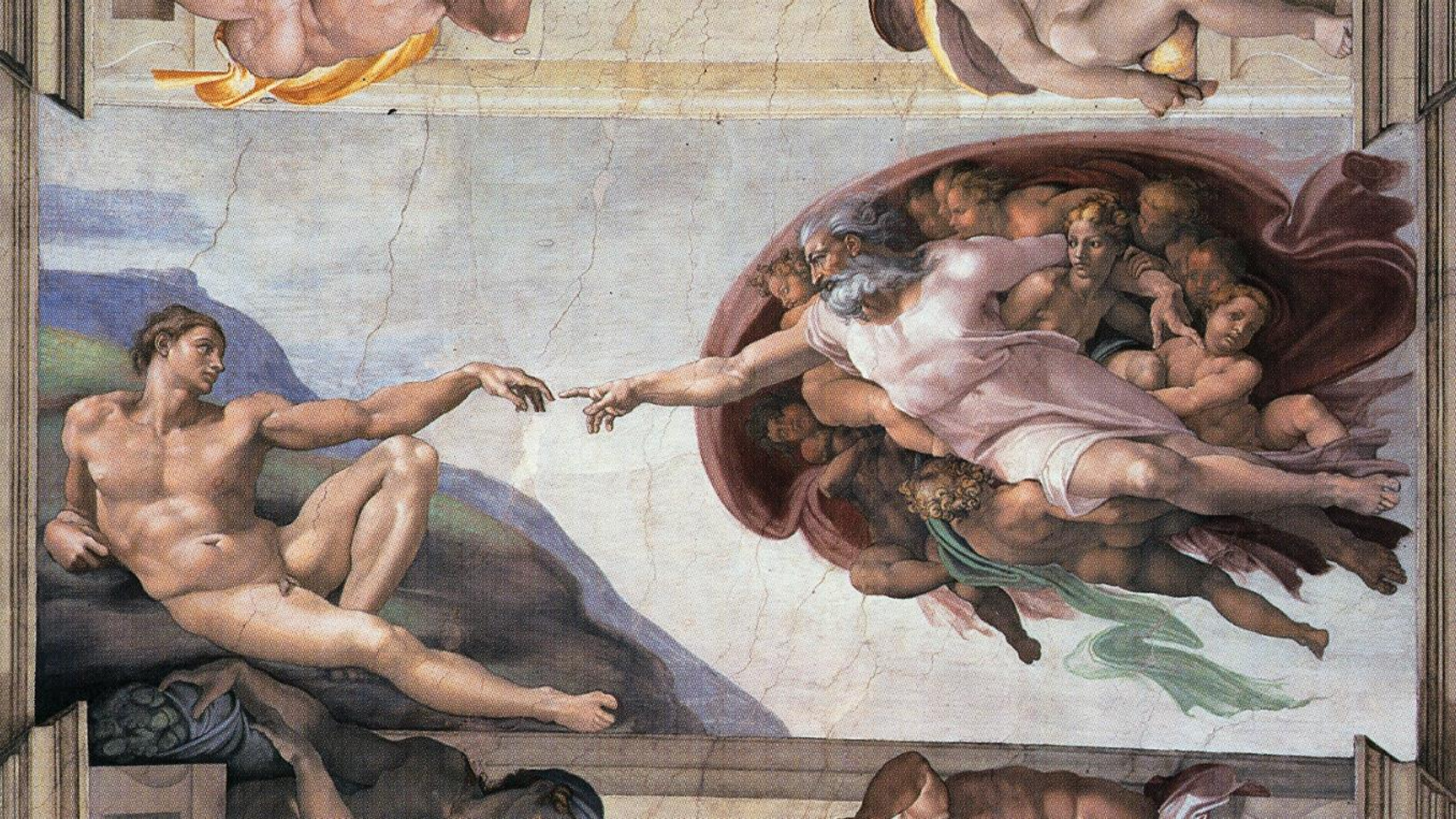




# Dilemma's in de Informatiesamenleving

Brenno de Winter - @brenno







**Afterglow Light  
Pattern  
375,000 yrs.**

