outside of the country, vital to Estonian business people abroad. Spam emails inundated government officials' inboxes, halting online communication from the Parliament's email server. Officials closed off large portions of their network to keep more vital areas online. A government briefing site was given high priority while the president's website was sacrificed. The 10 largest swarms of data requests by the hackers absorbed 90 megabits per second for up to 10 hours each, straining Estonia's networks. It was 'equivalent to downloading the entire Windows XP operating system every six seconds for 10 hours' (Landler and Markoff 2007). The cyber attacks on Estonia came close to shutting down the country's digital infrastructure. While these may seem more of a disruption than a collapse, the effects radiate out into society (Bright 2007; Estonia Hit by Moscow Cyber War 2007).

The month-long campaign caused companies to put resources into alternative infrastructure, such as going back to traditional mail, relying on telephones, fax, and libraries, and reinforcing alternative methods of payment. As well as the cost of material infrastructure, these type of cyber attacks cause a loss in productivity. This includes paying more people to staff bank tellers, increased traffic on the streets, and long lines at retail outlets. Newspaper outlets, telephone companies, and product distributors, have grown accustomed to using online tools, and now rely heavily on them. While this might be a boon for some industries, the whole restructuring process weakens the nation in the short term. The cyber attacks are comparable to the damage caused to industry (beyond tangible infrastructure) by flooding or blizzards. It places a nation in a state of flux, and leaves it more vulnerable to a traditional attack.

DDoS attacks offer an enemy country an effective low cost assault with high deniability. The majority of attacks on Estonia were DDoS, clogging its servers, switches, and routers. Analysis from Arbor Networks revealed thousands of bots were used against Estonia from locations as diverse as the US, Vietnam, Peru, and China. The cost to a state wanting to establish botnets is minimal, requiring only one person, an internet connection, and a basic computer. While the information for conducting such attacks can be found online, it is more likely someone with expertise, such as non-government hacker groups, would be involved in securing the rental of a botnet. This still keeps the number at a minimum, and hackers can find alternative ways to fund the rental of servers with high bandwidth, such as credit card theft (Waterman 2007; The Cyber Raiders Hitting Estonia 2007).

### **Deniability**

Determining the source of DDoS attacks is a difficult task, as they can be conducted with proxies or botnets. Even if an IP address is obtained, there is no certainty that that was the true source of the attack and not one link in a chain of computers or simply a compromised computer being used unbeknownst to the owner. Message boards and chat rooms located on Russian websites served as a meeting place for attackers, a place to coordinate their time of attack, discuss targets, and recruit others. Because these individuals can be scattered across the globe, it is difficult to assign a group identity to them. The web host may not be aware that plans are being laid on their website, or they may not realise the scope of such plans. These discussions can appear as a childish prank, overshadowing the serious repercussions of the actions taking place, with no individual feeling responsible to put a stop to it.

The Estonia cyber attacks raised debate as to whether they were sponsored by the Russian government. Some believed the attacks were too sophisticated to be the work of individuals or even organised crime. Others believed the attacks were endorsed and guided by the Russian government, but thought they were not directly involved – using online operatives and media warfare as mentioned in IO. Russia has been accused in the past of sponsoring ‘web brigades’ - cyber attack teams - that conduct PSYOPS, disinformation, spamming, and cyber bullying, such as revealing an enemy’s personal details (Polyanskaya 2006). From the perspective of officials from the United States Computer Emergency Readiness Team and the Pentagon’s Defense Advanced Research Projects Agency, the attacks were not conducted by sophisticated means, nor were they state-sponsored. The attackers used commercially available off-the-shelf computers and scripts that are readily available on the internet (Waterman 2007). Data from the Arbor Networks Active Threat Level Analysis System (ATLAS) indicated that the attacks were conducted by multiple distributed botnets which appeared to have been acting independently (Kerner 2007). Even if the attacks were traced to



Russian government computers there was no certainty that those computers had not been taken over by remote hackers. It would also seem foolish for the Russian government to use its own computers for such an attack, especially when it has the expertise to mask its identity, unless doing so *was* masking its identity (knowing that you know I know). Johannes Ullrich, chief research officer of the Bethesda, stated: “Attributing a distributed denial-of-service attack like this to a government is hard. It may as well be a group of bot herders showing patriotism, kind of like what we had with Web defacements during the US-China spy-plane crisis [in 2001]” (Brenner 2007).

As evidence of the Estonia case continued to be examined, the consensus was that the Russian government was not directly involved. It appeared to have been “hacktavists” or simply a mass number of individuals upset over the relocation of the statue. Plans for the attacks were posted on internet forums, message boards, and chat groups prior to the attacks, including detailed instructions on how to send disruptive messages and which Estonian websites to use as targets. The discussion of proposed attacks had become so popular that it was indexed by Google, causing a Google search for the topic to return these incendiary websites at the top of its search results, bringing them to the attention of even more people. Despite being aware of these discussions prior to the attacks, Estonia could do little to stop them. Estonian officials could not identify the individuals discussing attacks, as online (not real) names were used, and obtaining IP addresses would involve going after the website administrator and foreign ISP – a task with which mega-corporations such as the MPAA and RIAA have difficulty, despite their massive funding and even when going after domestic IP addresses. Further, there is no certainty that an individual participating in the discussion will act on his or her comments, there were mass numbers of people involved (each with a different IP address, ISP, and host state to deal with), and there is no solid legal apparatus in place to deal with such an undertaking. Nonetheless, there was a growing and visible threat.

Estonian officials may have been better off devoting their resources to plant online operatives. These operatives could have placed well thought out comments to try and sway the crowd. Rather than spending all resources on physical prevention, some resources could be used to train operatives in PSYOPS, mob mentality, propaganda, and logical deterrents such as subtly mentioning flaws in their arguments, or the consequences of participating in such an attack. In order to be effective this would also require an in-depth understanding of internet subcultures (List of Internet Phenomena 2008; Pang 2008; Slashdot Subculture 2008; Slashdot Trolling Phenomenon 2008). Subtle techniques, such as self-deprecating humour, can sway the crowd’s emotions and train of thought (Landler and Markoff 2007). Russian government involvement may have been as an instigator, knowingly or not, as “there [were] anti-Estonian sentiments, fuelled by Russian state propaganda, and the sentiments were voiced in articles, blogs, forums and the press” (The Cyber Raiders Hitting Estonia 2007). This could be a type of outsourcing of activity that provides a low cost attack with high deniability. Once in the hands of an unwitting mob, the tools necessary are readily available and the means are simple, thereby coordinating a massive data request simultaneously. On an individual level it takes very little effort, yet as a combined whole it has devastating effect with emergent sophistication. This small individual role, may also cause participants to feel less responsible (Estonia Fines Man for 'Cyber War' 2008).

## Legality

In addition to the difficulty of identifying the source of a cyber attack, a lack of legal framework to deal with such an attack makes it exceedingly problematic. Only one person

has been charged and convicted in connection with the Estonian attacks. Dmitri Galushkevich was fined 17,500 kroons for attacking the Reform Party website. Galushkevich admitted to his assault on the site, and he is believed to have acted alone. Several leads in identifying other potential participants in the Estonian attacks relied on Russian cooperation. Estonia made a formal investigation assistance request under a Mutual Legal Assistance Treaty (MLAT) between the states. Moscow appeared as though it would help, but after a delay in action, it ultimately refused to cooperate, stating that the proposed investigation was not covered by the MLAT. Further, the Head of the Russian Military Forecasting Centre stated that the attacks against Estonia had not violated any international agreements because no such agreements exist (Alo 2007; Sobrale 2007). A pro-Kremlin youth movement called The Commissar of the Nashi, claimed responsibility for some of the attacks – however, the group is located within Moldova and Transnistria which are beyond the jurisdiction of Interpol and no MLAT applies. This severely hampers the investigation as pursuing all-EU arrest warrants for these suspects would be largely a symbolic gesture (Commissar of Nashi 2007; Estonia Fines Man for 'Cyber War' 2008; Ministry of Internal Affairs 2007).

### **International Publicity**

Regardless of whether the attacks were state-sponsored, the Estonian incident brought cyber warfare to the attention of the global community. The case was studied intensively by many countries and military planners, since it was believed to have been state-sponsored and a modern example of a large-scale attack. Experts from the North Atlantic Treaty Organization (NATO), the European Commission, and organisations from the US and Israel were dispatched to offer assistance and collect first hand analysis of the event. The implications are far reaching: “For NATO, the attack may lead to a discussion of whether it needs to modify its commitment to collective defense, enshrined in Article V of the North Atlantic Treaty” (Landler and Markoff 2007). There is no precedence for an attack of this type. If a state’s communications centre is attacked by a missile, it is considered an act of war. But what is the response to a cyber attack on that same installation, with the same debilitating effect? The Estonian attacks have encouraged the development of a NATO Cybernetic Defence Centre in Estonia. This is an extension of Estonia’s 1996 push for the expansion of computer and network infrastructure in Estonia, nicknamed the Tiger’s Leap (Bright 2007; A Cyber-Riot 2007; Estonia Has No Evidence of Kremlin Involvement 2007).

### **Georgia**

The 2008 war between Russia and Georgia over South Ossetia appeared to mirror the Estonian attacks, hinting that cyber warfare may become a standard addition to traditional warfare, whether that be state-sponsored or not. Hours after fighting broke out, “Russian hackers had established a site, StopGeorgia.ru, where visitors could view a list of Georgian websites being targeted, showing which sites had been successfully brought down, and download a simple program that enabled their own computer to join the attack” (Waterman 2008). The attacks included DDoS attacks from six different botnets against government and news websites, webpage defacements, spamming, the distribution of Georgian officials’ email addresses, and distribution of a list of Georgian websites with known security flaws. The level of sophistication and intensity of the Georgian attacks surpassed that of the Estonian attacks, showing that capability is increasing. Russian-based hackers tried to halt the Georgian hacker community from responding, by taking down the two highest-profile Georgian hacker sites, hacker.ge and warez.ge, in their initial assault (Waterman 2008). However, Georgian hackers did respond, going after Russian news sites, and in some cases,

spoofing those sites to redirect traffic to pro-Georgian news sources (Coleman 2008; Griggs 2008). Georgian officials asserted that the Russian military was behind the attacks, but they could not provide concrete evidence. Regardless, it represents a new aspect to warfare that must be taken into account. Patriotic cyber attacks may now accompany all traditional wars. If this is not shaped according to government objectives, it runs the risk of undermining operations. For example, patriotic cyber attacks could damage soft power, they could incite damaging retaliatory attacks, and they could drag state powers into conflict.

## **Chanology**

China may wish to tap into the power of a broader range of internet users, those who are not government sponsored, nor skilled hackers, yet have wide-ranging knowledge of the internet through frequent use. In one view:

I've always argued that I do not believe the patriotic hackers are dedicated government agents, but I do believe that they are treated as useful idiots by the Chinese regime, and that the Chinese regime has figured out a rough method, using the propaganda apparatus, to shape the behavior of these patriotic hacker groups, many of whom are getting older and going from black hat to gray hat to white hat, and they want wives and jobs and houses, and the only way to get certified as an information security professional in China is to be certified by the ministries of public and state security. (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008)

A powerful array of tools is openly available to anyone with an internet connection, and they require little effort to learn. Free web-space, image and video uploading sites, such as blogs, Flickr and YouTube, give anyone with an internet connection multimedia sharing tools that rival traditional media. Social networking sites, such as Facebook and Digg, provide additional means to spread this information to a massive audience which, given enough popularity, draws in the traditional media as well. China can use propaganda and PSYOPs to influence this crowd, using it as a political tool. For example, it can be used to organise protest and cyber attacks denouncing Japan's lack of remorse for WWII atrocities, to criticize Falun Gong followers, or to rally support for the One China Policy (Faiola 2005). Project Chanology gives insight into how these non-hacker internet users can come together towards a common goal of disruption using the rapid growth of available internet capabilities. It also illustrates a growing need to understand these emergent communities as they pose a non-traditional security threat.

