Application Level DoS, The Rise of CDNs And The End of The Free Internet

Christian Folini / @ChrFolini

BLACK ALPS

Christian Folini: The Boring Bio

- Co-Lead OWASP CRS Project
- Author of the ModSecurity Handbook 2ed
- Program Chair Swiss Cyber Storm Conf
- Vice-President Swiss Cyber Experts

Christian Folini / @ChrFolini

BLACK ALPS

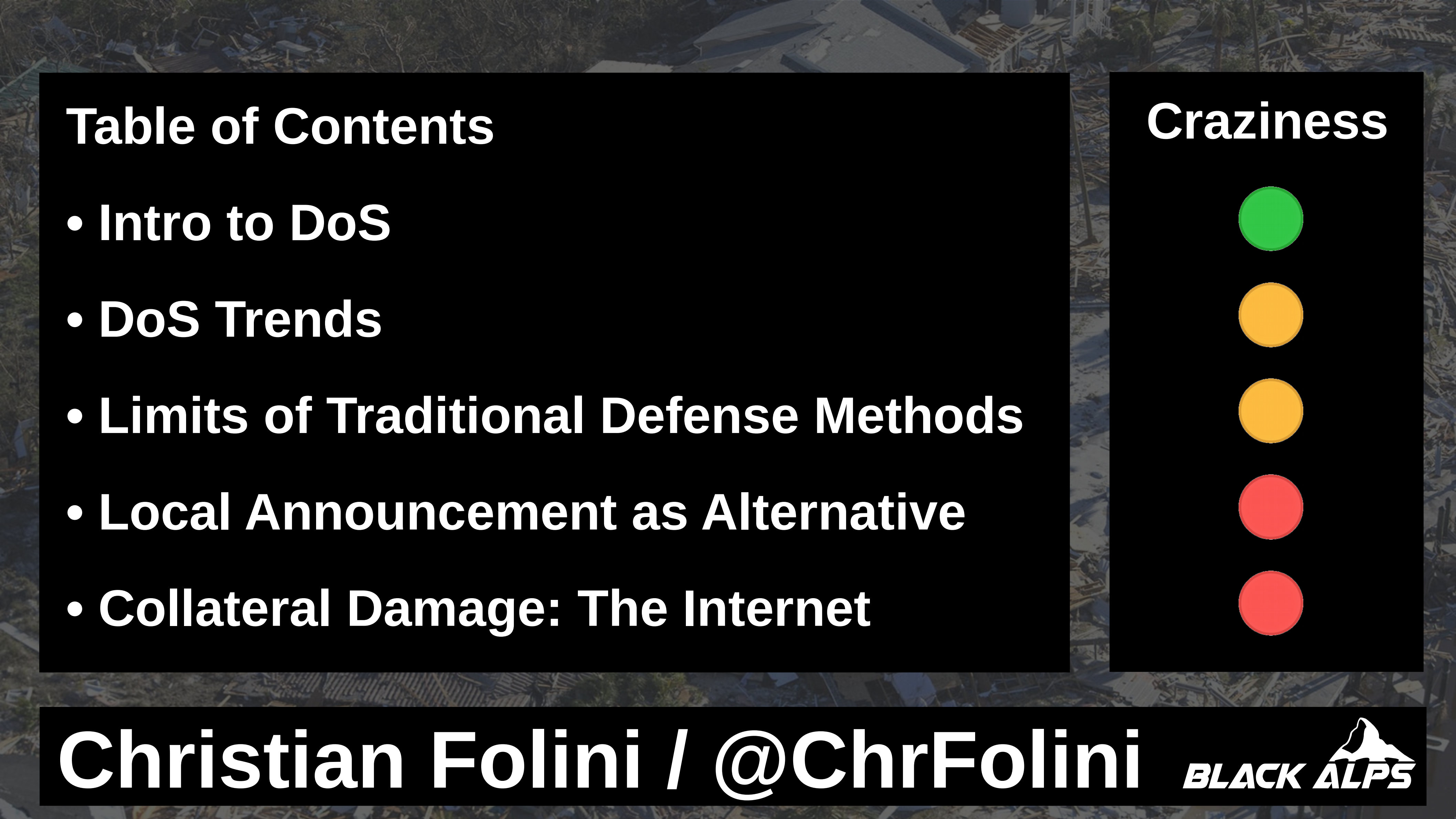
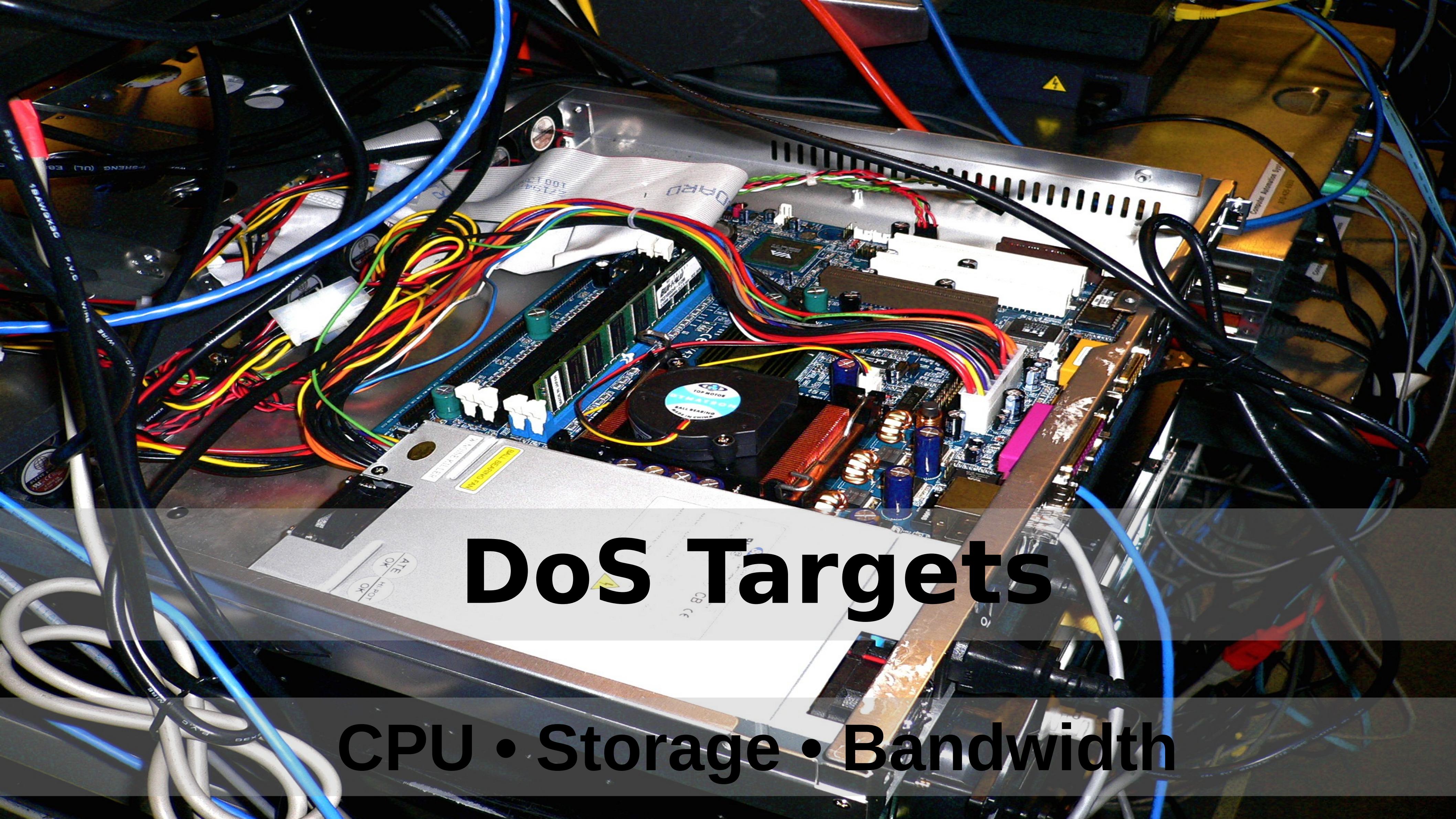


