

# **The Impact of Technology on Election Observation**

Douglas W. Jones\*  
University of Iowa

VoComp, July 16-18, 2007  
Portland Oregon

\*Partial support from NSF Grant CNS-052431 (ACCURATE)  
and from the Organization for Security and Cooperation in  
Europe Office for Democratic Institutions and Human Rights.

# Election Observation

- Non Government Organizations
  - Carter Center
- Treaty Organizations
  - Organization of American States (OAS)
  - Council of Europe
  - Organizaton for Security and Cooperation in Europe (OSCE)

# International Election Law

Created by treaty

details depend on what treaties a nation signs

- The Helsinki Final Act of 1975
- Charter of Paris of 1990
  - binding on former NATO & Warsaw Pact – everyone from Vancouver to Vladivostok
- Interamerican Democratic Charter of 2001
  - binding from Canada to Argentina

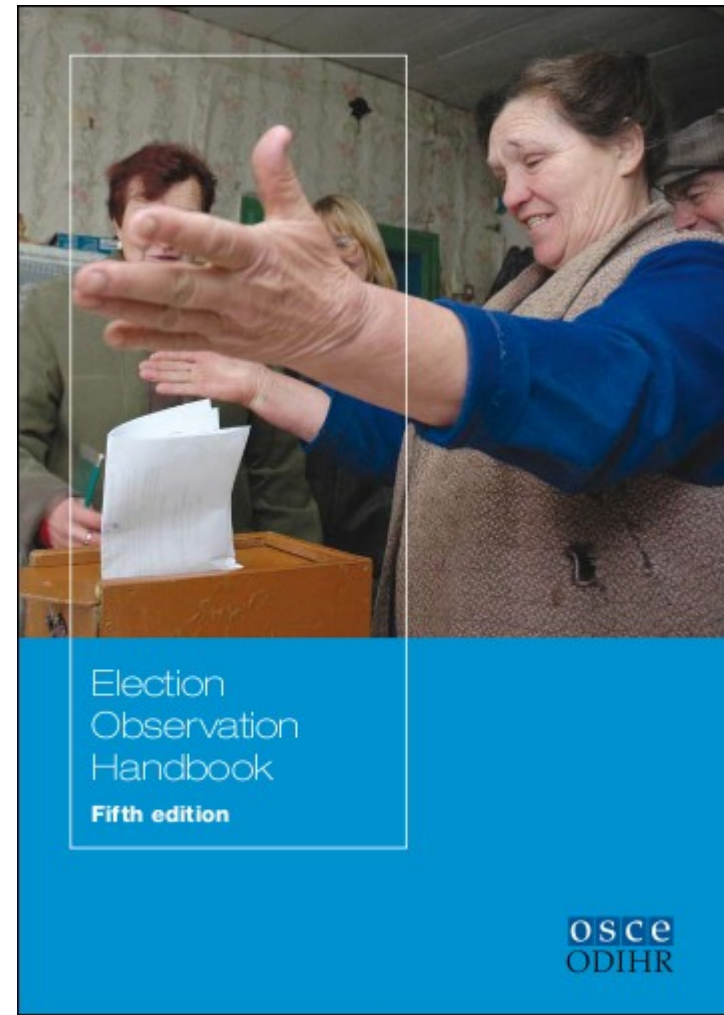
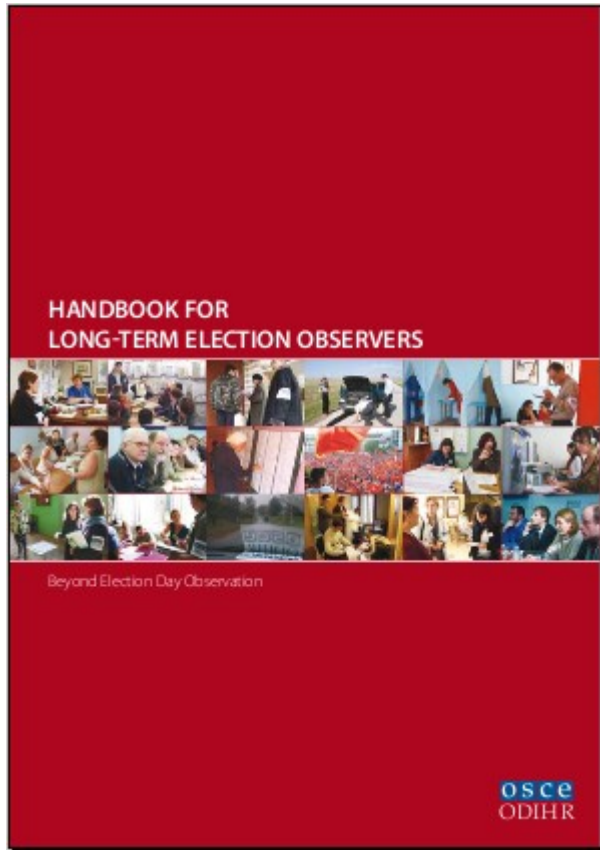
# Why Invite Observers

- To prove that you are obeying treaty
  - former Soviet republics invite OSCE observers
- To legitimize election or government
  - Palestinians invited Council of Europe
- To provide baseline for observers
  - Mature democracies, US, Netherlands, France
  - (but each has faced criticism!)

