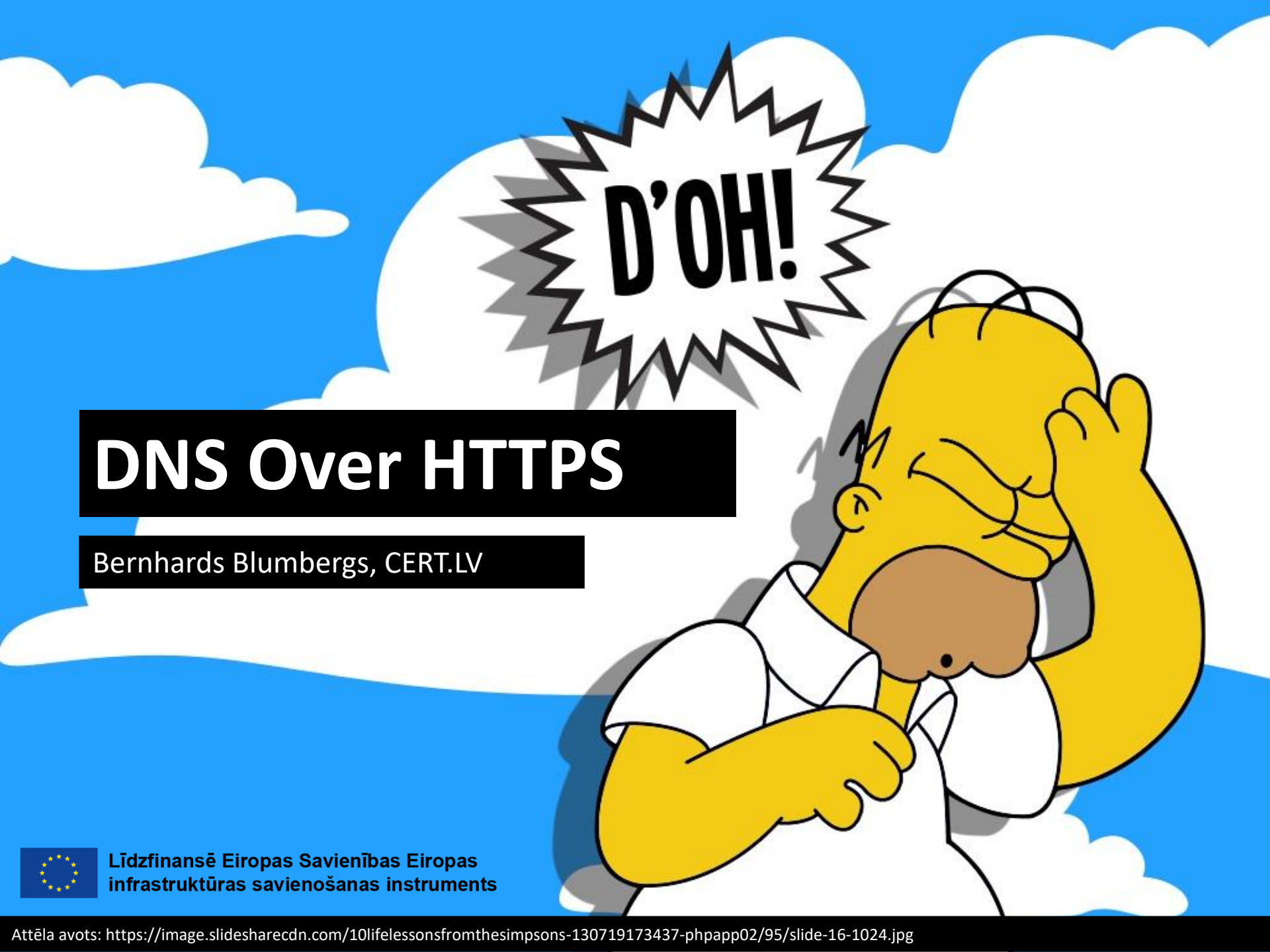


DNS Over HTTPS

Bernhards Blumbergs, CERT.LV

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments

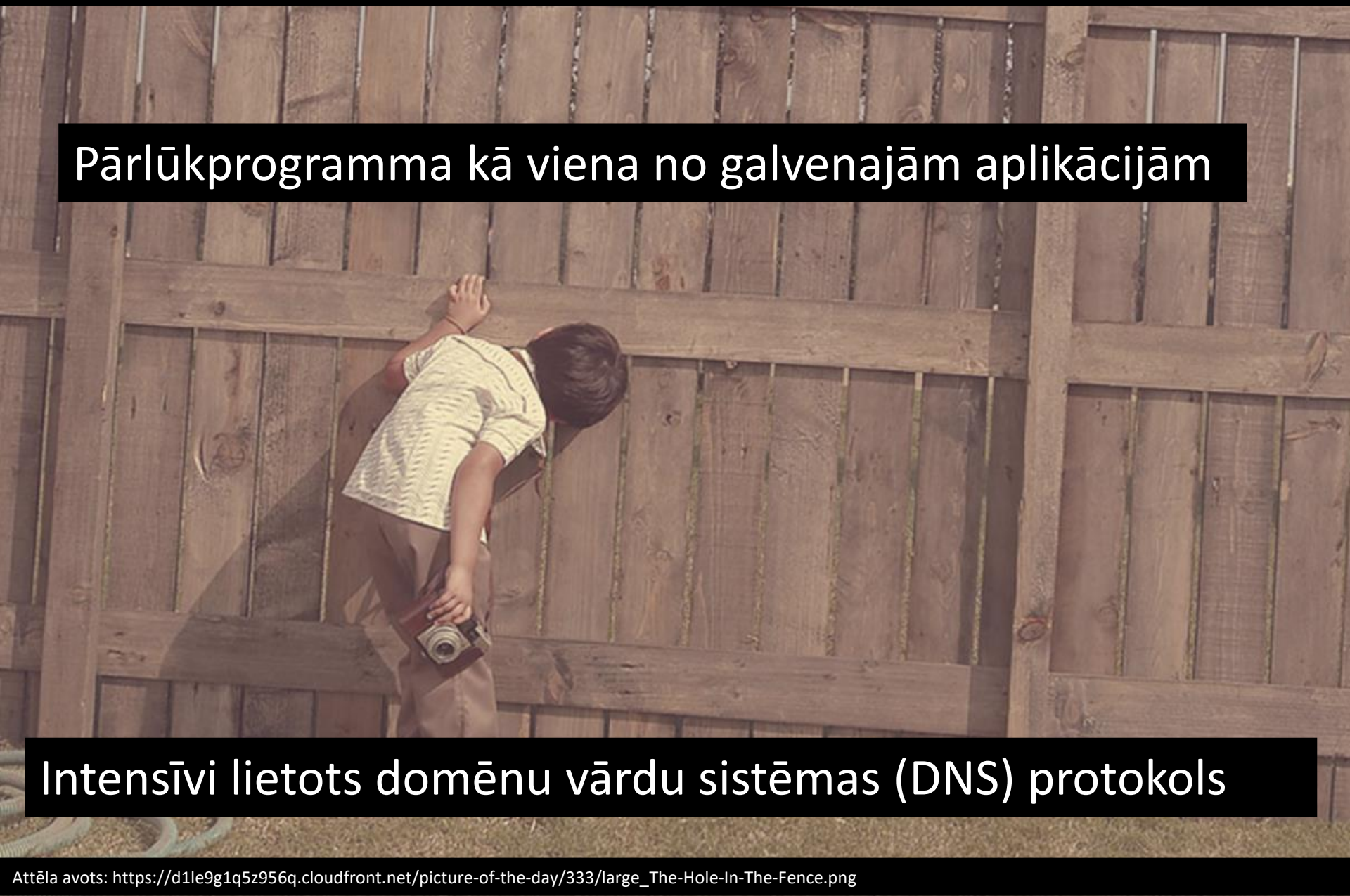
Attēla avots: https://image.slidesharecdn.com/10lifelessonsfromthesimpsons-130719173437-phpapp02/95/slide-16-1024.jpg

Saturs

- Nepieciešamība
- Tehnoloģija
- Problēmas

Attēla avots: https://cdn10.bigcommerce.com/s-60yzq6/products/683/images/1702/mini_milk_bottle__16715.1412749278.1280.1280.jpg

Internet pārlūkprogramma



Pārlūkprogramma kā viena no galvenajām aplikācijām

Intensīvi lietots domēnu vārdu sistēmas (DNS) protokols

Attēla avots: https://d1le9g1q5z956q.cloudfront.net/picture-of-the-day/333/large_The-Hole-In-The-Fence.png

