



STRATEGIC THREAT INTELLIGENCE
APPROACH TO E-VOTING
IN NSW 2015 ELECTION

Ian Brightwell,
CIO, NSW Electoral
Commission

Clinton Firth,
Cybersecurity Consulting
Partner, CSC

Agenda

- I. What is iVote**
- II. What is iVote Architecture & Security Principals**
- III. Why use iVote**
- IV. Comparative Risks**
- V. New Approach to Cyber**
- VI. iVote & Strategic Threat Assessment**
- VII. Questions & Discussion**

What is iVote

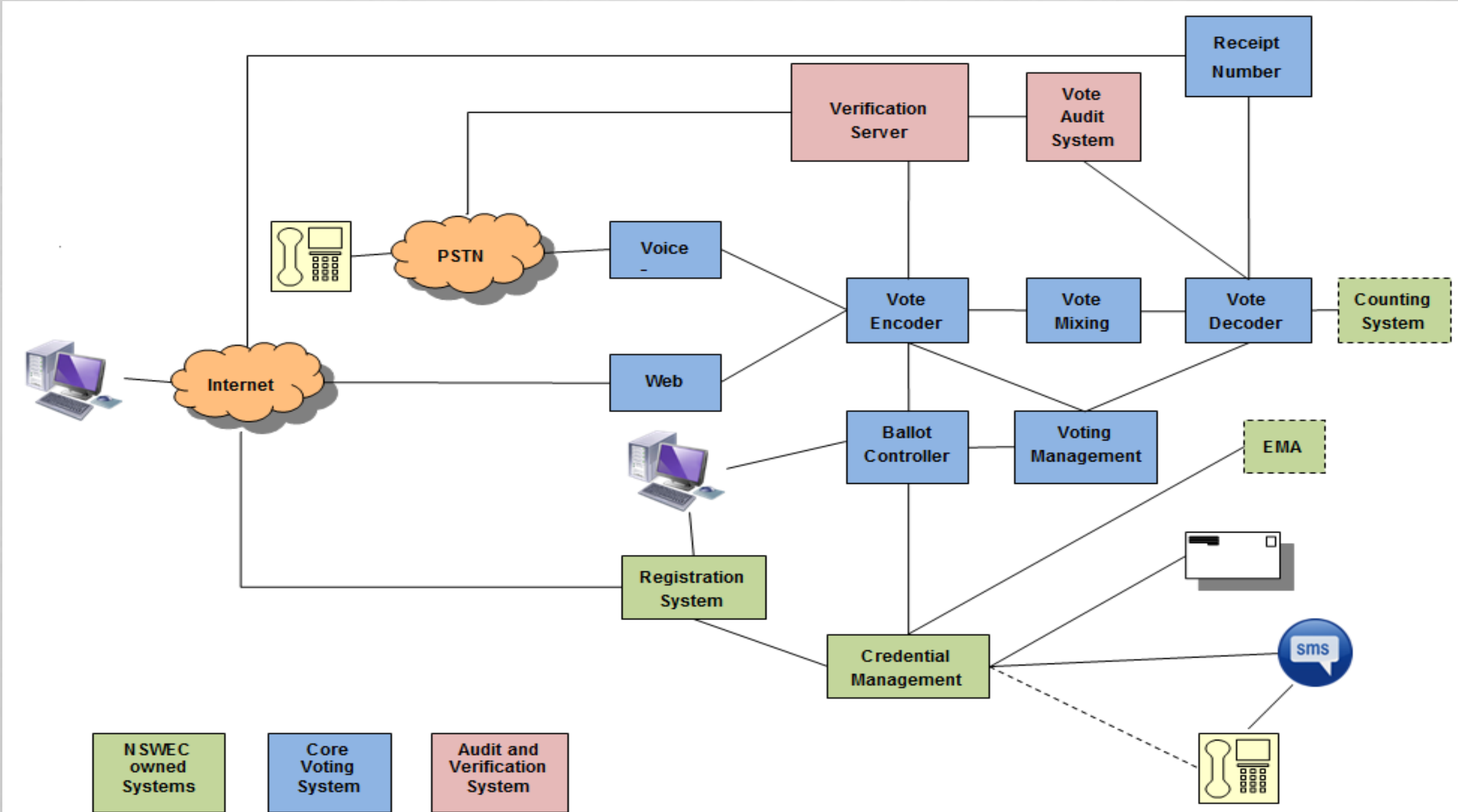
1. Was used at the Parliamentary election in March 2011 & took votes for 46,864 electors
2. Remote electronic Voting system for web or telephone;
 - Web browser over internet (including mobiles)
 - DTMF phone over PSTN
 - Human operator using voice from telephone to web browser
3. Registration required with eligibility only;
 - for Blind, Disabled, Remote and Interstate or Overseas
 - during early voting period (two weeks before election day)
4. Expect to take votes for 250,000 electors at the Parliamentary election in March 2015
5. Not replace paper current ballots for in electorate voting (over 60% of votes)