Table of Contents	Craziness
• Intro to DoS	🟢
• DoS Trends	🟠
• Limits of Traditional Defense Methods	🟠
• Local Announcement as Alternative	🔴
• Collateral Damage: The Internet	🔴

CIA

Confidentiality • Integrity • Availability

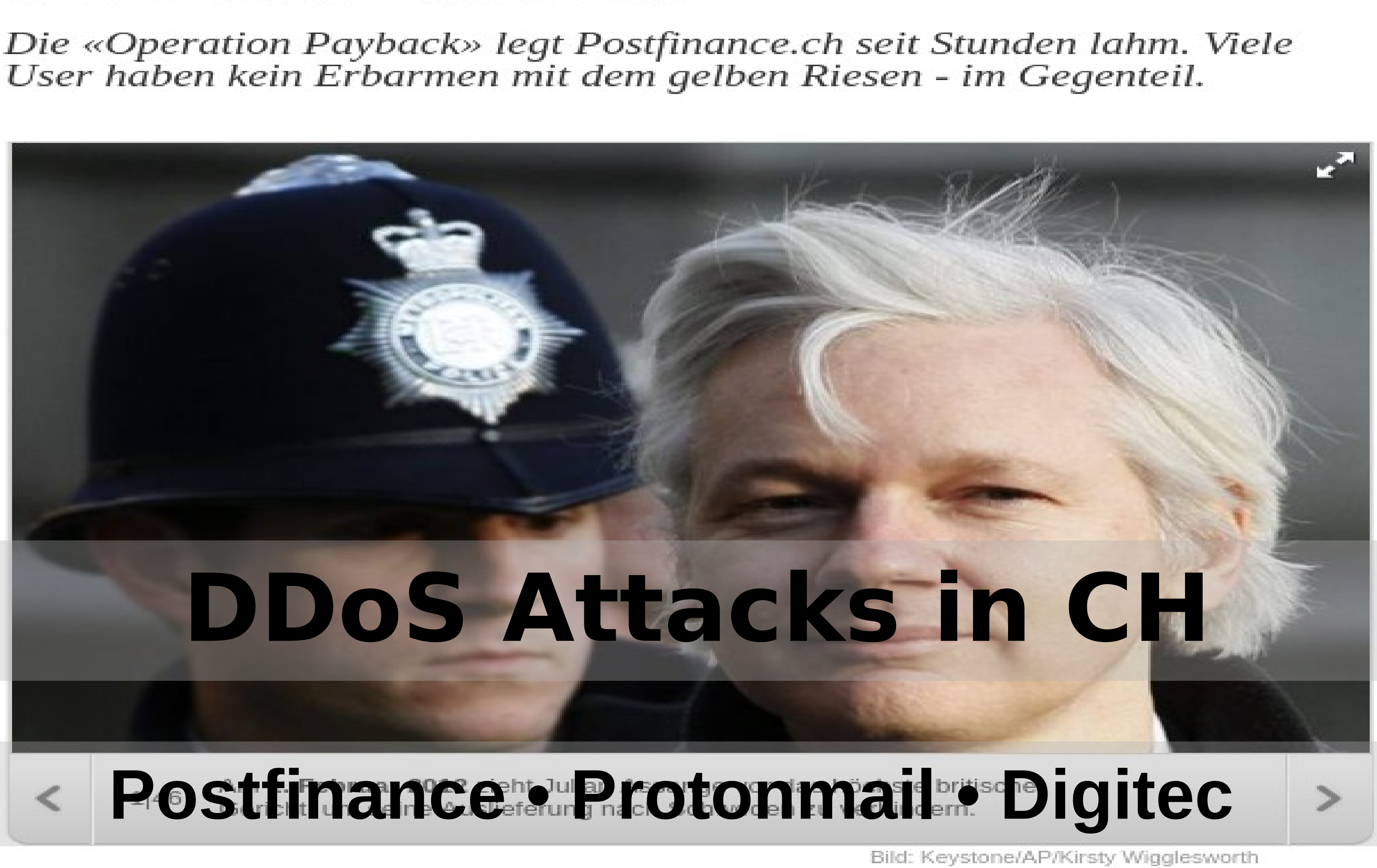


DoS Targets

CPU • Storage • Bandwidth

DDoS Attacks in CH

Postfinance • Protonmail • Digitec



Die «Operation Payback» legt Postfinance.ch seit Stunden lahm. Viele User haben kein Erbarmen mit dem gelben Riesen – im Gegenteil.

1/6 Am ... Februar 2012 zieht Julian Assange vor das höchste britische Gericht, um seine Auslieferung nach Schweden zu verhindern.

