How Sweden is taking the lead in time-as-a-service delivery

Karin Ahl, CEO, Netnod

National distribution of Swedish time

- Reasons and requirements for a national time distribution network
- Infrastructure we use to ensure security, accuracy and redundancy
- How we provide time-as-a-service
- Network Time Security (NTS)
- Main players: PTS, RISE and Netnod

We always know what time it is

The reasons and requirements for a national time distribution network

Why a national time distribution system?

- Citizens and critical community services are dependent on the availability of electronic communications
- Electronic communications have a dependency on correct time and frequency
- Time and frequency distributed by GNSS can be easily spoofed or interrupted

Given these factors we identified a public need which was not delivered by the market

GNSS - good, cheap but easily compromised

GPS - GLONASS - Galileo - BeiDou

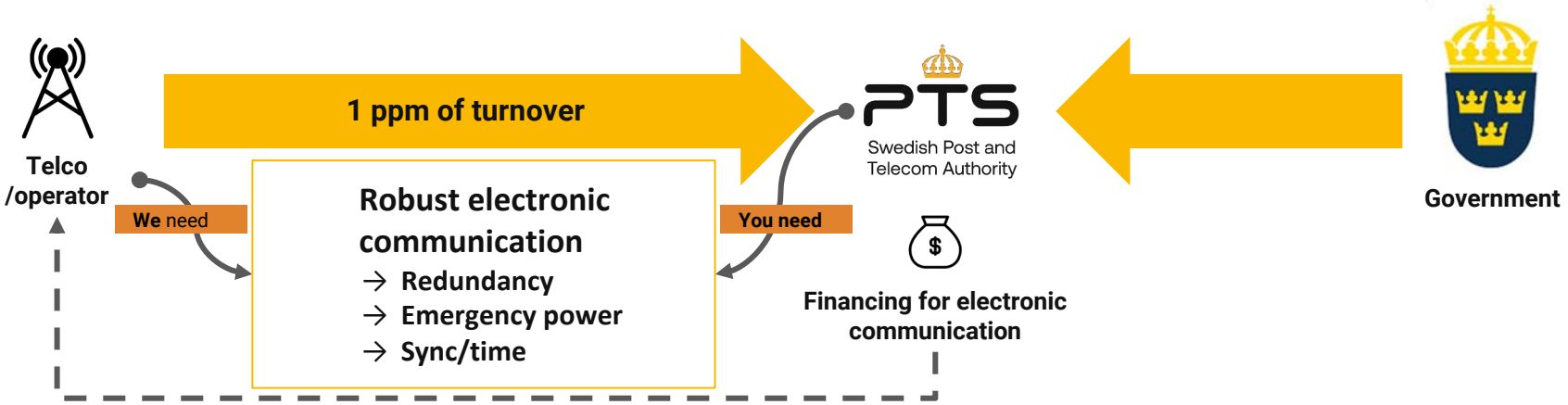
- Common even in critical infrastructure
- Easy to disrupt with cheap equipment (jamming)
- Easy to “fake the time” (spoofing)
- Not available all the time:
  - signal interference
  - outdated equipment and infrastructure problems
  - sabotage - “not peacetime”

€10 GNSS receiver
€250 software based radio that can be used to manipulate the receiver

A national time distribution system

- A system without GNSS dependency which, from a national perspective, can guarantee robust and secure time
- The system must be robust and available throughout the country
- The services delivered from the system must be affordable for operators of networks so that the price is not a barrier for use of the services
- The government must have visibility and direct input regarding the infrastructure, which means it must be located in, and operated from, Sweden

Robust financing



NET NOD

We always know what time it is

Outline of infrastructure

Netnod’s clock nodes – accurate and secure time

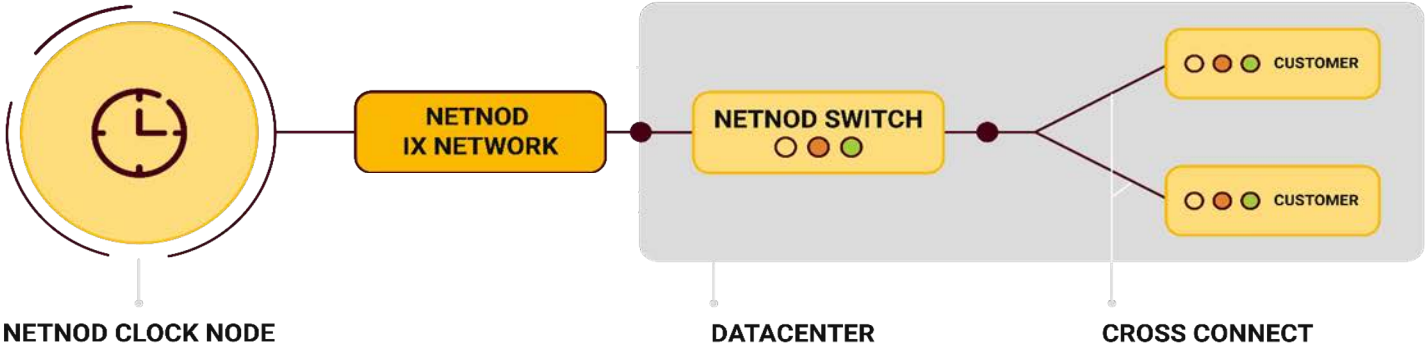
- Dual nodes with all critical equipment duplicated for redundancy (2x caesium clocks)
- Dedicated battery backup for all time components
- NTP/NTS servers use a custom-built FPGA-based hardware implementation