**Dark Ages**

**Development of  
Galaxies, Planets, etc.**

**Accelerated Expansion**

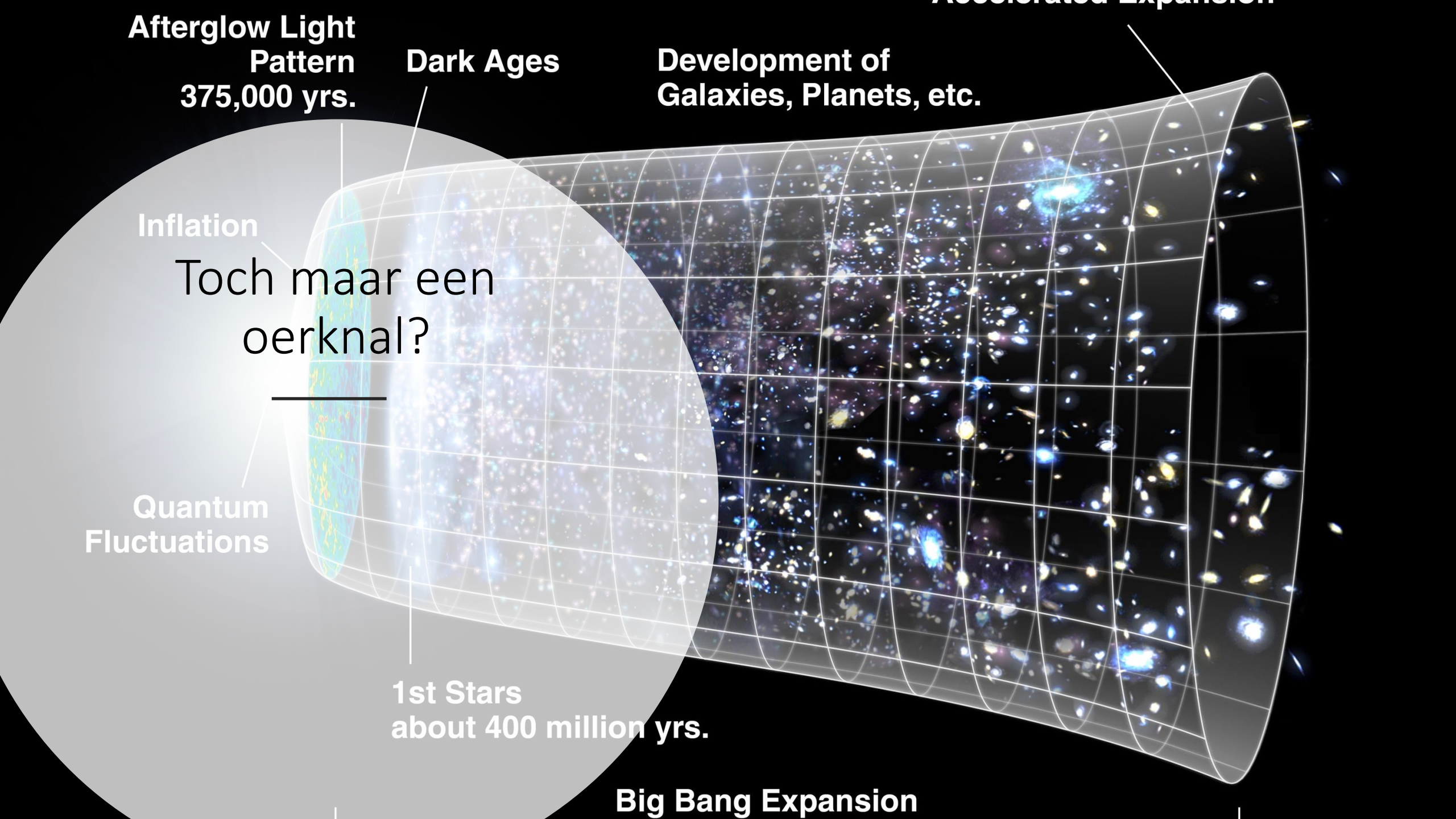
**Inflation**

Toch maar een  
oerknal?

