

# De derde golf



[Wim.bertels@ucll.be](mailto:Wim.bertels@ucll.be)

# Nep nieuws waar iedereen in gelooft

## Chronologie van het experiment [ bewerken ]

---

Jones beschrijft in zijn essay dat hij op de eerste dag van het experiment (maandag, 3 april 1967) zijn studenten een juiste manier van zitten leerde en een gedisciplineerde manier om de klas binnen te komen. Na enige oefening slaagden de leerlingen erin om binnen 30 seconden de klas binnen te komen en op een geruisloze manier te gaan zitten.

Op de tweede dag vormde hij de geschiedenisklas verder om tot een gedisciplineerde groep met een overheersend groepsgevoel. Ook introduceerde hij de naam *De Derde Golf*, verwijzend naar de veronderstelling dat in de **branding** van de zee een derde golf altijd krachtiger is dan de eerste en tweede. De leerlingen leerden vervolgens een groet die zij ook buiten de klas dienden te gebruiken om aan te geven dat zij onderdeel van *De Derde Golf* waren. De groet werd door alle leerlingen gebruikt.

Het experiment ging vanaf dit moment een eigen leven leiden: op de derde dag sloten ook leerlingen van buiten de geschiedenisklas zich aan. Leerlingen waren gemotiveerd, gedisciplineerd en presteerden significant beter. Lidmaatschapskaarten werden rondgedeeld en alle leden van *De Derde Golf* kregen opdrachten (zoals het ontwerpen van een vlag, het bewaken van de orde). Ook leerde Jones zijn leerlingen hoe ze anderen lid konden maken van de Derde Golf. Aan het eind van de derde dag was de aanhang gegroeid tot ruim 200 scholieren. Tot zijn verrassing begonnen leerlingen overtredingen van medeleerlingen te melden aan Jones.

Op de vierde dag leek de beweging uit de hand te lopen en besloot Jones om het te beëindigen. Hij kondigde aan dat *De Derde Golf* onderdeel was van een landelijke beweging en dat een kandidaat voor het landelijke leiderschap van de beweging zich de dag erop bekend zou maken.

?

- Wat vond je van ‘facebook en ik’

?

- Wat vond je van ‘humane tech’

?

- Zie je oplossingen?
- Heb je antwoorden?
- Heb je vragen?

# Feiten?

- Kwestbaarheid maatschappij
  - ‘Wir haben ..
- Hedendaagse verbondenheid werkt in 2 richtingen
  - De gemiddelde mens lijkt hier slecht tegen gewapend
  - Gevaarlijke verslavende beloningssystemen > een sterk vertekend beeld op de wereld
- Hedendaagse voorbeelden?
- Rol al informaticus?

# Humanetech stelling

**The race for attention is eroding the pillars of our society.**



## Mental Health

The race to keep us on screen 24/7 makes it harder to disconnect, increasing stress, anxiety, and reducing sleep.

## Our Children

The race to keep children's attention trains them to replace their self-worth with likes, encourages comparison with others, and creates the constant illusion of missing out.

