

Digitale Soevereiniteit

Van der Heijden ondernemingsrecht congres, Nijmegen,
22/11/2025

Bart Jacobs — Radboud Universiteit
bart@cs.ru.nl



Digitale Soevereiniteit

Wie is deze man?

- ▶ Hoogleraar in Nijmegen (NL), in computer security & privacy
 - studie wiskunde & filosofie, terecht gekomen in informatica
 - ook “nul-punt-nul” aanstellingen bij rechten en filosofie
 - KNAW lid en Stevin winnaar
- ▶ Regelmatig in media, maatschappelijk debat en parlementaire hoorzittingen
- ▶ Voormalig lid Cyber Security Raad (tot sept. 23), ook van evaluatiecommissie WiV (2020)
- ▶ Een van de oprichters van  iHub Nijmegen's inderdisciplinaire Hub voor digitalisering en samenleving, zie ihub.ru.nl



Where we are, so far

Inleiding computerbeveiliging

Bedreigingen soevereiniteit

Eigen initiatieven

Conclusies



Ervaring met grote ondernemingen

- ▶ **2008**: eigen groep ontdekt zwakheden in OV-chipkaart en meldt die vertrouwelijk aan producent **NXP**, samen met intentie om een half jaar later te publiceren
 - NXP stelt Radboud universiteit en ook individuele onderzoekers aansprakelijk voor alle gevolgschade, tot een miljard
 - NXP eist in kort geding **publicatieverbod**
 - rechter in Arnhem wijst eis af: wie verouderde producten verkoopt moet consequenties dragen en op de blaren zitten!
- ▶ **2013 Volkswagen** eist in kort geding **publicatieverbod** n.a.v. door ons vertrouwelijk gerapporteerde zwakheden in startonderbrekers
 - rechter in Londen kent toe; drie jaar later verbod opheffen in onderling overleg

Sindsdien is veel veranderd: verstandige bedrijven bieden **bug bounties** als je zwakheden aan ze meldt; OM vervolgt dan niet.



Waar gaat *computerbeveiliging* over?

Computer Security is about regulating access to (digital) assets

Essentie:

- ▶ **assets**: de waardevolle zaken die beschermd moeten worden
 - Bijv. bedrijfsgeheimen, of persoonlijke gegevens (privacy)
 - ▶ **regulating access** betreft wie kan erbij?
 - identificatie: wie ben je / wat zijn je kenmerken (attributen)
 - authenticatie: hoe bewijs je dat
 - autorisatie: wat mag je doen
- Auditvraag**: wie kan waar bij, hoe wordt dat gelogd en gecontroleerd?

Impliciet is er sprake van een kwaadaardige **aanvaller** die probeert onbedoelde toegang te krijgen om jouw computer systeem te ondermijnen

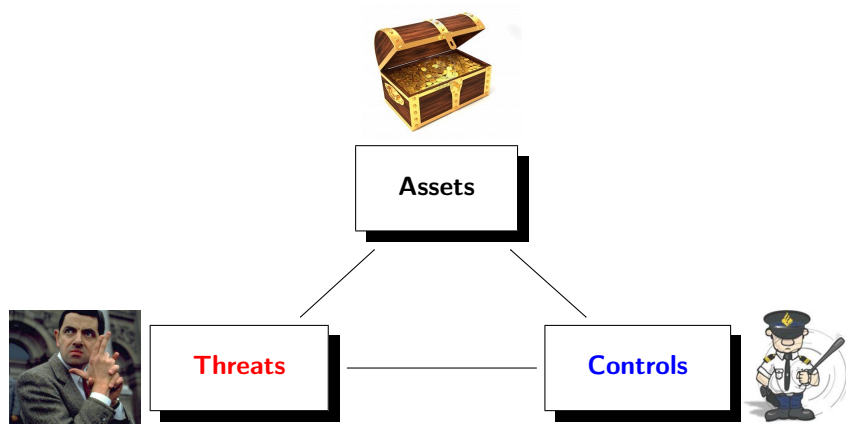


Onderscheid: beveiliging & veiligheid

- ▶ Belangrijk conceptueel verschil, subtiel in het Nederlands.
 - *Security* / *Schutz* / *sécurité*
 - *Safety* / *Sicherheit* / *sûreté*
- ▶ **Beveiliging** gaat over bescherming tegen een actieve kwaadaardige aanvaller die moedwillig een (computer) systeem wil ondermijnen
- ▶ **Veiligheid** gaat over bescherming tegen onbedoelde ongelukken of (ontwerp)fouten
- ▶ Denk aan het verschil tussen:
 - Veiligheid versus beveiliging van een kerncentrale
 - Voedselveiligheid / beveiliging



