


How Secure are Our Elections?

Introduction

- Nature of the voting transaction
 - History of voting technologies
 - Threat models
 - Detection
 - Risk mitigation
- 
- A large, light blue decorative shape at the bottom of the slide, resembling a rounded triangle or a wave, pointing towards the right.

“It's not who votes that counts...
it's who counts the votes.”

- Stalin

A blue gradient shape at the bottom of the slide, starting from the left and curving upwards towards the right.

Voting fundamentals

Voting is a special type of “civic transaction”

- In the modern world, voting is both private *and* anonymous
- Ancient voting systems were neither
- Sale and coercion of votes led to private ballots cast on paper
- Perceived problems with hand counted paper ballots led to automation
 - Mechanical lever (1890s)
 - Punch card (1960s)
 - Push button (1960s) ... touchscreen (1990s)
 - Optical scan (1980s)

Who runs elections?

The high school civics view of the world is wrong.

Election officials do not run elections!

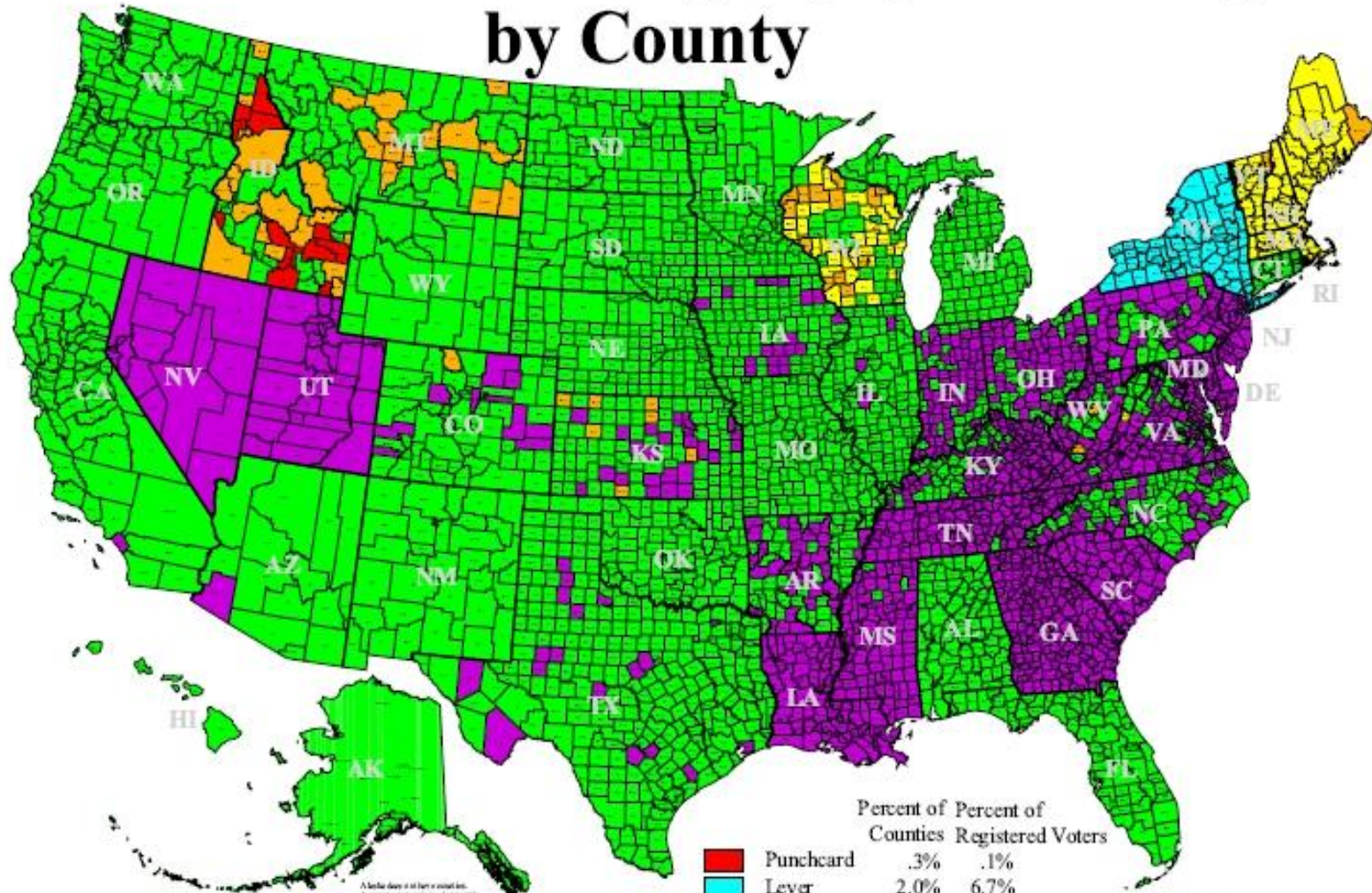
- Election officials have outsourced elections to private companies
 - Three companies control more than 80% of US elections
 - Private companies create, program and operate US voting equipment
 - A few private companies “certify” and “test” voting equipment
- Voting software is considered a trade secret