**Quantum  
Fluctuations**

**1st Stars  
about 400 million yrs.**

**Big Bang Expansion**



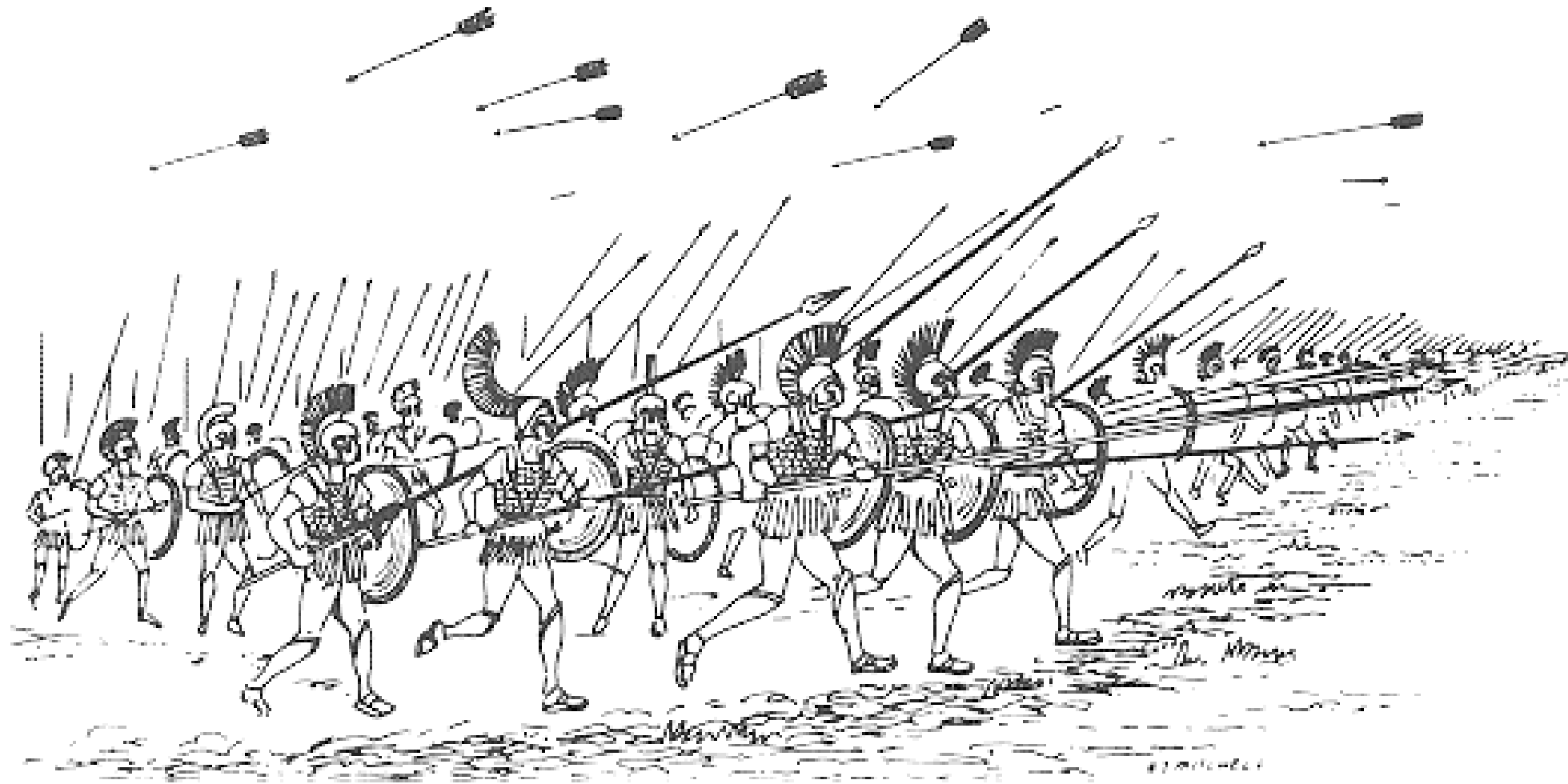


1520 Boeken Luther  
1521 Luther in de ban  
1546 Luther overlijdt  
1559 kwam de Index

2011 Diginotar  
29 augustus hack wordt bekend  
6 september overheid zegt  
vertrouwen op  
20 september failliet