# Election Observing Methodology

- Long Term Observers
  - Analyze local election law
  - Examine voting system
  - Determine what can be observed
  - Train short term observation team
- Short Term Observers
  - Large team for election day
- A large effort

# OSCE Handbooks



# Broad-Based Standards

DECLARATION  
OF PRINCIPLES  
FOR INTERNATIONAL  
ELECTION OBSERVATION

and

CODE OF CONDUCT  
FOR INTERNATIONAL  
ELECTION OBSERVERS

Commemorated October 27, 2005,  
at the United Nations, New York

**Endorsing Organizations as of October 24, 2005:**

African Union

Asian Network for Free Elections (ANFREL)

The Carter Center

Center for Electoral Promotion and Assistance (CAPEL)

Commonwealth Secretariat

Council of Europe European Commission for Democracy  
through Law (Venice Commission)

Council of Europe – Parliamentary Assembly

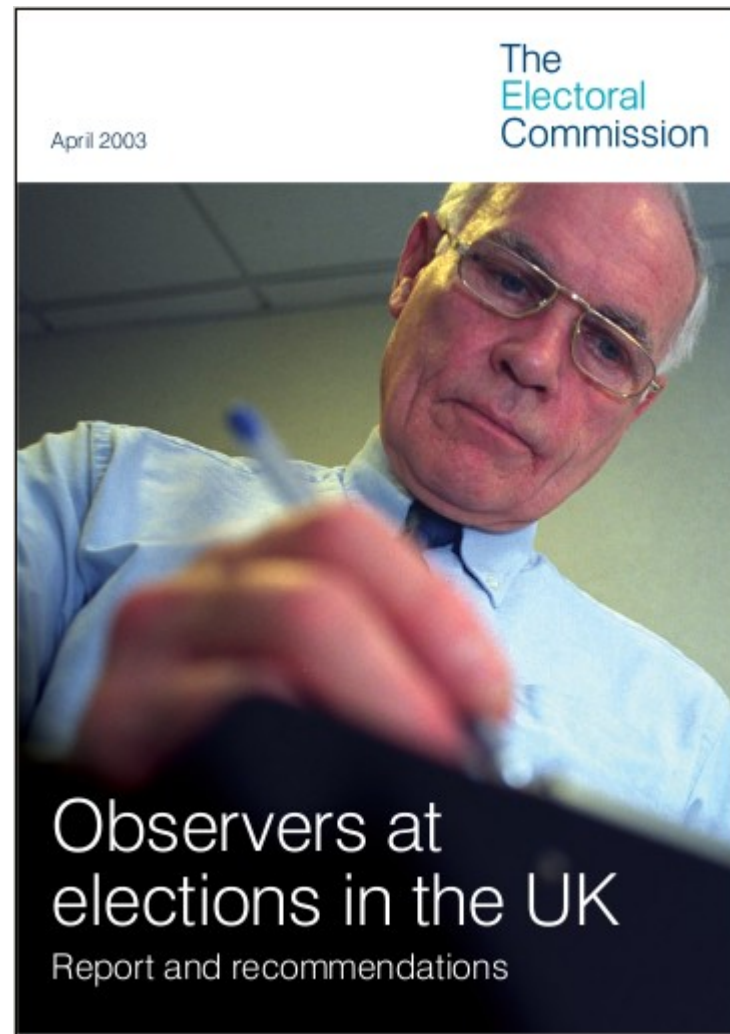
Electoral Institute of Southern Africa (EISA)

European Commission

European Network of Election Monitoring Organizations  
(ENEMO)

**etc!**

# National Rules





# Examples: Kazakhstan 2005

## Presidential Election



# Kazakh *Sailau* Voting System

Very simple machine in booth



Stateless vote recorder,  
no knowledge of election  
context, no need to prep  
for election specifics.

# Polling Place Computer



- Serves as E-pollbook
- Serves as E-ballot box
- Communicates with central election commission



# Sailau Smartcards

- Transmit ballot and election authorization to voting machine
- Transmit votes from voting machine
- Erase and reuse after vote recording



- Smart card has flash memory + small CPU
- Not COTS firmware – contents apparently unknown to election office.

