Tor projekt

Anonimnost na Internetu

Ivo Ugrina – ivo@iugrina.com

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Što je Tor?

- Tor == The Onion Router
- Otvorena mreža i aplikacija s ciljem povećanja anonimnosti na Internetu
- Nastao 2002. u Naval Research Laboratoryju u SAD-u. Trenutno pod okriljem The Tor Project, Inc.

42:72:61:76:6f:21:20:55:73 :70:6a:65:6c:69:20:73:74:6 5:20:70:72:6f:63:69:74:61: 74:69:20:6f:76:6f:20:3a:70

Što je anonimnost [1993] ?

"On the Internet, nobody knows you're a dog."

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Što je anonimnost [2011] ?

NOISE TO SIGNAL
RobCottingham.ca/cartoon

How the hell does Facebook know I'm a dog?

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Tko ima koristi od Tora?

Korisnici Tora su raznoliki, s jednim zajedničkim motivom – anonimnošću na Internetu. Najčešće ga koriste sljedeće skupine:

- Novinari i blogeri koji izvještavaju o osjetljivim temama
- Zviždači
- Državne agencije i vojska
- Državljani “problematičnih” zemalja koji žele pristupiti inače blokiranim informacijama na internetu (Kina, Iran,

42:72:61:76:6f:21:20:55:73 :70:6a:65:6c:69:20:73:74:6 5:20:70:72:6f:63:69:74:61: 74:69:20:6f:76:6f:20:3a:70

Tko ima koristi od Tora?

Korisnici Tora su raznoliki, s jednim zajedničkim motivom – anonimnošću na Internetu. Najčešće ga koriste sljedeće skupine:

- Novinari i blogeri koji izvještavaju o osjetljivim temama
- Zviždaći
- Državne agencije i vojska
- Državljani “problematičnih” zemalja koji žele pristupiti inače blokiranim informacijama na internetu (Kina, Iran, Hrvatska – registarbranitelja.com,...)

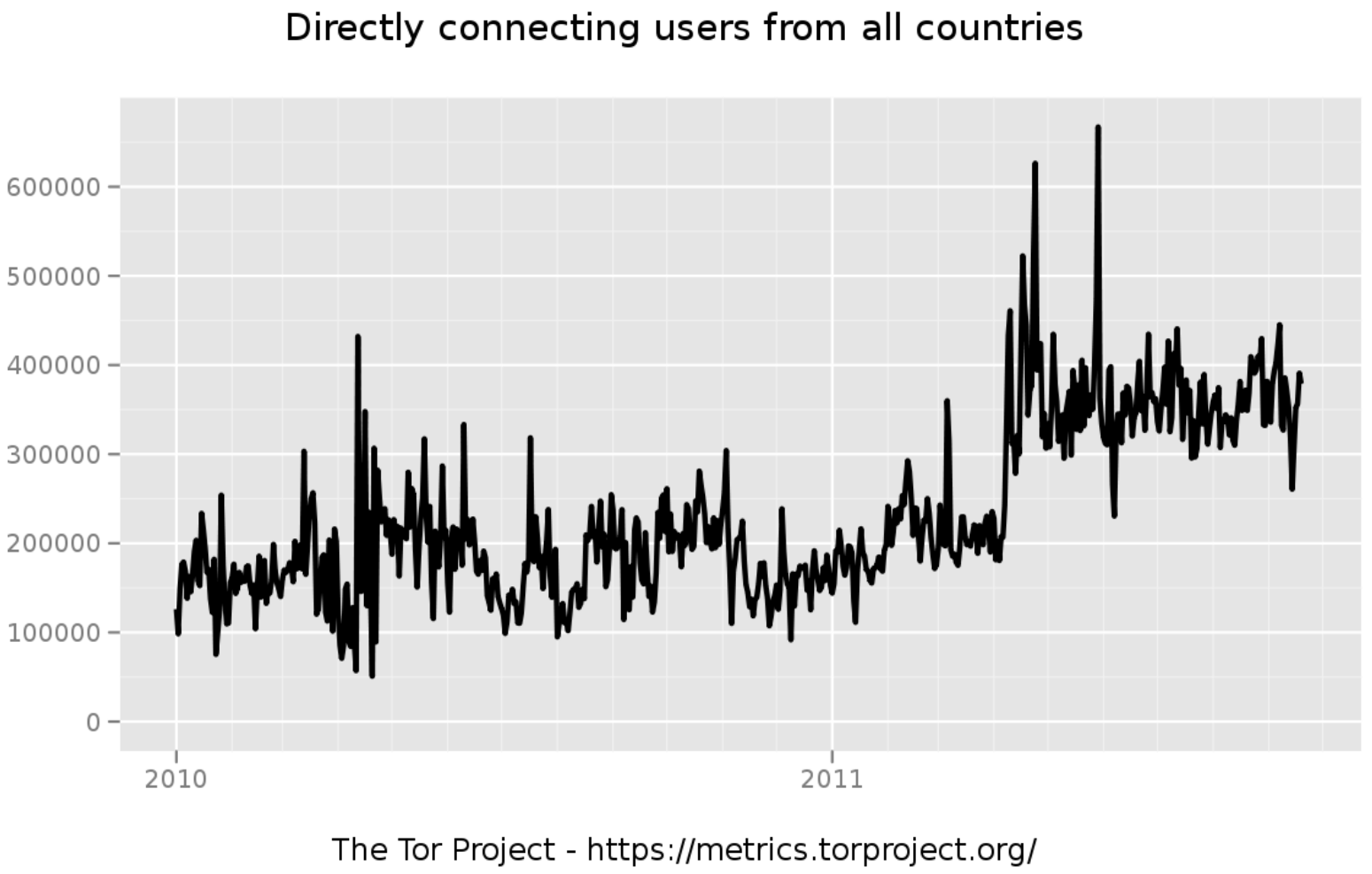
42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Tko ima koristi od Tora?

