# Vulnerability of elections

Data Protection Authority Meets Academia, Den Haag
9 sept 2025

Bart Jacobs, Radboud Universiteit Nijmegen
bart@cs.ru.nl





## Own involvement in "voting"

- Vothing is fascinating topic, from a security perspective
  - authentication, secrecy, integrity, availiability
  - with many creative (cryptographic) solutions
- Member of Korthals Altes committee, in 2007
  - report Stemmen met Vertrouwen still authorative
  - formal basis for abolishing voting computers in NL
- Topic of own research and public discussion
  - even before Gonggrijp's `wijvertrouwenstemcomputersniet.nl`
  - PC member at conference E-Vote-ID, since several years
  - new NWO research project about "local" voting





Vulnerability of elections

## Much emphasis on correctness of the outcome

- Voting computers (of Nedap en Sdu) have disappeared, because:
  - individual votes leaked via tempest emissions
  - software was unprotected — and could thus be manipulated
- Also the counting and merging of outcomes was vulnerable
- Electoral Board (Kiesraad) Interior Ministry) have invested in the correctnes and reliability of the election results
  - colleague in computer security Herbert Bos in Electoral Board
  - professionalisation of ICT-department of Electoral Board
  - with open source policy, for transparancy and autonomy





## Frequently used quote in this setting

*Those who vote decide nothing*

*Those who count the vote decide everything*

Attributed to Joseph Stalin





## Current variation

*Don't bother manipulating the vote outcome*

*when you can easily manipulate the voters*

Attributed to:





## Presidential elections Romenia (late 2024, early 2025)

- Out of the blue winner, in first round of Nov'24: Călin Georgescu
  - extreme-right, pro-Russian, critical of EU and NATO
  - campagne mainly via TikTok
- Romenian security council, based on intelligence-repports: Russia manipulated the presidential elections
  - 'stately actor' massively promoted Georgescu clips on TikTok
  - via coordinated accounts & recommendation algorithms
  - people voted on carefully constructed online illusion, fact-free
- Journalist Razvan Lutac (Snoop): "Not only Romenia is in danger. This may happen as well in Germany or The Netherlands"
- Romenian supreme court then excludes Georgescu
  - Does NL have such a emergency button / brake? Who does?
- In the end, narrow victory for pro-Europian candidate Nicusor Dan





## Disruption through "social" media

- Big "social" media are platforms for commercial and political manipulation
  - under control of tech-bro's of Trump — and also of Xi
  - with anti-democratic, and anti-Europian agenda
  - effective targeting and manipulation based on personal profiles
- Attention eeconomy leads to radicalisation and polarisation
  - Jaron Lanier: X/Twitter is a "asshole amplification network"
- Toxic environment for (wel-willing) public office holders, politicians, experts, esp. for women and minorities
  - undermining content-driven democratic debate
- Based on extreme interpretation of freedom of speech
  - not on human dignity and quality of debate
- In everybody's pocket, basis for "news" and personal judgements





## And there is also AI

- This summer BNR asked AI-chatbots vote recommendations
  - ChatGPT, Copilot, Gemini, Grok; only Copilot politely refused
- This is what people will do in large numbers
  - Tech-bro's only need to build in a slight bias
  - democrates and anti-democrates are close, in many places
- Manipulation and misleading are so much easier with AI-bots
  - via text, but also via (deepfake) video, making deeper impression
  - populists instrumentalise AI (more) effectively / shamelessly

## Painful questions

How did we let these controversial actors take total control over our information and decision space — making it such a hostile environment for running democratic elections?

- Maybe more important: *how do we get out of here?*
- I offer no solutions, at most some, separate directions:
  (1) invest in own decent alternatives — and use them too
  (2) regulate even more strictly, and even forbid certain "social" media
  (3) hardening of our ICT-infrastructure
  (4) digital resillience w.r.t. elections
  (5) stop being naive, for a resilient democracy
  (6) ...



## Ad (1): invest in and make alternatives standard

- Different NL initatives, based on public values:
  - Civic Social Media
  - #MakeSocialsSocialAgain
- Own community network PubHubs.net
  - aim is a combination of privacy and accountability
  - via flexible digital identities (later also with EU ID wallet)
  - including digital signatures
  - for decent contact with/among audience of organisations
  - now working on pilots, broader launch later this year
- Also relevant for discussions about youth and "sociale" media
  - when there are proper alternatives, (age) bans for the controversial platforms are less drastic



## Ad (2): stricter regulation

- EU has legal framework, but fines are slow and "after the fact"
  - EU is regulatory power, in need of "own" technology
- Tech-bro's are not impressed and organise political counter pressure
- Hard violations should lead to hard bans
  - violations like giving space to political manipulation (Romenia)
  - reluctance to moderate, even against threats and violence
- Quicker applicable: soft bans
  - TikTok, X, etc. no longer on work phone
  - banning access to juviniles
  - give the right example, quit yourself
- Clear normative positioning: this does not fit our democracy, based on mutual respect and dignity
  - do not go along with absolute interpretion of "freedom of speech"



## Ad (3): hardening ICT-infrastructure

- Our informatiespace is flooded with mis/dis-information, increasinly AI-generated
- Deliberate strategy: *flooding the zone with bullshit* (Steve Bannon)
  - the aim is reality fatigue among the population
  - so that people give up trying to find out what is true or not
  - in the US, now in the form of total self-destruction
- Own proposal: focus on authenticity of information
  - i.e. certainty about source and integrity
  - this is not the same as truth
  - great mechanism: digital signature
  - see article The Authenticity Crisis (Comp. Law Security Rev, 2024)

## Ad (4): increase digital resilience

- Task of security/intelligence services is to protect our democratic order
  - that is at stake, against stately actors & big corporations (like X)
  - an assertive approach is needed (take-downs, hacking etc)
  - expose, so that the public sees what is happening, like in Romenia
- In NL Electoral Board is silent and lacks an explicit mandate w.r.t. voter manipulation. This should come on the (political) agenda



## Ad (5): resilient democracy, without naivity

- **Example**: changing NL constitution for binding referendum
  - in final phase, only one last round through Senate is needed
- Emerged from well-intended "power to the people" thought (SP)
- The last 10 years have shown
  - referendums are hijacked by anti-democrates
  - ideal instrument for polarisation & distortion, for own agenda
- What do we do in NL? We make the referendum binding
  - we are preparing the instruments for disruption
  - Putin and Trump are gearing up ("spugen zich in de handen")
  - see NL op-ed: iBestuur (5/12/2024)
- Aside: preferendum is more constructive and nuanced alternative
  - with a spectrum of option, that invites deliberation



## Final remarks I

You might say:

- where is the proof that manipulation by these tech-bro's happens, and that it actually influences the election results?

My reply:

- you do not demand from a slave to give proof of being maltreated and that the treatment actually has negative influence
- you resits the very constellation/institution of slavery

Aside: this is the republican perspective (as opposed to the liberal view), that emphasises absence of (the possibility of) arbitrary interference, as hallmark of freedom



## Final remarks II

- Much attention for reliability of election results, but not (yet) for (external) manipulation of voters
- Supreme Court lawyer Ybo Buruma (NRC, 6/6/2025): "A democracy can kill itself" ("Een democratie kan zichzelf de nek om draaien")
- The anti-democratic strategy is familiar by now:
  - frame / make the current situation abnormal, dangerous, bad
  - manipulate voters via "social" media (esp. via disconent)
  - govern via emergency laws and decretes
- Urgency and priority needed in politics & institutions, with mandates
  - NL emergence button / brake needed at Electoral Board, or at Supreme Court, or at . . . ?
  - Authorities / supervisors (GDPR, DSA) can be more assertive
- Invest in sovereignty, own control, own hardened infra
  - "taking back control"
- Naivity has a very high price!