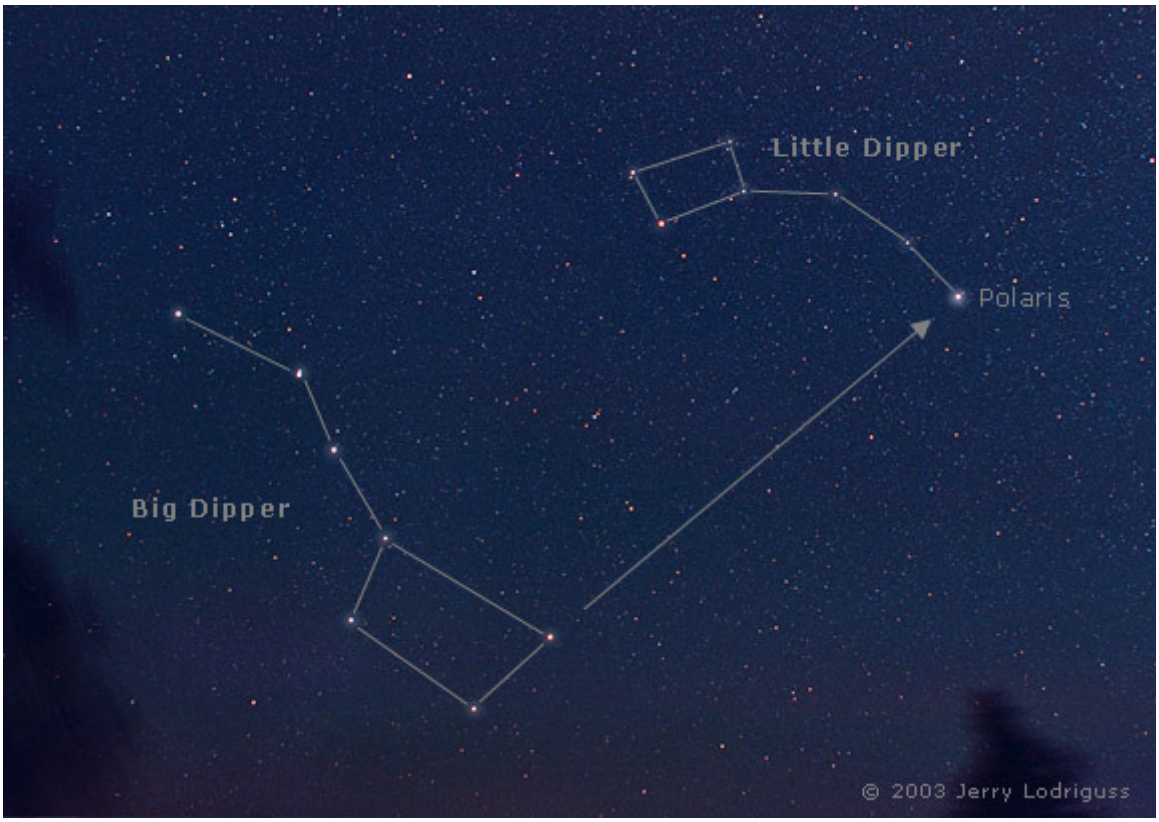
STELLA POLARIS NETWORK



Introduction: yesterday's hybrid war preparation

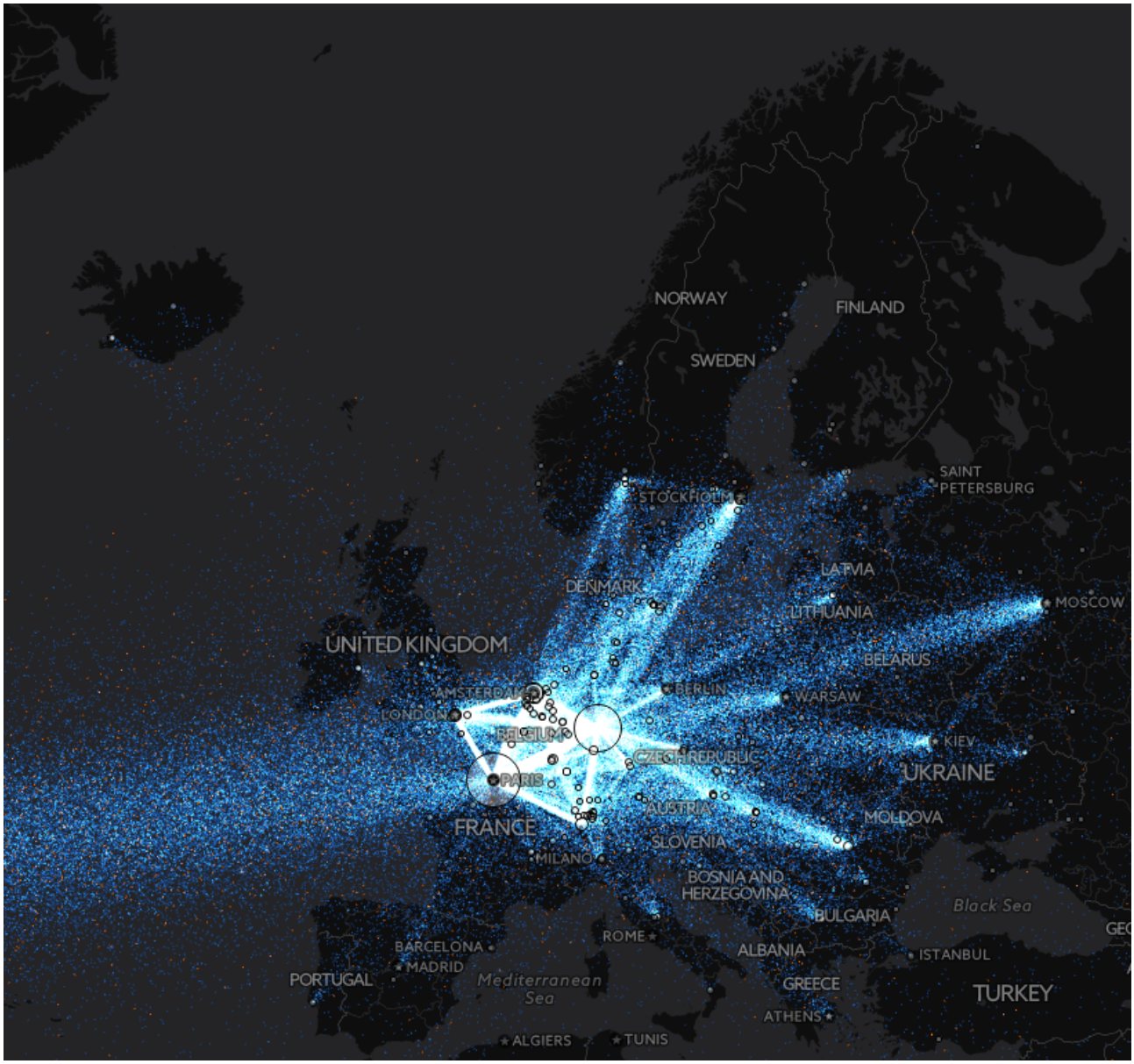
STELLA POLARIS IS A STAR

North Star is the prominent star that lies closest in the sky to the north celestial pole, and which appears (approximately) directly overhead to an observer at the Earth's North Pole. It is consequently known as Polaris (from Latin stella polaris "pole star").

ALSO, STELLA POLARIS WAS A COVER OPERATION

Operation Stella Polaris was the cover name for activity in which Finnish signals intelligence records, equipment and personnel were transported into Sweden after the ending of the Continuation War in 1944 so that the signals intelligence activities could continue in Sweden and the equipment would not end up in the hands of the Soviet Union. The threat of Soviet occupation was considered too likely and an operation was formed to support guerrilla warfare in Finland after occupation.