iVote Design Principles

The following are iVote design principles:

- Balance comparative risks of current paper approach with internet voting
- Mix of People-Process-Technology (not just a technology project)
- Segregation of Duties and Data, Systems and Communication Channels
- Voter can verify vote captured as cast
- Voter has evidence vote decrypted as captured (auditor, receipt number)
- Voter can check vote counted as decrypted (all preferences published)
- Voter coercion not considered a significant issue also voter able to revote
(see paper by Prof. Rodney Smith from Sydney Uni. - [Internet Voting and Voter Coercion](#))

iVote Architecture



Why use iVote?

- Independent voting for blind and low vision voters (BLV want all electors to use it)
- More accurate result
- Greater electoral Integrity than other declaration votes (see [Keelty](#) and [ANAO Rpt](#))
- Postal voting may be problematic in 5 to 10 years ([AustPost CEO](#))
- Postal voting currently failing overseas voters (over 60% not returned)
- Overseas voters able to vote (NSWEC got 20k to 30k extra votes in 2011)
- Used by other jurisdictions – [Norway](#), Switzerland, Estonia
- Increase Participation (especially with compulsory voting and dropping youth vote)
- Electors want it (most common question asked, see [NSWEC 2011 iVote Report](#))

Comparative Risks

	MITIGATION	
Risk	PAPER BALLOTS	ELECTRONIC VOTING
Impersonation	Using the current paper ballot approach potential voters only require a verbal declaration identifying themselves. The declaration requires them to know a name, DoB and address on the roll.	Similar to current paper ballot approach requirement but with option to provide additional information such as drivers licence or passport number or be sent a registration acknowledgement to their enrolled address.
Cast as intended	Elector can vote incorrectly causing their vote to be informal. General informality for paper ballots between 3% to 6%	Able to independently verify vote as cast. Guided to ensure vote complies with formality rules. Must make active decision to cast informal vote. Informality typically about 1%.
Captured* as Cast	Once the ballot paper is placed in the ballot box the voter must trust the Commission. Independent scrutiny is sporadic and mainly focused on polling place votes. The 30% of declaration votes are typically counted without independent scrutiny.	Voter can verify their vote has been decrypted by personally checking the vote appears on receipt website. Also independent auditor will confirm the votes decrypted match the votes available for verification.
Counted as Captured*	Trust the Commission staff manually counts the ballot papers correctly.	Published preference data which is validated by auditors and electors can be counted by anyone to check the count is correct. Compare to paper ballot results.

* Captured - is for paper ballots when the ballot box is emptied or declaration envelope is opened or for iVote is when the ballots are decrypted.

Comparative Risks cont.