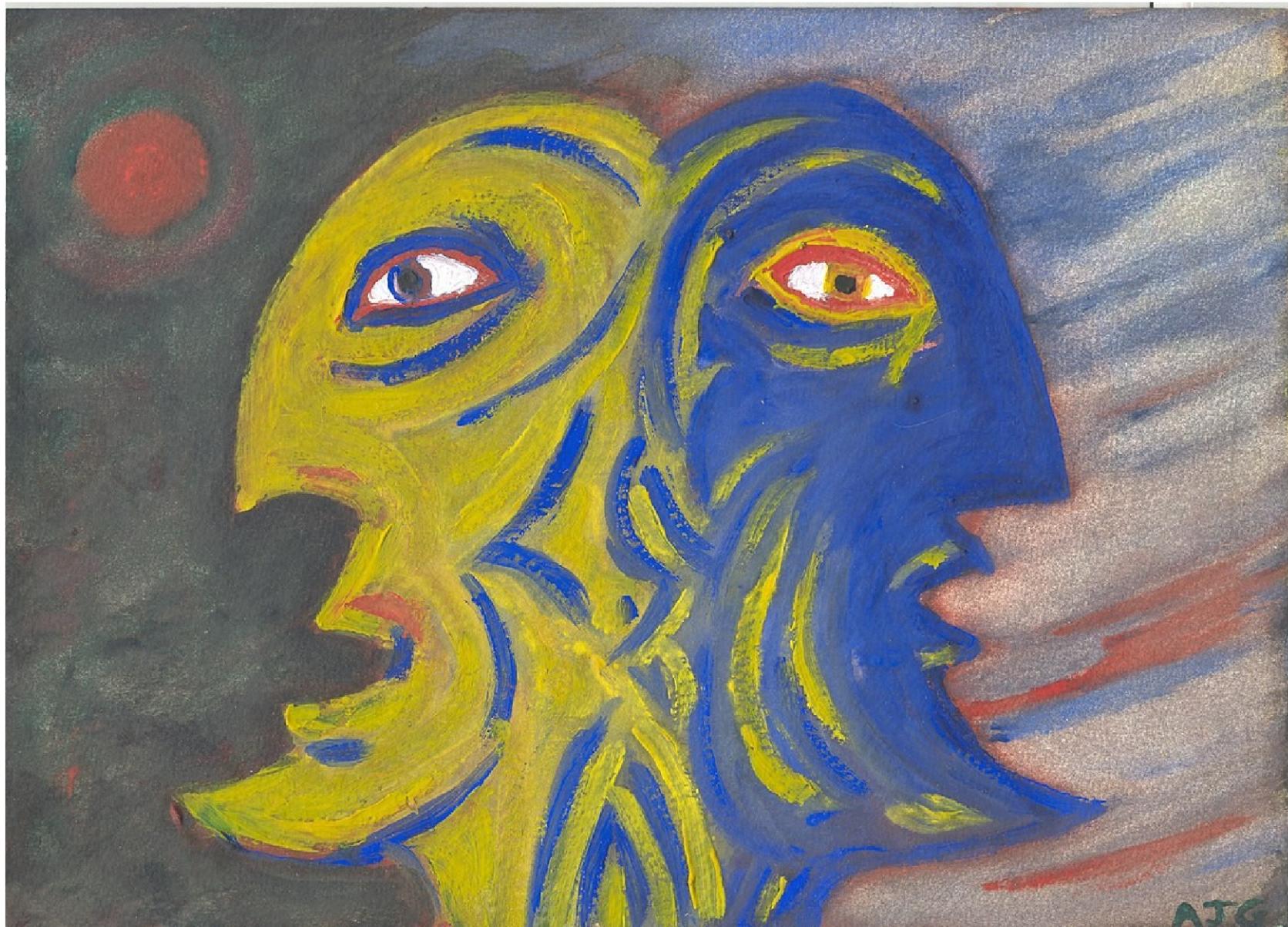
## Social Relationships

The race for attention forces social media to prefer virtual interactions and rewards (likes, shares) on screens over face-to-face community.

## Democracy

Social media rewards outrage, false facts, and filter bubbles – which are better at capturing attention – and divides us so we can no longer agree on truth.

# Sociaal..?



# Feiten

- **Wat is de onderliggende drijfveer?**
- Welke webpagina's met informatie bezoek je?
  - Bv VRT?
  - <https://mondediplo.com/>
  - <https://www.theguardian.com/international>
  - ..
  - Niet altijd zo duidelijk als <https://www.blik.be/>
  - <https://www.hln.be/>
  - Blogs?
  - Sociale media
  - ..
  - Vertrouwen!
- Gratis (en gesloten), dan ..
  - “Als het product gratis en gesloten is, dan bij je zelf het product” (  $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$  )  $(a \wedge b) \leftrightarrow \neg(a \vee b)$  )
  - “Als je zelf niet het product bent, dan is product betalend of open.” (niet omgekeerd)
- Verantwoording?
- Van lokaal > nationaal > globaal

# AI?

- De zeven menselijke hoofdzonden en een krachtig wapen?
  - (ijdelheid, hebzucht, wellust, jaloezie, vraatzucht, woede, luiheid)
- Kan AI:
  - Liegen?
  - Beïnvloeden?
  - Bewust zijn?
  - ..
- ( Versus voordelen AI )

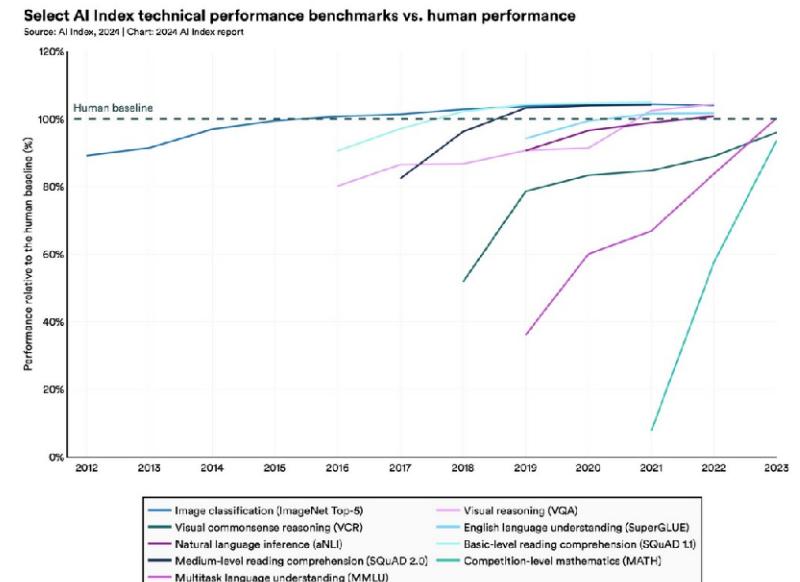
# AI?

- Evolutie kunstmatige intelligentie
  - Nivo dat de mens overstijgd
  - Globaal inter-net
  - Connectie met agents, virtueel en fysiek

## Neurale Netwerken

### Hersen vs Computer

|                      |   |   |
|----------------------|---|---|
| • Bewerkingseenheden | • $10^{11}$ Neuronen                    | • 1 CPU, $10^5$ Gates                     |
| • Geheugen           | • $10^{11}$ Neuronen $10^{14}$ Synapsen | • $10^{10}$ bits RAM, $10^{12}$ bits DISK |
| • Cyclus tijd        | • $10^{-3}$ sec                         | • $10^{-8}$ sec                           |
| • Bandbreedte        | • $10^{14}$ bits/sec                    | • $10^9$ bits/sec                         |
| • Neuron updates/sec | • $10^{14}$                             | • $10^5$                                  |



# Referenties

- [https://nl.wikipedia.org/wiki/De\\_Derde\\_Golf](https://nl.wikipedia.org/wiki/De_Derde_Golf)
- <http://humanetech.com>
- <https://www.vrt.be/vrtnu/a-z/facebook-en-ik/>
- Frontline: The Facebook Dilemma (EN)
- Ted Talk: How a handful of tech companies control billions of minds every day (EN)
- <https://aiindex.stanford.edu/report/>
- Capita Selecta 2003-2004, Sessie AI, KHLeuven, W.Bertels en G.Dierick

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License

# Ethiek



Wim.bertels@ucll.be

# Voorbeeld: tabel met persoonsgegevens

Wat is er gepast?

## 1.7 Respect the privacy of others.

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s).

These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code.

In these cases, the nature or contents of that information must be disclosed only to proper authorities.

<http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct>

# Moet data beveiligd zijn?

## **1. Public Interest**

You shall:

- a . have due regard for public health, **privacy, security** and wellbeing of others and the environment.
- b. have due regard for the legitimate rights of Third Parties.
- c. conduct your professional activities without discrimination in the grounds of sex, sexual orientation, marital status, nationality, colour, race, ethnic origin, religion, age or disability, or of any other condition or requirement.
- d. promote equal access to the benefits of IT and seek to promote the inclusion of all sectors in society where opportunities arise.

<http://www.bcs.org/upload/pdf/conduct.pdf>

# Met wie kan je praten?

## 1.7 Respect the privacy of others.

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

<http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct>

Verschillende gedragsregels  
Bij twijfel: vergelijk met de fysische wereld

<http://www.ieee.org/about/corporate/governance/p7-8.html>

<http://icie.zkm.de/publications/journals/ie>

Tijd voor een micropauze

The ethical values as defined in 1992 by the Computer Ethics Institute; a nonprofit organization whose mission is to advance technology by ethical means, lists these rules as a guide to computer ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

<https://en.wikipedia.org/wiki/Cyberethics>

(ISC) an organization committed to certification of computer security professional has further defined its own code of ethics generally as:

1. Act honestly, justly, responsibly, and legally, and protecting the commonwealth.
2. Work diligently and provide competent services and advance the security profession.
3. Encourage the growth of research - teach, mentor, and value the certification.
4. Discourage unsafe practices, and preserve and strengthen the integrity of public infrastructures.
5. Observe and abide by all contracts, expressed or implied, and give prudent advice.
6. Avoid any conflict of interest, respect the trust that others put in you, and take on only those jobs you are qualified to perform.
7. Stay current on skills, and do not become involved with activities that could injure the reputation of other security professionals.