Klienta-puses uzbrukumi

Ļaundabīgas saites

Sociālie tīkli un saziņas kanāli

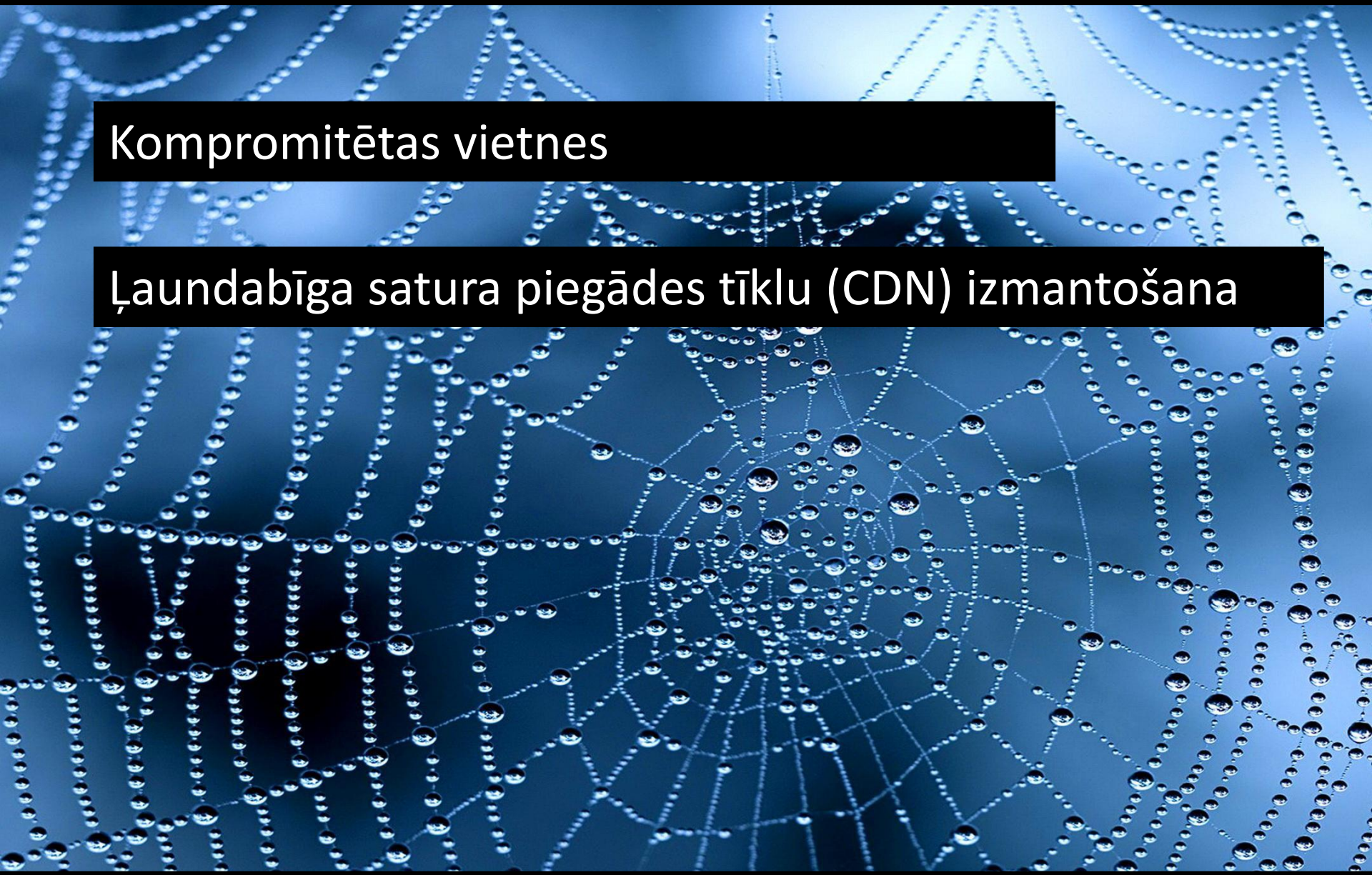
Ļaundabīga HTML/JavaScript renderēšana

Attēla avots: https://cdn10.bigcommerce.com/s-p1mhyx/products/1044/images/4469/CricketLollipopMain__97801.1529878505.1280.1280.jpg?c=2

Tīmekļa-puses uzbrukumi

Kompromitētas vietnes

Ļaundabīga satura piegādes tīklu (CDN) izmantošana



Attēla avots: https://images5.alphacoders.com/699/699941.jpg

Tīkla-puses uzbrukumi

- Uzbrukumi pret domēnu vārdu sistēmu (DNS)
  - DNS nolaupīšana (hijacking)
  - DNS saindēšana (poisoning)
- Tīkla iestatījumu izmaiņas
- Kompromitēts WiFi
- DHCP
- Trafika pārtveršana, noklausīšanās un cenzēšana

Attēla avots: https://i0.web.de/image/540/32932540,pd=1/dna.jpg

DNS over TLS (DoT)