Swedish distributed time service

- 6 time nodes placed in secure bunkers throughout Sweden (Stratum-1 time servers)
- Time traceable to UTC
- Free and commercial service with SLA
- Operated by Netnod, monitored by RISE and financed by PTS

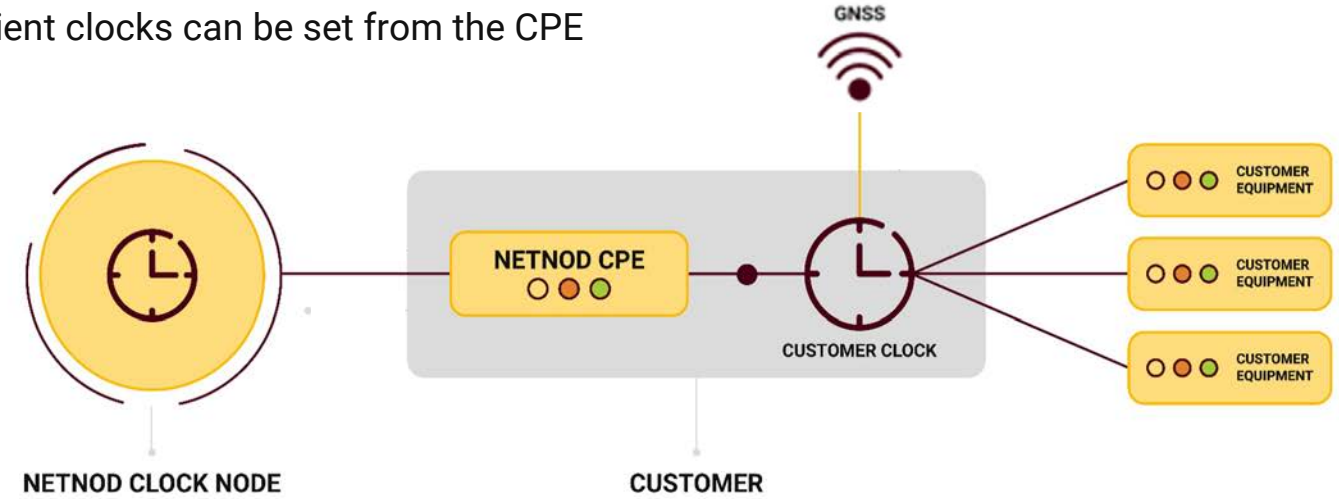
Direct delivery model - time-as-a-service

- A fully managed time service with SLA that guarantees 30µs accuracy from UTC
- Delivered over separate VLAN at IX port or dedicated port



Remote delivery model - time-as-a-service

- Fibre connection from Netnod's central clock nodes to locally placed equipment (CPE) provided by Netnod
- The CPE's clock is set by Netnod's central clocks
- The CPE delivers high precision, stable time: within 1ms of UTC guaranteed by SLA
- Client clocks can be set from the CPE



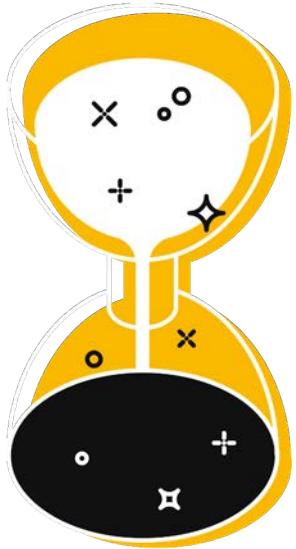
NET NOD

We always know what time it is

Network Time Security

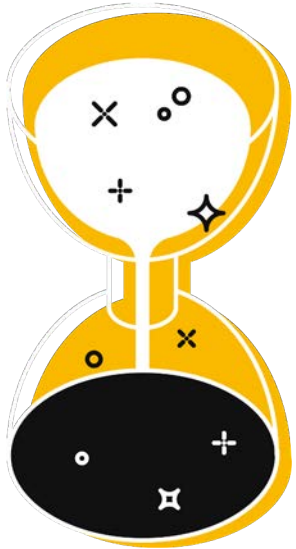
NTP is vulnerable

- No security
  - Plain text, vulnerable to man-in-the-middle attacks
  - Time is important
    - TLS, HTTPS, SMTPS, IMAPS, POP3S
    - DNSSEC
    - Timestamps on logs and transactions
- Actually: no scalable security
  - Authentication using a shared secret and MD5/SHA1
    - Limited number of shared keys (16 bits)
    - Key distribution is hard
  - Autokey never caught on

