

Počítačová bezpečnost, soukromí a svoboda

NOLOG.CZ



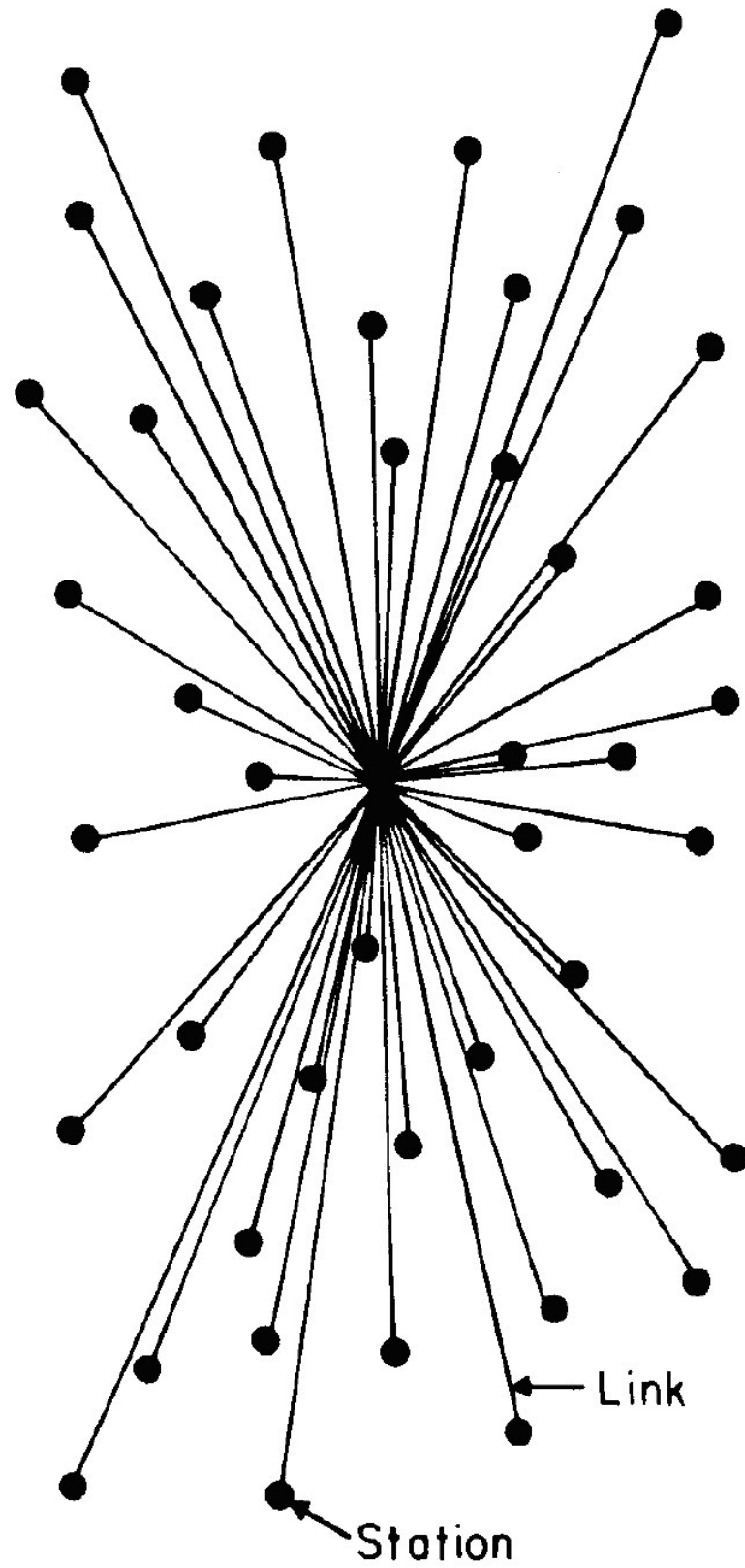
Letní škola KISK 2019

NOLOG.CZ

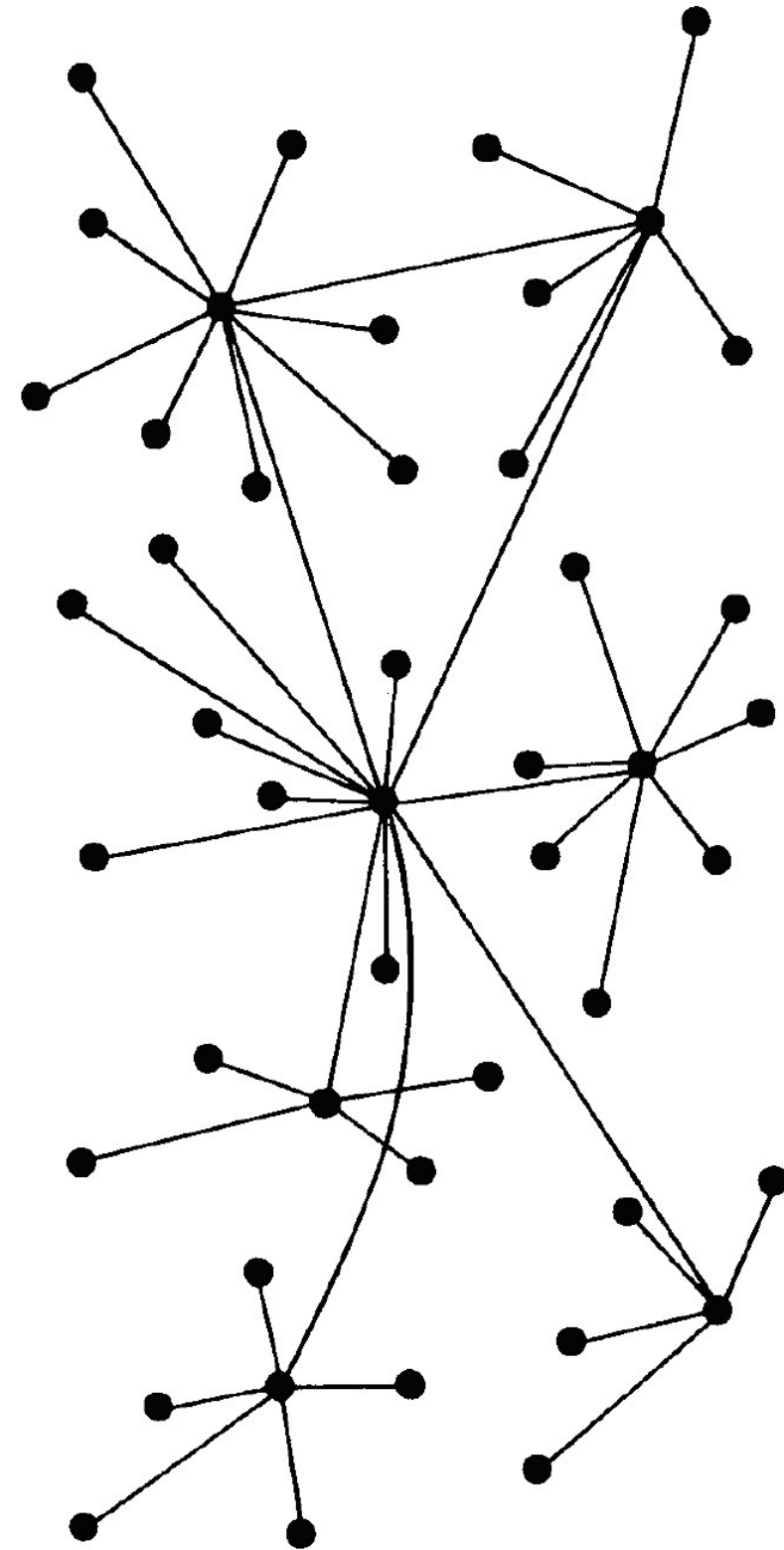
- Aktivistický IT kolektiv (od roku 2017)
- **Podporujeme antiautoritářské aktivity, skupiny a organizace**
- Poskytujeme bezpečné internetové služby
- Vytváříme bezpečnostní manuály pro politické aktivistky a aktivisty, snažíme se v antiautoritářském/anarchistickém hnutí budovat **bezpečnostní kulturu**

Co je špatně s Internetem?

- Internet je extrémně **centralizovaný**.
- V mnoha zemích je internet **cenzurovaný**.
- Sílí snahy o plošné **monitorování provozu** na internetu.
- Dezinformace, nízká míra zabezpečení, kybernetické útoky.



CENTRALIZED
(A)



DECENTRALIZED
(B)

PRISM a další



- Sledovací program NSA
- “Boj proti terorismu” - v praxi plošné šmírování
- Microsoft, Apple, Google, Yahoo...
- Informace vynesl v roce 2013 **Edward Snowden**

TOP SECRET//SI//ORCON//NOFORN



facebook



Hotmail

YAHOO!