Security management samenvatting



Where we are, so far

Inleiding computerbeveiliging

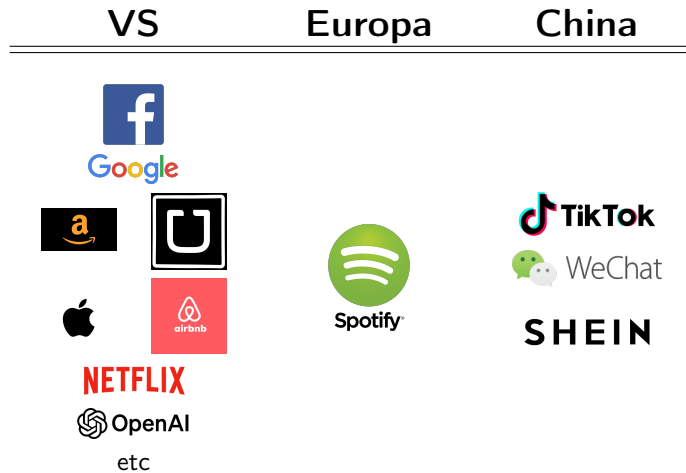
Bedreigingen soevereiniteit

Eigen initiatieven

Conclusies



Globale platformen



EU situatie

We run American software on Chinese hardware
(and increasingly, Chinese software too)

Where did we go wrong?



Belangrijkste digitale autonomie bedreigingen in EU

- (1) **Poetin** trekt meer zeekabels stuk — i.h.b. transatlantische
 - “kleinere” vernielingen zijn gaande, m.n. in de Baltische zee
- (2) **Trump** misbruikt IT-dominantie voor chantage/sancties (“kill switch”)
 - International Criminal Court (ICC) hoofdaanklager Khan afgesloten van Microsoft, na Israël onderzoeken
- (3) **Tech-bro's van Trump** domineren onze informatie/beslis ruimte
 - met een anti-democratische en anti-Europese agenda
- (4) **European Court of Justice** kan EU-US gegevensuitwisselingsverdrag (wederom) ongeldig verklaren
 - na succesvolle “Schrems I” (2015), “Schrems II” (2020) bezwaren
- (5) **Xi** gebruikt zeldzame metalen voor geopolitieke chantage
 - ook chip-leveringen in Nexperia zaak



Ad 1. Poetin's dreiging

- ▶ AIVD & MIVD directeuren: we zitten in een **donkergrijze** zone tussen oorlog en vrede met Rusland
- ▶ Poetin ondermijnt systematisch **EU samenleving & infrastructuur**
 - spoofing GPS, dreiging voor m.n. burgerluchtvaart
 - grootschalige cyberaanvallen, voor spionage en sabotage
 - drone incidenten, bij militaire and civiele vliegvelden
 - verbreken data/stroom kabels, m.n. in Baltische zee
 - fysieke aanvallen: brandstichting, explosies, poging tot moord
 - desinformatie, i.h.b. t.b.v. anti-democratische partijen
- ▶ Voorspelbare volgende stap in conflict (met EU/Ukraine) is het **saboteren van transatlantische zeekabels**
 - Russische schepen actief op relevante locaties
 - moeilijk te verdedigen, hoge *plausible deniability*
 - zonder die kabels werkt bijna niks meer in Europa
 - is dit onderdeel van audits? wat zijn de *fall-backs*?



Ad 2. Trump's dreiging

- ▶ Afsnijden van ICC aanklager werkte als **wake-up call**
 - Trump verbiedt VS-bedrijven diensten te verlenen aan ICC
 - aanklager Khan kon niet langer bij e-mails, files, etc.
 - besluit is **politiek gemotiveerd** — Israël onderzoek
 - Microsoft zelf is ongelukkig / ongemakkelijk met de situatie
- ▶ ICC besloot **Microsoft te dumpen** en schakelt nu over op open source alternatieven
 - OpenDesk collaboration platform, via Zendis, ge-host in Duitsland
 - voorbeeld voor de sector?
- ▶ Bredere angst voor machtsmisbruik in huidig **IT-feodalisme**
 - waar Trump een hekel aan heeft is doelwit, o.a. voor afsluiting
 - gevolg: groeiende investering in EU IT-infrastructuur
 - vraagt om **industrie politiek**, zie later