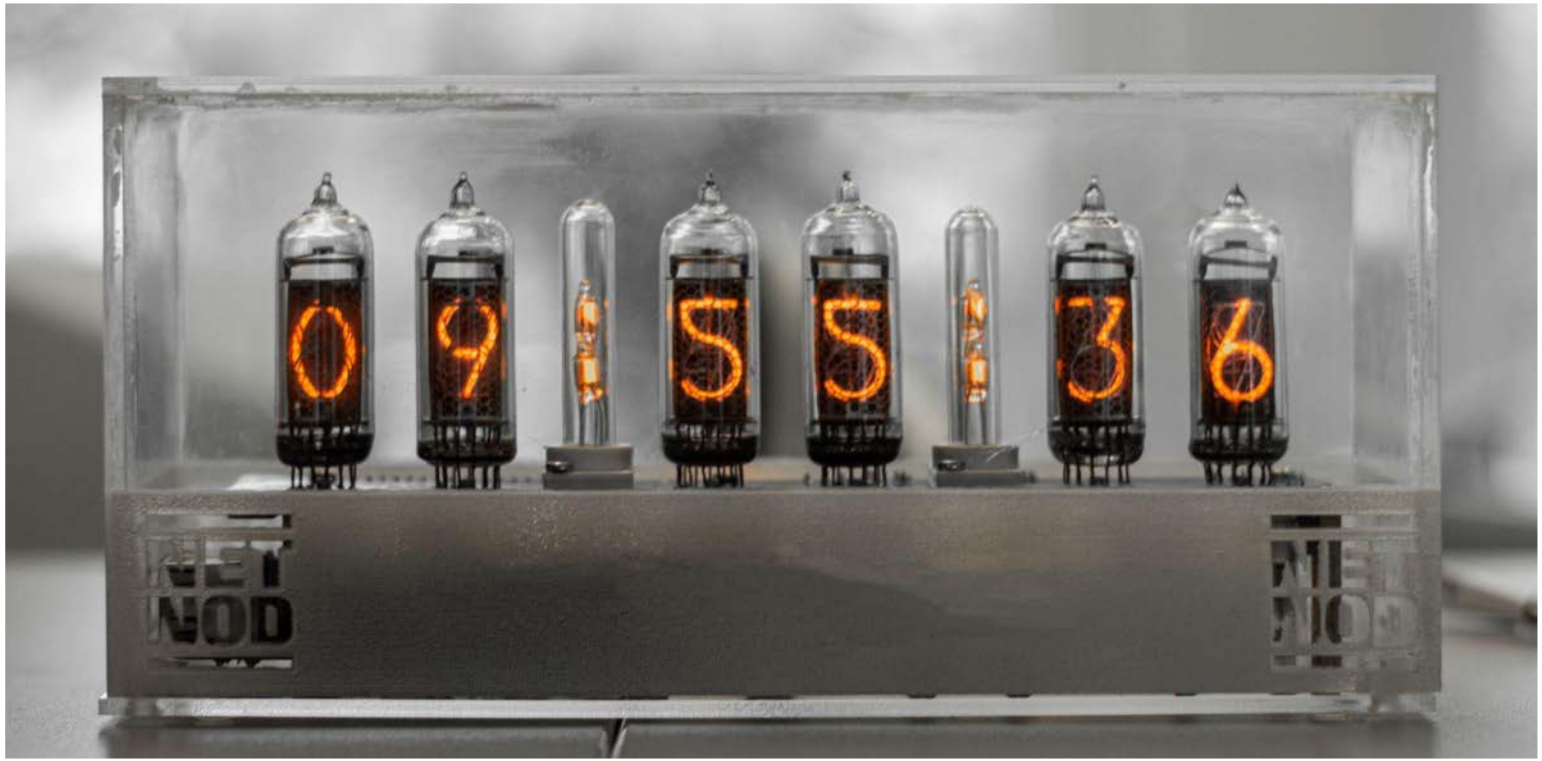


What is NTS?

- NTP with security
  - Adds authentication and encryption to NTP
  - Scales to an unlimited number of clients
  - Netnod got involved as co-authors in IETF draft process during 2018
  - Published as RFC 8915 in September 2020



nts.netnod.se

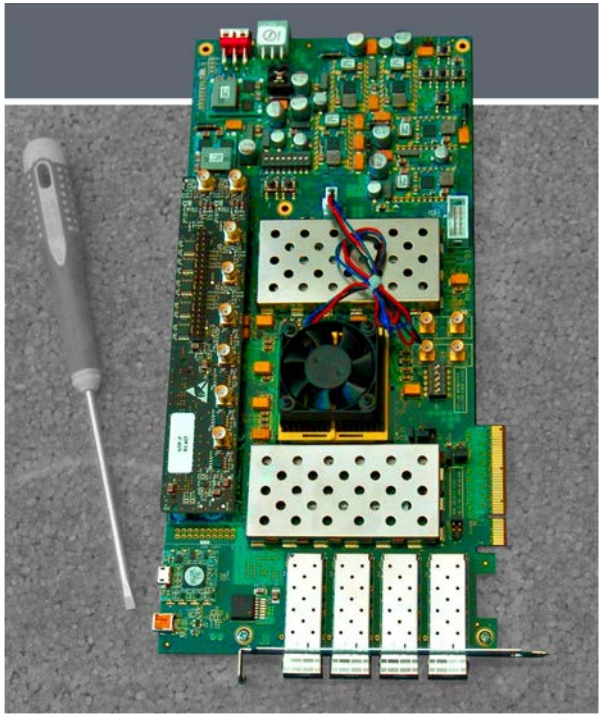


NTS sites

- We operate 6 nodes with Stratum-1 NTS servers
  - Luleå
  - Sundsvall
  - Stockholm x2
  - Gothenburg
  - Malmö/Copenhagen

Hardware NTP server in FPGA

- Public Internet service
- 4 x 10 Gb/s full wire speed
- IPv4 and IPv6
- Secure - NTP traffic stays in the FPGA
- Standard FPGA board, with custom interface for time input and output (1 PPS & 10 MHz)
- Open source FPGA code