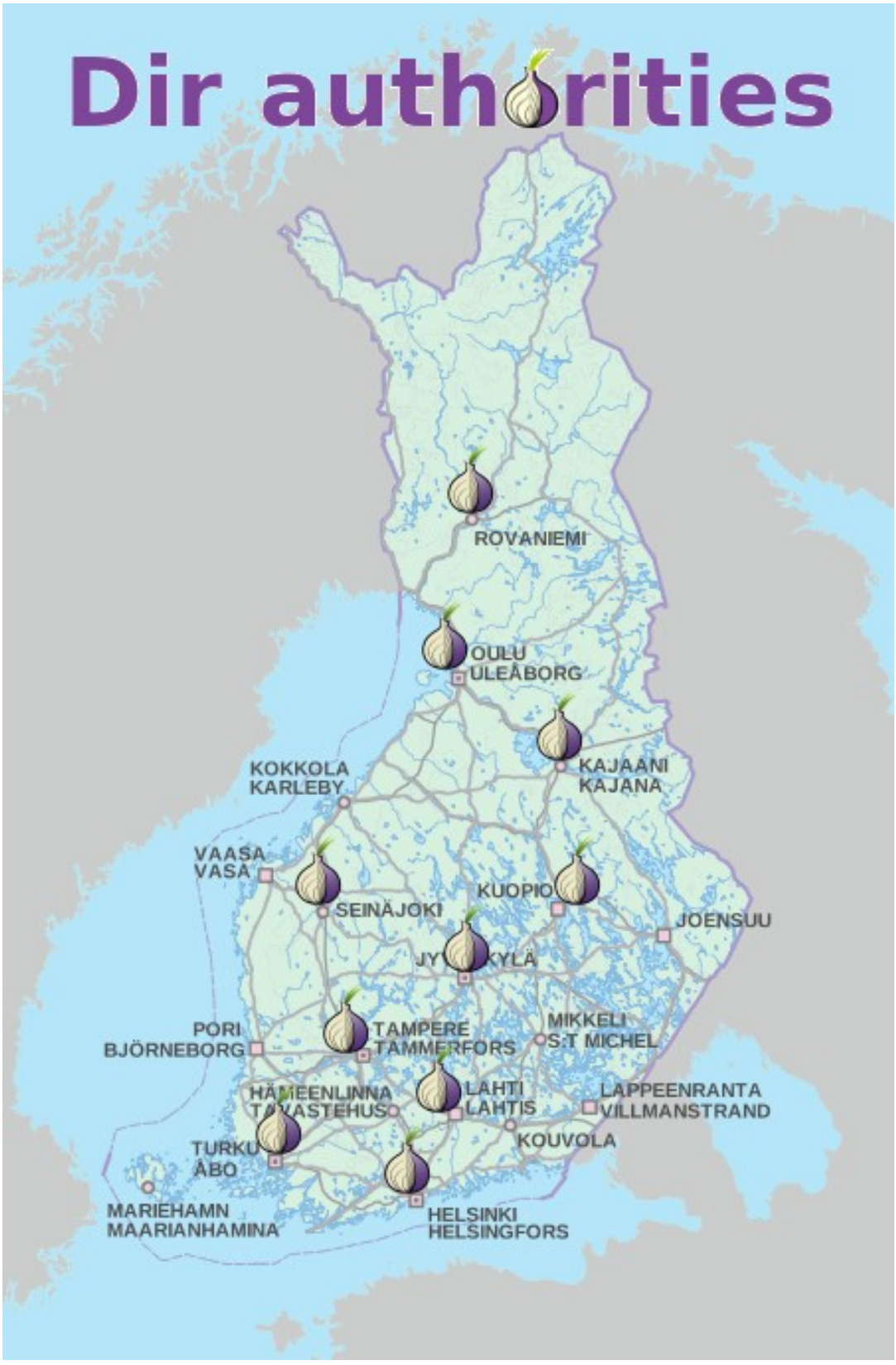
Background: The Tor network currently



- Global resilient p2p network, end-to-end crypto, anonymous TCP
- Voluntary people have installed relays, only 50 relays in Finland: Half of the bandwidth capability operated by Juha Nurmi!
- No current test cases or plans to survive netsplit situations
- Tor has default hard-coded directory authorities
- These servers are the weakest centralized links of the network