# Wendbaarheid





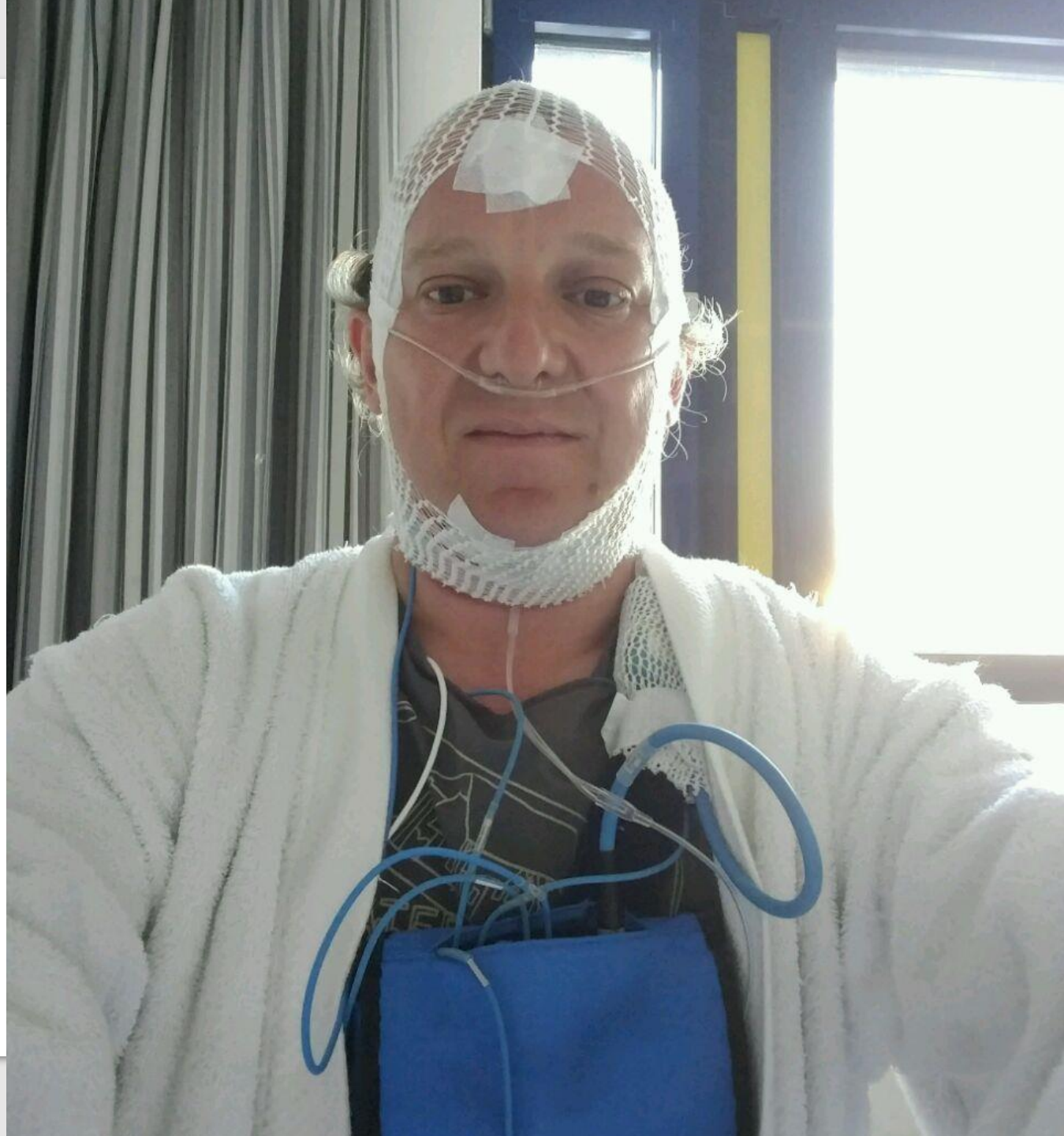




# Techno-optimisme

Ik kan mij niet voorstellen dat zich een probleem zou kunnen voordoen waardoor deze nieuwe software ooit nog tot gehackt kan worden en dat ze problemen geven die niet meer te herstellen valt. Tegenwoordig is de technologie zover dat we definitief hebben afgerekend met dit soort voorvallen.