# Sailau Network



Server writes USB key  
Download election def  
Periodic turnout upload

At end of day, upload results

USB key has small CPU +  
flash memory.

Firmware is not COTS, uses  
customized PK crypto system  
Details not know to election  
office.



# End-to-End Voter Verification

- Voter may request (before ballot commit) to verify ballot
- Voting terminal issues voter 4-digit verification code, records code on smartcard with voted ballot
- At end of day, verification codes and corresponding votes are printed and posted at the polling place
- 2 consecutive OSCE ODIHR reports commented on the conflict this poses with secret ballots

# Examples: Netherlands, 2006

## Parliamentary election

- 586 candidates
- Elected at large
- Vote for one
- Party list election rules where direct election can override list order set by party caucus.





# Nedap voting machine

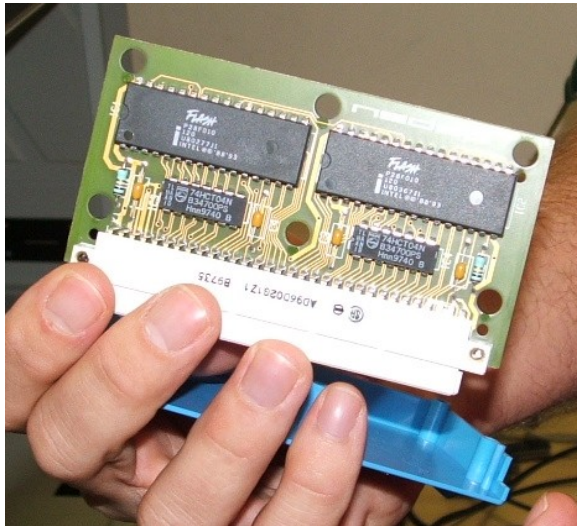
- 1<sup>st</sup> generation DRE
- Membrane keyboard behind printed ballot label
- In Dutch context, very fast – typical capacity 4 voters per minute!



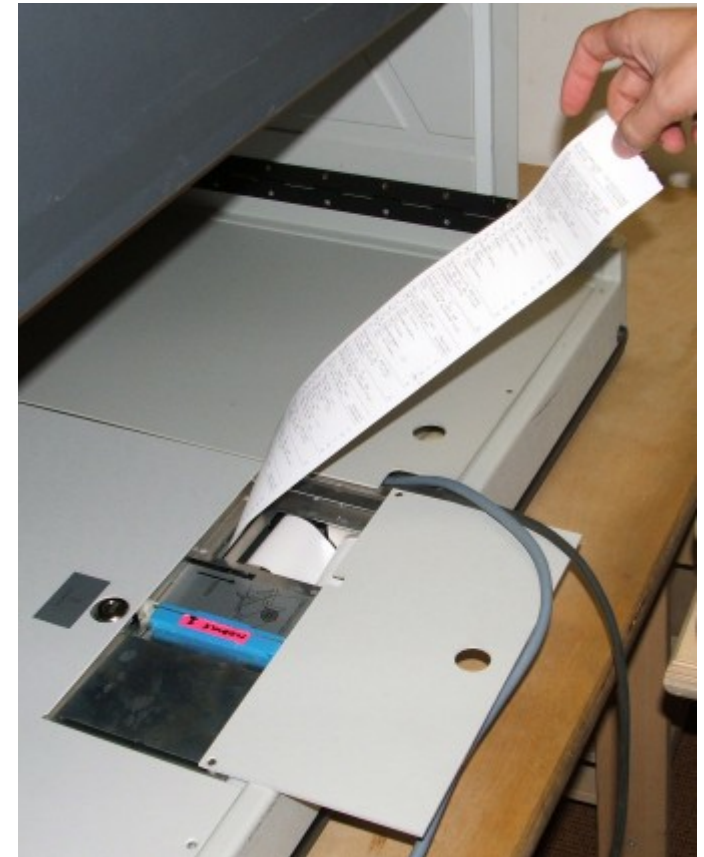


# Results Reporting

- No networking
- Prints results to adding machine tape
- Records results in flash memory module



memory  
module



**Security?** No technical safeguards.

# Nedap and Tempest

- Rop Gonggrijp showing Tempest vulnerability of Nedap machine
- Gonggrijp also proposed workable short term solution
- Dutch security services found that the competing DRE system made by SDU posed a more significant problem



# The Pollworker Control Panel

- Allegations of fraud in spring municipal elections in village of Zeeland in Brabants
- Possible that a pollworker manipulated enable switch to cancel voter's ballot just before commit
- Event logs could have helped investigation, but were not brought forward in court; we may never know what really happened.