IETF RFC7858, 2016MAI

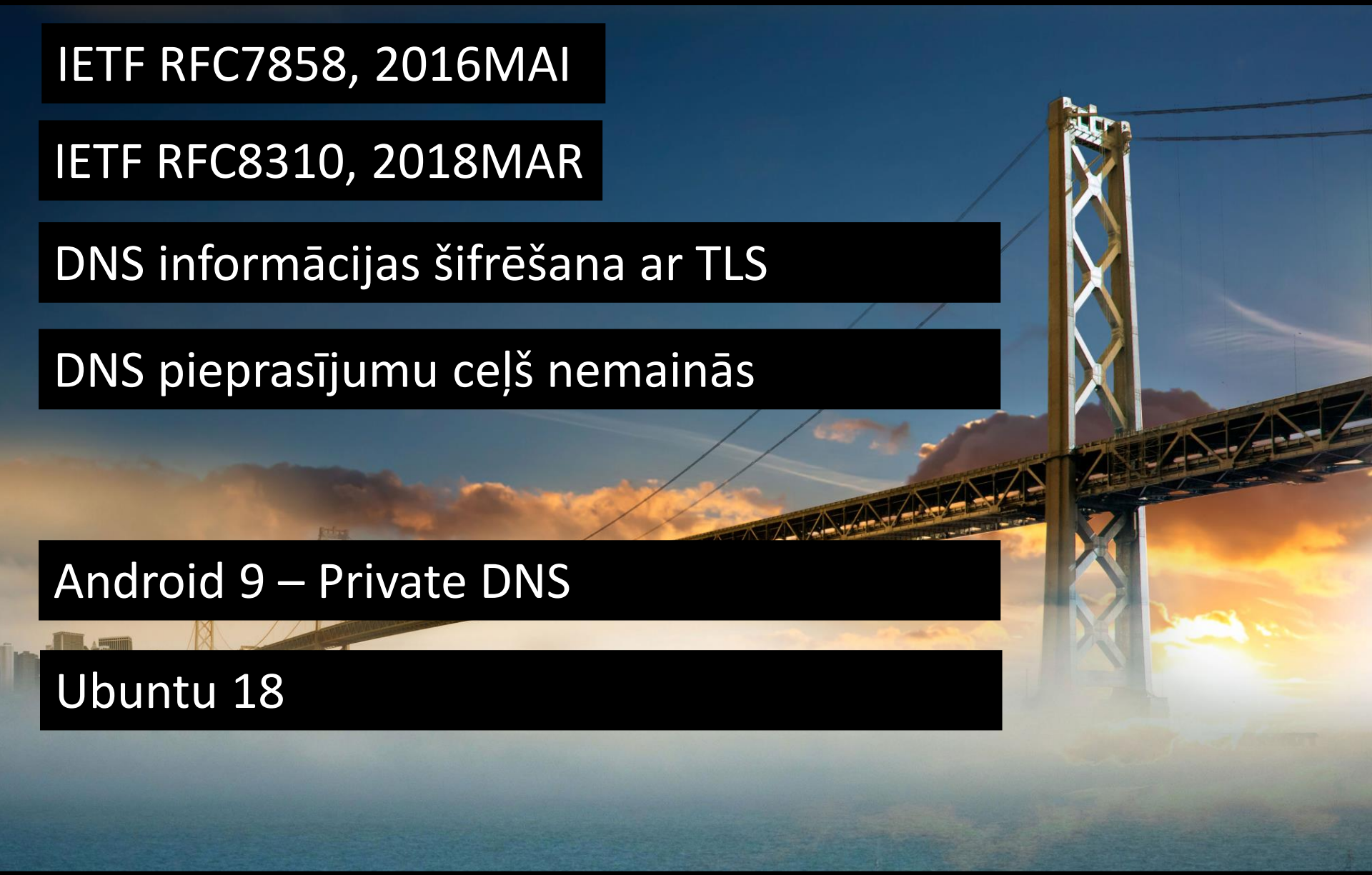
IETF RFC8310, 2018MAR

DNS informācijas šifrēšana ar TLS

DNS pieprasījumu ceļš nemainās

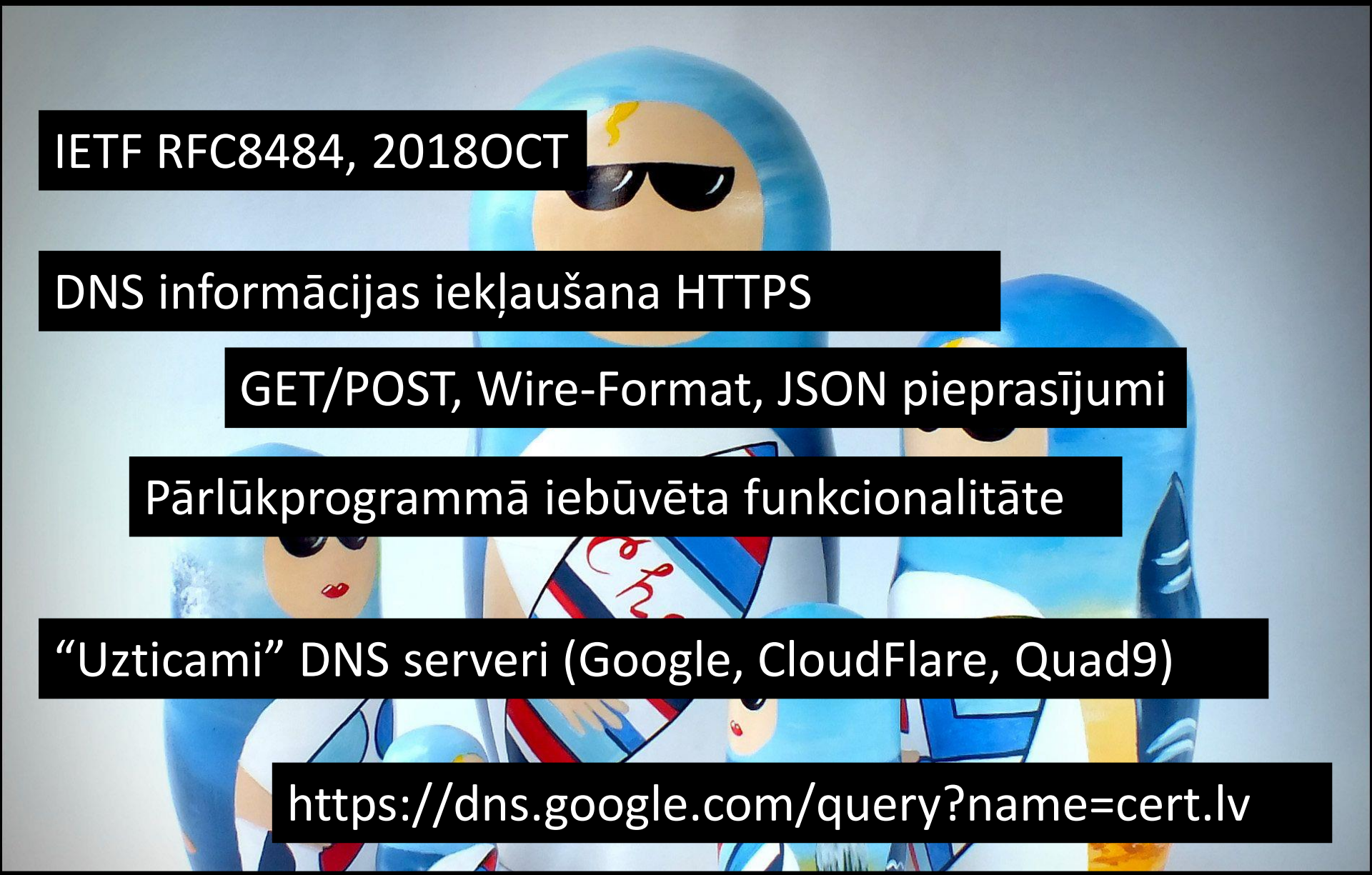
Android 9 – Private DNS

Ubuntu 18



Attēla avots: http://www.skybridge.com/wp-content/themes/skybridge-v1/img/body-bg-1.jpg

DNS over HTTPS (DoH)



IETF RFC8484, 2018OCT

