

Dark web

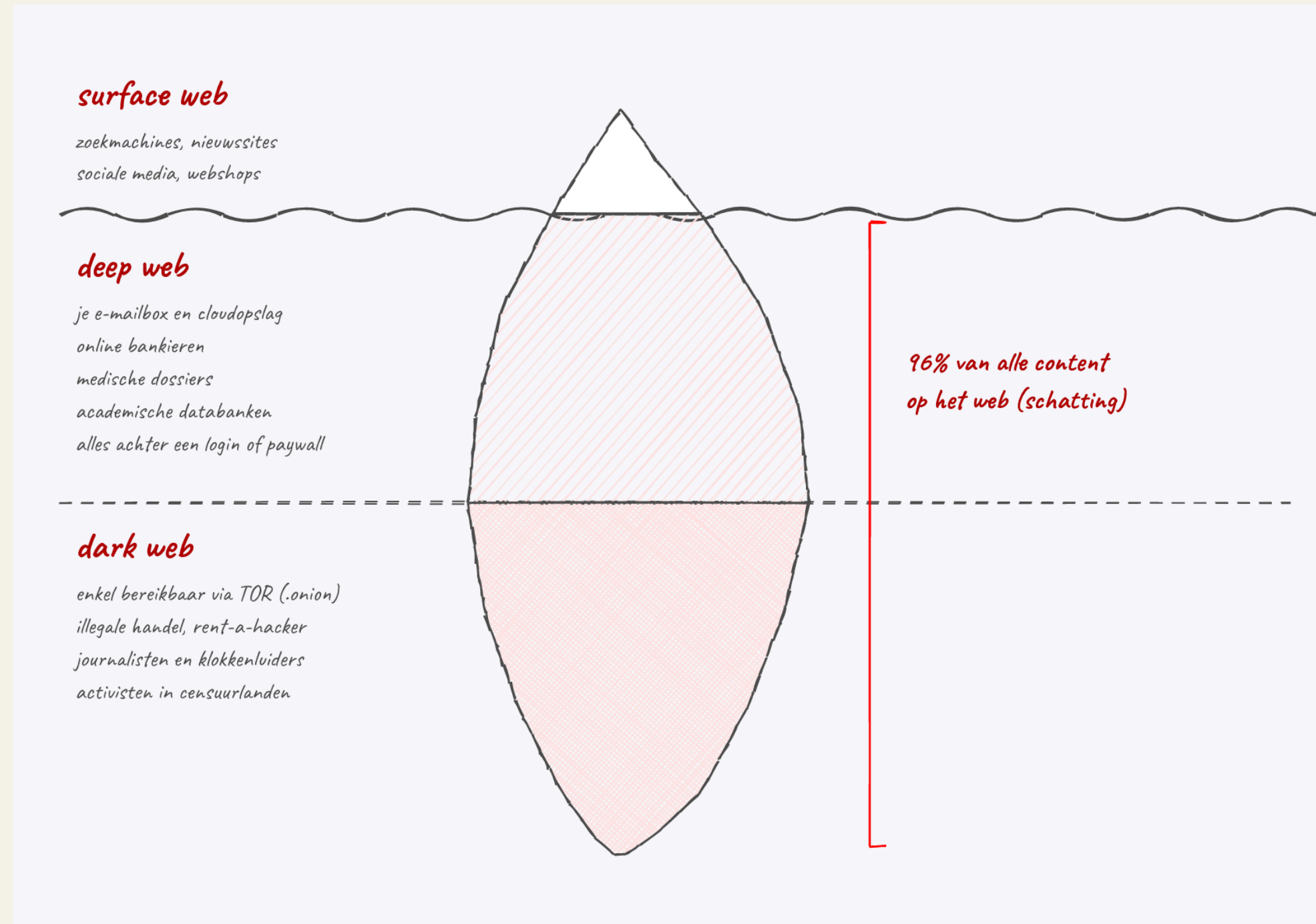
Cyberboswachters

Tim Dams

Deze cursus werd gemaakt met hulp van AI-assistentie. Sommige afbeeldingen zijn door AI gegenereerd.