	MITIGATION	
Risk	PAPER BALLOTS	ELECTRONIC VOTING
Tampering	It is difficult to identify evidence of vote tampering with paper ballots. Notwithstanding there is no evidence of this actually occurring in Australian elections.	Vote encrypted by voter's computer are not accessible by the Commission or others until decrypted. Decrypted votes are matched to verified votes to ensure their validity. Electors can compare paper ballot results with electronic results which should have a very similar proportion of votes for candidates.
Ballot Box "Stuffing"	It is difficult to identify the ballot papers associated with ballot box "stuffing". Notwithstanding there is no evidence of this actually occurring in Australian elections.	Ongoing monitoring of registrations against votes would identify "stuffing" and potentially allow these papers to be identified and removed.
Integrity	Integrity of paper based elections relies on Commission staff following procedures and being trusted.	Combination of technology and procedures give confidence that votes have been counted as cast. Also electors can compare to paper ballot results with electronic results which should have a very similar proportion of votes for candidates.
Ballot Secrecy	Ballot secrecy is persevered in ordinary polling place voting but secrecy could be breached for declaration votes as the voter's details are available to Commission staff at the time of opening the declaration envelope.	Voter identity is held separately from the actual preferences voted by a given voter. Voters can not be associated with their vote without very significant breaches of multiple systems.



LANDSCAPE

STRATEGIC THREAT INTELLIGENCE

Importance of enhancing cyber information
sharing and collaborative action.

A New Approach to Cyber

“If you know the enemy and know yourself, you need not fear the result of a hundred battles...”

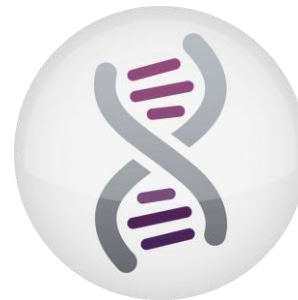
- Sun Tzu, the Art of War



Military have long used intelligence



Threats traverse ALL in a global cyber war




Threats evolve & calibrate



Threats to e-voting

eVote Threats or No Strategy?

Anonymous claims to have blocked GOP election theft with Ohio firewall  1k

See also [Anonymous](#) / [Karl Rove](#) / [Hackers](#) / [Politics](#)

Ansip: Election Identified

31.05.2013 15:02

Category: [Politics](#)

Prime Minister Andrus Ansip said a member of his party has admitted to manipulating e-votes in the Reform Party's leadership election last week and in another election in 2011.



Prime Minister Andrus Ansip Photo: Postimees/Scanpix

Voting Blogs: Hacking the Polls: Vulnerability in Electronic Voting Systems Independent Voter Network

Washington DC Test e-vote server camera



(c) Typical workers, before attack



(d) Workers, after learning of attack

Estonian MEP denies involvement in Reform Party voting fraud

MEP Kristiina Ojuland has denied involvement in voting fraud after finding herself at the center of the scandal in the wake of allegations that e-votes were cast in the Reform Party's internal leadership elections in the name of party without their knowledge.



December 17, 2013

Foreign attackers hacked elections site during government shutdown



Abhaxas Dumps Details of the Internal Florida Voting Database Online



Strategic Threat Assessment



**Research
& Analysis**



**Wargame,
Test & Assess**



Monitor & Respond

Why?

- Confidence and Assurance beyond compliance
- Drives pragmatic effective security strategy
- Supports Incident Response planning



A photograph of a tablet lying on a wooden surface. The tablet screen shows the 'iVote' logo in blue, where the 'o' is a play button icon. Below the logo, the word 'QUESTIONS' is written in a grey, sans-serif font. The tablet is tilted slightly to the right.

iVote

QUESTIONS

MORE INFORMATION

General Information on iVote

<https://www.elections.nsw.gov.au/voting/ivote>
<https://www.elections.nsw.gov.au/about-us/plans-and-reports/i-vote-reports>
<http://www.ivote.nsw.gov.au/>

Norway Parliamentary Election Reports

<http://www.osce.org/odihr/elections/109517?download=true>
http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/valgobservatorer/2013/Rapport_Cartersenteret2013.pdf

CSC Cybersecurity site

<http://www.csc.com/cybersecurity>

Handout

CSC Whitepaper – Intelligence
Driving Security Governance

Book

Offensive Countermeasures:
The Art of Active Defense
By: John Strand, Paul Asadoorian,
Ethan Robish, Benjamin