Bild: Keystone/AP/Kirsty Wigglesworth

GROWTH

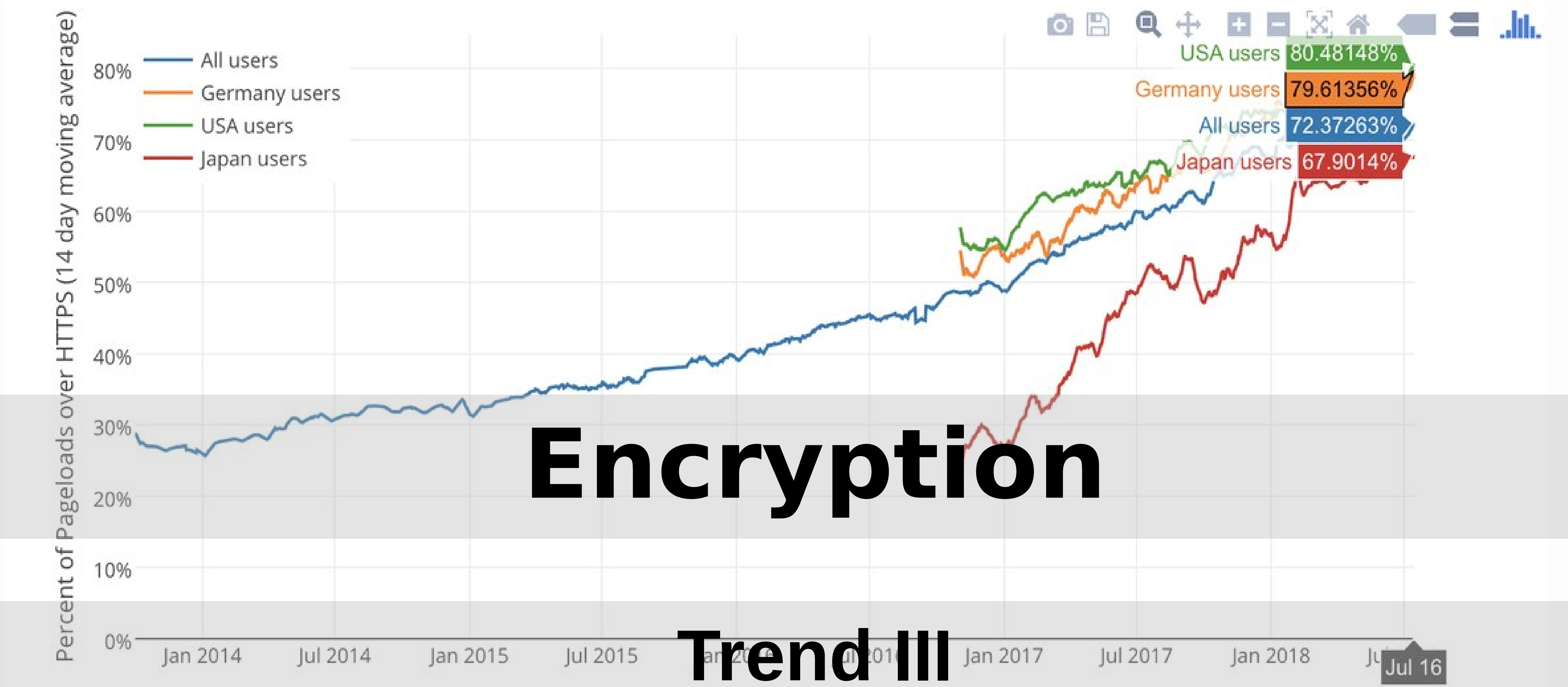
Trend I

Application Level DDoS

Trend II

Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)