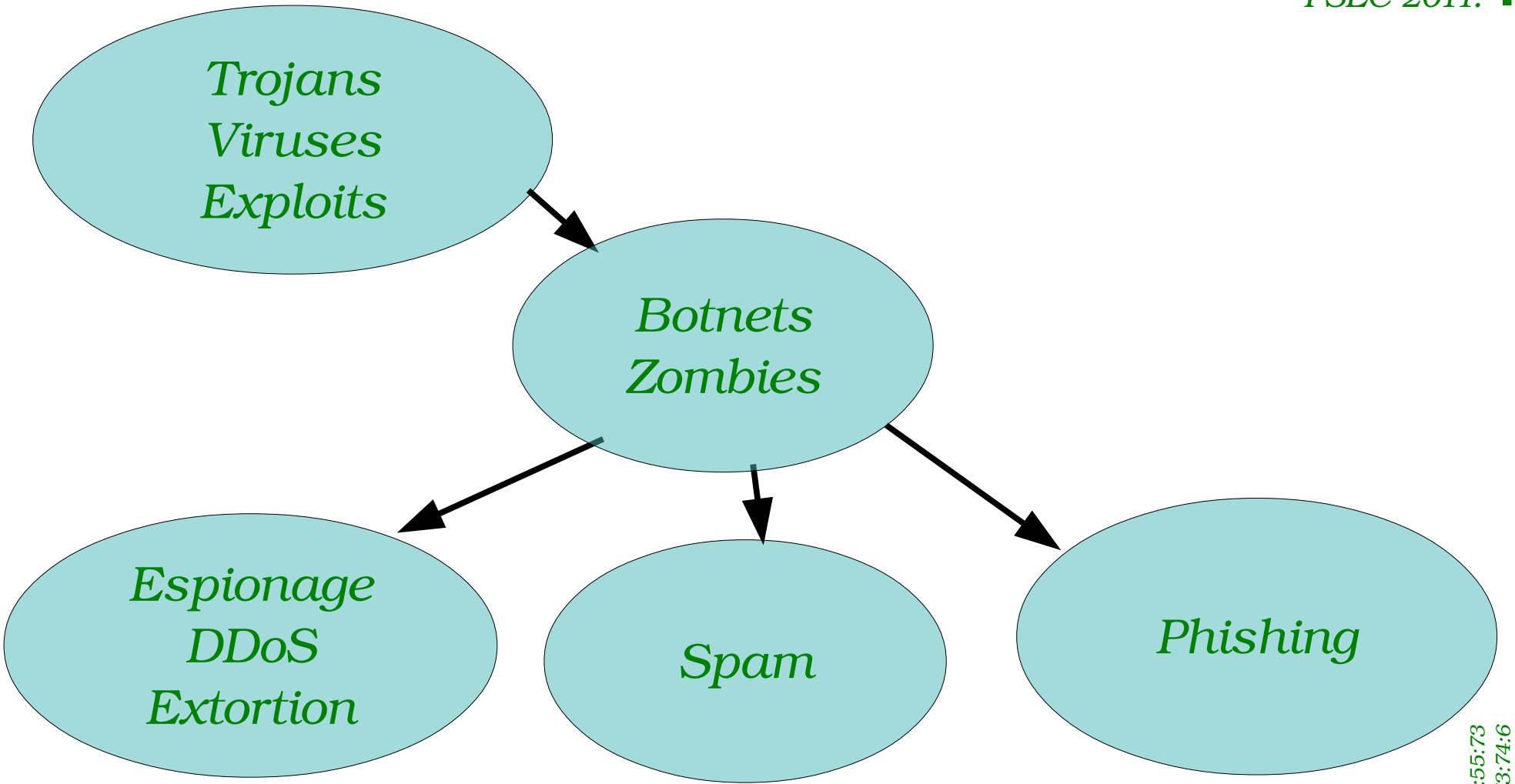
Zemlja	**Prosječan broj dnevnih korisnika**
SAD	75509 (20.97 %)
Njemačka	38390 (10.66 %)
Iran	27211 (7.56 %)
Francuska	19024 (5.28 %)
Republika Koreja	16610 (4.61 %)
Rusija	13279 (3.69 %)
Italija	12055 (3.35 %)
Velika Britanija	9913 (2.75 %)
Saudijska Arabija	9480 (2.63 %)
Indija	7837 (2.18 %)