Project Chanology was a series of cyber attacks and real life protests organised over the internet against the Church of Scientology (CoS). The CoS is the largest organization devoted to the practice and promotion of the Scientology belief system. They are often criticized as being a cult which tries to exploit people for financial gain. A loose group of internet users named Anonymous orchestrated attacks against the CoS using multiple image boards, such as 4chan, 7chan, 12chan, 420chan, and 711chan, as well as supplementary wikis, IRC channels, YouTube, Facebook, Slashdot, Digg, and Encyclopaedia Dramatica. Users of the channels are collectively known as Anonymous, or anon, due to the website's use of anonymous posting; however their internet networks extend beyond the image boards. A large and diverse population of internet users identify with the name Anonymous, many having differing viewpoints and objectives. This point is often lost on the media, who mistakenly believe Anonymous represents a cohesive group. Anonymous is connected, but the nodes which connect each member are not the same, and therefore they do not all rally to the same cause.

Project Chanology was officially launched in the form of a video posted on YouTube on January 21, 2008. The video stated that the attacks were in response to Scientology's internet censorship, dubious recruitment tactics, saturating of disaster areas to 'help' victims, and overall belief system. Of particular contention was Scientology's forced removal of a leaked Tom Cruise video interview, in which he expounded his love for Scientology. Additional complaints against the CoS include the removal of leaked Scientology belief documents (part of a 10-year legal battle against Karin Spaink and several ISPs), and the attempted removal of the newsgroup alt.religion.scientology from Usenet, which led the hacker group Cult of the Dead Cow to declare war on the Church of Scientology as early as 1995. Anonymous's stated intent was to 'expel the church from the internet' and to 'save people from Scientology by reversing the brainwashing'. This was followed by DDoS attacks, black faxes, prank calls, false deliveries to CoS buildings, the dissemination of Church leaders personal information (telephone numbers, social security numbers, and addresses), and the publishing of the contended leaked material on a wide range of websites.

Project Chanology members grew to approximately 9,000 people. They successfully took down the Scientology website on January 18, 2008 with a mid-range DDoS attack. By comparison a botnet can launch a simultaneous attack from 50,000 computers. Nonetheless, Anonymous managed to cripple the Scientology website for a period of two weeks. In response to the attacks, the CoS moved its internet domain to a more secure provider. The original declaration of war video, which utilized a synthesized voice, was viewed over two million times within 18 days of its release. Project Chanology garnered mainstream media coverage on an international scale. Mainstream media's attention created an unintended DDoS attack by drawing more attention to the CoS website. Anonymous further raised questions about Scientology's actions, including the death of Lisa McPherson, a scientologist who died in 1995, for which the CoS was previously under federal investigation. Anonymous used a Google bomb technique to make the Scientology.org website the first result in a Google search for 'dangerous cult' (McMillan 2008; O'Connell 2008; Vamosi 2008; Cook 2008; Single 2008; Ramadge 2008; The Passion of Anonymous 2008).

Utilizing a wide range of online communication tools, and a new YouTube video titled "Call to Action", Anonymous coordinated a series of protests. In the video anon states: 'We have no leaders, no single entity directing us.' On February 10, 2008, approximately 7,000 people protested throughout 100 cities in 14 countries. Protesters wore Guy Fawkes masks from the V for Vendetta film, and made Rick Astley's pop single "Never Gonna Give You Up", a theme song for the protests against Scientology. The seemingly bizarre and childish behaviour of Anonymous is a part of their cohesion, a subculture of memes, slang, and humour. A second series of protests began on March 15, 2008, with approximately 7,000 to 8,000 protestors throughout 100 cities in 10 countries. CoS has not released an official estimate of the financial damage caused by Project Chanology. However, they have publicly stated that they were forced to increase online security, hired off-duty police officers to provide physical security at their churches, and have suffered increasing negative press and scrutiny from the US Federal Bureau of Investigation. CoS has denounced Anonymous as cyber terrorists and Anonymous has since switched its campaign to go after Scientology's tax-exempt status.

China could use online operatives to incite this type of internet based 'mob'. It could be used constructively within China, such as undermining the Falun Gong, or destructively against an enemy country, such as inciting protests against pro-democracy Taiwanese leadership.

Additionally, these online communities pose a security threat, and should therefore be examined if only as a means of deterrence. As mentioned in IO, this sort of emergent mob is not one that can be quickly understood. To be used as a military tool, China would need a deep understanding of the asset's culture. In the case of Anonymous, this equates to a heavy reliance on inside jokes, slang, internet and pop culture. Anonymous uses humour to unite and to obfuscate logic and responsibility. Credence within the group may come from inside jokes and creativity, rather than sound information – they even revel in their own failure. Internet communities can lack a centre of command, and be composed of serious, moderate, and casual participants, all of whom may change their level of participation on a whim.

## 5. Assassin's Mace

Assassin's Mace, or *shashoujian*, is used in Chinese military writings to describe a weapon or tactic 'which can deliver decisive blows in carefully calculated surprise moves and change the balance of power' (Johnston 2002). Similar concepts can be seen throughout China's history, from Sun Zi's (tr. 1963) *The Art of War* to Mao Zedong's (tr. 2000) *On Guerrilla Warfare*. An assassin's mace gains strength by ignoring pre-established rules of conduct. It has many similarities to asymmetric warfare, such as being a novel way to level the playing field, but it differs in that it is a decisive weapon, aimed at incapacitating an enemy, 'suddenly and totally' (Navrozov 2005). China possesses several asymmetric, highly devastating weapons, such as a limited but modernising nuclear weapons capacity, China's ASAT capability, and its electromagnetic pulse (EMP) capability. However each of these has considerable drawbacks. For example, human rights and environmental concerns have relegated nuclear weapons to the role of deterrent and introduced limited warfare. By using cyber warfare, China could achieve the same asymmetric destructive power while bypassing the drawbacks.

It is unlikely that China would use kinetic kill weaponry, such as its direct ascent ASAT, in an attempt to disrupt US space based assets. To disrupt US satellite dominance would require a massive sky clearing operation, because the US has constellations of satellites with multiple redundancy. The US GPS provides tactical communication and precision navigation, making it a desirable target – however, the GPS uses at least five space satellite constellations. When one is destroyed, others can be manoeuvred to fill holes in the net. Not all of these satellites are within striking range at any given time. This means a sky clearing operation would take a significant amount of time, thereby revealing Beijing's intentions. This would cause international dispute due to space debris, and allow the US to manoeuvre its other satellites out of harm's way. It would risk retaliation in which China would be at a disadvantage. Additionally, there is no guarantee an attempt would be successful, as each launch requires precise targeting, and China's ASAT has only been tested once. It is more likely China would attempt to knock out the corresponding relay stations on Earth by using a cyber attack. Chinese tacticians have focused on neutralising the uplinks and downlinks of the space-based systems through diverse forms of cyber attack including simple DoS attack. This gives the advantages of deniability and low cost. It would remove distance from the equation, allowing multiple targets to be taken out simultaneously regardless of location, and it would remove international condemnation and/or involvement (Waterman 2008; Tellis 2007; International Assessment and Strategy Center 2005).

China could destroy a vast majority of US electronics, including computers, cars, phones, and the power grid, using EMP weaponry. This is something of which all nuclear armed states

are capable by means of high altitude nuclear explosions, taking as few as three to blanket the continental US (Electromagnetic Pulse 2005). Open source materials have shown the US, China, France, and Russia all using an EMP burst as a surprise first strike in war games (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008; Winn 2008; Nock and Lizun 2007; Qian and Wang 1999). However, it is unlikely China would use such brute-force tactics. Using a high altitude atomic burst would cause international outrage as it violates an international treaty, it damages the environment, and it indiscriminately disrupts everything in its blast radius. Alternatively, shutting down the US power grid, production lines, water utilities, chemical plants, telecommunications, and transportation routes is possible through cyber attack, and it would provide the benefit of deniability. Details on how such an attack would be conducted are scarce in OSINT as governments do not wish to publicize their weaknesses or give away their assets. It is important however that they do acknowledge them, since any computer system which is connected to the internet is vulnerable to attack. In 2008, the CIA reported that multiple cities outside the US had their electrical power shut off by hackers. The reports were vague, supposedly due to security concerns; however it was reported that the attacks came from online, through the internet, not by physical means (Bridis 2008; McMillan 2008).

### **Weapons of Mass Disruption**

OSINT continually points to cyber warfare being capable of crippling a state's electric power transmission, transportation systems, and communications systems (Phone Phreaking 2008; Weber 2008; Trahan 2008; McMillan 2007; Tkacik 2007; Reid 2007; Robson 2004; Miklaszewski 1999). If the Russian government was behind the cyber attacks on Estonia, it did not use such a dramatic assault. The Russians may simply have been testing their cyber warfare capabilities, saving their most devastating capability for when it is needed most, as it may only work once. Such an attack would cripple the flow of goods, effectively starving the population and shutting down business. Evidence that such a possibility exists can be seen across the globe. In 1997, a teenager shut down air and ground communication at a US airport in Massachusetts, and in 2000, the Russian government announced that hackers had succeeded in taking control of the world's largest natural gas pipeline network, Gazprom, by using a type of Trojan. In 2000, Vitek Boden took control of a sewage pumping station in Australia. He remotely triggered the release of a million litres of sewage into public waterways (Barker 2002). Computers and manuals seized in Al Qaeda training camps contained large amounts of SCADA information related to dams and critical infrastructure. In 2003, the Slammer Worm took a US nuclear power plant's safety monitoring system offline, and the Blaster Worm was connected with a massive blackout in the Eastern US (Maynor and Graham 2006).

The United States is particularly vulnerable as much of the communication, manufacturing, water, transportation, and energy infrastructure is owned by the private sector, as opposed to China and Russia where infrastructure is predominantly in the hands of the government (Greenemeier 2007). The relative ease with which the Titan Rain attacks were conducted make private sector computer networks look like an easy target (Almeida 2006). The government and defence installations are heavily funded for security, whereas the private sector is not. Initially the US power grid control systems were on closed networks (not connected to the internet). However, over time companies began deciding it was too costly to maintain separate networks. The internet became essential for operations, meaning they would need two separate systems for operation, one connected and one not. Through the decision-making process companies decided it was cheaper to have only the one that was

connected, but focus on keeping it secure. Over time security became lax, and no network that is connected can be entirely secure. Many of these systems do not support authentication, encryption, or basic validation protocols; of those that do support them, most run with security features disabled (Maynor and Graham 2006). In addition to the internet, SCADA systems may be compromised through outdated modems used for maintenance purposes, wireless access points, or roaming notebooks. Further, power companies may buy and trade power amongst themselves, so loopholes designed to check available capacity have provided another entry point (Winkler 2007). The vulnerability of the private sector's computer network, due to a lack of understanding or a lack of incentive, provides China (or other cyber-capable groups) with the opportunity to cripple US infrastructure.