Ad 3. Techbro's dreiging

- ▶ Grote "sociale" media platformen zijn instrumenten voor commerciële en politieke **manipulatie**
 - effectieve targeting & manipulatie, via **persoonlijke** profielen
 - steun voor extreem-rechtse populistten (bijv. Musk en AFD)
- ▶ In deze **toxische omgeving** organiseren wij onze **verkiezingen** ...
 - platform eigenaren pushen extreme opvattingen / kandidaten
 - mensen vragen nu Gen-AI tools om stemadvies 😞
 - het is erg makkelijk / verleidelijk om die adviezen te tweaken
- ▶ Presidentsverkiezingen Roemenië (eind 2024, begin 2025)
 - totaal onbekende winnaar in eerste ronde, campagne via TikTok
 - extreme-rechts, pro-Russisch, kritisch over EU en NAVO
 - Roemeense autoriteiten: Rusland manipuleerde verkiezingen
 - Roemeense Hoge Raad sloot pro-Russische kandidaat uit
 - TikTok schond "Digital Services Act" — nog in onderzoek
- ▶ Urgente vraag: hebben wij in NL ook zo'n **handrem**?



Ad 4. CJEU's dreiging / bescherming

- ▶ AVG **verbiedt** in beginsel verwerking van persoonsgegevens van EU burgers **buiten de EU**
- ▶ Kan wel met speciale regeling, die vergelijkbaar beschermingsniveau biedt, zoals **EU-US-privacy shield**
- ▶ Inlichtingendiensten VS hebben wel toegang tot al die data
 - privacy activist Max Schrems succesvol in EU-hoven: onvolgende bescherming voor EU-burgers tegen overheidssurveillance
- ▶ Laatste pleister onder Biden is "Data Protection Court of Review"
 - Trump ondermijnt regeling en versterkt verzet in EU hoven
 - US cloud kan **illegaal** verklaard worden door EU rechters
 - (eerste poging door Franse MP Latombe onlangs niet geslaagd)
 - is hier een "plan B" voor?



Ad 5. Xi's dreiging

- ▶ Systematisch hacking, grotendeels met economische doelen, voor eigen gewin
- ▶ Toenemende zorgen over back-doors en kill switches in geavanceerde producten (GSM, auto's, batterijen, zonnepanelen)
 - ook over data verzameling voor manipulatie — i.h.b. via TikTok
- ▶ Toenemend strategische inzet van eigen productie & grondstoffen dominantie
 - China's economische macht wordt gebruikt voor geopolitieke doelen
 - China opereert (inter)nationaal niet als markteconomie
 - afhankelijkheid daarvan maakt je heel kwetsbaar



Pijnlijke vraag

Hoe hebben we zulke controversiële spelers totale controle laten nemen over onze informatie & beslis ruimte? Deze ruimte is nu een vijandige omgeving, botsend met Europese waarden (zoals privacy en waardigheid)?

- ▶ Naïviteit, luiheid, gemakzucht, nalatigheid, stommitieit
- ▶ Misschien belangrijker: *how do we get out of there?*
- ▶ Ik heb geen oplossingen maar wel enkele **richtingen**:
 - (1) voer **industriebeleid** met gerichte investering en bescherming
 - (2) investeer in eigen fatsoenlijke oplossingen — en gebruik ze ook
 - (3) **reguleer en handhaaf** nog stricter — en durf bepaalde “sociale” media ook te **verbieden**
 - (4) maak onze ICT-infrastructuur robuuster
 - (5) stop naïviteit, voor een veerkrachtige democratie
 - (6) ...



IT-sector functioneert niet als markt

- (1) **Productaansprakelijkheid** bestaat niet voor software
 - daar is de industrie van begin af aan mee weggekomen
 - gevolg: lage kwaliteit, veel beveiligingslekken
 - voorbeeld: Citrix lek had grote gevolgen, niemand claimt
- (2) Ook geen aansprakelijkheid voor het doorgeven van **content**
 - verabsolutering van vrijheid van meningsuiting
 - geen aandacht voor inhoud en kwaliteit van discussie
 - gevolg: veel online mis/des-informatie, bedreigingen, ontsporing van debatten, afhaken van goedwillenden en kwetsbaren
- (3) Extreem dominante IT-partijen hebben **buitensporige macht**
 - kunnen alles kopen, concurrentie via te lage prijzen kapot maken
 - activiteiten van nuttige bedrijven worden overgenomen (Zivver, Solvinty)
 - bedreigende bedrijven worden gekocht en geliquideerd (“killer acquisitions”)



Voer gericht en gezamenlijk beleid

- ▶ **Open source** is een geopolitiek instrument, houdt big-tech op afstand
 - als je de programma code niet zelf hebt, ben je niet autonoom
 - “closed source” is voordeel voor verkoper, niet voor koper
- ▶ Voer **industriebeleid** voor **collectieve autonomie**
 - Organiseer/investeer in eigen Europese (open source) dienstverleners
 - zet daar noodzakelijke beschermingsconstructies om heen
 - organiseer dit gezamenlijk, als **sectoren**
 - ICT moet je niet outsourcen zoals catering
 - probeer niet *Silicon Valley* te kopiëren — zoals Draghi wil
 - speel op ander schaakbord, met open source