# Het kan niet fout gaan

---

Ik kan mij niet voorstellen dat zich een probleem zou kunnen voordoen waardoor een van deze nieuwe schepen ooit nog tot zinken kan worden gebracht en dat ze averij oplopen die niet meer te herstellen valt. Tegenwoordig is de scheepvaart zover dat we definitief hebben afgerekend met dit soort voorvallen. – New York Times 1907

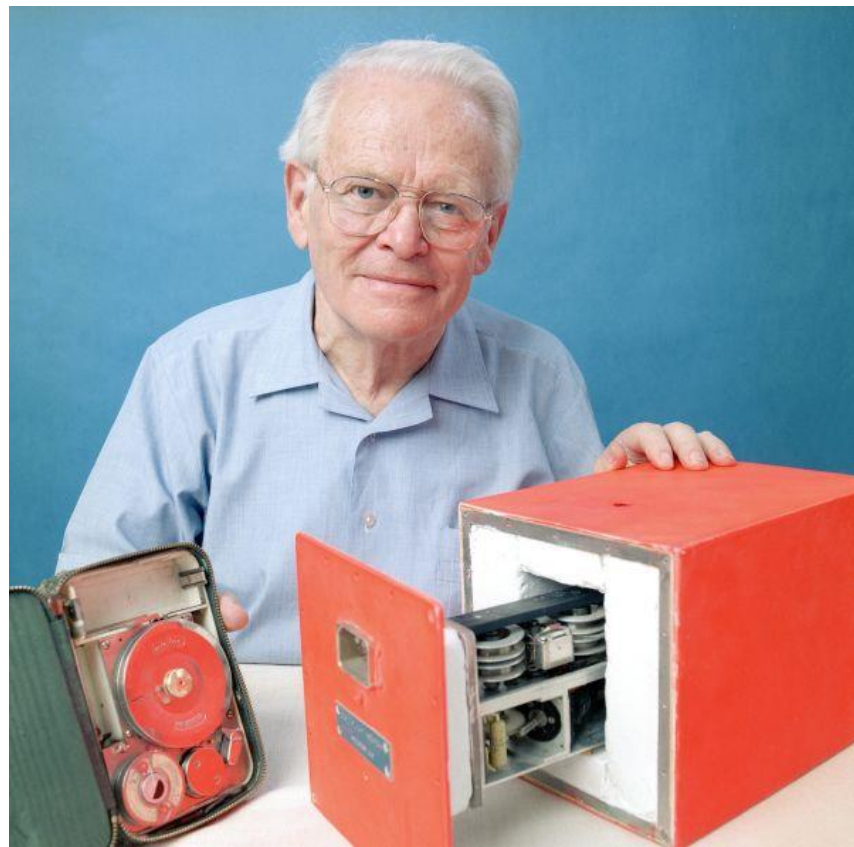
# APT Timeline of Events

- Advanced - Geavanceerd
- Persistent - Aanhoudend:
- Threat – Dreiging





# Vergaren bewijs 7-18 juni



# Crisis

- Eerste resultaten

- Aanvallen begonnen op 20 december 2018
- Met enige regelmaat gebeuren handelingen
- Groeiend aantal systemen wordt betrokken
- Geen meerfactorauthenticatie breed ingezet
- Er zijn onbekende systemen
- Er zijn systemen verouderd
- Om niet verklaarbare redenen staat RDP (remote beheer aan)
- Diverse pogingen malware te activeren. Antivirus stopt deze pogingen
- Meldingen niet opgemerkt



A medium shot of a man with dark, wavy hair, a beard, and glasses. He is wearing a light-colored blazer over a dark, patterned shirt. He is looking out of a large window with multiple panes, which shows a bright outdoor scene with greenery and a building. The window is flanked by dark, patterned curtains. The lighting is soft and natural, coming from the window.

Ja, die eerste uren waren de zorgen enorm.



# De ergste nachtmerrie

- Op 12 juni 2019 wordt duidelijk dat er een vorm van toegang tot Active Directory is geweest
- Niet uit te sluiten: daders hebben golden ticket
- Diverse losgeldberichten op computers
- Dus opnieuw opbouwen

Everything you  
<code> can and  
will be used  
against you



**Naast het ongemak voor de inwoners van de gemeente Lochem was er ook aanzienlijke financiële schade.**

# Lochem's tijdlijn



20 december 2018 eerste  
inbraak



5 juni 2019 aanval



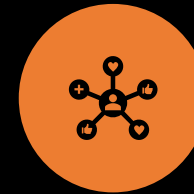
6 juni 2019 ontdekking



7 juni 2019 start  
forensisch onderzoek



12 juni 2019 vrees nog  
bestaande toegang



13 juni 2019  
gemeentehuis een dacht  
dicht voor veel taken



18 juni 2019 einde  
vergaren bewijs