### **Point of Sale**

Using a modern fuel service station as a parallel for a cyber attack on commercial infrastructure, one can see the debilitating effects of a cyber attack. Magnetic stripe cards have replaced tangible notes as the primary method of payment. By overwhelming a bank through something as simple as a DDoS attack, an adversary could knock the point of sale banking system offline. Few service stations are equipped to handle this for duration longer than one day, and the Estonian attacks demonstrated a month-long capability. Lines in the store would grow as the speed of transactions dramatically slowed. Nearby ATMs would be taxed as people begin withdrawing more notes. As the ATM runs out of its supply of money, an internal alert is sent to notify the ATM provider to send an armoured car to restock the machine. This would require additional workflow, disrupting a fine tuned system of allocated staff hours and drivers. The long lines at the register would disrupt the productivity and efficiency of working customers who are unaccustomed to the long wait, and it would radiate frustration and anger throughout the community.

As the service line grows and employees struggle to keep up, the amount of store theft (fuel and merchandise) increases. More hours would be allocated to review surveillance footage, and the local police would be inundated with cases of theft. Panic may ensue, as seen with small disruptions at service stations, comparable to the temporary collapse of Optus telecommunications or the temporary collapse of Westpac banking (Strem 2008). A sustained disruption could lead to mob mentality. The fragility of social order was demonstrated in 2008 when fuel price increases led to widespread violent protests across the globe, including Argentina, Belgium, France, India, Indonesia, Malaysia, Portugal, South Korea, Spain, Thailand, and the UK (Arrests Following Jakarta Fuel Price Increases 2008; Banerjee and Zappei 2008; Cowell 2008; Fuel Demo Adds To Road Taxes Row 2008; Indonesia: Growing Fuel Price Protests Meet Repression 2008; Thai Truckers Join Global Fuel Price Protest 2008).

Alternatively, the registers themselves are operated by using the internet and could be targeted. China could bypass banking systems, energy providers, transportation systems, or communications systems and go after the less guarded, and less funded, point-of-sale software. Few service stations remain in the western world that use unconnected registers, as it would be difficult to remain competitive. Similarly, there are few competitors in the service station industry due to strong competition. This means there are only a small group of service station vendors within a large city, and all of the computers within those companies are running off of the same network. The six largest non-state owned energy companies, known as super majors, are: Exxon Mobil, Royal Dutch Shell, BP, Chevron Corporation, ConocoPhillips, and Total SA. These six companies control the vast majority of service

stations (SBDCNET 2001). This is sometimes obscured by the use of alternative store names, despite being contracted to a supermajor, or the continued use of an old company name despite having been bought out by a supermajor. This illustrates a lack of diversity in the retail industry. By attacking only a few targets, an entire city's service stations could be knocked offline. There are a limited number of independent operators within a typical city; however their numbers are too few to facilitate the influx of customers from the larger competitors.

Without the online register, PLUs (price look-up codes) cannot scan and prices would have to be manually added. Any extended duration of this process could shutdown a store, and depending on the system, fuel may not be able to be dispensed without the computer. Service stations are not known for their sophistication in computer defence as they routinely tighten budgets to their limits and they have not seen a need to harden this infrastructure. As community hostility rises, employees may resign due to stress. It would be difficult training new employees during this time with extended lines and the employees themselves suffering an inability to access fuel. New staff would also cause lost time and money for training. All delivery trucks create online invoices sent and received by the service station. Assuming they are able to maintain the fuel for their trucks, they would be forced to adapt to old methods of interaction and record keeping. A store's stock might also suffer shortages from hoarding of products due to panic in the community.

These systems could be attacked solely online, or operatives could be placed into the store to learn the system's weaknesses and install malware directly. Operations could be expanded beyond a service station to attack grocery and a wide range of retail outlets. Rather than going after the transport of goods, it may be easier to disrupt them online at their point of sale. The effects would radiate outward, knocking down additional infrastructure unable to handle the increased stress. A service station is only one example of weak commercial infrastructure that relies on computers to operate. If China could gain market dominance in the point of sale software industry, or in the registers used for sales, it would gain an even greater access to disruption. This disruption could be used as a deterrent, as blackmail, or as a force multiplier in traditional warfare.

### **Market Dominance**

China may seek to establish market dominance in the production of ICT software and hardware as a means of increasing its cyber warfare capability. On an infrastructure level, China could seek to control ownership of submarine cable infrastructure allowing it further access to cyber reconnaissance or the option of shutting down portions of internet connectivity during times of war (Whitney 2008; *Of Cables and Conspiracies* 2008). Further, if China could unseat Microsoft as the industry standard in software, it could install backdoors, latent viruses, or remotely triggered ex-filtration devices. This type of tactic was examined in section 3, above (Cyber Reconnaissance and Attack), with Sony BMG's use of rootkits. China used legal and financial prowess to convince Microsoft to teach its software engineers how to insert their own software into Windows applications. As a part of the Chinese argument for doing so, was an insistence that Microsoft Windows was a secret tool of the US government. By providing China with "skeleton keys" to the Windows Operating System, inadvertently China was given advanced knowledge on how to infiltrate foreign computers and craft advanced exploits (Marsal 2008; Tkacik 2007).



US concerns over Chinese market dominance have begun to surface. In 2006, the State Department banned the purchase of computers from the Lenovo Group, the Chinese firm that acquired the IBM personal computing division, following penetrations using a zero-day flaw in Microsoft software. China is also growing in the field of microchips, something other states need for defence related electronics. Not only could China embed exploits, but also dominance in this field gives it access to critical individuals and information through partnership, such as a chance to liaise with industry insiders, come close to sensitive information and hardware, and conduct social engineering or HUMINT. In 2003, the Huawei Shenzhen Technology Company was charged with stealing secrets and wholesale pirating of Cisco software, a US company. In 2007, Huawei then attempted to buy 3Com, a US company which supplies the US government with security software, routers, and servers. India turned down a \$60 million Huawei investment deal in 2005 after concerns over cyber reconnaissance, noting that Huawei is the same company that conducts sweeping and debugging of the Chinese embassy. India's Defence Ministry stated 'the choice was between cheap Chinese equipment and national security' (Tkacik 2007).

China consistently reverse engineers ICT hardware and software in an attempt to maintain a stronghold on its own markets. This can be seen with the reverse engineering of Skype Protocol and Voice over Internet Protocol (VoIP), and 'knock offs' of the iPhone (VoIP WkiBlog 2006). The One Laptop Per Child (OLPC) project, which has the potential to rapidly spread internet connectivity to China's remaining population, uses an open source operating system and software, helping to free China from US owned Microsoft. Yet China has denounced the sale of OLPC, promoting instead various domestic versions that were reversed engineered from the OLPC model. Further, the Chinese have secured manufacturing rights to produce OLPC within China even though they do not intend to promote OLPC sales domestically (O'Brien 2008). China also has a history of reverse engineering websites that become popular and profitable in the Western world; examples include clones of YouTube, Google, MySpace, Facebook, Wikipedia, and eBay being YoQoo, Baidu, Baidu Space, Xiaonei/Zhanzuo, Baidu Baike/Hoodong, and Taobao respectively (Marshall 2008; Wei 2008; Burns 2006).

### **Peacetime Operations**

During peacetime, China is likely to rely on cyber reconnaissance to gather information and catalogue exploits/weaknesses in the US military and infrastructure. Automobile companies, food services, oil companies, financial institutions, and telecommunications all play a vital role in supporting military operations, as well as housing technological advances, expertise, and inside information which could prove useful for leapfrogging (Winkler 2005). Technology transfer allows China to skip years of costly research and development, and it removes the competitive edge of foreign militaries and companies (Tkacik 2007). In unrestricted fashion, China may also seek advantage during peacetime to battle military export restrictions of the EU, purchase vital capital in the US financial system, and help shape the international legal structure being developed for cyber warfare. Cyber reconnaissance against US military logistics networks could reveal force deployment information, such as the names of ships deployed, readiness status of various units, timing and destination of deployments, and rendezvous schedules. It could also reveal the details of weaponry sold to Taiwan.

China has repeatedly shown interest in the US Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) (China's Proliferation Practices, and the Development of Its

Cyber and Space Warfare Capabilities 2008). NIPRNet is used to exchange unclassified but sensitive information between internal users. The network is connected to the broader internet to improve collaboration between scientists and officers located in different organizations and in remote locations. This means it can provide intruders with data such as 'ballistic weapons research, aircraft and ship design, military payroll, personnel records, procurement, modelling of battlefield environments, and computer security research' (Lewis 1994). The US places classified military information on the Secret Internet Protocol Router Network (SIPRNet) and secret information on the Joint Worldwide Intelligence Communications System (JWICS). While these networks are not connected to the internet, examining NIPRNet may give insight into the contents through cross talk, or it may provide a means of escalating privileges, providing information on how to access SIPRNet and JWICS either directly or indirectly via an asset.

## **Taiwan**

China can use the internet to manipulate the Taiwanese populace, either to set up for an attack, or to undermine Taiwan independence peacefully and avoid conflict altogether. This may include PSYOPS/propaganda, recruitment and identification of sympathizers, or cataloguing of cyber and defence weaknesses. For example, an internet rumour in 1999 that a Chinese Su-27 had shot down a Taiwan aircraft caused the Taipei stock market to drop more than two percent in less than four hours. An earthquake in 1999 and a typhoon in 2001 revealed weaknesses in Taiwan's telecommunications, electric power, and transportation infrastructure; weaknesses which could be targeted in physical sabotage. Further, a landslide revealed that the loss of a single power grid tower is capable of knocking out 90 percent of the power grid in the central mountainous region. Building information, including the location of the President's office, and daily activities, are openly available on the internet. This is even more significant given the lack of security present during the 2004 assassination attempt on President Chen Shui-bian and Vice President Annette Lu (China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities 2008; Taiwan Assassin 2004).

In the event of a Taiwan conflict, China could use cyber attacks to delay US involvement long enough for Taiwan to capitulate. For example, China could go after the US logistical apparatus, using information gained via NIPRNet, in order to delay the force deployment phase. This would include the organization of forces, food supplies, uniforms, and/or communication which are often organised through networks that are connected to the internet. Cyber attack could also delay re-supply to the region by misdirecting stores, fuel, and munitions, corrupting or deleting inventory files, and thereby hindering mission capability. If the Chinese lack the capability to find exploits in NIPRNet, they could simply conduct DDoS attacks to bring it down long enough for a Taiwanese surrender. While delaying the US, China could use traditional military forces in concert with cyber warfare against Taiwan. The cyber warfare component could include online PSYOPS, media warfare, special forces aided by cyber reconnaissance information, and cyber attacks against Taiwan's point of sale and banking infrastructure.