DNS informācijas iekļaušana HTTPS

GET/POST, Wire-Format, JSON pieprasījumi

Pārlūkprogrammā iebūvēta funkcionalitāte

“Uzticami” DNS serveri (Google, CloudFlare, Quad9)

https://dns.google.com/query?name=cert.lv

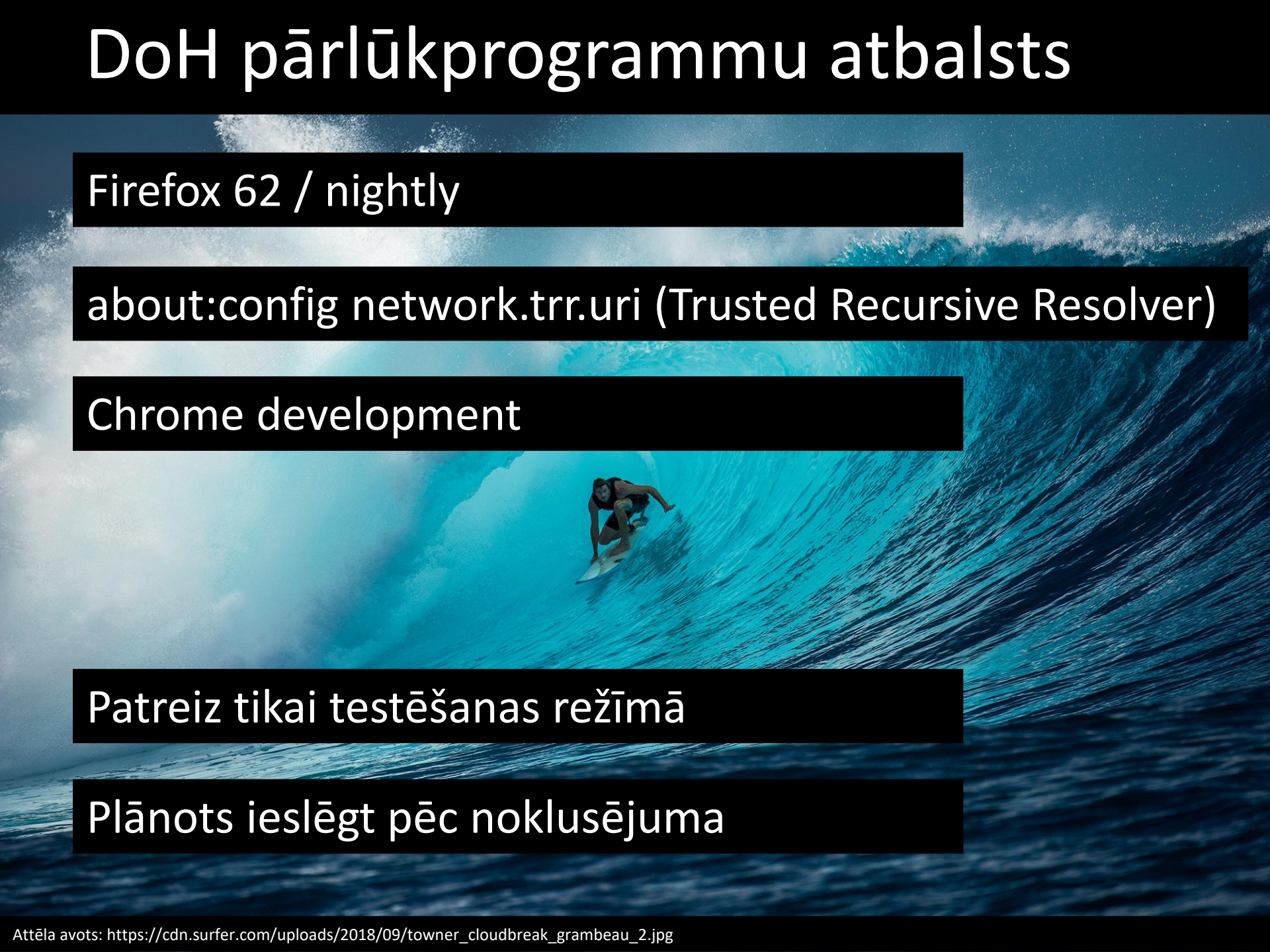
Attēla avots: https://i.pinimg.com/originals/ff/10/63/ff10633d0c53c1a2b2d98bff796db2f6.jpg