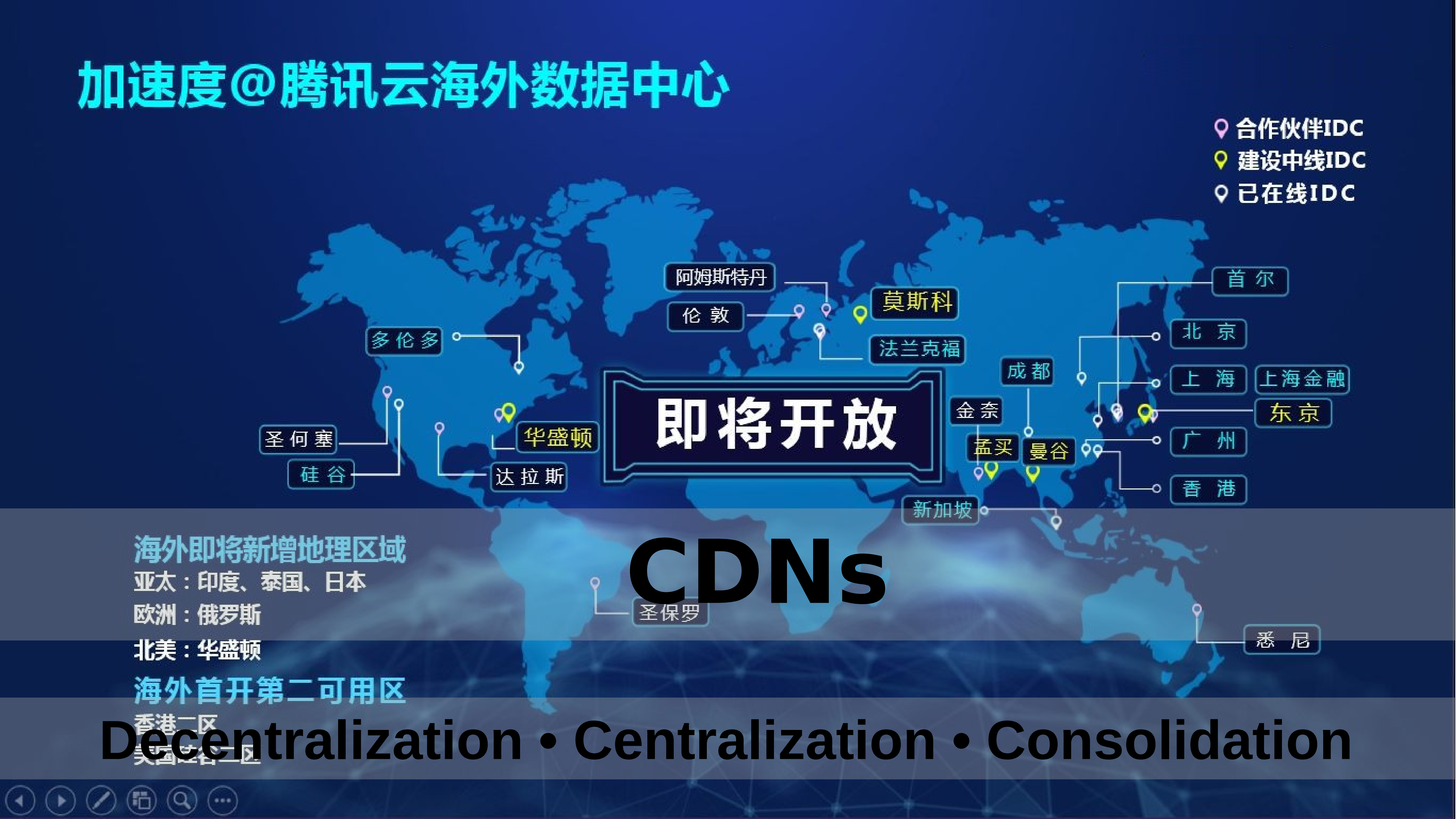


Encryption

Trend III

CDNs

Decentralization • Centralization • Consolidation



加速度@腾讯云海外数据中心

海外即将新增地理区域

亚太：印度、泰国、日本

欧洲：俄罗斯

北美：华盛顿

海外首开第二可用区

香港二区

美国硅谷二区

> “In a not-so-distant future, if we're not there already, it may be that if you're going to put content on the Internet you'll need to use a company with a giant network like Cloudflare, Google, Microsoft, Facebook, Amazon, or Alibaba.”
>
> Matthew Prince, CEO Cloudflare

> “Within 2-3 years, there will be only 2-3 players in the world that are able to withstand the biggest DDoS attacks and protect websites on a global scale.”
>
> Damian Menscher, Google,
> Usenix Enigma Conference, February 2017

“I think we are going to see a future where people will accept to pay money in extortion. It will be part of the costs of doing business. As an alternative, there will be a handful of expensive services that can protect you from DDoS attacks and these services effectively control what new startups will be allowed to operate on the internet.”