## **6. Conclusion**

This research has shown that China seeks to leapfrog in military competitiveness by utilizing cyber warfare. Chinese military doctrine places an emphasis on asymmetric attack. Cyber

warfare epitomizes this a low cost means of levelling the playing field. Cyber attack strikes at a superior adversary's weakness – in the case of the US, a heavy reliance on hi-tech computerized weaponry and a civilian population reliant on an unsecured computer infrastructure. Cyber reconnaissance follows China's tradition of technology transfer and reverse engineering for domestic production as a means of leapfrogging. Cyber reconnaissance gives the added benefit of providing deniability, low cost, a lack of legal framework against it, and the removal of geographical distance. Foreign allegations, such as the Titan Rain incursions, suggest China is making rapid progress in cyber reconnaissance and attack capabilities. The PRC openly states in its National Defense White Paper that it is seeking informationization and modernization of the PLA. This follows the US, China's perceived greatest threat, in its pursuit of NCW, IO, and FCS. Cataloguing adversary weaknesses not only provides an asymmetric advantage in the event of a conflict, it also acts as a deterrent while China catches up in traditional military might. By utilizing cyber reconnaissance, China can accelerate its advancement in hi-tech weaponry. Unrestricted warfare has shown a blurring of the lines between military and non-military spheres. China can tap into the power of its online population for military purposes, such as seen in the Estonian, Georgian and Chanology case studies. Following the US example of IO, China can leverage the internet as a means of boosting soft power. Using cyber reconnaissance, the Chinese can gain market dominance in the fields of ICT. This will provide increased cyber security, by removing foreign influence, and it will provide improved cyber offence, such as pre-installed exploits or ownership of internet infrastructure. Market dominance also relates to financial gain, which China has stated is intrinsically related to military capabilities and strategic interests.

## References

- Adams, Eric. 2004. Rods From God. Retrieved on March 10, 2008, from <http://www.popsci.com/scitech/article/2004-06/rods-god>.
- Alberts, David S. 2002. Information Age Transformation. Retrieved on February 22, 2008, from [http://www.dodccrp.org/files/Alberts\\_IAT.pdf](http://www.dodccrp.org/files/Alberts_IAT.pdf).
- Alberts, David S., Garstka, John J., Stein, Frederick P. 2000. Network Centric Warfare. Retrieved on February 2, 2008, from [http://www.dodccrp.org/files/Alberts\\_NCW.pdf](http://www.dodccrp.org/files/Alberts_NCW.pdf).
- Allen, Kenneth. 2005. Reforms in the PLA Air Force. Retrieved on February 12, 2008, from [http://www.jamestown.org/publications\\_details.php?volume\\_id=408&issue\\_id=3390&article\\_id=2369972](http://www.jamestown.org/publications_details.php?volume_id=408&issue_id=3390&article_id=2369972).
- Allen, Kenneth W., Glenn Krumel, Jonathan D. Pollack. 1995. China's Air Force Enters the 21st Century. Retrieved 1 February 2008, from [http://www.rand.org/pubs/monograph\\_reports/2005/MR580.pdf](http://www.rand.org/pubs/monograph_reports/2005/MR580.pdf).
- Almeida, Marcelo. 2006. Cyberwar: The Beginning. Retrieved on March 3, 2008, from [http://www.zone-h.org/index.php?option=com\\_content&task=view&id=13932&Itemid=30&msgid=710](http://www.zone-h.org/index.php?option=com_content&task=view&id=13932&Itemid=30&msgid=710).
- Annual Report to Congress: Military Power of the People's Republic of China 2008. 2008. Retrieved on March 15, 2008, from <http://www.globalsecurity.org/military/library/report/2008/2008-prc-military-power.htm>.
- Annual Report to Congress: Military Power of the People's Republic of China 2007. 2007. Retrieved on February 18, 2008, from <http://www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf>.
- A Cyber-Riot. 2007. Retrieved on February 2, 2008, from [http://www.economist.com/world/europe/displaystory.cfm?story\\_id=9163598](http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598).
- Amnesty International. 2004. People's Republic of China Controls tighten as Internet activism grows. Retrieved on August 1, 2008, from <http://www.amnesty.org/en/library/asset/ASA17/001/2004/en/dom-ASA170012004en.html>.
- Appel, Edward. 2004. China's Espionage: What's At Stake. Retrieved on March 20, 2008, from <http://www.pbs.org/wgbh/pages/frontline/shows/spy/spies/atstake.html>.

- Armoured Fighting Vehicles. 2008. Retrieved on April, 10, 2008, from <http://www.sinodefence.com/army/armour/default.asp>.
- Arrests Following Jakarta Fuel Price Increases. 2008. Retrieved on August 1, 2008, from <http://www.radioaustralia.net.au/news/stories/200806/s2285064.htm>.
- Baard, Mark. 2007. Sentient World: War Games on the Grandest Scale. Retrieved on March 20, 2008, from [http://www.theregister.co.uk/2007/06/23/sentient\\_worlds/](http://www.theregister.co.uk/2007/06/23/sentient_worlds/).
- Banerjee, Manik and Zappei, Julia. 2008. Fuel Price Hikes Spark Protests In India And Malaysia That Could Undermine Governments. Retrieved on August 1, 2008, from <http://www.aol.com.au/news/story/Fuel-price-hikes-spark-protests-in-India-and-Malaysia-that-could-undermine-governments/550071/index.html>.
- Barker, Garry. 2002. Cyber terrorism a mouse-click away. Retrieved on February 24, 2008, from <http://www.theage.com.au/articles/2002/07/07/1025667089019.html>.
- Basu, Indrajit. 2008. India Faces Cyber Challenge From China. Retrieved on June 10, 2008, from [http://www.upiasiaonline.com/Security/2008/05/09/india\\_faces\\_cyber\\_challenge\\_from\\_china/5587/](http://www.upiasiaonline.com/Security/2008/05/09/india_faces_cyber_challenge_from_china/5587/).
- Beam It Right There Scotty. 2005. Retrieved on January 26, 2008, from <http://www.wired.com/science/discoveries/news/2005/07/68152>.
- Berkeley Bionics Human Exoskeleton. 2007. Retrieved On March 10, 2008, from <http://www.youtube.com/watch?v=EdK2y3lphmE>.
- Block, Ryan. 2006. The Brain Port, Neural Tongue Interface Of The Future. Retrieved on March 10, 2008, from <http://www.engadget.com/2006/04/25/the-brain-port-neural-tongue-interface-of-the-future/>.
- Bloom, James. 2008. Robots ready to support soldiers on the battlefield. Retrieved on June 26, 2008, from <http://www.guardian.co.uk/technology/2008/jun/26/robots.weapons.technology>.
- Bonsor, Kevin. 2008. How Augmented Reality Will Work. Retrieved on March 10, 2008, from <http://www.howstuffworks.com/augmented-reality.htm>.
- Boyd, Clark. 2008. Profile: Gary McKinnon. Retrieved on August 4, 2008, from <http://news.bbc.co.uk/2/hi/technology/4715612.stm>.
- Bradsher, Keith. 2006. Hong Kong enlists youth to fight piracy. Retrieved on July 20, 2008, from <http://www.iht.com/articles/2006/07/18/business/piracy.php>.
- Braukus, Michael. 2004. NASA Develops System To Computerize Silent Subvocal Speech. Retrieved on March 2008, from [http://www.nasa.gov/home/hqnews/2004/mar/HQ\\_04093\\_subvocal\\_speech.html](http://www.nasa.gov/home/hqnews/2004/mar/HQ_04093_subvocal_speech.html).
- Brenner, Bill. 2007. Experts doubt Russian government launched DDoS attacks. Retrieved on February 18, 2008, from [http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_gci1255548,00.html](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1255548,00.html).
- Bingemann, Mitchell. 2008. Buggy Software Sends Optus Offline. Retrieved on August 8, 2008, from <http://www.australianit.news.com.au/story/0,,24141034-15306,00.html>.
- Brenner, Bill. 2005. Myfip's Titan Rain Connection. Retrieved on January 8, 2008, from [http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_gci1120855,00.html](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1120855,00.html).
- Bridis, Ted. 2008. CIA: Hackers demanding cash disrupted power. Retrieved on February 2, 2008, from <http://www.msnbc.msn.com/id/22734229/>.
- Bright, Arthur. 2007. Estonia Accuses Russia Of Cyberattack. Retrieved on March 10, 2008, from <http://www.csmonitor.com/2007/0517/p99s01-duts.html>.
- Brookes, Peter. 2006. China's Influence In Africa. Retrieved on March 15, 2008, from <http://www.heritage.org/Research/AsiaandthePacific/bg1916.cfm>.
- Bruno, Greg. 2008. The Evolution of Cyber Warfare. Retrieved on March 12, 2008, from <http://www.cfr.org/publication/15577/>.
- Burns, Simon. 2006. MySpace and Wikipedia Clones Storm China. Retrieved on July 31, 2008, from <http://www.itnews.com.au/News/NewsStory.aspx?story=35422>.
- Center for Strategic and International Studies. 2003. China's Space Program. Retrieved on April 3, 2008, from [http://www.csis.org/index.php?option=com\\_csis\\_progj&task=view&id=76](http://www.csis.org/index.php?option=com_csis_progj&task=view&id=76).
- China and Internet Censorship. 2006. Retrieved on August 5, 2008, from <http://www.cnn.com/interactive/world/0603/explainer.china.internet/frameset.exclude.html>.
- China defends internet regulation. 2006. Retrieved on July 15, 2008, from <http://news.bbc.co.uk/2/hi/asia-pacific/4715044.stm>.
- China hires Net squad to sway opinion. 2005. Retrieved on July 15, 2008, from <http://www.asiamedia.ucla.edu/article.asp?parentid=24609>.
- China internet use grows. 2006. Retrieved on August 1, 2008, from <http://news.bbc.co.uk/>