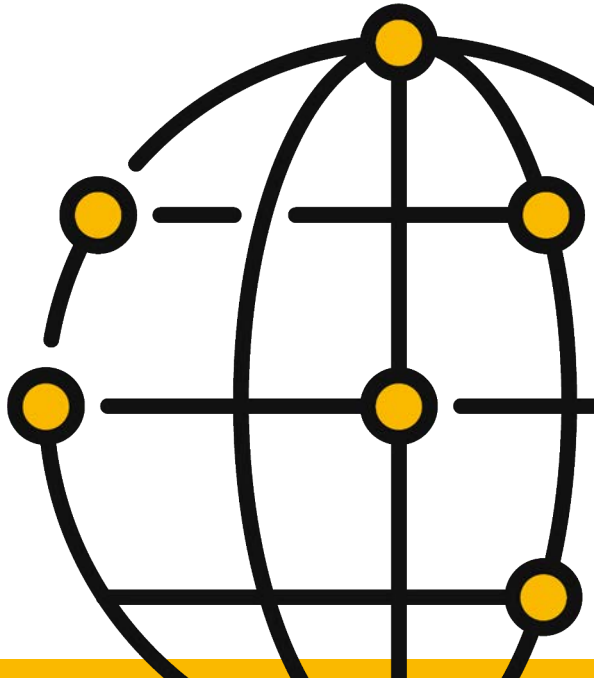
Hardware NTP with NTS server in FPGA

- NTP with Network Time Security
- RFC 8915
- Public Internet service
- Our implementation runs in a commercial vendor’s box (white box), many other variants possible
- Open source FPGA code

How to connect to NTS

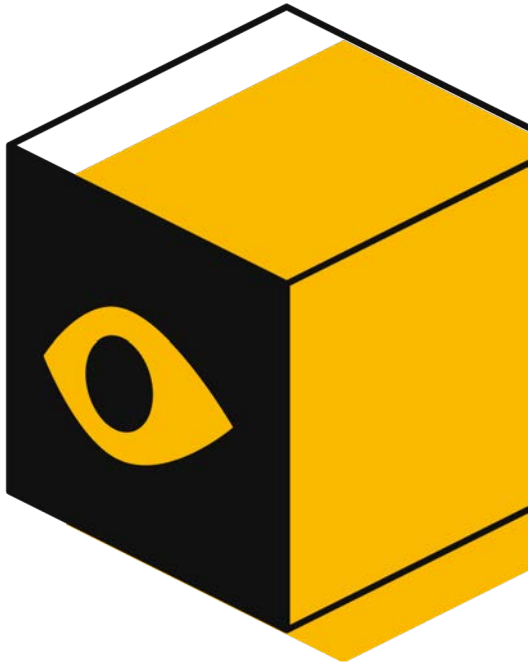
- Most LINUX distributions allow you to run Chrony or NTPsec which supports NTS
- Install Chrony/NTPsec or similar as NTP client
- Configure NTS [point at Netnod's NTS servers]
- Verify

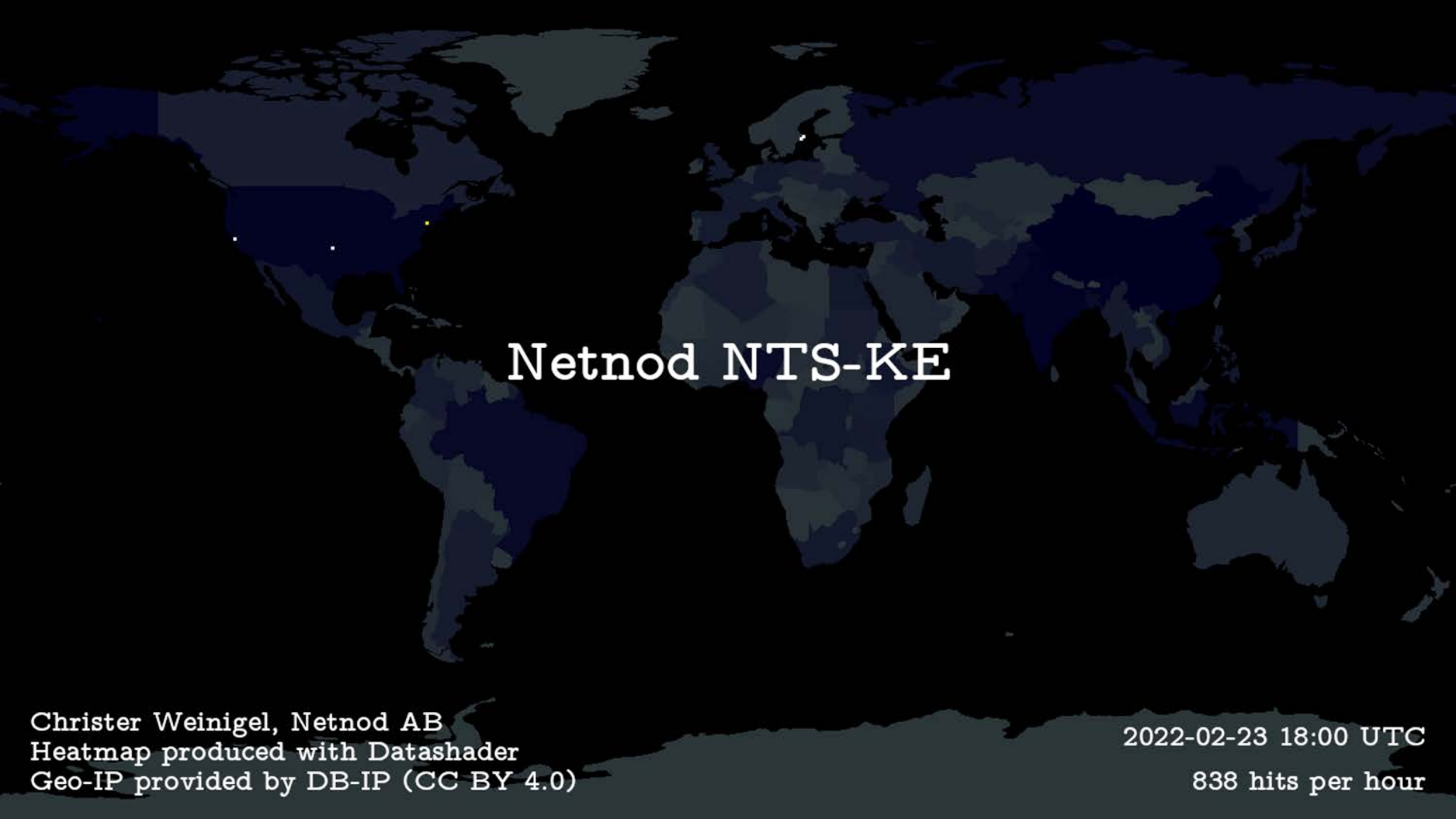
Full how to available here: https://www.netnod.se/netnod-time/how-to-use-nts