Het internet is een ijsberg



De internet ijsberg: surface web, deep web en dark web.

De drie lagen



Surface web

Alles wat Google indexeert.

Gewone browser.



Deep web

Databanken, afgeschermdes sites, privé-accounts.

Niet geïndexeerd, vaak login vereist.



Dark web

Anoniem, versleuteld, niet geïndexeerd.

Speciale software (TOR).

Het **deep web** is veel groter dan het surface web: bedrijfsdatabases, medische dossiers, cloud-opslag, ... Het **dark web** is er een klein maar berucht stukje van.

INTERNET IS NIET ANONIEM

Op het gewone internet ben je **bijna altijd**
traceerbaar.

IP-adres

cookies

provider-logs

trackers

Sommige landen gaan verder



Volledige controle

De overheid monitort al het verkeer en logt wie wat doet.



Blacklisting

Sociale media, nieuwssites of messengers worden gewoon geblokkeerd.

China

Saudi-Arabië

Iran

Egypte

Noord-Korea

Cuba

NOM-DE-PLUME

Niet iedereen, en zeker niet de overheid, moet weten wat jij **legaal** in je vrije tijd doet.

Onder een schuilnaam je mening kunnen uiten is belangrijk voor een democratie. Privacy tegenover opsporing blijft een **moeilijke afweging**.

Kenmerken van het dark web



Anoniem

Je verbinding loopt via meerdere tussenliggende servers. Wie wat bezoekt, is vrijwel niet te achterhalen.



Versleuteld

Verkeer **binnen** het TOR-netwerk is versleuteld. Wie onderweg meekijkt, ziet niet wat je doet.



Moeilijk te censureren

Duizenden relais van vrijwilligers. Niemand kan het netwerk in z'n eentje stilleggen.

Goed én slecht gebruik

Legitiem

- Journalisten die veilig communiceren vanuit dictaturen
- Klokkenluiders (bv. WikiLeaks-bronnen)
- Activisten in landen met censuur
- Anonieme vrije meningsuiting

vs

Crimineel

- Handel in drugs, wapens en gestolen data
- Verkoop van creditcardgegevens
- “Rent-a-hacker”-diensten
- Ransomware-as-a-Service
- Kindermisbruikmateriaal



Het dark web is **niet** per definitie illegaal. Wat je er doet, kan dat wel zijn.

Anonimiteit is geen vrijgeleide: politiediensten sporen ook op het dark web criminelen op.

Landen zoals Rusland en China blokkeren TOR, en wie het daar toch gebruikt, kan in de problemen komen.