- [2/hi/business/2145865.stm](#).
- China Tightens Vice On Internet. 2006. Retrieved on June 11, 2008, from <http://cryptome.cn/china-vice.htm>.
- China's National Defense in 2006 (White Paper). 2006. Retrieved on March 3, 2006, from <http://www.fas.org/nuke/guide/china/doctrine/wp2006.html>.
- China's Navy 2007. 2007. US Office of Naval Intelligence. Retrieved January 10, 2008, from <http://fas.org/irp/agency/oni/chinanavy2007.pdf>.
- China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities. 2008. Retrieved on June 30, 2008, from [http://www.uscc.gov/hearings/2008/hearings/transcripts/08\\_05\\_20\\_trans/08\\_05\\_20\\_trans.pdf](http://www.uscc.gov/hearings/2008/hearings/transcripts/08_05_20_trans/08_05_20_trans.pdf).
- China's Space Program Aims at Peaceful Use of Space Resources. 2005. Chinanews.cn, 15 October. Retrieved on July 10, 2006, from [www.chinanews.cn/news/2005/2005-10-15/12428.html](http://www.chinanews.cn/news/2005/2005-10-15/12428.html)
- Chinese Submarines. 2008. Retrieved on April 10, 2008, from <http://www.sinodefence.com/navy/sub/default.asp>.
- Christensen, John. 1999. Bracing For Guerrilla Warfare In Cyberspace. Retrieved on February 2, 2008, from <http://edition.cnn.com/TECH/specials/hackers/cyberterror/>.
- Code Red Worm Spreading, Set To Flood Whitehouse. 2001. Retrieved on July 18, 2008, from <http://slashdot.org/articles/01/07/19/2230246.shtml>.
- Cost of Code Red Rising. 2001. Retrieved on February 2, 2008, from <http://archives.cnn.com/2001/TECH/internet/08/08/code.red.II/>.
- Coleman, Kevin. 2008. Cyber War 2.0 – Russia V. Georgia. Retrieved on August 13, 2008, from <http://www.defensetech.org/archives/004363.html>.
- Commissar of Nashi says he waged cyber attack on Estonian government sites. 2007. Retrieved on March 10, 2008, from [http://www.sbcc-chamber.com/index.php?lng=en&page\\_id=60&news\\_id=888](http://www.sbcc-chamber.com/index.php?lng=en&page_id=60&news_id=888).
- Cook, John. 2008. Cult Friction. Retrieved on July 14, 2008, from [http://www.radaronline.com/from-the-magazine/2008/03/scientology\\_anonymous\\_protests\\_tom\\_cruise\\_01.php](http://www.radaronline.com/from-the-magazine/2008/03/scientology_anonymous_protests_tom_cruise_01.php).
- Cooper, Simon. 2006. How China Steals US Military Secrets. Retrieved on April 2, 2008, from [http://www.popularmechanics.com/technology/military\\_law/3319656.html](http://www.popularmechanics.com/technology/military_law/3319656.html).
- Cordesman, Anthony, and Kleiber, Martin. 2006. Overview of Major Asians Powers. Retrieved on March 12, 2008, from [http://www.csis.org/media/csis/pubs/060626\\_asia\\_balance\\_powers.pdf](http://www.csis.org/media/csis/pubs/060626_asia_balance_powers.pdf).
- Corpus, Victor N. 2006. Americas Acupuncture Points, Part 1. Retrieved on March 18, 2008, from <http://www.atimes.com/atimes/China/HJ19Ad01.html>.
- Corpus, Victor N. 2006. Americas Acupuncture Points, Part 2. Retrieved on March 18, 2008, from <http://www.atimes.com/atimes/china/HJ20Ad01.html>.
- Cowell, Alan. 2008. French Truckers Protest Fuel Prices. Retrieved on August 1, 2008, from <http://www.nytimes.com/2008/06/17/world/europe/17fuel.html>.
- Cox Report. 1999. Retrieved on June 12, 2008, from [http://www.fas.org/spp/starwars/congress/1999\\_r/cox/ch1bod.htm](http://www.fas.org/spp/starwars/congress/1999_r/cox/ch1bod.htm).
- Cuban, Brian. 2008. Confessions of a Banned Digger. Retrieved on September 5, 2008, from <http://www.briancuban.com/confessions-of-a-banned-digger/>.
- Cyberwarfare in International Law. 2008. Retrieved on March 8, 2008, from [http://yro slashdot.org/article.pl?no\\_d2=1&sid=08/01/24/2151233](http://yro slashdot.org/article.pl?no_d2=1&sid=08/01/24/2151233).
- Davidson, Keay. 2004. Air Force Pursuing Antimatter Weapons. Retrieved on March 10, 2008, from <http://www.sfgate.com/cgi-bin/article.cgi?file=c/a/2004/10/04/MNGM393GPK1.DTL>.
- Delio, Michelle. 2001. Code Blue Targets China Firm. Retrieved on February 10, 2008, from <http://www.wired.com/science/discoveries/news/2001/09/46624>.
- Delio, Michelle. 2001. It's Cyber War: China vs. US. Retrieved on July 2, 2008, from <http://www.wired.com/politics/law/news/2001/04/43437>.
- Derene, Glenn. 2008. Inside NSA Red Team Secret Ops with Government's Top Hackers. Retrieved on August 10, 2008, from [http://www.popularmechanics.com/technology/military\\_law/4270420.html](http://www.popularmechanics.com/technology/military_law/4270420.html).
- Dick, Stevens J. 2006. The Importance of Exploration. Retrieved on March 3, 2008, from [http://www.nasa.gov/missions/solarsystem/Why\\_We\\_01pt1.html](http://www.nasa.gov/missions/solarsystem/Why_We_01pt1.html).
- DoS Attacks on Estonia Were Launched by Student. Retrieved on March 8, 2008, from [http://politics slashdot.org/article.pl?no\\_d2=1&sid=08/01/25/0120221](http://politics slashdot.org/article.pl?no_d2=1&sid=08/01/25/0120221).
- Economy, Elizabeth C. And Segal, Adam. 2008. China's Olympic Nightmare. Retrieved on June 30, 2008, from <http://www.foreignaffairs.org/20080701faessay87403-p0/elizabeth->

- [c-economy-adam-segal/china-s-olympic-nightmare.html](http://c-economy-adam-segal/china-s-olympic-nightmare.html).
- Espiner, Tom. 2006. Academics break the Great Firewall of China. Retrieved on July 4, 2008, from [http://news.com.com/2100-7348\\_3-6090437.html?part=rss&tag=6090437&subj=news](http://news.com.com/2100-7348_3-6090437.html?part=rss&tag=6090437&subj=news).
- Espiner, Tom. 2005. Security Experts Lift Lid On Chinese Hack Attacks. Retrieved on February 9, 2008, from [http://news.zdnet.com/2100-1009\\_22-5969516.html](http://news.zdnet.com/2100-1009_22-5969516.html).
- Estonia Fines Man for Cyber War. 2008. Retrieved on February 12, 2008, from <http://news.bbc.co.uk/2/hi/technology/7208511.stm>.
- Estonia Has No Evidence of Kremlin Involvement. 2007. Retrieved on March 10, 2008, from <http://en.rian.ru/world/20070906/76959190.html>.
- Estonia Hit by Moscow Cyber War. 2007. Retrieved on January 23, 2008, from <http://news.bbc.co.uk/2/hi/europe/6665145.stm>.
- Everett, Margaret. Latin America On-line: The Internet, Development, and Democratization. 1998. Retrieved on March 2, 2008, from <http://library.nmsu.edu/subject/bord/laguia/everett.html>.
- Faiola, Anthony. 2005. Anti-Japanese Hostilities Move to the Internet. Retrieved on June 8, 2008, from <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/09/AR2005050901119.html>.
- FCS Watch. Retrieved on March 10, 2008, from [http://www.defensetech.org/archives/cat\\_fcs\\_watch.html](http://www.defensetech.org/archives/cat_fcs_watch.html).
- French, Howard W. 2006. Chinese Tech Buffs Slake Thirst for U.S. TV Shows. Retrieved on August 4, 2008, from [http://www.nytimes.com/2006/08/09/world/asia/09\\_china.html/partner/rssnyt?\\_r=2&oref=slogin](http://www.nytimes.com/2006/08/09/world/asia/09_china.html/partner/rssnyt?_r=2&oref=slogin).
- Friedman, Elisabeth Jay. 2005. The Reality of Virtual Reality. Retrieved February 22, 2008, from <http://programs.ssrc.org/itic/publications/friedman.pdf>.
- Fuel Demo Adds to Road Taxes Row. 2008. Retrieved on August 1, 2008, from [http://news.bbc.co.uk/2/hi/uk\\_news/7420792.stm](http://news.bbc.co.uk/2/hi/uk_news/7420792.stm).
- Future Combat Systems. 2008. Retrieved on March 10, 2008, from <http://www.globalsecurity.org/military/systems/ground/fcs.htm>.
- Gannon, John C. 2001. The National Security Telecommunications and Information Systems Security Committee. Retrieved on February 12, 2008, from [http://www.dni.gov/nic/speeches\\_telecommunications.html](http://www.dni.gov/nic/speeches_telecommunications.html).
- General Staff Department. 1997. Retrieved on March 20, 2008, from [http://www.fas.org/irp/world/china/pla/gen\\_staff.htm](http://www.fas.org/irp/world/china/pla/gen_staff.htm).
- GOA. 1996. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Retrieved on February 5, 2008, from <http://www.fas.org/irp/gao/aim96084.htm>.
- Goodin, Dan. 2008. India and Belgium Decry Chinese Cyber Attacks. Retrieved on June 10, 2008, from [http://www.theregister.co.uk/2008/05/08/belgium\\_india\\_china\\_warnings/](http://www.theregister.co.uk/2008/05/08/belgium_india_china_warnings/).
- Google censors itself for China. 2006. Retrieved on July 22, 2006, from <http://news.bbc.co.uk/2/hi/technology/4645596.stm>.
- Graham, Bradley. 2005. Hackers Attack Via Chinese Websites. Retrieved on January 8, 2008, from <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html>.
- Greenberg, Andy. 2007. Apples For The Army. Retrieved on January 20, 2008, from [http://www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx\\_ag\\_1221army.html](http://www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx_ag_1221army.html).
- Greenberg, Andy. 2007. Worst Cybersecurity Meltdowns. Retrieved on February 18, 2008, from [http://www.forbes.com/2007/10/26/tjx-northrop-mcafee-ent-tech-cx\\_ag\\_1026worsthacks.html](http://www.forbes.com/2007/10/26/tjx-northrop-mcafee-ent-tech-cx_ag_1026worsthacks.html).
- Greenemeier, Larry. 2007. China's Cyber Attacks Signal New Battlefield Is Online. Retrieved on July 7, 2008, from <http://www.sciam.com/article.cfm?id=chinas-cyber-attacks-sign>.
- Grier, Peter. 2005. Spy Case Patterns The Chinese Style of Espionage. Retrieved on March 23, 2008, from <http://www.csmonitor.com/2005/1130/p01s01-usfp.html>.
- Griggs, Brandon. 2008. US at risk of Cyberattacks, Experts Say. Retrieved on August 25, 2008, from <http://edition.cnn.com/2008/TECH/08/18/cyber.warfare/index.html>.
- Hacker Attacks in US Linked to Chinese Military. 2005. Retrieved on July 21, 2006, from <http://www.breitbart.com/news/2005/12/12/051212224756.jwmkvntb.html>.
- Hacking Textfiles. 2008. Retrieved on June 8, 2008, from <http://www.textfiles.com/hacking/>.