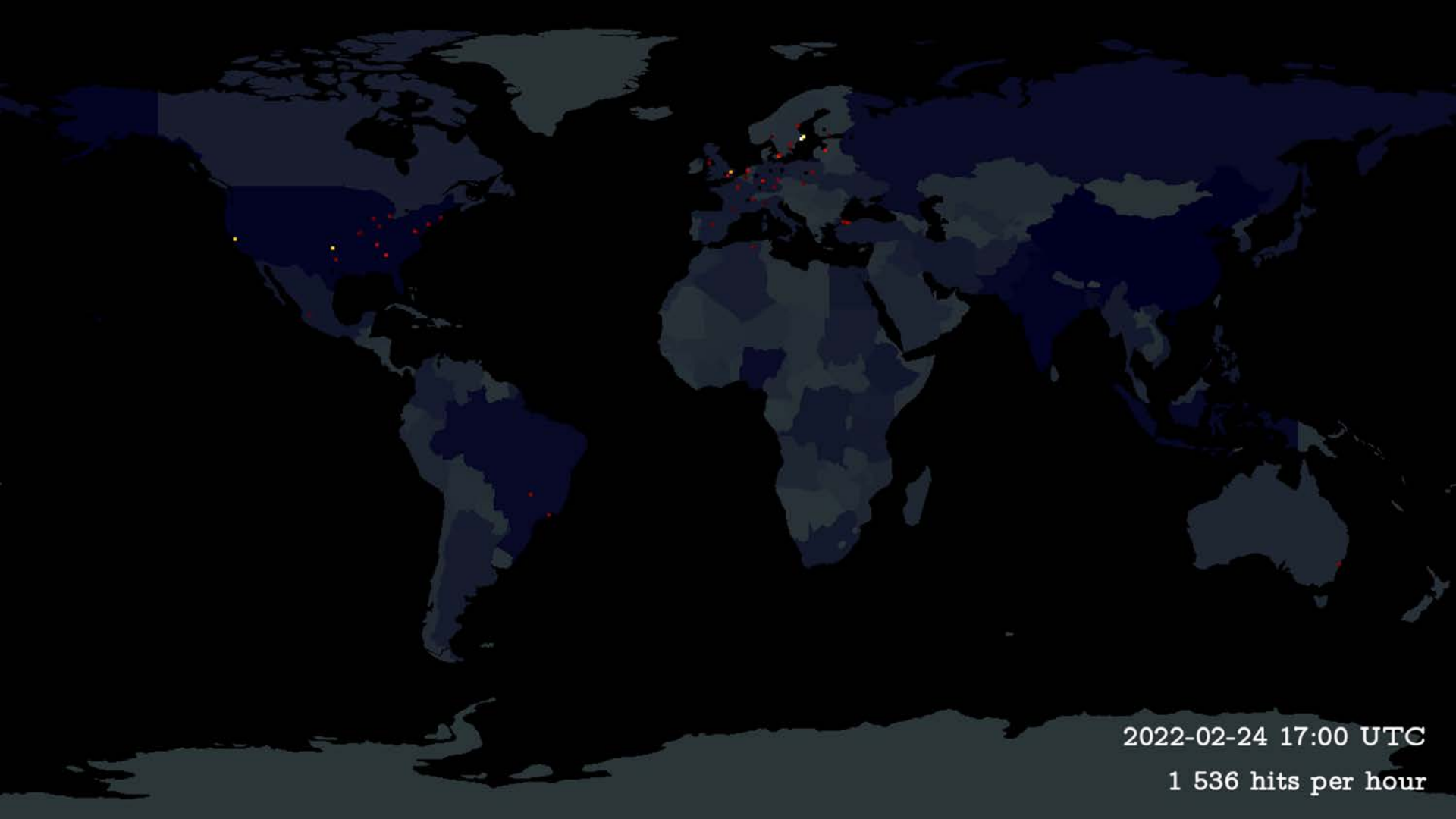


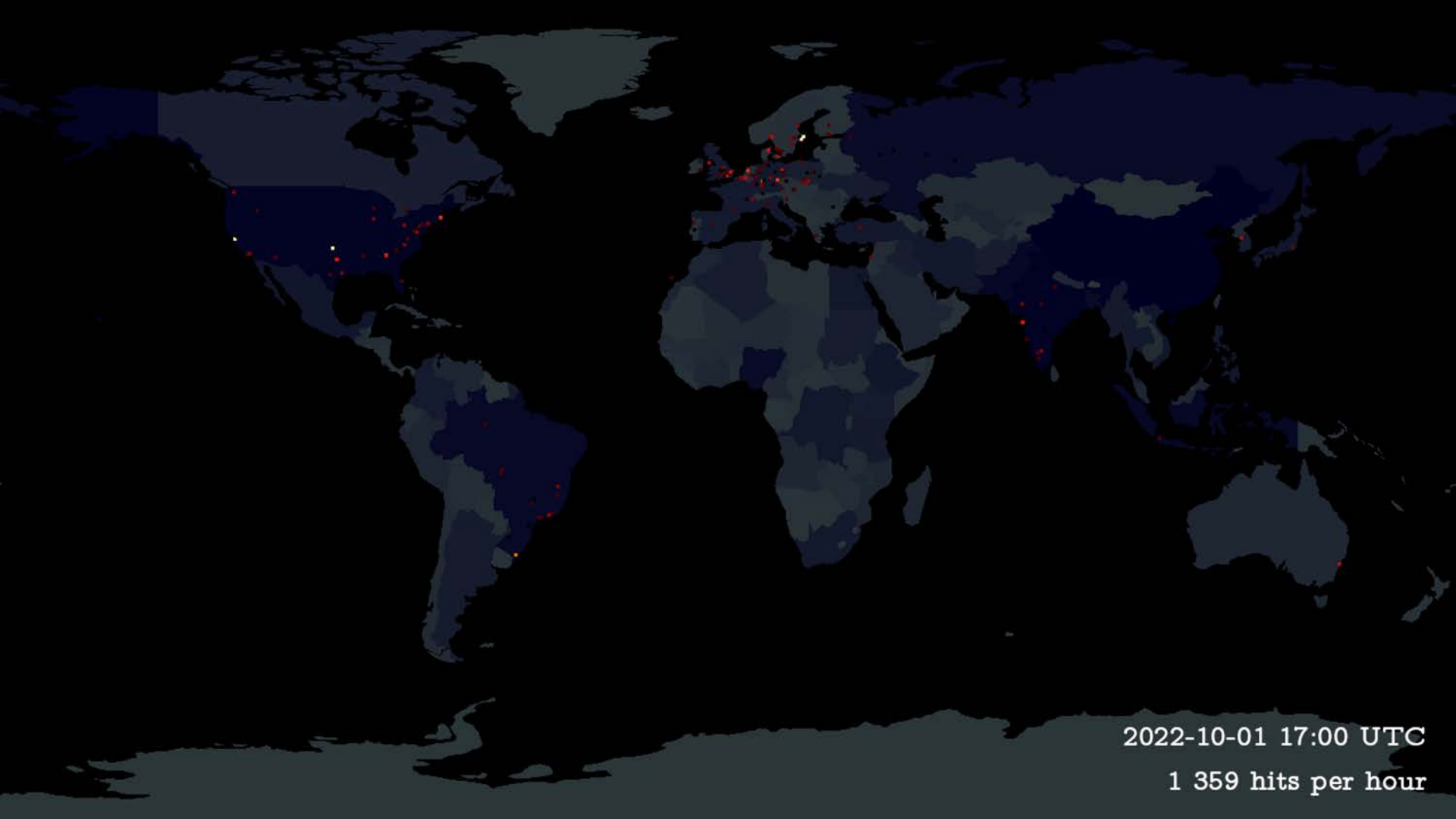
Conclusions

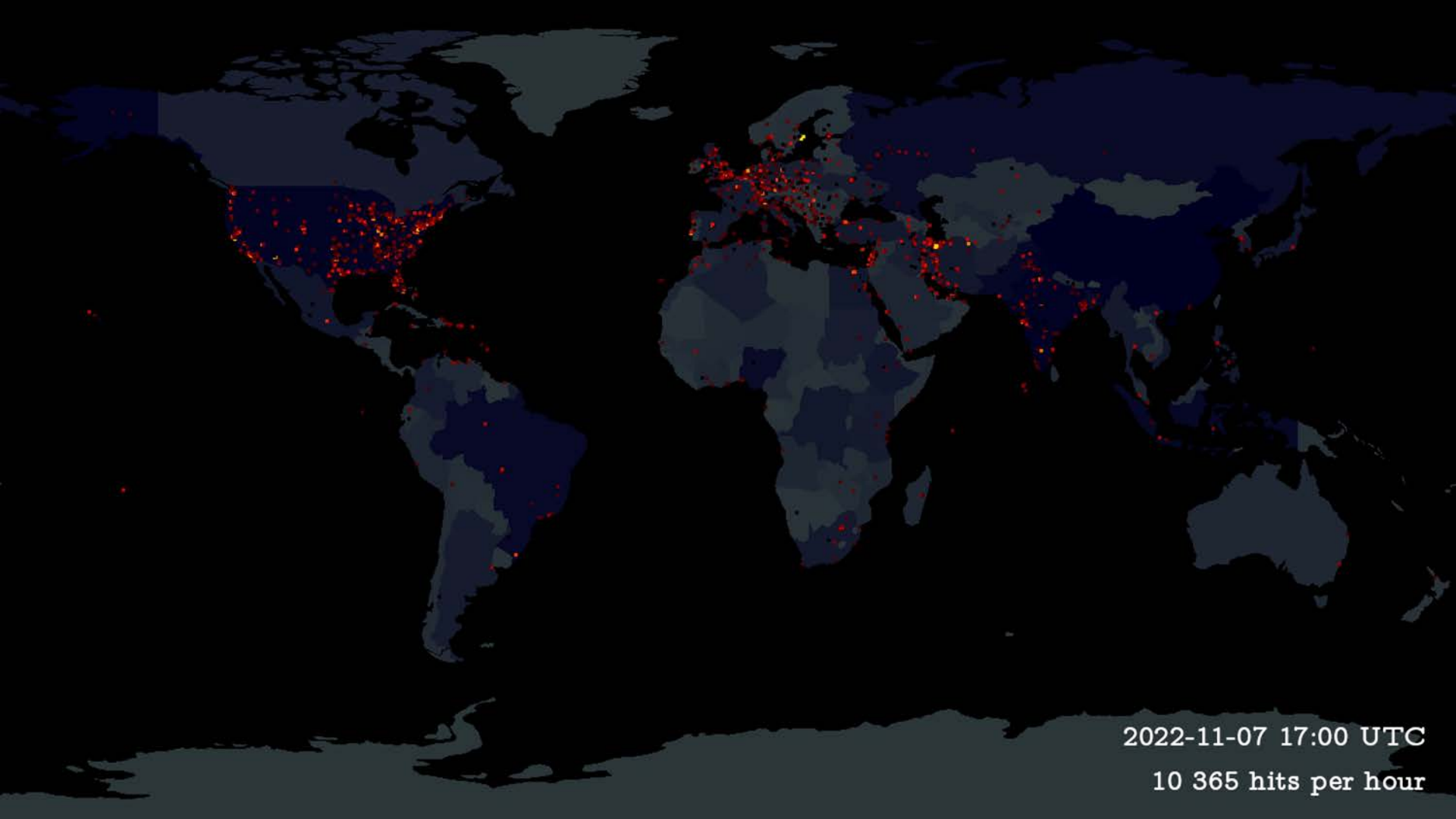
- Developing a national time distribution service is hard!
  - High-level of expertise
  - Investment
  - Cooperation
- Private public cooperation has been a huge success factor
- The customer doesn’t always know what they need
- Time distribution requirements/technologies are changing (upcoming challenge: time for IoT devices)
- Use NTS!