You Tube

AOL

mail



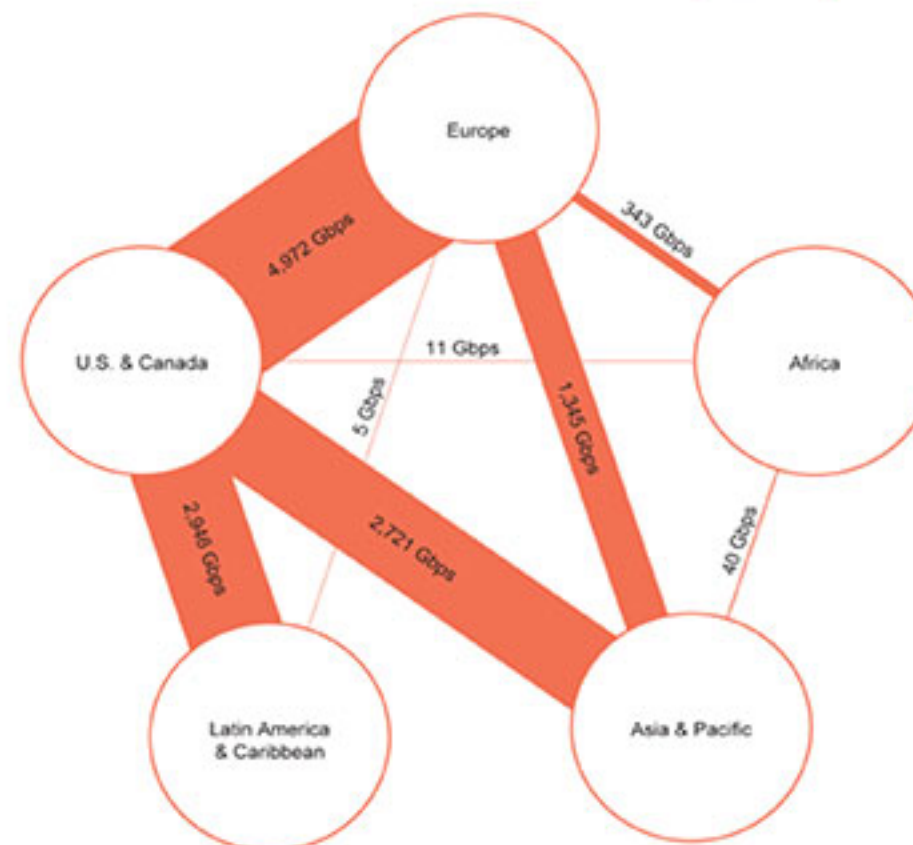
(TS//SI//NF)

Introduction

U.S. as World's Telecommunications Backbone



- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

Když státy hackují

- Jak obejít šifrování? Je třeba zaútočit přímo na koncové zařízení.
- Vlády si pořizují nedetekovatelný malware od soukromých společností
- Využíván k útokům na politické aktivistky a aktivisty

HackedTeam

- Italská společnost HackingTeam
- V roce 2015 napadena hacktivistou “Phineasem Phisherem” (má na svědomí i několik dalších útoků na podobné společnosti)
 - masivní únik dat, desítky gigabajtů e-mailů, softwaru atd.
- HackingTeam prodával nedetekovatelný malware represivním vládám (např. Saudská Arábie, Kazachstán), který ho využívat při útocích na opozici
- Software od HackingTeamu nakupovala i PČR

A black and white photograph of a smiling frog puppet. The puppet has large, round eyes and a wide, open mouth showing its tongue. It is positioned in the center-right of the frame against a solid black background. To the left of the puppet, there is a white rectangular box containing the text "Phineas Fisher" and "Hacker" stacked vertically.

Phineas Fisher
Hacker

Co je to šifrování?

- “End-to-end šifrování” (E2E encryption) znamená, že data zašifrujete “u sebe” a nikdo kromě vás k nim nemá přístup
- **Není E2E šifrované:** Skype, Facebook Messenger, Instagram chat apod.
- **E2E šifrované:** Signal, Whatsapp, Telegram

Co je to anonymita?

- Internet **není anonymní**
- Pokud chcete být anonymní, musíte **schovat původ dat**
- Tor, VPN služby
 - <https://www.torproject.org/>
 - Příklad VPN služby: <https://protonvpn.com/>

Co s tím?

- **Používejte šifrovaná řešení**
 - Signal, Tor, šifrované e-maily (např. ProtonMail)
- **Sledujte legislativu** týkající se internetu
- Minimalizujte množství dat, která předáváte korporacím (Facebook, Instagram apod.)
- Važte si svého soukromí.
- **Doražte na workshop :)**