- Hacking US Government Computers from Overseas. 2001. Retrieved on February 2, 2008, from [http://www.totse.com/en/hack/understanding\\_the\\_internet/163724.html](http://www.totse.com/en/hack/understanding_the_internet/163724.html).
- Hanson, Stephanie. 2008. China, Africa, and Oil. Retrieved on June 12, 2008, from <http://www.cfr.org/publication/9557/>.
- Ha, Michael. 2008. China Gateway for Most Cyber-Attacks. Retrieved on June 20, 2008, from [http://www.koreatimes.co.kr/www/news/nation/2008/05/116\\_24499.html](http://www.koreatimes.co.kr/www/news/nation/2008/05/116_24499.html).
- Heilemann, John. 2006. How Digg.com is Democratizing the News. Retrieved on March 27, 2007 from <http://money.cnn.com/2006/03/24/magazines/business2/diggdemocratizes/index.htm>.
- Hershkovitch, Ady. 1998. Plasma Window Technology for Propagating Particle Beams and Radiation from Vacuum to Atmosphere. Retrieved on March 10, 2008, from <http://www.techbriefs.com/content/view/1834/32/1/0/>.
- Hi-tech Thieves Target Olympics. 2008. Retrieved on August 20, 2008, from <http://news.bbc.co.uk/2/hi/technology/7548870.stm>.
- Hill, John. 2004. China's Assassin's Mace Meets The Taiwanese Scorpion. Retrieved on March, 18, 2008, from <http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1044>.
- Hines, Matt. 2008. Be prepared: ActiveX attacks will persist. Retrieved on March 10, 2008, from [http://www.infoworld.com/article/08/02/19/08NF-activex-horror\\_1.html](http://www.infoworld.com/article/08/02/19/08NF-activex-horror_1.html).
- Hollis, Duncan. Why States Need an International Law For Information Operations. Retrieved on March 2, 2008, from [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1083889](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1083889).
- Ikenberry, John G. 2008. The Rise of China and the Future of the West. Retrieved on February 10, 2008, from <http://www.foreignaffairs.org/20080101faessay87102-p0/g-john-ikenberry/the-rise-of-china-and-the-future-of-the-west.html>.
- Indonesia: Growing Fuel Price Protest Meet Repression. 2008. Retrieved on August 1, 2008, from <http://www.greenleft.org.au/2008/752/38852>.
- Information Operations Roadmap. 2003. Declassified US Government document. Retrieved on March 1, 2008, from [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info\\_ops\\_roadmap.pdf](http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf).
- International Assessment and Strategy Center. 2005. Top Ten Chinese Military Modernization Developments. Retrieved on February 15, 2008, from [http://www.strategycenter.net/research/pubID.65/pub\\_detail.asp](http://www.strategycenter.net/research/pubID.65/pub_detail.asp).
- International Institute for Strategic Studies. 2008. The Military Balance 2008. Routledge for IISS, Abingdon.
- Internet censorship in the People's Republic of China. 2006. Retrieved on August 2, 2008, from [http://en.wikipedia.org/wiki/The\\_Great\\_Firewall](http://en.wikipedia.org/wiki/The_Great_Firewall)
- Internet Filtering in China in 2004-2005. 2005. Retrieved on July 21, 2008, from <http://opennet.net/studies/china>.
- Internet Group Declares War on Scientology. Retrieved on March 8, 2008, from [http://yro.slashdot.org/article.pl?no\\_d2=1&sid=08/01/24/1311252](http://yro.slashdot.org/article.pl?no_d2=1&sid=08/01/24/1311252).
- Iran Missile Test Provocative. 2008. Retrieved on August 2, 2008, from [http://news.bbc.co.uk/2/hi/middle\\_east/7498214.stm](http://news.bbc.co.uk/2/hi/middle_east/7498214.stm).
- Isachenkov, Vladimir. 2007. Russian Space Exec Convicted For Aiding China. Retrieved on March 10, 2008, from <http://www.msnbc.msn.com/id/22082431/>.
- ISN. 2001. Code Red virus probably began in China. Retrieved on July 18, 2006, from <http://www.landfield.com/isn/mail-archive/2001/Sep/0007.html>.
- Jesdanun, Anick. 2008. Chinese Internet Users Up to 210 Million. Retrieved on February 20, 2008, from <http://www.physorg.com/news119947914.html>.
- Johnston, Alastair. 2002. Toward Contextualizing the Concept of a Shashoujian (Assassin's Mace). Retrieved on February 24, 2008, from <http://www.people.fas.harvard.edu/~johnston/shashoujian.pdf>.
- Jordan, Jakes. 2008. US Charges 2 In China Spy Case. Retrieved on April 1, 2008, from <http://www.time.com/time/world/article/0,8599,1726799,00.html>.
- Kiezer, Gregg. 2005. Dutch Botnet Suspects Ran 1.5 Million Machines. Retrieved on August 1, 2008, from <http://www.techweb.com/wire/security/172303160>.
- Kerner, Sean. 2007. Estonia Under Russian Cyber Attack? Retrieved on February 19, 2008, from <http://www.internetnews.com/security/article.php/3678606>.
- Klein, Alec. 2007. The Army's \$200 Billion Makeover. Retrieved on March 10, 2008, from <http://www.washingtonpost.com/wp-dyn/content/story/2007/12/06/ST2007120602927.html>.

- Kumar, T. 2006. Human Rights and the Internet in China. Retrieved on August 4, 2008, from <http://www.amnestyusa.org/document.php?id=ENGUSA20060201001>.
- Lam, Willy Wo-lap. 2004. Beijing's New "Balanced" Foreign Policy: An Assessment. China Brief, Vol. 4, No. 4, 20 February. The Jamestown Foundation, Retrieved on February 6, 2006, from [http://www.jamestown.org/publications\\_details.php?volume\\_id=395&&issue\\_id=2912](http://www.jamestown.org/publications_details.php?volume_id=395&&issue_id=2912)
- Landler, Mark and Markoff, John. 2007. Digital Fears Emerge After Data Siege in Estonia Retrieved on February 2, 2008, from [http://www.nytimes.com/2007/05/29/technology/29estonia.html?\\_r=2&ref=technology&oref=slogin&oref=slogin](http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=2&ref=technology&oref=slogin&oref=slogin).
- Lasker, John. 2005. US Military's Elite Hacker Crew. Retrieved on February 18, 2008, from <http://www.wired.com/politics/security/news/2005/04/67223>.
- Layer 8. 2007. Did her MySpace photo derail teacher's career? Retrieved on June 18, 2008, from <http://www.networkworld.com/community/?q=node/14584>.
- Lemon, Sumner. 2008. China Crafts Cyber Weapons. Retrieved on June 2, 2008, from [http://www.pcworld.com/article/132284/china\\_crafts\\_cyberweapons.html](http://www.pcworld.com/article/132284/china_crafts_cyberweapons.html).
- Lemon, Sumner. 2007. Chinese Police Arrest Eight For Computer Virus. Retrieved on March 20, 2008, from [http://www.infoworld.com/article/07/02/13/HNchinesearresteight\\_1.html](http://www.infoworld.com/article/07/02/13/HNchinesearresteight_1.html).
- Lewis, Jeffrey. 2005. Autonomous Nanosatellite Guardian For Evaluating Local Space (ANGELS). Retrieved on March 10, 2008, from <http://www.defensetech.org/archives/001996.html>.
- Lewis, Peter. 1994. Computer Snoopers Imperil Pentagon Files, Experts Say. Retrieved on July, 2, 2008, from <http://query.nytimes.com/gst/fullpage.html?res=9F04E3DD143EF932A15754C0A962958260>.
- Leyden, John. 2007. France blames China for hack attacks. Retrieved on January 2, 2008, from [http://www.theregister.co.uk/2007/09/12/french\\_cyberattacks/](http://www.theregister.co.uk/2007/09/12/french_cyberattacks/).
- Leyden, John. 2004. Telenor Takes Down Massive Botnet. Retrieved on August 1, 2008 from [http://www.theregister.co.uk/2004/09/09/telenor\\_botnet\\_dismantled/](http://www.theregister.co.uk/2004/09/09/telenor_botnet_dismantled/).
- Leyden, John. 2001. Code Blue Targets Red China. Retrieved on July 18, 2006, from [http://www.theregister.co.uk/2001/09/10/code\\_blue\\_targets\\_red\\_china/](http://www.theregister.co.uk/2001/09/10/code_blue_targets_red_china/).
- Levinson, Charles. 2008. Hackers Attack Iraq's Vulnerable Computers. Retrieved on August, 25, 2008, from <http://abcnews.go.com/Technology/story?id=5685746&page=1>.
- Liedtke, Michael. 2005. Google Agrees to Censor Results in China. Retrieved on July 22, 2006, from <http://www.breitbart.com/news/2006/01/24/D8FBC4C02.html>.
- List of Internet Phenomena. 2008. Retrieved on April 10, 2008, from [http://en.wikipedia.org/wiki/List\\_of\\_Internet\\_phenomena](http://en.wikipedia.org/wiki/List_of_Internet_phenomena).
- Lo, Joseph. 1996. Internet Chat Relay FAQ. Retrieved on March 15, 2006, from <http://irchelp.org/irchelp/altircfaq.html>.
- Luard, Tim. 2005. China's Spies Come Out From The Cold. Retrieved on April 2, 2008, from <http://news.bbc.co.uk/2/hi/asia-pacific/4704691.stm>.
- Lynch, David. 2007. Law Enforcement Struggles To Combat Chinese Spying. Retrieved on March 23, 2008, from [http://www.usatoday.com/money/world/2007-07-22-china-spy-1\\_N.htm](http://www.usatoday.com/money/world/2007-07-22-china-spy-1_N.htm).
- Malone, Scott. 2008. Hackers stole 40 million credit card numbers. Retrieved on August 10, 2008, from <http://www.australianit.news.com.au/story/0,24897,24136467-15306,00.html>.
- Marshall, Matt. 2008. Xiaonei, The Facebook Of China, Raises \$430M. Retrieved on April 2, 2008, from <http://venturebeat.com/2008/04/30/xiaonei-the-facebook-of-china-raises-430m-better-funded-than-facebook/>.
- Magnuson, Stew. 2006. Wikipedia for Intel Officers Proves Useful. Retrieved on July 7, from <http://www.allbusiness.com/public-administration/national-security-international/3932331-1.html>.
- Mao, Tse-Tung [Zedong]. 2000. On Guerrilla Warfare (trans. Samuel B. Griffith). Chicago: University of Illinois Press
- Mark, David. 2008. Scientists one step closer to invisibility cloak. Retrieved on August 12, 2008, from <http://www.abc.net.au/news/stories/2008/08/11/2330897.htm>.
- Marquand, Robert. 2007. China Emerges As Leader In Cyber Warfare. Retrieved on April, 10, 2008, from <http://www.csmonitor.com/2007/0914/p01s01-woap.html>.
- Marsal, Katie. 2008. China asking Apple to intentionally cripple iPhones. Retrieved on September 26, 2008, from [http://www.appleinsider.com/articles/08/09/25/china\\_mobile\\_asking\\_apple\\_to\\_intentionally\\_cripple\\_iphones.html](http://www.appleinsider.com/articles/08/09/25/china_mobile_asking_apple_to_intentionally_cripple_iphones.html).
- Maynor, David and Graham, Robert. 2006. SCADA Security and Terrorism: We're Not