Stella polaris network: Finnish Private Tor network

- State wide private Tor network, operates independently
- 10 distributed main relays, so called directory authority servers



Stella polaris network: Finnish Private Tor network

- 10 dirAuthories
- A few middle relays
- Few exit relays, Juha Nurmi can operate them :)
- DNS cache
- Client users
- Onion services
- Own search engine for the content, Juha Nurmi can build it :)
- Transparent HTTP proxy mirroring of important public web sites
  - 234.onion → mpk.fi
  - abc.onion → suomi.fi
  - xyz.onion → eduskunta.fi
  - 567.onion → puolustusvoimat.fi
  - Again, Juha Nurmi can build it :)

Tor settings

Start configuring a few Directory Authorities

This step is generating the keys for them and the DirServer lines. Run **tor-gencert** to generate an identity key. Then run tor **--list-fingerprint**. Create your DirServer lines like *DirServer orport=<port> v3ident=<fingerprint from authority_certificate, no spaces> <ip>:<port> <fingerprint from --list-fingerprint in ABCD EF01 format>*. These DirServer lines are what put you onto an alternate tor network instead of the official one. You need one line per Directory Authority, and all DirServer lines need to be in the configuration of every DirAuth, Node, and Client you want to talk to this network.

Finish the Directory Authorites configuration

You should set **SOCKSPort** to 0, **ORPort** to something, and DirPort to something.

You need to set **AuthoritativeDirectory** and **V3AuthoritativeDirectory**. You can also set **VersioningAuthoritativeDirectory** along with **RecommendedClientVersions** and **RecommendedServerVersions** - why not. Perhaps you want to copy **ConsensusParams** out of a recent consensus, also. If you're going to run multiple tor daemons off a single IP address, you should set **AuthDirMaxServersPerAddr** 0 (0 is unlimited, default is two servers per IP.)

You will also (probably) want to lower the voting times, so you can generate a consensus quicker. I'd suggest, to start off with, **V3AuthVotingInterval 5 minutes**, **V3AuthVoteDelay 30 seconds**, and **V3AuthDistDelay 30 seconds** . You can also set **MinUptimeHidServDirectoryV2** to something like **1 hour**.

Start up your Directory Authorities

They should all be running, and you should see stuff like 'Time to vote' and 'Uploaded a vote to...' in the notices.log

You will also see *Nobody has voted on the Running flag. Generating and publishing a consensus without Running nodes would make many clients stop working. Not generating a consensus!* This is normal. If TestingAuthDirTimeToLearnReachability is not set (and it's not) - a Directory Authority will wait 30 minutes before voting to consider a relay to be Running. You should either wait 30 minutes and be patient, or set AssumeReachable to skip the 30 minute wait. They will shortly begin generating a consensus you can see at *http://<ip>:<port>/tor/status-vote/current/consensus*

Start adding more nodes

Configure some Exit and Relay nodes (and optionally Bridges). For each node, you will need to put the **DirServer** lines. If you're running your nodes in the same /16, you will also need to set **EnforceDistinctSubnets 0**.

There is one other thing you will need to set for the first few nodes though: **AssumeReachable 1**. This is because if the consensus has no Exit Nodes, a subtle bug will manifest, and nodes will get in a loop and will not upload their descriptors to the Directory Authorities for inclusion in the consensus. By setting AssumeReachable, we skip the test. (The other option is to set up one of your Directory Authorities as an Exit node.)

Reference: https://ritter.vg/blog-run_your_own_tor_network.html

Magnetic Storm Experiment: Northern Lights

- Cyber war simulation experiment: Netsplit cuts Finland out the net
- As a result, the Stella Polaris Network works independently
- Tor clients can use the Finnish private Tor network
- Provides end-to-end encrypted communication, onion services...