Where we are, so far

Inleiding computerbeveiliging

Bedreigingen soevereiniteit

Eigen initiatieven

Conclusies



Digitale identiteit: Yivi.app

- ▶ Digitale identiteit is startpunt voor veel security oplossingen
 - als je identiteitsbeheer aan een ander overlaat ben je kansloos
- ▶ Yivi.app voor privacy-vriendelijk, open source inloggen met attributen
 - attribuuft voorbeelden: “voornaam”, “achternaam”, “geboortedatum”, “ouder dan 18”, “e-mail”, “06”, “postcode”
 - deze attributen kun je met Yivi selectief onthullen
 - volgt AVG eisen van data minimalisatie en doelbinding
 - Yivi al jaren up-and-running, $\geq 100K$ gebruikers
 - privacy-vriendelijke leeftijdsverificatie kan allang
- ▶ Yivi is zeer invloedrijk: inspiratie en voorbeeld voor EU plannen
 - identity wallets, worden ingevoerd in EU in 2026
 - cruciaal voor EU autonomie
- ▶ Afgeleid product: Postguard.nl, voor beveiligde file transfer
 - denk: beveiligde WeTransfer of DopBox, maar in NL handen
 - open source alternatief voor Zivver — nu in VS-Is handen



Authenticiteit van gegevens

- ▶ Onze informatieruimte wordt overspoeld met mis/des-information, steeds meer door AI-gegenereerd
- ▶ Bewuste strategie: *flooding the zone with bullshit* (Steve Bannon)
 - doel is reality fatigue onder de bevolking
 - zodat mensen het opgeven om uit te zoeken wat wel / niet waar is
 - actieve ondermijning van geïnformeerd democratisch debat
- ▶ Eigen voorstel: richt je op authenticiteit van informatie
 - technische term, geef zekerheid over bron en inhoud
 - dit is niet hetzelfde als waarheid; authenticiteit kan technische gegarandeerd worden, via digitale handtekeningen
 - dit kan instituties online versterken — als ze gaan ondertekenen
 - ook essentieel voor AI, voor authenticiteit van training data
 - zie artikel [The Authenticity Crisis](#) (Comp. Law Security Rev, 2024)
- ▶ Identity wallets (zoals Yivi) kunnen basis vormen voor rolgebaseerd ondertekenen



PubHubs als alternatief sociaal platform

- ▶ Huidige “sociale” media hebben verwoestende effecten
 - fake news, extremisme, polarisatie, via engagement optimisation
- ▶ Attention economy leidt to radicalisatie en polarisatie
 - Jaron Lanier: X/Twitter is an “asshole amplification network”
- ▶ Nieuw initiatief PubHubs.net: betrouwbaar, fatsoenlijk alternatief
 - reclame-vrij, open source, gebaseerd op publieke waarden
 - passende combinatie van privacy en accountability
 - optionele authenticatie en ondertekening voor zekerheid
 - communicatie in lokale gemeenschappen, met moderatie
- ▶ PubHubs.net in pilot fase, begonnen aan spin-out
 - doelgroepen: patiëntenorganisaties, gemeenten, bibliotheken, ook zakelijke partijen, voor een betrouwbaar kanaal met klanten
 - steward ownership beoogd, met zakelijke opzet, zonder winstoogmerk
 - financiële boost gezocht, voor versnelling ...



Where we are, so far

Inleiding computerbeveiliging

Bedreigingen soevereiniteit

Eigen initiatieven

Conclusies



Afsluitende opmerkingen

- ▶ We zijn enorme sukkels geweest, zitten nu onder **IT-feodalisme**
 - niet alleen economisch & geopolitiek bedreigend
 - maar ook m.b.t. onze waarden en democratie
- ▶ IT-sector gedomineerd door super-machtige private partijen
 - geen **level playing field**, geen functionerende markt
 - Europa moet op een ander schaakbord gaan spelen
 - met **open source** as tegen strategie, zonder *lock-ins*
 - durf platformen af te sluiten — net als bij Russia Today
- ▶ Europese IT-heroriëntatie biedt ook kansen
 - herinrichting van IT op basis van eigen Europese waarden
 - zodat EU niet alleen een reguleringsmacht is, maar ook een technologiemacht wordt
- ▶ Eigen werk i.h.b. over **digitale identiteit** — met vele toepassingen
 - boodschap: er zijn alternatieven, er is een keuze
 - die zullen we systematischer moeten willen realiseren!



Dank voor de aandacht! Vragen / opmerkingen?