- Crying Wolf. Retrieved on February 27, 2008, from <http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf>.
- McLaughlin, Martin. 1999. China Spy Scare. Retrieved on March 23, 2008, from <http://www.wsws.org/articles/1999/mar1999/chin-m10.shtml>.
- McLean, Doug. 1995. Hacking in 17 Easy Steps. Retrieved on January 15, 2008, from <http://web.archive.org/web/20010708111438/http://www.claws-and-paws.com/personal/hacking/17steps.shtml>.
- McMillan, Robert. 2008. CIA Says Hackers Have Cut Power Grid. Retrieved on January 19, 2008, from <http://www.pcworld.com/article/id,141564-pg,1/article.html>.
- McMillan, Robert. 2008. Hackers Hit Scientology With Online Attack. Retrieved on July 14, 2008, from [http://www.pcworld.com/article/141839/hackers\\_hit\\_scientology\\_with\\_online\\_attack.html](http://www.pcworld.com/article/141839/hackers_hit_scientology_with_online_attack.html).
- McMillan, Robert. 2007. Couple Swarmed By SWAT Team After 911 Hack. Retrieved on June 7, 2008, from <http://www.macworld.com/article/60576/2007/10/swat.html>.
- Miklaszewski, Jim. 1999. Pentagon and Hackers in Cyberwar. Retrieved on February 2, 2008, from [http://news.zdnet.com/2100-9595\\_22-513930.html](http://news.zdnet.com/2100-9595_22-513930.html).
- Milchman, Eli. 2006. Yahoo 'Strictest' Censor in China. Retrieved on July 15, 2006, from <http://www.wired.com/news/technology/internet/0,71166-0.html?tw=rss.index>.
- Miller, Chuck 2008. The Rustock botnet spams again, SC Magazine July 25, from <http://www.scmagazineus.com/The-Rustock-botnet-spams-again/article/112940/>
- Ministry of Internal Affairs Lists PMR's 10 Most Wanted. 2007. Retrieved on March 10, 2008, from [http://www.tiraspoltimes.com/news/ministry\\_of\\_internal\\_affairs\\_lists\\_pmrs\\_10\\_most\\_wanted.html](http://www.tiraspoltimes.com/news/ministry_of_internal_affairs_lists_pmrs_10_most_wanted.html).
- Missiles and Space Programme. 2008. Retrieved on March 20, 2008, from <http://sinodefence.com/strategic/default.asp>
- Moore, Frank W. China's Military Capabilities. 2000. Retrieved on February 18, 2008, from <http://www.comw.org/cmp/fulltext/iddschina.html>.
- Moss, William. 2006. Chinese YouTubes courting controversy. Retrieved on July 20, 2006, from <http://asia.cnet.com/reviews/blog/littleredblog/0,39056119,39375940,00.htm>.
- Musharbash, Yassin. 2008. Insights Into The Cyber-Jihad. Retrieved on August 30, 2008, from <http://www.spiegel.de/international/world/0,1518,575276,00.html>.
- Navrozov, Lev. 2005. Chinese Geostrategy: The Assassin's Mace. Retrieved on February 10, 2008, from <http://archive.newsmag.com/archives/articles/2005/10/20/172811.shtml>.
- Newhouse, Barry. 2006. Group Accuses Internet Companies in China of Rights Violations. Retrieved on July 21, 2006, from <http://www.voanews.com/english/2006-07-20-voa16.cfm>.
- New Technology Can Be Operated By Thought. 2007. Retrieved on March 10, 2008, from <http://www.sciencedaily.com/releases/2007/11/071107210708.htm>.
- Nock, Howard and Lizun, Daniel. 2007. Cyberterrorism and Cybercrime: Are You Prepared. Retrieved on January 28, 2008, from <http://www.clevelandfed.org/bsr/Conditions/v3n2/v3n2.htm>.
- Norton-Taylor, Richard. 2007. Titan Rain: How Chinese Hackers Targeted Whitehall. Retrieved on January 8, 2008, from <http://www.guardian.co.uk/technology/2007/sep/04/news.internet>.
- Nuclear Electromagnetic Pulse. 2005. Retrieved on August 23, 2008, from <http://cryptome.org/bartlett-060905.txt>.
- O'Brien, Kevin. 2008. OLPC XO Review and Teardown. Retrieved on January 14, 2008, from <http://www.notebookreview.com/default.asp?newsID=4199>.
- O'Connell, Kelly. 2008. Internet Law: Hackers Disable Scientology Website & Declare War. Retrieved on July 14, 2008, from [http://www.ibls.com/internet\\_law\\_news\\_portal\\_view.aspx?s=latestnews&id=1972](http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1972).
- Of Cables and Conspiracies. 2008. Retrieved on July 4, 2008, from [http://www.economist.com/world/international/displaystory.cfm?story\\_id=10653963](http://www.economist.com/world/international/displaystory.cfm?story_id=10653963).
- Oliver, Chris. 2008. China's foreign exchange reserves jump 61.6 bln in January. Retrieved on March 13, 2008, from <http://www.marketwatch.com/news/story/chinas-foreign-exchange-reserves-jump/story.aspx?guid=%7BEBE6E206-9BE9-4329-B71A-2AF2F903A5AD%7D>.

- Onley, Dawn and Wait, Patience. 2006. Red Storm Rising. Retrieved on January 8, 2008, from [http://www.gcn.com/print/25\\_25/41716-1.html](http://www.gcn.com/print/25_25/41716-1.html).
- Operation Spam Zombies. 2005. Retrieved on August 1, 2008, from <http://www.ftc.gov/bcp/online/edcams/spam/zombie/partners.htm>.
- Pang, Kevin. 2008. Chinese text-message primer. Retrieved on August 25, 2008, from <http://www.chicagotribune.com/features/lifestyle/chi-chinese.text.0812aug12.0.606145.story>.
- Paramilitary Olympics: Beijing: at least 94,000 security staff – but only 10,500 athletes. 2008. The Independent, April 13. Retrieved on September 20, 2008, from <http://www.independent.co.uk/news/world/asia/paramilitary-olympics-beijing-at-least-94000-security-staff-ndash-but-only-10500-athletes-808490.html>.
- Pasternack, Alex. 2008. When Nature Won't Cooperate in China, Photoshop! Retrieved on April 10, 2008, from [http://www.treehugger.com/files/2008/02/fake\\_photo\\_tibet\\_railway\\_antelope\\_greenwashing.php](http://www.treehugger.com/files/2008/02/fake_photo_tibet_railway_antelope_greenwashing.php).
- Paul, Ryan. 2007. Top US government research labs infiltrated by hackers. Retrieved on February 10, 2008, from <http://arstechnica.com/news.ars/post/20071209-top-us-military-research-labs-infiltrated-by-hackers.html>.
- People's Daily Online. 2006. Authorities make first hit in anti-piracy campaign. Retrieved on July 29, 2008, from [http://english.people.com.cn/200607/29/eng20060729\\_288072.html](http://english.people.com.cn/200607/29/eng20060729_288072.html).
- People's Armed Police. 2005. Retrieved on March 20, 2008, from <http://www.globalsecurity.org/intell/world/china/pap.htm>.
- People's Armed Police Force Organisation. 2007. Retrieved on March 20, 2008, from <http://www.sinodefence.com/organisation/armedpolice/introduction.asp>.
- Phone Phreaking. 2008. Retrieved on June 26, 2008, from <http://www.textfiles.com/phreak/>.
- Pike, John. 2008. China's Defense Budget. Retrieved on February 2, 2008, from <http://www.globalsecurity.org/military/world/china/budget.htm>.
- Pike, John. 2008. X-45 Unmanned Combat Air Vehicle (UCAV). Retrieved on August 10, 2008, from <http://www.fas.org/man/dod-101/sys/ac/ucav.htm>.
- Pillsbury, Michael. 2000. China Debates the Future Security Environment. National Defense University Press. Retrieved on February 2, 2008, from <http://www.fas.org/nuke/guide/china/doctrine/pills2/part08.htm>.
- Pirates of the Orient. 2006. Retrieved on July 15, 2008, from [http://www.thestandard.com.hk/weekend\\_news\\_detail.asp?pp\\_cat=30&art\\_id=22887&sid=8816949&con\\_type=3&d\\_str=20060715](http://www.thestandard.com.hk/weekend_news_detail.asp?pp_cat=30&art_id=22887&sid=8816949&con_type=3&d_str=20060715).
- Polyanskaya, Anna. 2006. Commissars of the Internet. Retrieved on June 12, 2008, from <http://lrtranslations.blogspot.com/2007/02/commissars-of-internet.html>.
- PRC Acquisitions of US Technology. 1998. Retrieved on March 10, 2008, from [http://www.fas.org/spp/starwars/congress/1999\\_r/cox/ch1bod.htm](http://www.fas.org/spp/starwars/congress/1999_r/cox/ch1bod.htm).
- Put Your Mobile Where Your Mouth Is. 2002. Retrieved on March 10, 2008, from <http://news.bbc.co.uk/2/hi/science/nature/2055654.stm>.
- Qiao, Liang and Wang Xiangsui. 1999. Unrestricted Warfare. Retrieved on February 10, 2008, from <http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf>.
- Raduege, Harry. 2004. Net-Centric Warfare Is Changing The Battlefield Environment. Retrieved on April 2, 2008, from [http://www.stsc.hill.af.mil/crosstalk/2004/01/0401\\_Raduege.html](http://www.stsc.hill.af.mil/crosstalk/2004/01/0401_Raduege.html).
- Ramadge, Andrew. 2008. Scientology protest surge crashes websites. Retrieved on July 14, 2008, from <http://www.news.com.au/technology/story/0,25642,23212002-5014239,00.html>.
- Raun, Alo. 2007. Venemaa jätab Eesti küberrünakute uurimisel õigusabita. Retrieved on March 10, 2008, from <http://www.postimees.ee/060707/esileht/siseudised/270899.php>.
- Reid, Tim. 2007. China's cyber army is preparing to march on America, says Pentagon. Retrieved on February 21, 2008, from [http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/the\\_web/article2409865.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece).
- Reporters Without Borders. 2006. Yahoo ! implicated in third cyberdissident trial. Retrieved on July 25, 2008, from [http://www.rsf.org/article.php3?id\\_article=17180](http://www.rsf.org/article.php3?id_article=17180).
- Richards, Jonathan. 2008. China Blocks YouTube Yahoo! Over Tibet. Retrieved on March 12, 2008, from [http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/article3568040.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/article3568040.ece).
- Robson, Gary. 2004. The Origins of Phreaking. Retrieved on June 28, 2008, from <http://www.robson.org/gary/writing/phreaking.html>.
- SBDCNET. 2001. Convenience Store/Gasoline Station Market Profile. Retrieved on June 1,