DoH pārlūkprogrammu atbalsts

Firefox 62 / nightly

about:config network.trr.uri (Trusted Recursive Resolver)

Chrome development



Patreiz tikai testēšanas režīmā

Plānots ieslēgt pēc noklusējuma

Attēla avots: https://cdn.surfer.com/uploads/2018/09/towner_cloudbreak_grambeau_2.jpg

DoH privātuma apsvērumi

Daži pārlūkprogrammu izstrādātāji 

Pāris publiskie, “uzticamie” DNS pakalpojumu sniedzēji

Pamatā ārpus ES

DNS pieprasījumu pieejamība

Tirgus kontrole?

1.1.1.1

8.8.8.8

9.9.9.9

Attēla avots: http://i.imgur.com/YQXMx6x.jpg

DoH drošības apsvērumi

Iestāžu drošības prasību īstenošanas zaudēšana

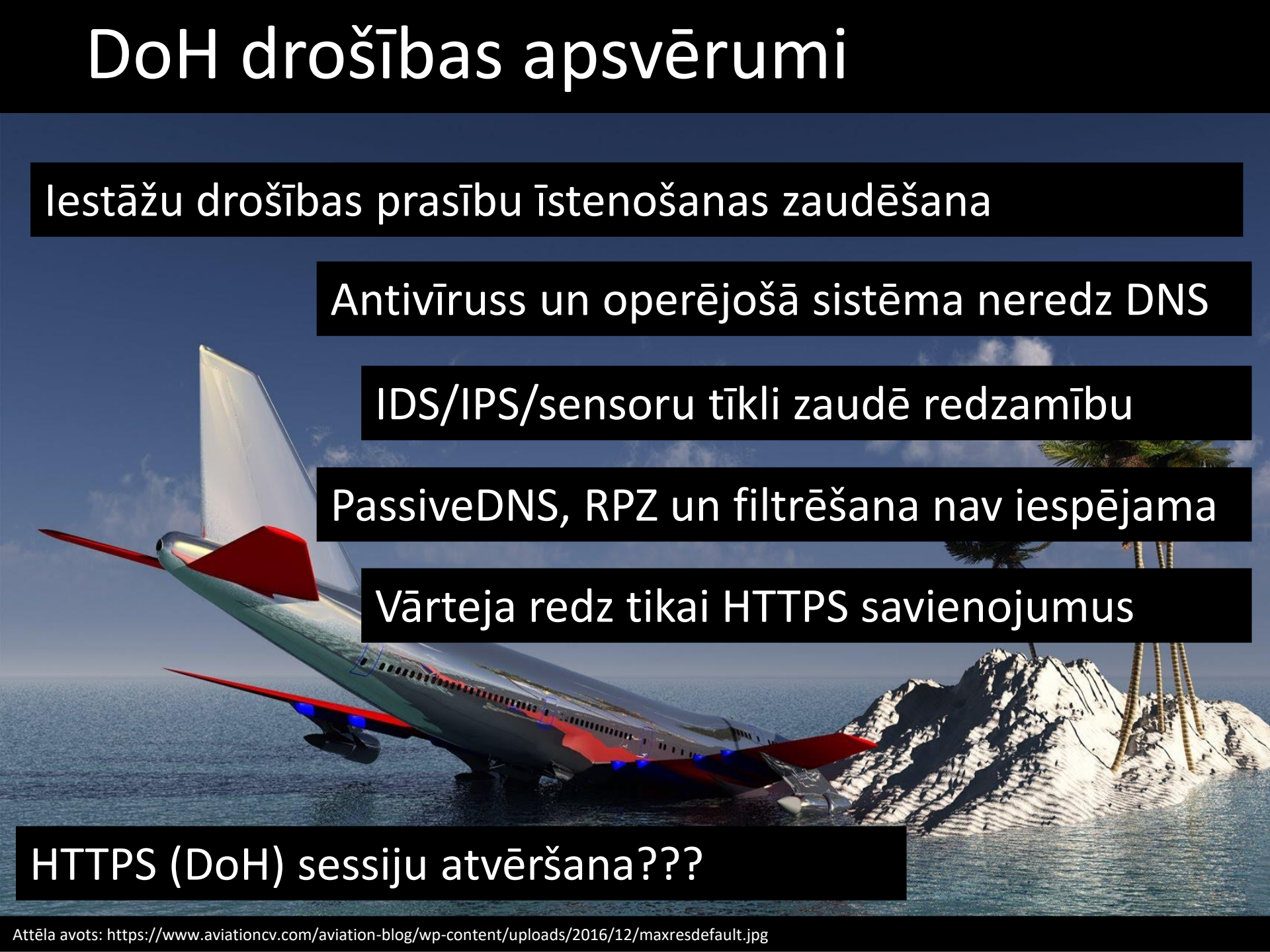
Antivīruss un operējošā sistēma neredz DNS