Voting problem space

US elections are run on an extremely large, very insecure distributed computing environment

- 170,000+ precincts, 3700 counties, 50 Secretaries of State
- Primary technologies
 - “Punch cards” now phased out
 - Optical scan (as in MN)
 - Touchscreen DRE, with or without paper trail
- Independent contractors and private companies
- Local, county and state IT staff
- Elected, appointed, volunteer and temporary paid administrators

November 2008 Voting Equipment Usage by County



	Percent of Counties	Percent of Registered Voters
■ Punchcard	.3%	.1%
■ Lever	2.0%	6.7%
■ Paper	1.8%	.2%
■ Optical	58.9%	56.2%
■ Electronic	34.3%	32.6%
■ Mixed Systems	2.7%	4.2%

A hole does not alter a vote but a record is kept of the vote.

Equipment expected to be used in the November 2008 election as reported by state election officials and news media. The map shows equipment used at polling places, not necessarily absentee or disabled balloting.

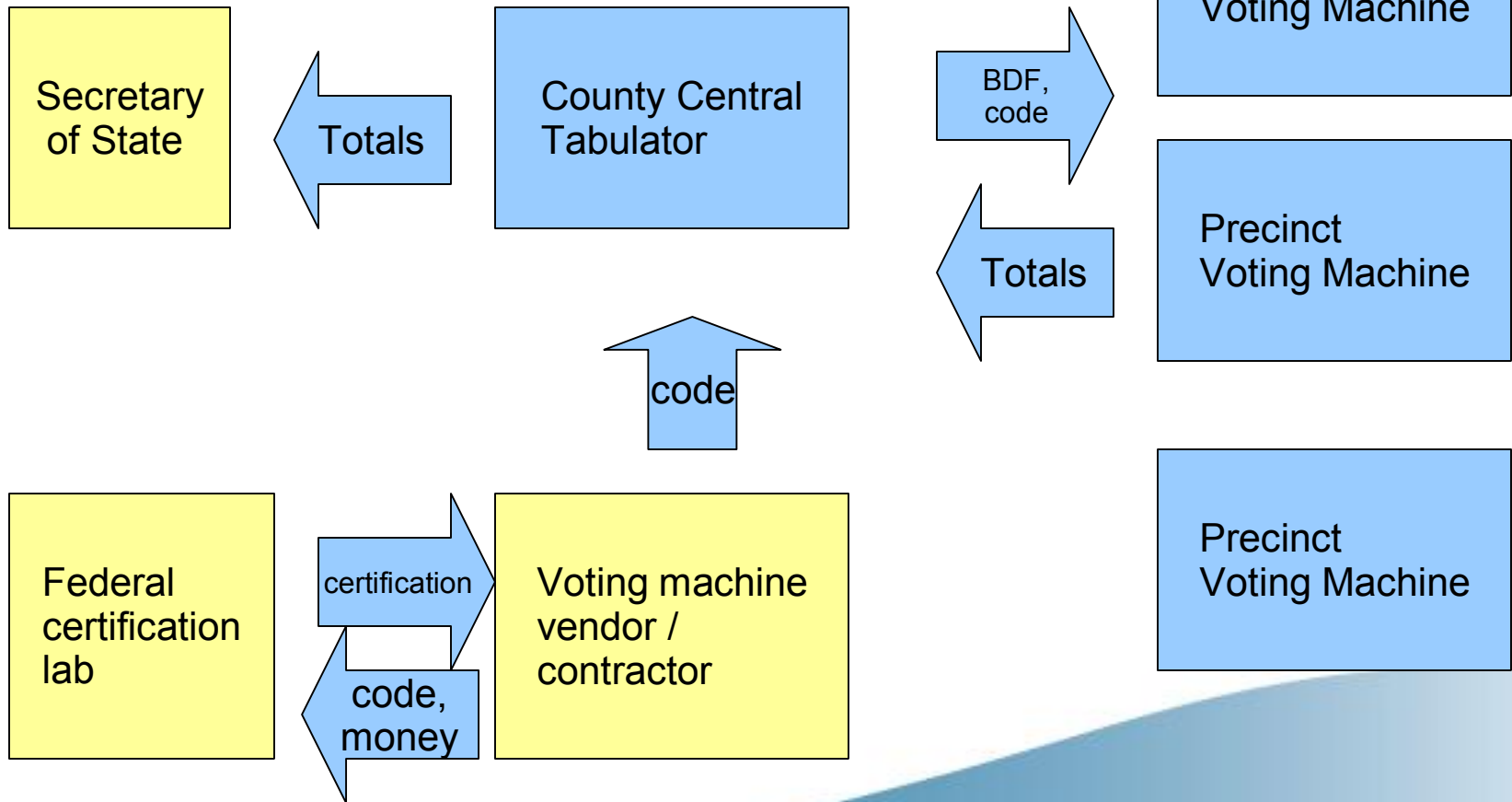
Voting problem space

Client-server architecture almost universal

- In-precinct devices
- Central tabulators
- Modems or memory cards pass between the two
 - Ballot definitions, totals... and code
 - Cards couriered between locations
- Wireless capabilities
- Often run on Windows CE
- More than 120 known vulnerabilities (Brennan Center Report) and counting

Logic and Accuracy Tester

Voting System Context



Trust me, or else...

As you have likely read in the news media, certain New Jersey election officials have stated that they plan to send to you one or more Sequoia Advantage voting machines for analysis.

*I want to make you aware that if the County does so, it violates their established Sequoia licensing Agreement for use of the voting system. Sequoia has also retained counsel to stop any infringement of our intellectual properties, including any **non-compliant analysis**. We will also take appropriate steps to protect against any publication of Sequoia software, its behavior, reports regarding same or any other infringement of our intellectual property.*

- Letter sent by Sequoia Election Systems to Princeton University, March 2008

For there to be a problem here, you're basically assuming a premise where you have some evil and nefarious election officials who would sneak in and introduce a piece of software...

I don't believe these evil elections people exist.

-

David Bear, a representative of Diebold Election Systems, New York Times, May 12, 2006, in response to a report of a security vulnerability in Diebold touch screens

Why so concerned?

In 2003, an investigator found an unsecured ftp site containing source code for Diebold touch-screen electronic voting equipment.

- First independent review of any modern voting software

- Conclusion:

- “this voting system is **far below even the most minimal security standards applicable in other contexts**. We identify several problems including **unauthorized privilege escalation, incorrect use of cryptography**, vulnerabilities to **network threats**, and poor software development processes... voters, without any insider privileges, can **cast unlimited votes** ... our outsider attacks could have been discovered and executed **without access to the source code**.... the insider threat is also quite considerable, showing that an insider, such as a poll worker, modify votes... **We conclude that this voting system is unsuitable for use in a general election.**
(Kohno, Subblefield, Rubin and Wallach, “Analysis of an Electronic Coting System”, February 2004

- A component of this system tabulated more than 24 million votes in 2004

Man behind the curtain

Jeffrey W. Dean was the senior vice president of Global Election Systems and a director of the company in 2000 and 2001.