<https://en.wikipedia.org/wiki/Cyberethics>

# GDPR

- EU General Data Protection Regulation
- Nieuwe wet rond persoonlijke data
  - Transparantie
  - Iedereen
- Vanaf 25 mei 2018
- Achtergrond
  - Analytics
  - Data Mining
  - Big Data
  - Ethiek

# Enkele sleutelelementen

- Inbraak moet gemeld worden
- Legale toestemming
- Recht op inzage
- Data overdraagbaarheid
- Recht om vergeten te worden
- Wereldschaal

# Referenties

- General Data Protection Regulation and PostgreSQL, warsaw, 26/10/2017, Mladen Marinović

Wim Bertels (CC)BY-SA-NC

# Beveiliging



[Wim.bertels@ucll.be](mailto:Wim.bertels@ucll.be)

# Security

- Hardware
- Het platform waar het op draait
- De databank software
- Binnen sql zelf (grant, revoke, view,...)
- Sql als “vertaler”
- Applicaties
- Gebruikers
- Algemeen terugkerende security problematiek (bv CIA, AAA, maar ook reserve kopies, ..)
- ..

# Ondersteunend platform

- Bijdetijs (Up to date) houden
- Beveiligen (infrastructuur vakken)
- (D)DoS-attack's
- ...

# Databank software

- Up to date houden
- Configuratie
  - Local
  - Remote
    - Eg postgresql: pg\_hba.conf, postmaster.conf en postgresql.conf
- Known exploits -> Wat doe je?

# Binnen SQL zelf

- User management (roles)
- Privileges (grant / revoke)
- Views
- Stored procedures
- Row Security Policies

# SQL

- SQL wordt niet gecompileerd
- SQL wordt “vertaald” in de onderliggende/omsluitende laag
- Dit kan gebruikt worden om sql ongewenste instructies te laten uitvoeren
- Het is probleem dat bij elke taal die “vertaald”, terugkomt (eg php)

# SQL Injection

- Indien we de onderliggende sql code van bv een formulier niet kennen, dan gaan we proberen te raden wat de sql code is die erachter zit.
- Ipv gewone waarden gaan sql code meegeven met het formulier.
- Pas op serial, identity, autoincrement..?

# Incorrectly Filtered Escape Characters

- Fout: input is niet gefilterd op escape characters
- Bv
  - statement := "SELECT \* FROM users WHERE naam = " + userNaam + ";"
  - UserNaam:= a' or 't='t
  - Gevolg: SELECT \* FROM users WHERE naam = 'a' or 't='t';
  - Dus.. , andere voorbeelden?

# Incorrect Type Handling

- Fout: types van de input worden niet gecheckt
- Bv
  - statement := "SELECT \* FROM data WHERE id = "  
+ a + ";" (a wordt enkel verwacht als int)
  - Voor a := 1;DROP TABLE users;
  - Gevolg: SELECT \* FROM data WHERE id = 1;DROP TABLE users;
  - Dus..

# Oplossingen

- Escape character verwijderen uit de invoervelden
- Invoer validatie, controleren of het invoerveld bv wel het juiste type heeft
- Prepared statements
- Stored procedures
  - Type
  - ; en escaping
  - Grants..
  - Dicht bij de bron
  - ..

# Opgepast

- Enkel Escaping is niet voldoende:
- Bv
  - `SELECT * from items where userid=$userid;`
  - `$userid := "33 or userid is not null or userid=44";`
  - `SELECT * from items where userid=33 or userid is not null or userid=44;`
- Dus zeg eerder wat wel mag zijn als invoer, ipv wat niet mag; het eerste is eenvoudiger, er zijn (meestal) maar een eindig aantal mogelijkheden.

# Handige Functies

- `quote_ident ( text ) → text`
- `quote_literal ( anyelement ) → text`
  - `quote_nullable ( anyelement ) → text`

# Dieper

- <https://www.postgresql.org/docs/current/ddl-rowsecurity.html>

```
CREATE TABLE users (
```

```
    manager text,
```

```
    company text );
```

```
ALTER TABLE users ENABLE ROW LEVEL SECURITY;
```

```
CREATE POLICY users_manager
```

```
    ON users TO managers -- groep rol managers
```

```
    USING (manager = current_user);
```

- <https://www.postgresql.org/docs/current/sepgsql.html>
- <https://www.postgresql.org/docs/current/sql-security-label.html>

# Links

- <http://www.w3schools.com/>
- <http://www.postgresql.org/>
- <http://en.wikipedia.org/>

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License