IDS/IPS/sensoru tīkli zaudē redzamību

PassiveDNS, RPZ un filtrēšana nav iespējama

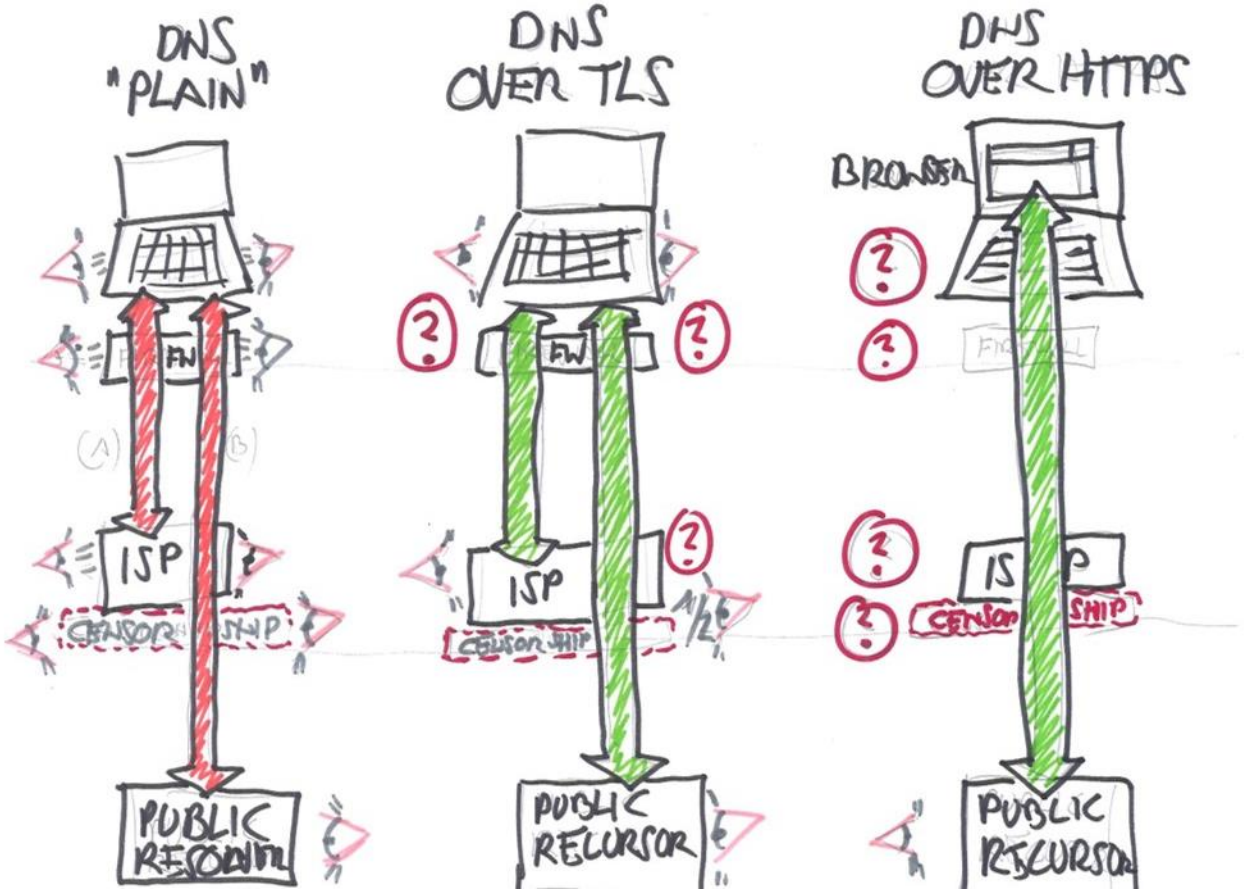
Vārteja redz tikai HTTPS savienojumus

HTTPS (DoH) sessiju atvēršana???