- He was a lead developer of the 1.94w optical scan voting system and the GEMS central tabulator.
- At the time, a convicted felon, 23 counts of financial fraud using a computer system
- “the crimes and their cover-up involved a **high degree of sophistication and planning** in the use and **alteration of records in the computerized accounting system** that defendant maintained for the victim” - findings of fact in case no. 89-1-04034-1, King County, Washington

Still, Deans' contribution not wholly

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



National Cyber Alert System

Cyber Security Bulletin SB04-252

Summary of Security Items from
September 1 through September 7, 2004

Diebold
GEMS Central
Tabulator 1.17.7, 1.18

A vulnerability exists due to an undocumented backdoor account, which could allow a local or remote authenticated malicious user to modify votes.
No workaround or patch available at time of publishing.

Any indication vulnerabilities being exploited?

Voting is private and anonymous and is inherently difficult to secure or to verify.

- More than 30% of all votes have no independent audit trail; faith based voting.
- Paper records are never checked unless the outcome is close - “sore loser”
- Chain of custody issues (e.g., 2004 Ohio, 2008 in NH)
- MN leads the nation in post-election audit
 - about 5% of precincts, weeks after the election

Other tools?

Only indirect means are available to assess the accuracy of US elections.

- Opinion polls
- Exit polls
- US Census survey
- Reports of anomalies

Opinion poll anomalies

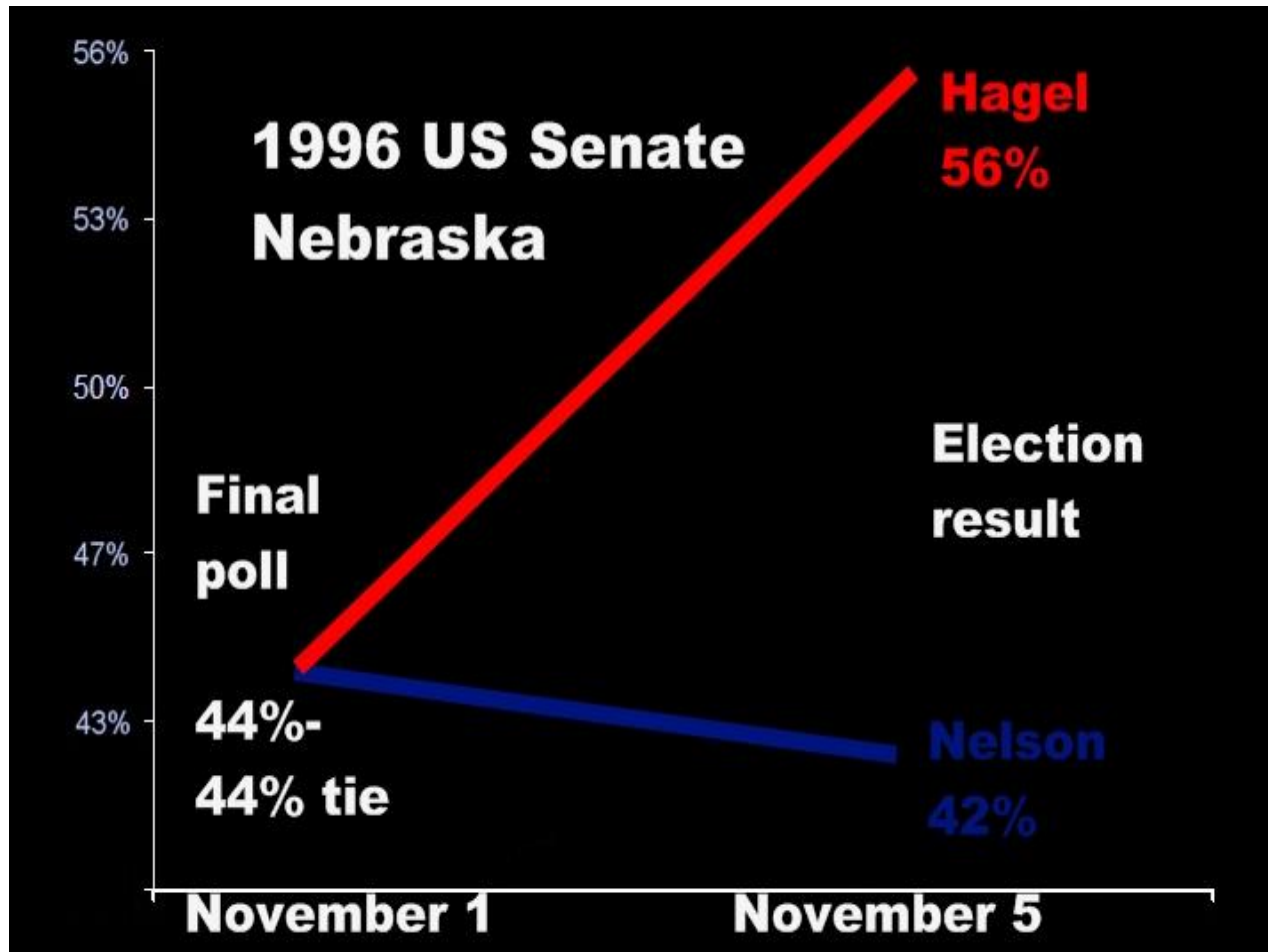
Investigators have reported a number of unusual last minute shifts in election results, as compared with public opinion polls.

Nebraska, 1996: Hagel v. Nelson

Conservative talk show host runs against popular incumbent governor

“Upset of the year” in 1996

Unexpected result?



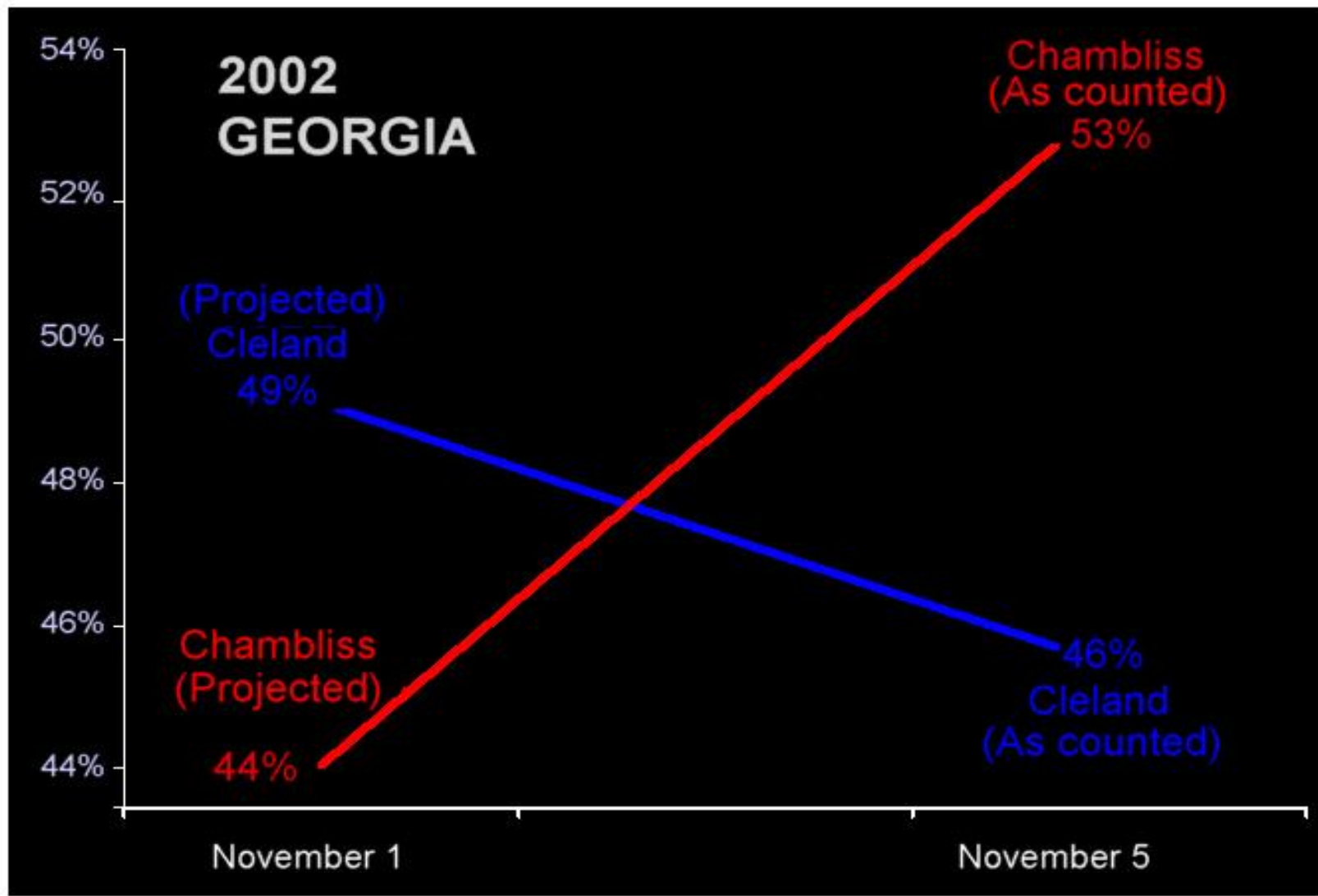
Six years later, it was discovered that Hagel was former chairman and still part owner of ES&S, the company that counted votes in Nebraska in 1996.

Opinion poll anomalies

Georgia, 2002: first election in state run on Diebold paperless touch screen machines

Last minute “patch” applied to machines in Fulton & DeKalb counties (home to more than 50% of Georgia Democrats)

Unexpected result?



Anomaly reports

Since the widespread deployment of touchscreen voting after 2000, there have been widespread reports of votes switching between one candidate to another.

In 2004, such incidents were reported in 13 states.

In over 90% of the reported incidents, votes for Kerry switched to Bush.

Denial of service?

A large, light blue, curved shape at the bottom of the slide, resembling a stylized wave or a decorative element.

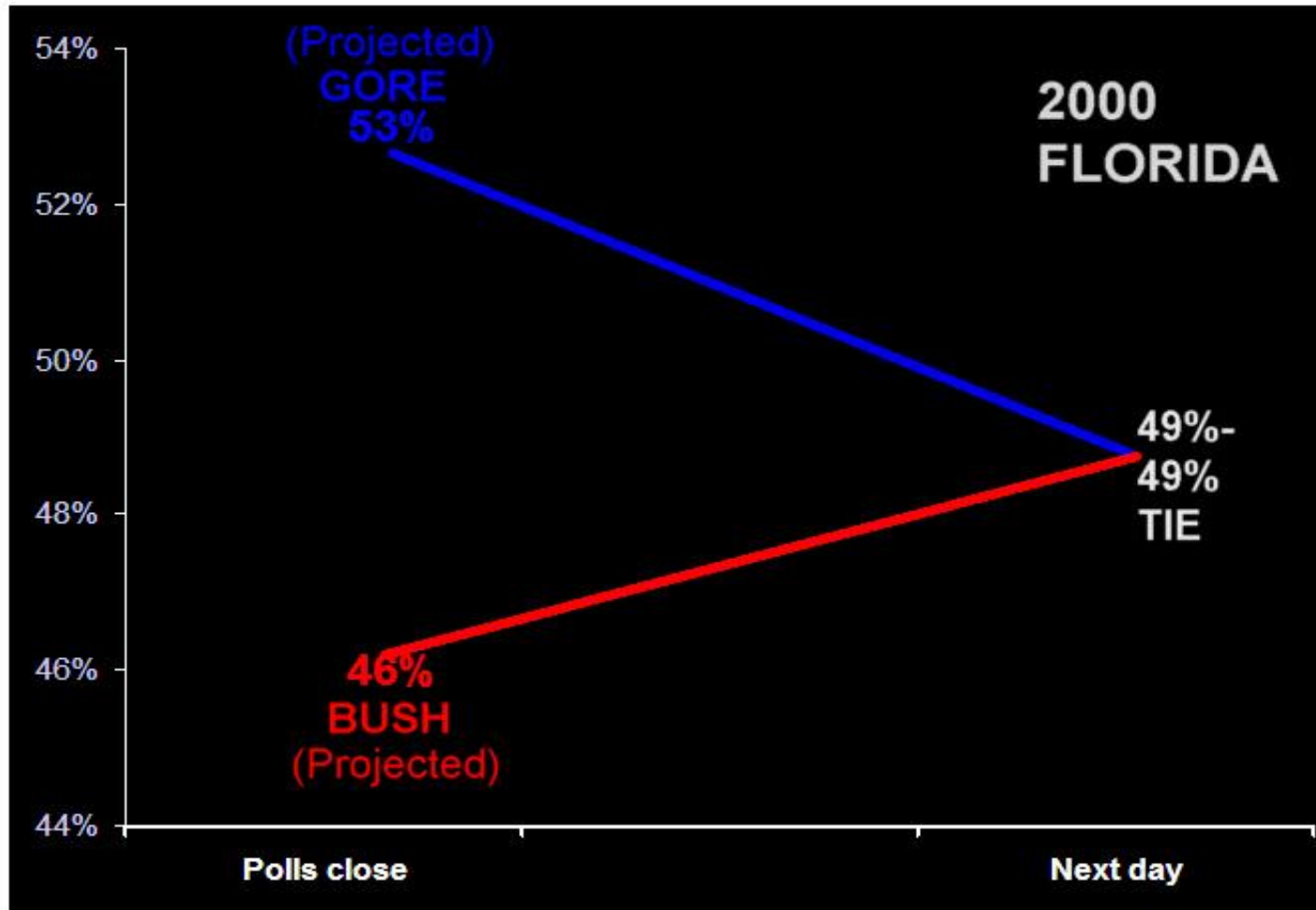
Exit poll anomalies

Traditionally quite accurate, in recent years exit polls have become increasingly inaccurate and controversial.

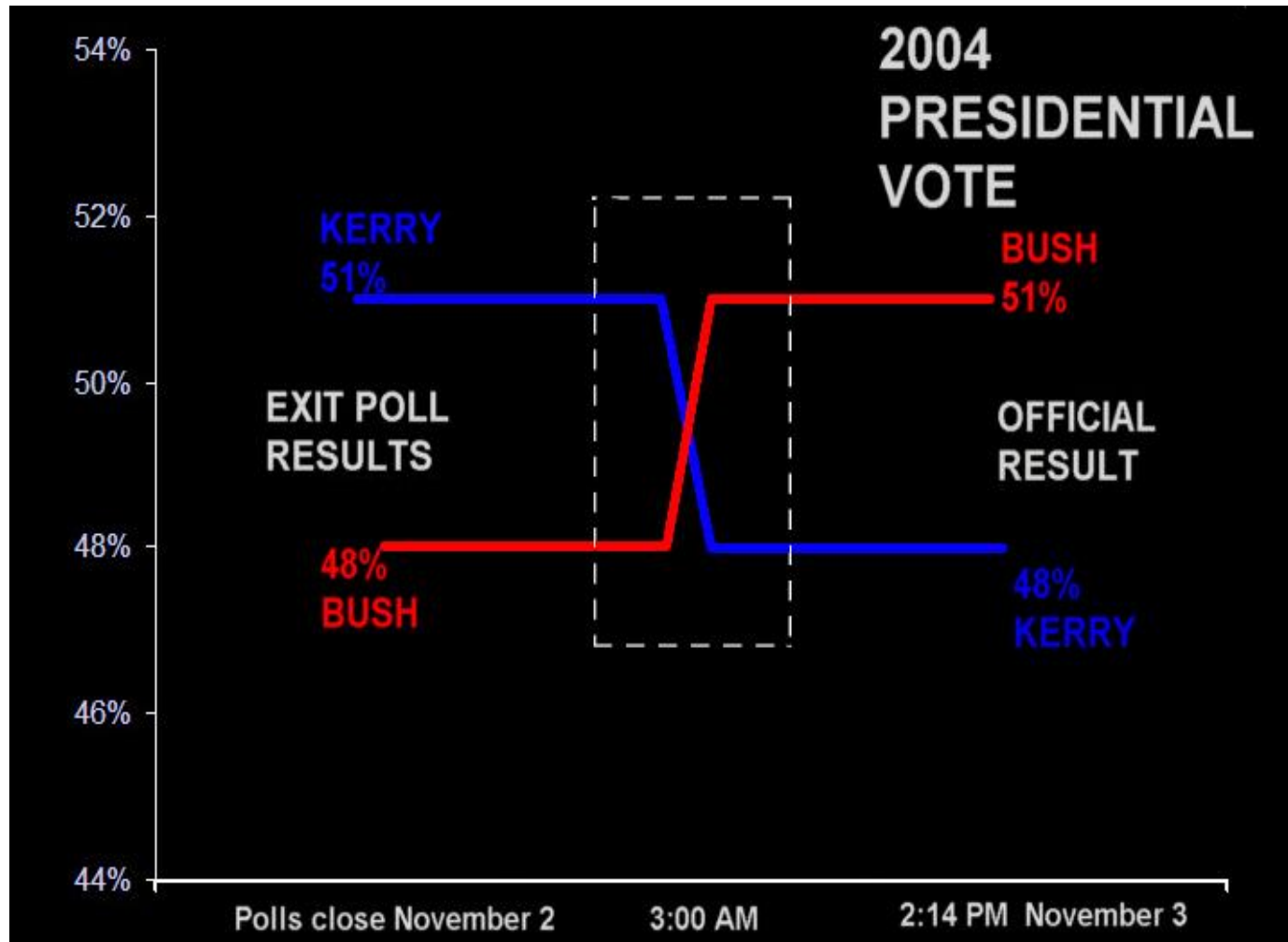
Florida, 2000: Gore v. Bush

Networks call Florida for Bush on basis of 7% lead in exit polls confirmed by sample precincts

Unexpected result?



2004 Exit Polls



2004 ELECTION NIGHT
Nov. 2 - Early Evening

Electoral votes according to Exit Polls

KERRY 309

BUSH 174

Too close to call 55

2004 PRESIDENTIAL ELECTION “Battleground State” Exit Poll Discrepancies

	% change	Candidate favored	NET CHANGE
OHIO	6.7%	BUSH	November 3 6:00 AM
FLORIDA	7.9%	BUSH	
NEW MEXICO	3.7%	BUSH	
IOWA	2.2%	BUSH	
NEVADA	3.9%	BUSH	
COLORADO	3.4%	BUSH	
MINNESOTA	5.5%	BUSH	
PENNSYLVANIA	6.5%	BUSH	
MICHIGAN	1.6%	BUSH	
NEW HAMPSHIRE	9.5%	BUSH	
MISSOURI	3.0%	BUSH	
WISCONSIN	0.0%	NONE	


Since 2004

Anomaly reports and exit and opinion poll discrepancies continued in 2006.

And in the presidential primaries in 2008.

But... in 2008, no significant Presidential exit poll anomaly!

... but there was a 10% discrepancy in Minnesota US Senate race, recount underway

A large, light blue decorative shape at the bottom of the slide, resembling a stylized wave or a rounded triangle pointing to the right.

Exit poll anomalies

Traditionally quite accurate, in recent years exit polls have become increasingly inaccurate and controversial.

Florida, 2000: Gore v. Bush

Networks call Florida for Bush on basis of 7% lead in exit polls confirmed by sample precincts



Thank you