# RIES for Expatriate Voters

- Rijnland Internet Election System
- Developed by academics for Rijnland Water Board elections
- Developed from a student government election system!!!
- End to end cryptographic verification
- Designed to replace postal voting
- 20,000 votes cast on RIES by expatriate voters during parliamentary elections



# The RIES “Polling Place”

- Very boring work
- Cast periodic test votes
- Open and close polls

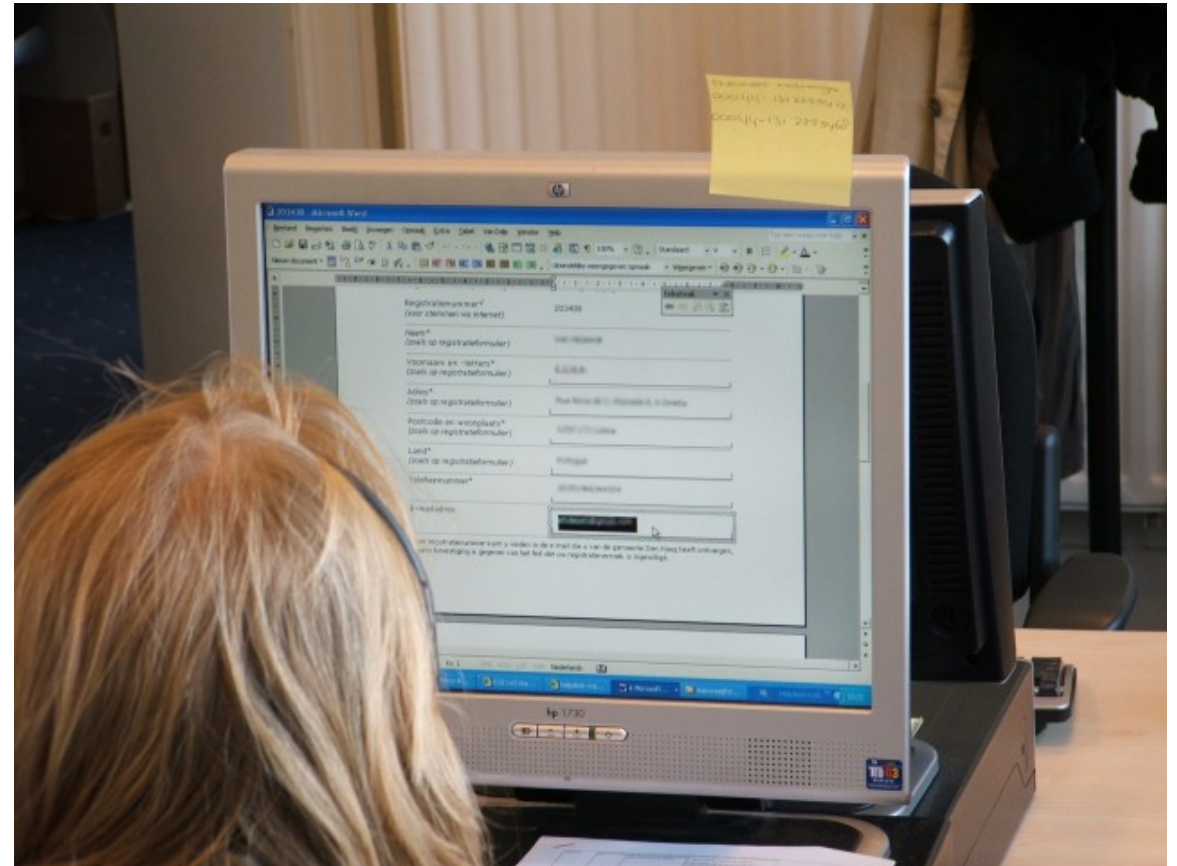


# RIES scheme

- Open source Javascript voting applet
- Internet voting authorization sent by post
- Applet uses keyed trapdoor function to encrypt vote (technical vote)
- Ballot box contains all votes cast, can be inspected to check that technical vote is recorded
- Codebook mapping all possible technical votes to actual votes published after polls close
- Codebook electronic signature published early!

# RIES Help Desk

- Wrong web browser?
- Voting authorization lost in the mail?
- In case of lost authorization, able to cancel it and issue replacement



# RIES Critique

- End to end verifiable
- But secret ballot properties are weak – *no weaker than postal ballots!*
- Integrity depends crucially on fact that codebook is not leaked! Proof of non-leakage is extremely difficult.
- Ballot invalidation mechanism creates new security problems.
- Casting invalid test ballots allows audits of network interference.



# Observing Critique

- We failed to observe creation or secure distribution of Sailau keys
- We failed to observe pre-election configuration or testing of NEDAP machines
- We failed to observe RIES codebook generation

*These critical processes happened before the observers were in place to see them!*

Must all advanced voting tech be this way?