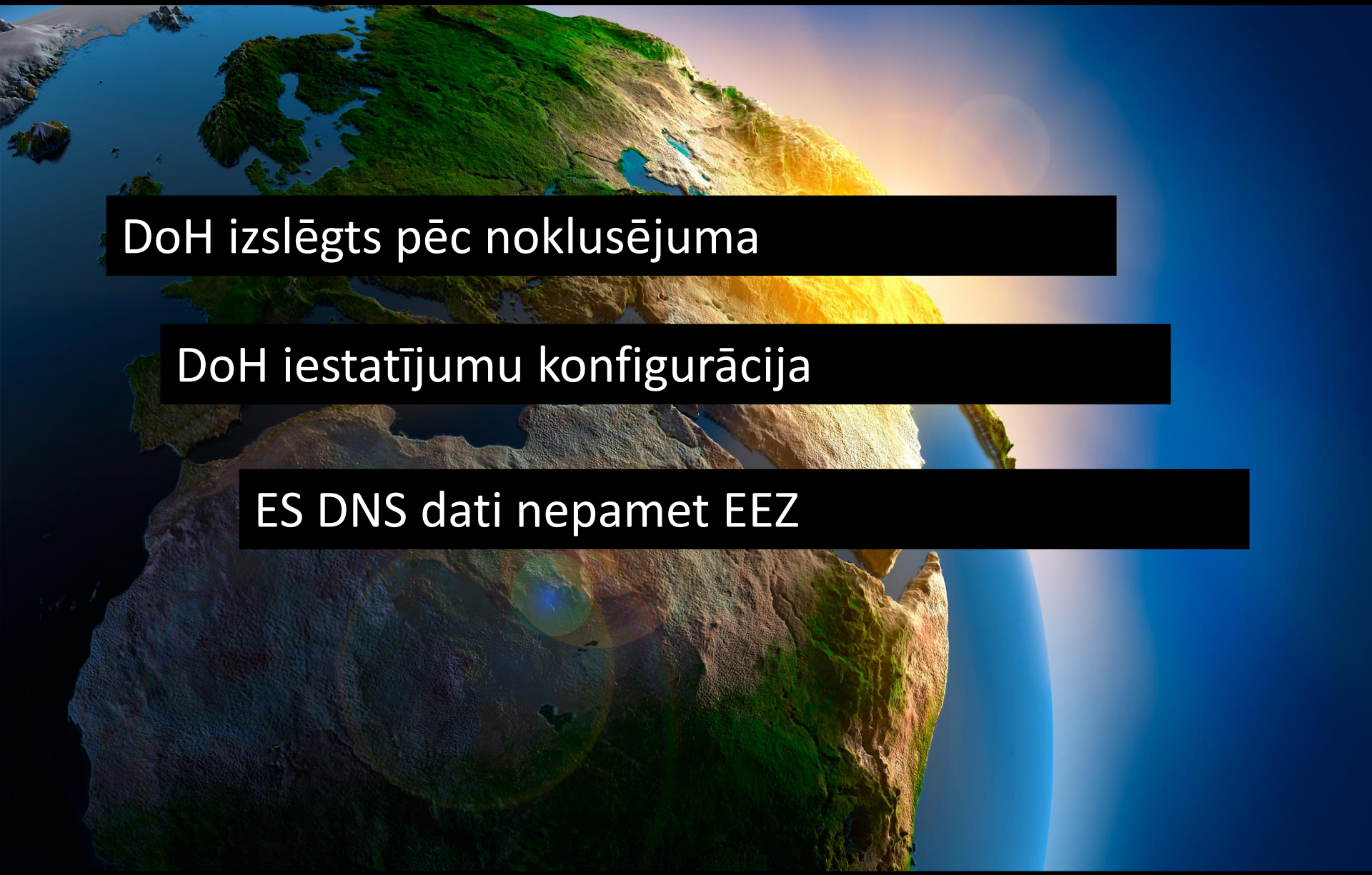
Attēla avots: https://www.aviationcv.com/aviation-blog/wp-content/uploads/2016/12/maxresdefault.jpg

DNS vs DoT vs DoH



Attēla avots: CERT.at/CERT.LV prezentācija

CSIRT Network aicinājums



DoH izslēgts pēc noklusējuma

DoH iestatījumu konfigurācija

ES DNS dati nepamet EEZ

Attēla avots: http://gaiaenergyre.com/wp-content/uploads/2014/09/Earth-from-Space-3D.jpg

Esi Drošs!

cert@cert.lv
https://www.cert.lv

certlv

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments