Digital Autonomy

iHub
Radboud University

NWO ICT-open, April 16, 2026

Bart Jacobs — Radboud University Nijmegen, NL
bart@cs.ru.nl

Overview

Digital Autonomy

Where we are, so far

Timeliness of this topic

Coalition agreement, Jetten cabinet

- Digital autonomy must be the starting point for the government. We opt for a European digital infrastructure and strategically phase out dependencies in cloud, data, and critical systems.
- Digital procurement and tenders will be standardised and centralised, guided by principles such as security-by-design, zero-trust, sovereignty, open source, and supply chain security.

Junior minister for Economic Affairs - digital economy and sovereignty

Willemijn Aerdts (D66)

Global platforms

US	Europe	China
Google, Amazon, Uber, Apple, airbnb, NETFLIX, etc	Spotify	TikTok, WeChat, SHEIN

EU situation

We run American software on Chinese hardware

(and increasingy, Chinese software too)

Where did we go wrong?

Where we are, so far

Main autonomy (disruption) concerns in EU

(1) Putin pulling more sea cables — esp. transatlantic (and Pacific)
- "smaller" destructions ongoing, esp. in Baltic sea

(2) Trump using IT-dominance for leverage & sanctions ("kill switch")
- International Criminal Court (ICC) prosecutor Khan no longer served by Microsoft, after unwelcome Israel investigations

(3) Tech-bro's of Trump dominate our information and decision space
- with anti-democratic and anti-European agenda

(4) European Court of Justice may (once again) declare EU-US data transfer agreement illegal
- after succesful "Schrems I" (2015) and "Schrems II" (2020) objections

(5) Xi using rare metals for geopolitical influence
- also chip-supply (e.g. to car industry) blocked in Nexperia case

Ad 1. Putin's disruption

- Dutch intelligence chiefs: we're in a dark grey zone between war and peace with Russia
- Putin is actively disrupting European societies & infrastructure
  - spoofing GPS, endangering civil aviation
  - large scale cyber attacks, for espionage and sabotage
  - drone incidents, near military and civil airports
  - cutting data/power cables, esp. in Baltic sea
  - physical attack: arson, explosions, murder attempts
  - disinformation, esp. supporting anti-democratic movements
- An obvious next step if the conflict (with Europe/Ukraine) heats up more is to cut undersea transatlantic data cables
  - Russian ships have been monitoring & preparing cable trajectories
  - hard to defend against, high plausible deniability
  - without the cables, hardly anything still works in Europe
  - is this part of IT-audits? what are the fall-backs?

Ad 2. Trump's disruption

- The ICC prosecurity cut-off worked as wake-up call for many
  - Trump forbids US-companies to provide services to court
  - prosecutor Khan no longer had access to emails, files, etc.
  - decision is politically motivated — Israel investigations
  - Microsoft is very unhappy / uncomfortable with the situation
- ICC decided to ditch Microsoft and is switching to open source alternative
  - OpenDesk collaboration platform, via Zendis, hosted in Germany
- Broader fear of power abuse within current IT-feudalism (Passchier)
  - anything that Trump dislikes may be targeted / cut off
  - resulting in growing investments in EU IT-infrastructure
  - industrial policy is needed, against abuse of market power / excessive dominance, e.g. via killer acquisitions

Trump's threats, continued

- *US National Security Strategy* (Nov. 2025)
  - frontal assault on Europe, destroying itself through migration, censorship of free speech, regulatory suffocation
  - US wants to rescue Europe, together with "political allies in Europe" and with "patriotic European parties"
  - Ukraine must stop war, must not be NATO member
- *President Trumps Cyber Strategy for America* (March 2026)
  - full freedom for US private sector, only own "commons sense" regulation, certainly not from EU
  - US technology is *weaponised*, for own interest:

    > *We will secure the data, infrastructure, and models that underpin U.S. leadership in AI and we will call out and frustrate the spread of foreign AI platforms that censor, surveil, and mislead their users*

Ad 3. Techbro's disruption

- Big "social" media platforms are instruments for commercial and political manipulation: they are weaponised against us
  - effective targeting and manipulation based on personal profiles
  - support for right-wing populists is evident (e.g. Musk and AFD)
- In this toxic environment we still run public elections ...
  - platform owners pushing extreme opinions / candidates
  - people are now asking Gen-AI tools for voting advice ☹
  - it is easy to tweak the recommendations
- Presidential elections Romania (late 2024, early 2025)
  - Out of the blue winner, in first round, campagne via TikTok
  - extreme-right, pro-Russian, critical of EU and NATO
  - Rom. authorities: Russia manipulated the presidential elections
  - Romanian supreme court then excluded this pro-Russian candidate
  - TikTok violating "Digital Services Act" — still under investigation
- Urgent question: do other countries also have such emergency breaks?

Ad 4. CJEU's disruption / protection

- Europe's data-protection laws ("General Data Protection Regulation", GDPR) in principle forbids processing of personal data of European citizens outside EU
- Special arrangements can be needed, guaranteeing a similar level of protection, such as EU-US-privacy shield
- Still, US intelligence agencies have access to the data
  - privacy activist Max Schrems has succesfully contested these arrangements in EU-courts multiple times: inadequate protection for EU citizens from government surveillance
- Latest fix under Biden is "Data Protection Court of Review"
  - Trump is undermining it, strengthening contestants in EU courts
  - US cloud may be declared illegal by European judges
  - (first attempt by French MP Latombe failed recently)

Ad 5. Xi's disruption

- Systematic hacking, largely with economic goals, for own benefit
- Concerns about back-doors and kill switches in advanced products (GSM, cars, batteries, solar panels)
  - also about data collection for manipulation — esp. via TikTok
- Increasing strategic use of its production & resource dominance
  - CN's economic power is used for geopolitical goals
  - not discussed further here

Painful question

How did we let such controversial actors take total control over our information and decision space — making it such a hostile environment, so at odds with basic European values (like privacy and dignity)?