- 2008, from [http://sbdnet.utsa.edu/industry/gas\\_stations.pdf](http://sbdnet.utsa.edu/industry/gas_stations.pdf).
- Schearf, Daniel. 2006. Chinese Intellectuals Condemn Web Site Closure. Retrieved on August 4, 2008, from <http://www.voanews.com/english/2006-08-04-voa17.cfm>.
- Second Artillery Corps. 2000. Retrieved on March 20, 2008, from <http://www.fas.org/nuke/guide/china/agency/2-corps.htm>.
- Second Intelligence Department. 2005. Retrieved on March 24, 2008, from [http://www.globalsecurity.org/intell/world/china/pla-dept\\_2.htm](http://www.globalsecurity.org/intell/world/china/pla-dept_2.htm).
- Schwartz, John. 2007. When Computers Attack. Retrieved on February 2, 2008, from [http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html?\\_r=1&oref=slogin](http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html?_r=1&oref=slogin).
- Shaughnessy, Larry. 2008. CIA, FBI push Facebook for Spies. Retrieved on September 5, 2008, from [http://edition.cnn.com/2008/TECH/ptech/09/05/facebook.spies/index.html?eref=rss\\_latest](http://edition.cnn.com/2008/TECH/ptech/09/05/facebook.spies/index.html?eref=rss_latest).
- Single, Ryan. 2008. War Breaks Out Between Hackers And Scientology. Retrieved on July 14, 2008, from <http://blog.wired.com/27bstroke6/2008/01/anonymous-attac.html>.
- Skype Protocol Has Been Cracked. 2006. Retrieved on July 14, 2008, from <http://politics.slashdot.org/article.pl?sid=06/07/14/1514226>.
- Slashdot Subculture. 2008. Retrieved on April 10, 2008, from [http://wikipedia.qwika.com/en/Slashdot\\_subculture](http://wikipedia.qwika.com/en/Slashdot_subculture).
- Slashdot Trolling Phenomenon. 2008. Retrieved on April 10, 2008, from [http://wikipedia.qwika.com/en/Slashdot\\_trolling\\_phenomena](http://wikipedia.qwika.com/en/Slashdot_trolling_phenomena).
- Small Arms. 2008. Retrieved on April 10, 2008, from [http://www.sinodefence.com/army/small\\_arms/default.asp](http://www.sinodefence.com/army/small_arms/default.asp).
- Smith, Charles. 2001. Russian Rocket Torpedo Arms Chinese Subs. Retrieved on February 10, 2008, from <http://archive.newsmax.com/archives/articles/2001/4/23/220813.shtml>.
- Sobrale, Saada. 2007. Venemaa keeldus koostööst küberrünnakute uurimisel. Retrieved on March 10, 2008, from <http://www.epl.ee/artikkel/392271>.
- Stroom. 2008. Westpac Glitch Leaves Customers Cashless. Retrieved on August 13, 2008, from <http://www.stroom.com.au/breaking-news/6326-thousands-blocked-as-westpac-crashes>.
- Sun Tzu [Zi]. 1963. *The Art of War* (trans. Samuel B. Griffith). London: Oxford University Press.
- Surface Combatants. 2008. Retrieved on April 9, 2008, from <http://www.sinodefence.com/navy/surface/default.asp>.
- Taiwan Assassin. 2004. Retrieved on April 7, 2008, from <http://www.tzengs.com/News/Assasin/photos.htm>.
- Talmadge, Caitlin. 2008. Closing Time: Assessing the Iranian Threat to the Strait of Hormuz. Retrieved on August 2, 2008, from [http://belfercenter.ksg.harvard.edu/publication/18409/closing\\_time.html](http://belfercenter.ksg.harvard.edu/publication/18409/closing_time.html).
- Tellis, Ashley. 2007. China's Military Space Strategy. Retrieved on January 28, 2008, from <http://www.informaworld.com/smpp/section?content=a780978527&fulltext=713240928>.
- Thai Truckers Join Global Fuel Price Protest. 2008. Retrieved on August 1, 2008, from <http://business.smh.com.au/business/thai-truckers-join-global-fuel-price-protest-20080611-2oy3.html>.
- The Christian Science Monitor. 2006. China's new shopping craze: 'team buying'. Retrieved on August 1, 2008, from <http://articles.moneycentral.msn.com/SavingandDebt/FindDealsOnline/ChinasNewShoppingCrazeTeamBuying.aspx>.
- The Cyber Raiders Hitting Estonia. 2007. Retrieved on February 12, 2008, from <http://news.bbc.co.uk/2/hi/europe/6665195.stm>.
- The Passion of Anonymous. 2008. Retrieved on July 14, 2008, from <http://www.newsweek.com/id/109410>.
- Thornburgh, Nathan. 2005. Inside the Chinese Hack Attack. Retrieved on July 21, 2008, from <http://www.time.com/time/nation/article/0,8599,1098371,00.html>.
- Thornburgh, Nathan. 2005. The Invasion of the Chinese Cyberspies. Retrieved on March 2, 2008 from <http://www.time.com/time/magazine/article/0,9171,1098961,00.html>.
- Tkacik, John J Jr. 2007. Trojan Dragons: China's Cyber Threat. Retrieved on March 20, 2008, from <http://www.heritage.org/Research/asiaandthepacific/bg2106.cfm>.
- Towards one laptop per child. 2006. Retrieved on July 28, 2008, from <http://www.sunstar.com.ph/static/ceb/2006/07/24/bus/towards.one.laptop.per.child.html>.
- Trahan, Jason. 2008. Teen wouldn't quit his hacking ways, FBI says. Retrieved on August 31, 2008, from [http://www.dallasnews.com/sharedcontent/dws/news/nation/stories/DN-swating\\_31met.ART0.West.Edition1.4ddc7cf.html](http://www.dallasnews.com/sharedcontent/dws/news/nation/stories/DN-swating_31met.ART0.West.Edition1.4ddc7cf.html).

United States General Accounting Office (GAO), Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures, Statement of Keith A. Rhodes, Chief Technologist, August 29, 2001 (GAO-01-1073T), see <http://www.gao.gov/new.items/d011073t.pdf>

Use of Social Network Websites in Investigations. 2008. Retrieved on August 12, 2008, from [http://en.wikipedia.org/wiki/Use\\_of\\_social\\_network\\_websites\\_in\\_investigations](http://en.wikipedia.org/wiki/Use_of_social_network_websites_in_investigations).

Vallance, Chris. 2008. US Seeks Terrorists In The Web Worlds. Retrieved on March 8, 2008, from <http://news.bbc.co.uk/2/hi/technology/7274377.stm>.

Vamosi, Robert. 2008. Anonymous posts another video against Scientology. Retrieved on July 14, 2008, from [http://news.cnet.com/8301-10789\\_3-9859513-57.html](http://news.cnet.com/8301-10789_3-9859513-57.html).

VoIPWiki Blog. 2006. Skype Protocol Has Been Cracked. Retrieved on July 14, 2008, from <http://www.voipwiki.com/blog/?p=16>.

Wagstaff, Jeremy. 2005. The First U.S.- China Cyberwar. Retrieved on July 27, 2008, from [http://loosewire.typepad.com/blog/2005/12/the\\_first\\_uschi.html](http://loosewire.typepad.com/blog/2005/12/the_first_uschi.html).

Warrick, Joby and Johnson, Carrie. 2008. Chinese Spy Slept In US For 2 Decades. Retrieved on April 3, 2008, from <http://www.washingtonpost.com/wp-dyn/content/story/2008/04/02/ST2008040204050.html>.

Warren, Peter. 2006. Smash and grab, the hi-tech way. Retrieved on July 18, 2008, from <http://technology.guardian.co.uk/weekly/story/0,,1689093,00.html>.

Waterman, Shaun. 2008. Analysis DHS Stages Cyberwar Exercise. Retrieved on April 10, 2008, from [http://www.spacewar.com/reports/Analysis\\_DHS\\_stages\\_cyberwar\\_exercise\\_999.html](http://www.spacewar.com/reports/Analysis_DHS_stages_cyberwar_exercise_999.html).

Waterman, Shaun. 2008. Analysis: Russia-Georgia Cyber War Doubted. Retrieved on August 18, 2008, from [http://www.spacewar.com/reports/Analysis\\_Russia-Georgia\\_cyber\\_war\\_doubted\\_999.html](http://www.spacewar.com/reports/Analysis_Russia-Georgia_cyber_war_doubted_999.html).

Waterman, Shaun. 2008. Chinese Cyberattacks Target US Think Tanks. Retrieved on March 8, 2008, from [http://www.spacewar.com/reports/Chinese\\_Cyberattacks\\_Target\\_US\\_Think\\_Tanks\\_999.html](http://www.spacewar.com/reports/Chinese_Cyberattacks_Target_US_Think_Tanks_999.html).

Waterman, Shaun. 2007. China Has .75 Million Zombie Computers In US. Retrieved on March 17, 2008, from [http://www.upi.com/International\\_Security/Emerging\\_Threats/Briefing/2007/09/17/china\\_has\\_75m\\_zombie\\_computers\\_in\\_us/7394/](http://www.upi.com/International_Security/Emerging_Threats/Briefing/2007/09/17/china_has_75m_zombie_computers_in_us/7394/).

Waterman, Shaun. 2007. Who cyber smacked Estonia? Retrieved on January 17, 2008 from [http://www.upi.com/Security\\_Terrorism/Analysis/2007/06/11/analysis\\_who\\_cyber\\_smacked\\_estonia/2683/](http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/).

Wayner, Peter. 1999. Hacker Attacks on Military Networks May Be Closer to Espionage. Retrieved on August 10, 2008, from <http://www.landfield.com/isn/mail-archive/1999/Mar/0022.html>.

Weber, Harry. 2008. FAA Says Communications Breakdown Delaying Flights. Retrieved on August 28, 2008, from [http://news.yahoo.com/s/ap/20080826/ap\\_on\\_re\\_us/faa\\_communication\\_breakdown;\\_ylt=A0WTUeXUlbRISucAawSs0NUE](http://news.yahoo.com/s/ap/20080826/ap_on_re_us/faa_communication_breakdown;_ylt=A0WTUeXUlbRISucAawSs0NUE).

Weber, Tim. 2007. Criminals may overwhelm the web. Retrieved on August 1, 2008, from <http://news.bbc.co.uk/1/hi/business/6298641.stm>.

Wei, Michael. 2008. Facebook Targets China, World's Biggest Web Market. Retrieved on June 20, 2008, from <http://www.reuters.com/article/ousiv/idUSSHA17883120080620>.

Wensheng, Wang. 2006. Bridging the Digital Divide Inside China. Retrieved on July 28, 2008, from <http://zoushoku.narc.affrc.go.jp/ADR/AFITA/afita/afita-conf/2002/part7/p533.pdf>.

WFTV. 2008. Girls Record Brutal Attack On Teen To Allegedly Post on YouTube. Retrieved On May 10, 2008, from <http://www.wftv.com/news/15817394/detail.html>.

Winkler, Ira. 2005. Guard Against Titan Rain Hackers. Retrieved on January 8, 2008, from <http://www.computerworld.com/securitytopics/security/story/0,10801,105585,00.html>.

Winkler, Ira. 2007. How To Take Down The Power Grid. Retrieved on June 7, 2008, from [http://www.internetevolution.com/author.asp?section\\_id=515&doc\\_id=136047](http://www.internetevolution.com/author.asp?section_id=515&doc_id=136047).

Winkler, Tim. 2003. Dragonflies Prove Clever Predators. Retrieved on February 10, 2008, from [http://info.anu.edu.au/ovc/media/Media\\_Releases/2003/030605Dragonflies.asp](http://info.anu.edu.au/ovc/media/Media_Releases/2003/030605Dragonflies.asp).

Winn, Patrick. 2008. Hypothetical attack on U.S. outlined by China. Retrieved on February 23, 2008, from [http://www.airforcetimes.com/news/2008/01/airforce\\_china\\_strategy\\_080121/](http://www.airforcetimes.com/news/2008/01/airforce_china_strategy_080121/).

Whitney, Mike. 2008. Three Internet Cables Slashed In A Week. Retrieved on July 4, 2008,

- from <http://www.globalresearch.ca/index.php?context=va&aid=7987>.
- World Wide Military Expenditures. 2007. Retrieved on August 12, 2008, from <http://www.globalsecurity.org/military/world/spending.htm>.
- Wortzel, Larry M. 2007. China's Nuclear Forces: Operations, Training, Doctrine, Command, Control, and Campaign Planning. US Strategic Studies Institute. Retrieved on December 11, 2007, from [www.StrategicStudiesInstitute.army.mil/](http://www.StrategicStudiesInstitute.army.mil/).
- Yahoo Implicated In Third Cyberdissident Trial. 2006. Retrieved on March 11, 2008, from [http://www.rsf.org/article.php3?id\\_article=17180](http://www.rsf.org/article.php3?id_article=17180).
- Yeates, Ed. 2007. Exoskeleton Turns Humans Into Terminators. Retrieved on March 10, 2008, from <http://www.youtube.com/watch?v=h2jIIRKswnQ>.
- Yue, Qi and Yue Qin. 2008. China Regime Implicated In Staging Violence In Tibetan Protest. Retrieved on April 3, 2008, from <http://chinaview.wordpress.com/2008/03/29/photo-china-regime-implicated-in-staging-violence-in-tibet-protest/>.
- Zheng, Yongnian and Sow Keat Tok. 2007. 'Harmonious Society' and 'Harmonious World': China's Policy Discourse under Hu Jintao. Briefing Series, Issue 26, October. China Policy Institute. Retrieved on October 2, 2008, from [http://www.nottingham.ac.uk/shared/shared\\_cpi/documents/policy\\_papers/Briefing\\_26\\_Harmonious\\_Society\\_and\\_Harmonious\\_World.pdf](http://www.nottingham.ac.uk/shared/shared_cpi/documents/policy_papers/Briefing_26_Harmonious_Society_and_Harmonious_World.pdf).