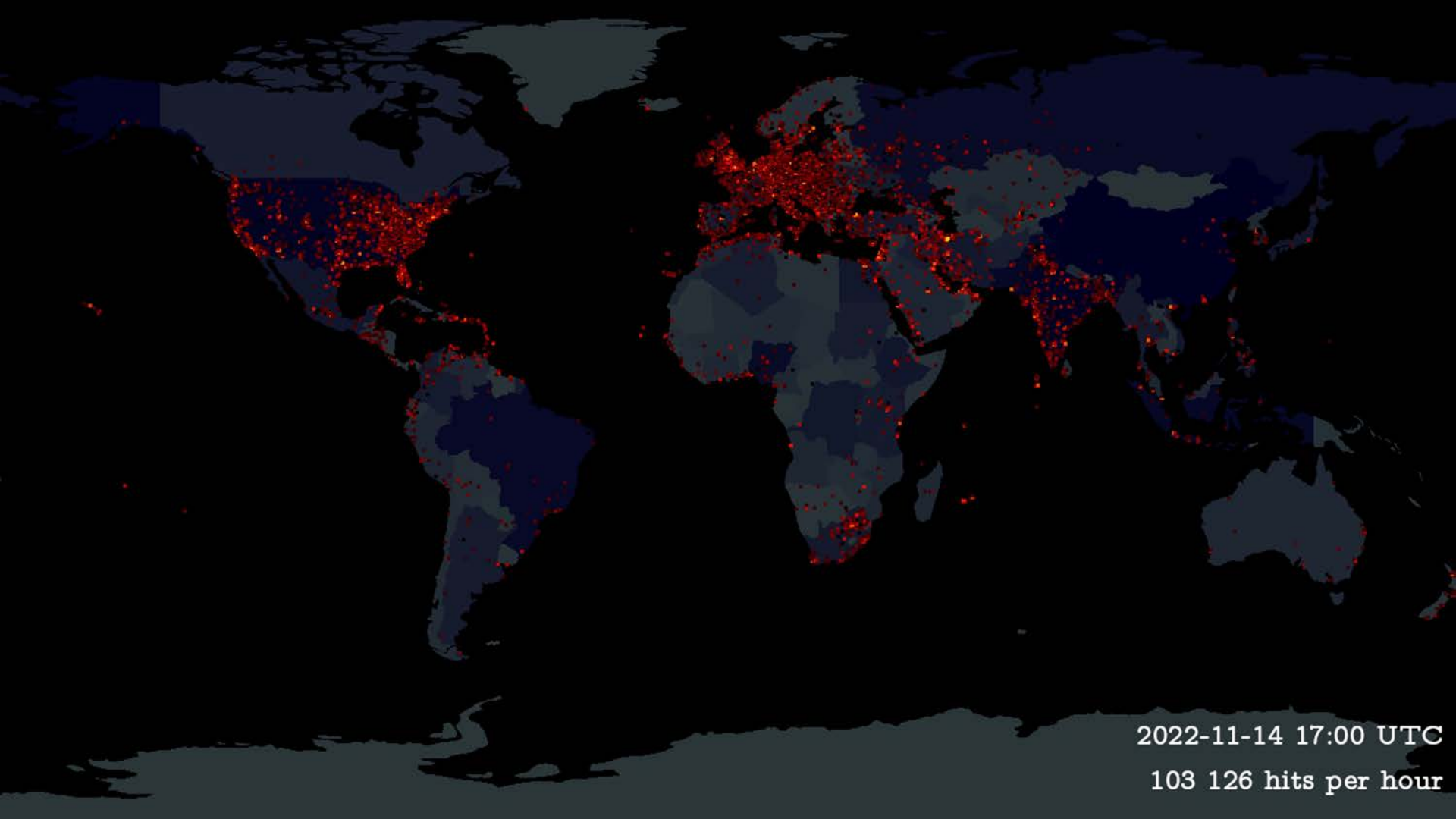


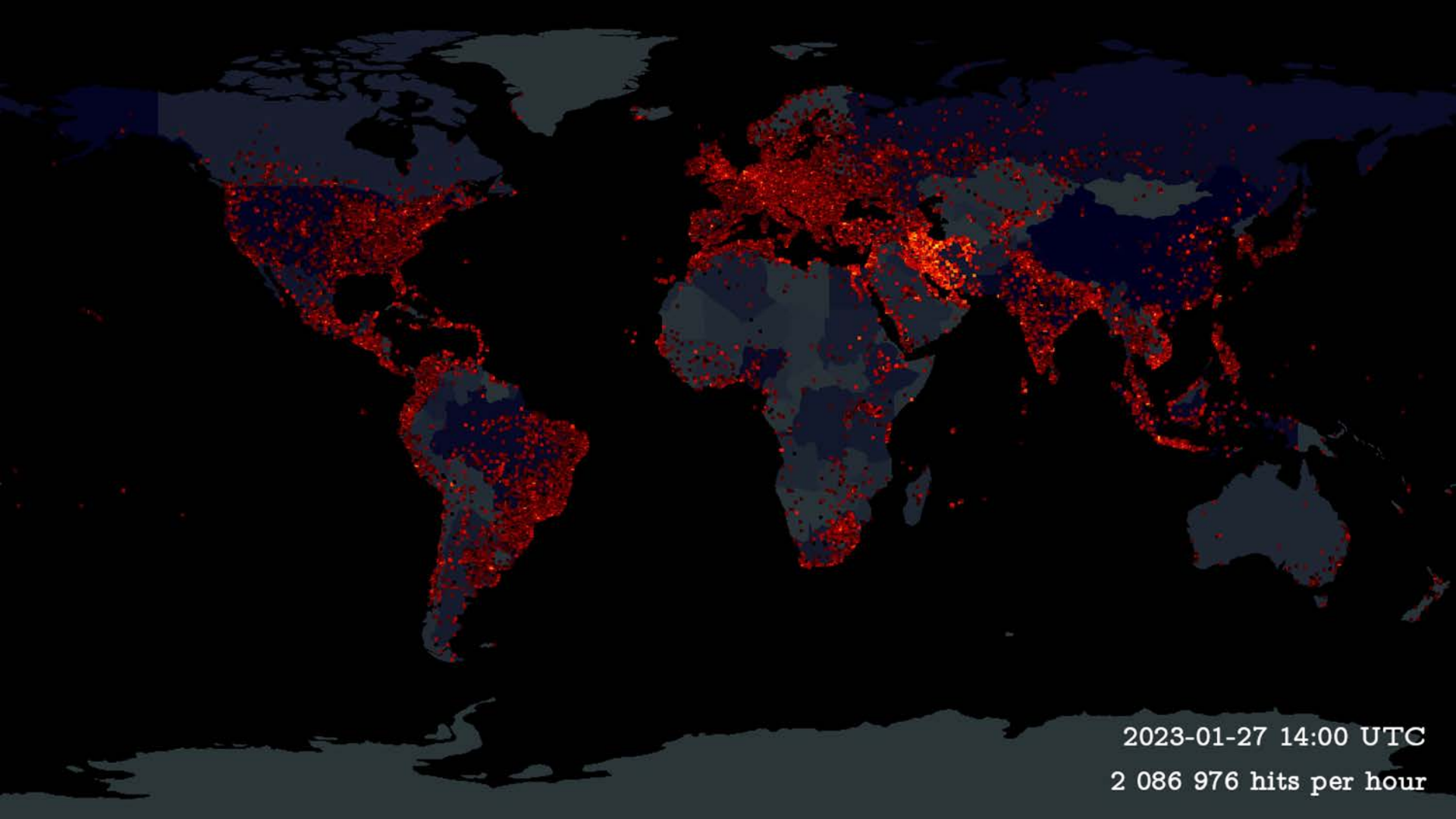

Netnod NTS-KE
Christer Weinigel, Netnod AB
Heatmap produced with Datashader
Geo-IP provided by DB-IP (CC BY 4.0)
2022-02-23 18:00 UTC
838 hits per hour


2022-02-24 17:00 UTC
1 536 hits per hour


2022-10-01 17:00 UTC
1 359 hits per hour

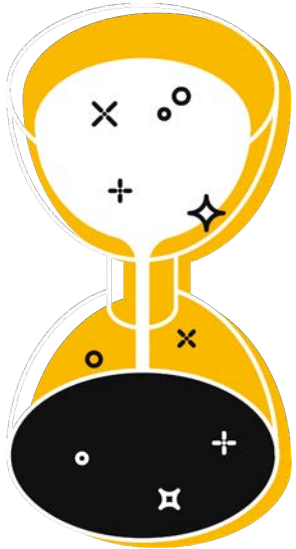

2022-11-07 17:00 UTC
10 365 hits per hour


2022-11-14 17:00 UTC
103 126 hits per hour


2023-01-27 14:00 UTC
2 086 976 hits per hour

Timeline

- New servers in Stockholm
  - February 2022, 1 000-2 000 hits per hour, only enthusiasts
- Nothing happened for 8 months
  - Mid October, usage started to rise slowly
- During November usage exploded
  - November 7, 10 000 hits per hour
  - November 14, 100 000 hits per hour
- Usage kept rising until January
  - Mid January, 1 000 000 hits per hour
  - End of January, 2 000 000 hits per hour
- Thousandfold increase in traffic in less than three months
- At least 5 million unique IP addresses



Thanks for listening!

netnod.se