- Naivety, laziness, convenience, indolence, stupidity
- Maybe more important: *how do we get out of there?*
- 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) stop being naive, for a resilient democracy
  (5) ...

I will expand on "alternatives" and "hardening", in relation to my own work

IT-sector does not function as market

(1) Product liability is absent for software
  - from the start, the IT-industry got away with this
  - consequence: low quality, many security vulnerabilities
  - example: Citrix leak (2019) had big consequences, no-one claims

(2) Also no liability for content carriers
  - freedom of speech is instrumentalised, as excuse to do nothing
  - it deteriorated into: freedom for the most aggressive
  - no attention for content or "quality of discussion"
  - consequence: lots of online mis/dis-information, threats, derailed debates, disengagement of well-intentioned & vulnerable people

(3) Extremly dominant IT-parties have disproportional power
  - can buy-up everyone, kill competition with too low prizes
  - take over activities of useful companies (Zivver, Solvinity)
  - buy and liquidate threatening companies ("killer acquisitions")

Strengthen alternative industrial policies

- Open source is a geopolitical instrument
  - it keeps Big Tech at a distance
  - when you don't own the software, you are not autonomous
  - "closed source" benefits the seller, not the buyer
- Pursue industrial policy for collective autonomy
  - organize/invest in European (open source) service providers
  - put necessary protection structures in place around them
  - ICT should not be outsourced like catering (Bert Hubert)
  - do not try to copy Silicon Valley—as Draghi wants
  - play on a different chessboard, with open source
  - with steward ownership models ("mission over profit")
  - do this jointly, as sectors
  - offer/enforce alternatives against (understandable) local optimisations

Break-free strategy

To break free from Big Tech, distinguish:

(1) **Short term** (think: data cable broken)
  - organise emergency fall-back now ("digitaal noodpakket")
  - need not be perfect, to be used when the shit hits the fan
  - identity and communication are essential starting points

(2) **Long term**
  - put a point on the horizon, as clear goal
  - e.g. Univ. Groningen: free from Google in 2030!
  - all decisions should be meandering towards that goal
  - challenges are technical, organisational, and social

Own *Digitaal Noodpakket* blog at: ibestuur.nl (Jan.'26)

Where we are, so far

Digital identity: Yivi.app

- Digital identity is starting point for many security solutions
  - if you outsource identity management, you're doomed
- Yivi.app for privacy-friendly, open source login with attributes
  - attribute examples: "given name", "family name", "date of birth", "older than 18", "email", "mobile", "postal code", etc.
  - with Yivi you can selectively disclose such attributes
  - matching GDPR's data minimisation and purpose binding
  - Yivi is up-and-running for years, $\geq 100K$ users
  - privacy-friendly age verificatie does really exist ...
- Yivi is very influential: inspiration, leading example for EU plans
  - identity wallets, are being introduced in EU in 2026
  - crucial for EU sovereignty
- Derived product: Postguard.eu, for secure file transfer
  - think: secure WeTransfer or DopBox, but in NL hands
  - open source alternative for Zivver — now under US control

Authenticity of data

- Our information space is flooded with misinformation and disinformation, increasingly generated by AI
- Deliberate strategy: *flooding the zone with bullshit* (Steve Bannon)
  - goal: induce reality fatigue in the population
  - so people give up trying to determine what is true or false
  - active undermining of informed democratic debate
- Our proposal: focus on the authenticity of information
  - technical term: provides certainty about source and content
  - not the same as truth; authenticity can be technically guaranteed via digital signatures
  - this can strengthen institutions online — if they start signing
  - Also essential for AI, to ensure the authenticity of training data
  - see article The Authenticity Crisis (Comp. Law Security Rev, 2024)
- Identity wallets (such as Yivi) support role-based signing

PubHubs.net as an alternative conversation platform

- Current "social" media have devastating effects
  - fake news, extremism, polarisation, via *engagment optimisation*
- *Attention economy* leads to radicalisation and polarisation
  - Jaron Lanier: X/Twitter is an "asshole amplification network"
- New initiative: PubHubs.net — a trustworthy, decent alternative
  - ad-free, open source, based on public values
  - balanced combination of privacy and accountability
  - optional authentication and signing for additional certainty
  - communication in local communities, with moderation
- PubHubs.net is in the pilot phase, starting spin-out
  - target groups: patient organizations, municipalities, libraries, also business partners (for a trustworthy channel with customers)
  - aim: steward ownership with a business setup but no profit motive
  - seeking a financial boost to accelerate deployment ...

Where we are, so far

Concluding remarks

- Re-election of Trump has made existing IT-feudalism visible and problematic, threatening European democracies and values
- IT-sector dominated by super-powerful private parties
  - no level playing field, no functioning market — see killer acquisitions — highly problematic political agenda
  - Europe has to start playing on a different chess-board
  - with open source as counter strategy, avoiding lock-ins
- European IT-reorientation also offers opportunities
  - rebuild IT based on public / European values
  - academics have role to play — e.g. with prototypes
- Own work esp. in digital identity — with applications
  - Broader message: there are alternative approaches, there is a choice!