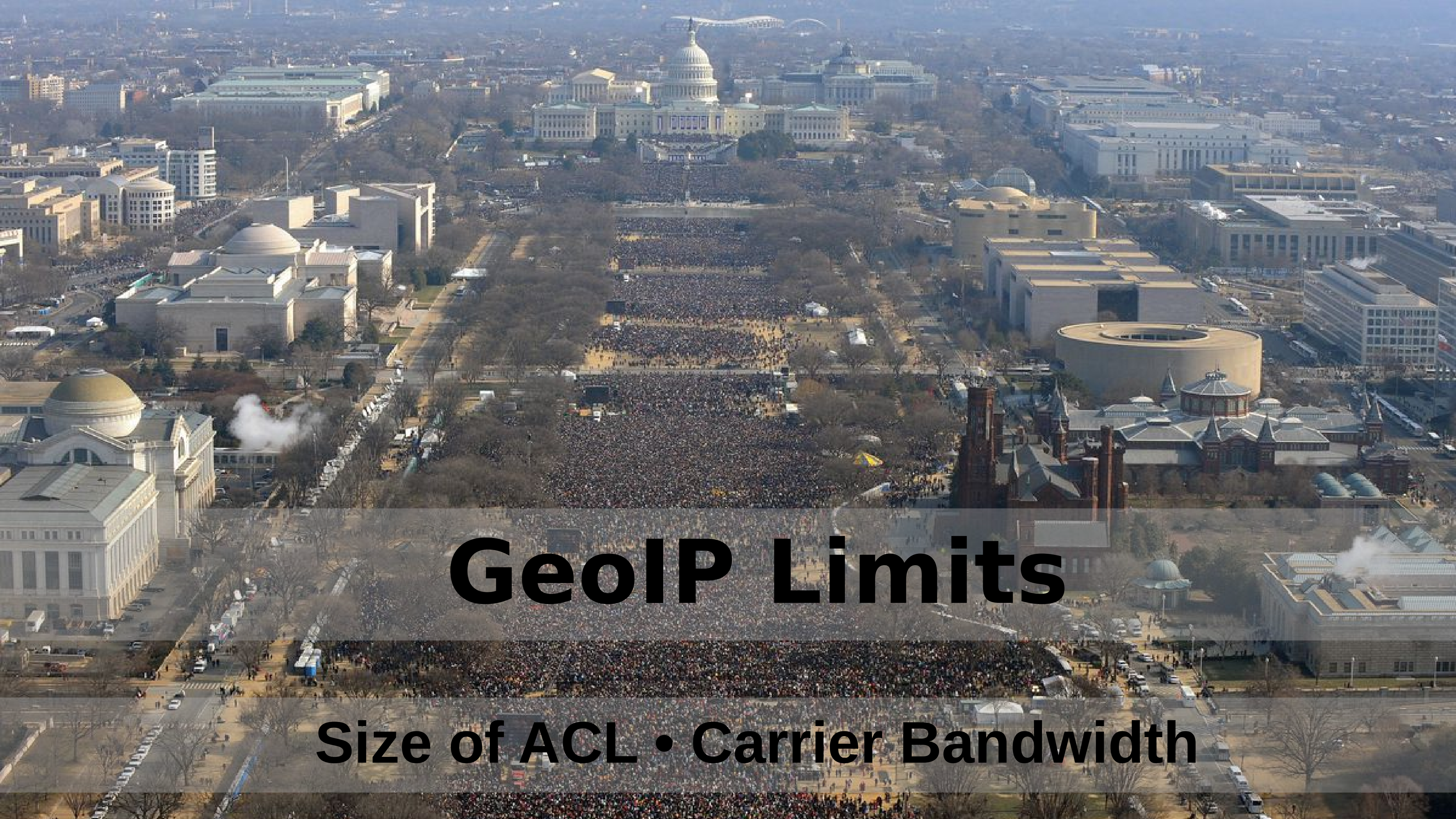
Dr. Paul Vixie, April 2017 in Zurich

CDN Limits

Integration • Directories • Encryption Keys

GeoIP

Local Userbase • ACL • Control

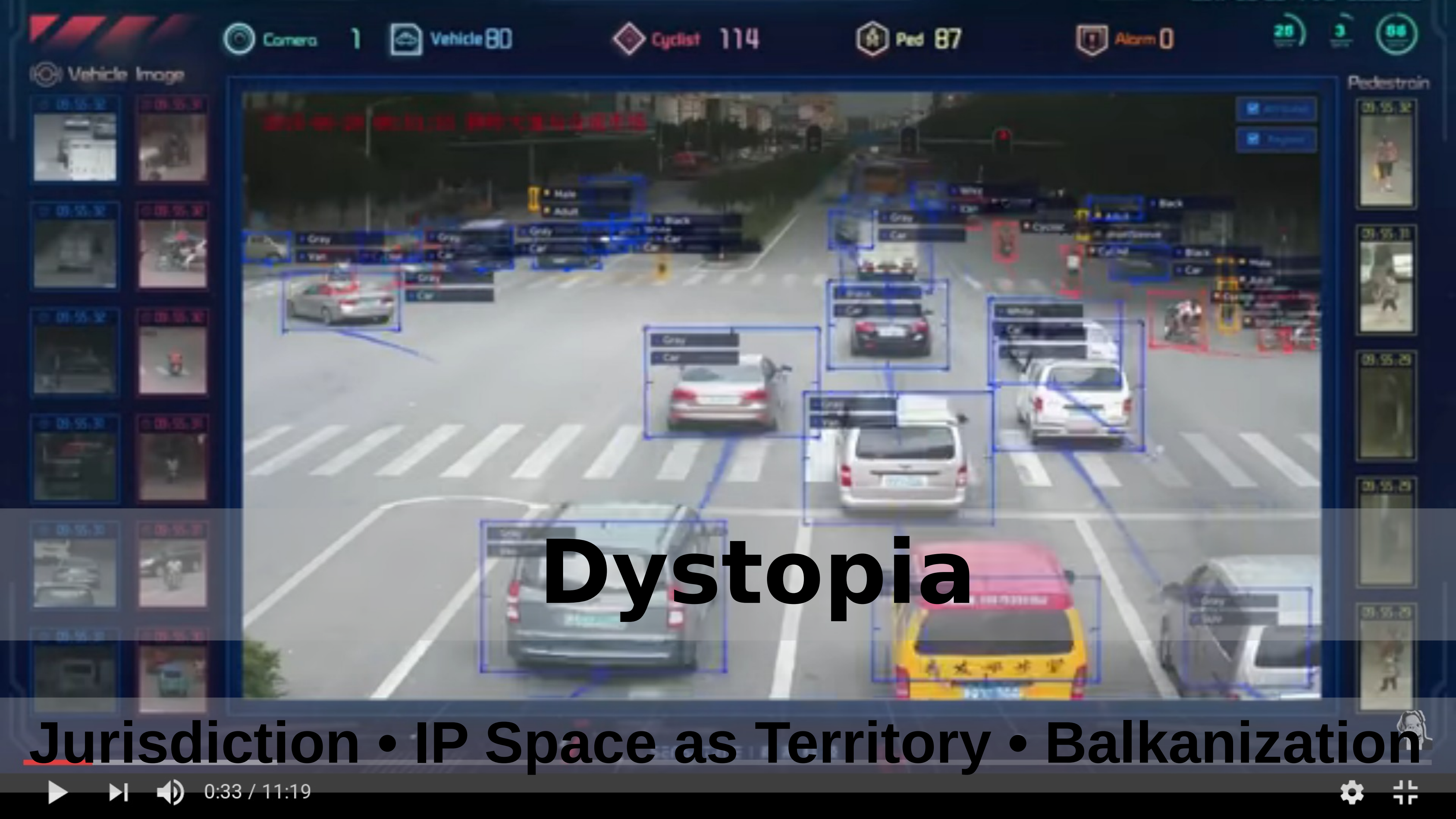


GeoIP Limits

Size of ACL • Carrier Bandwidth

Local Route Announcement

BGP • Peering • No Route Export



Dystopia

Jurisdiction • IP Space as Territory • Balkanization

Summary

- Trend I: DDoS Attacks Are Getting Bigger All The Time
- Trend II: More and More Attacks are Application Level DDoS
- Trend III: Widspread Use of Encryption Make Defense Harder
- CDNs Are Here To Help And They Rule The Internet
- Limiting BGP Route Announc. Can Guarantee Ultimate GeoIP
- States May Fail To Protect Traffic Outside Their Jurisdictions

Christian Folini / @ChrFolini

BLACK ALPS

Sources for Slides (Mostly CC)

- https://www.flickr.com/photos/nirak/29124106183
- https://www.flickr.com/photos/timdorr/63630545
- https://www.flickr.com/photos/the_ewan/3772847639
- https://www.flickr.com/photos/3336/
- https://www.flickr.com/photos/barsen/5484256163/
- https://twitter.com/letsencrypt/status/1020058447922978816
- https://www.yicaiglobal.com/news/tencent-cloud-puts-its-seoul-data-center-online
- https://www.youtube.com/watch?v=aE1kA0Jy0Xg
- https://alt929boston.com/2017/12/07/canadian-postal-worker-laughing-driving-recklessly/
- https://blog.cloudflare.com/why-we-terminated-daily-stormer/

Thank you for attending my talk

- christian.folini@netnea.com
- @ChrFolini
- https://christian-folini.ch

Christian Folini / @ChrFolini

BLACK ALPS