THE ONION ROUTER

Toegang via TOR

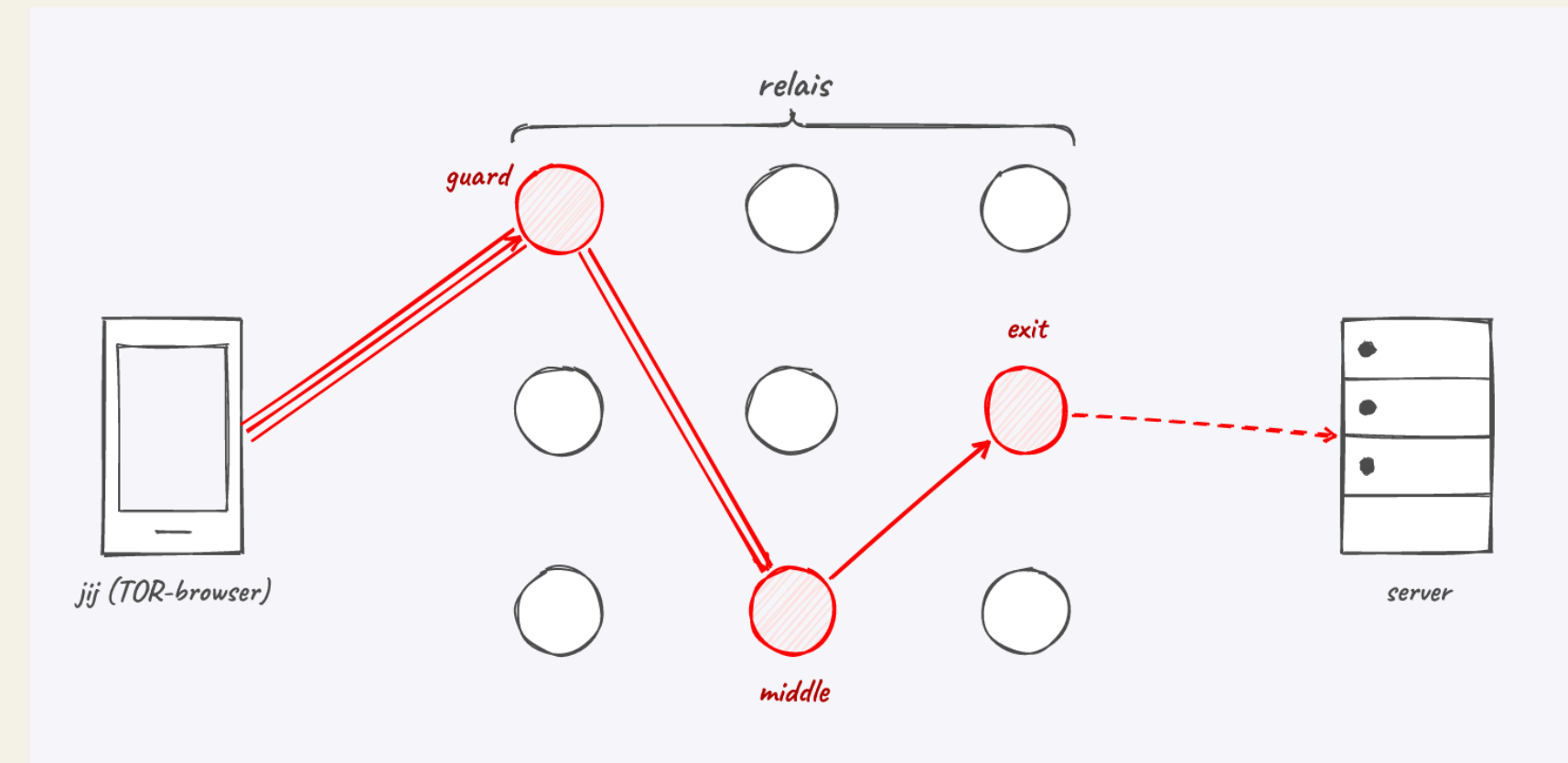
Lagen, zoals bij een ui

Je browser kiest drie relais: **guard**, **middle** en **exit**, en versleutelt je verzoek **drie keer**.

Elk relais pelt één laag af en kent enkel de vorige en de volgende stap. Niemand kent het volledige pad.

Tussen exit en website zit **geen TOR-encryptie** meer: gebruik dus ook HTTPS.

Onion services (`.onion`) blijven volledig binnen TOR: geen exit, en ook de server blijft anoniem.



TOR heeft ook nadelen



Traag

Je verkeer passeert meerdere servers wereldwijd.



Geblokkeerd

Sommige sites weigeren verkeer van TOR-servers.



Firewalls

Bedrijfsnetwerken blokkeren TOR standaard.

Browsers zoals **Brave** hebben TOR ingebouwd. Handig, maar **minder anoniem** dan de echte TOR-browser.

Waarom moet je dit weten?



Gestolen data

Wachtwoorden, creditcards en bedrijfsgeheimen worden er **verhandeld**.



Criminele tools

Exploits en tools zijn er **te koop of te huur**.



Threat intelligence

Beveiligingsteams houden het dark web in de gaten voor vroege waarschuwingen.



Privacytechnologie

Wie TOR begrijpt, kan beter verdedigen én onderzoeken.