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Tko ima koristi od Tora?

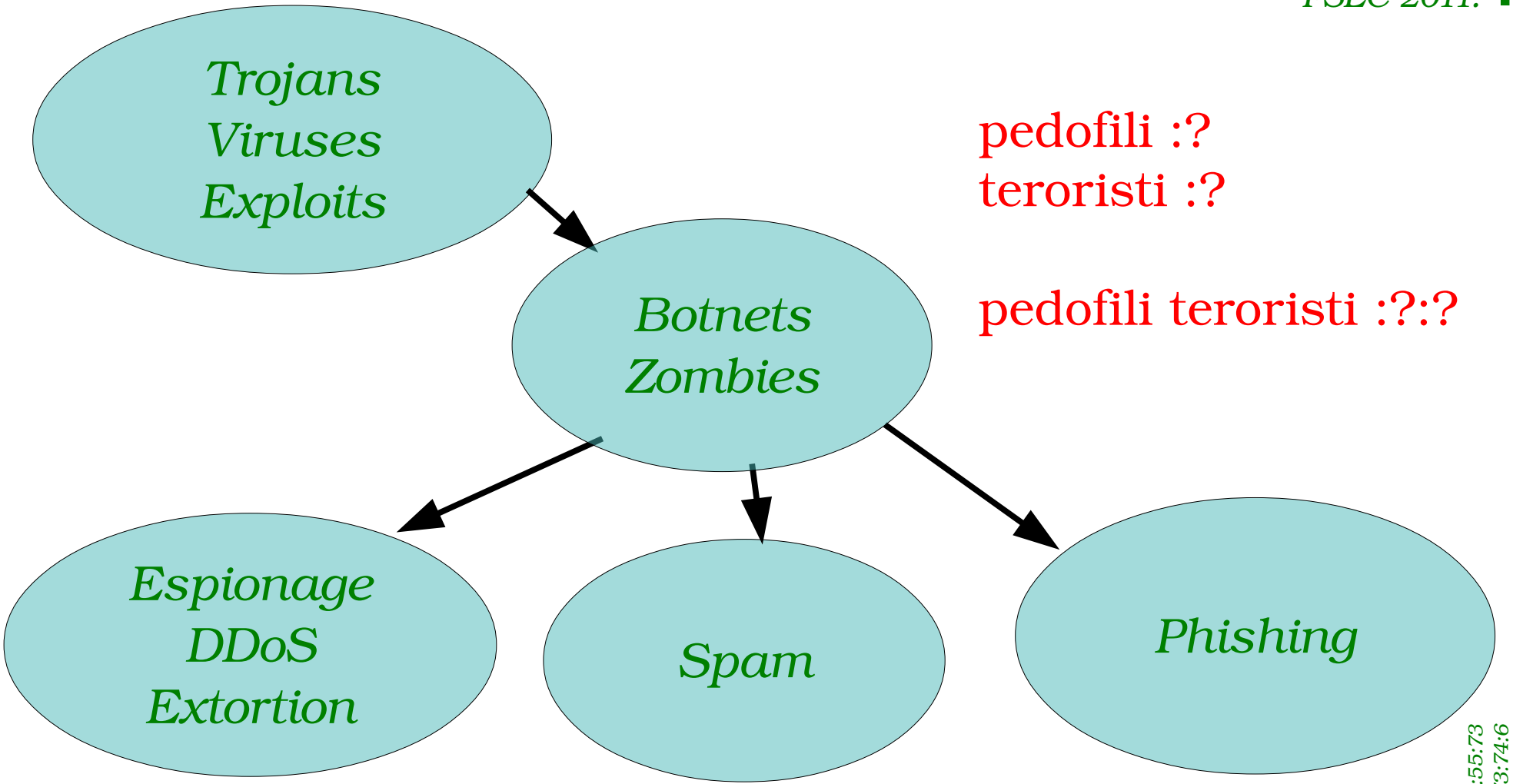


Tor i zločesti ljudi



42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Tor i zločesti ljudi

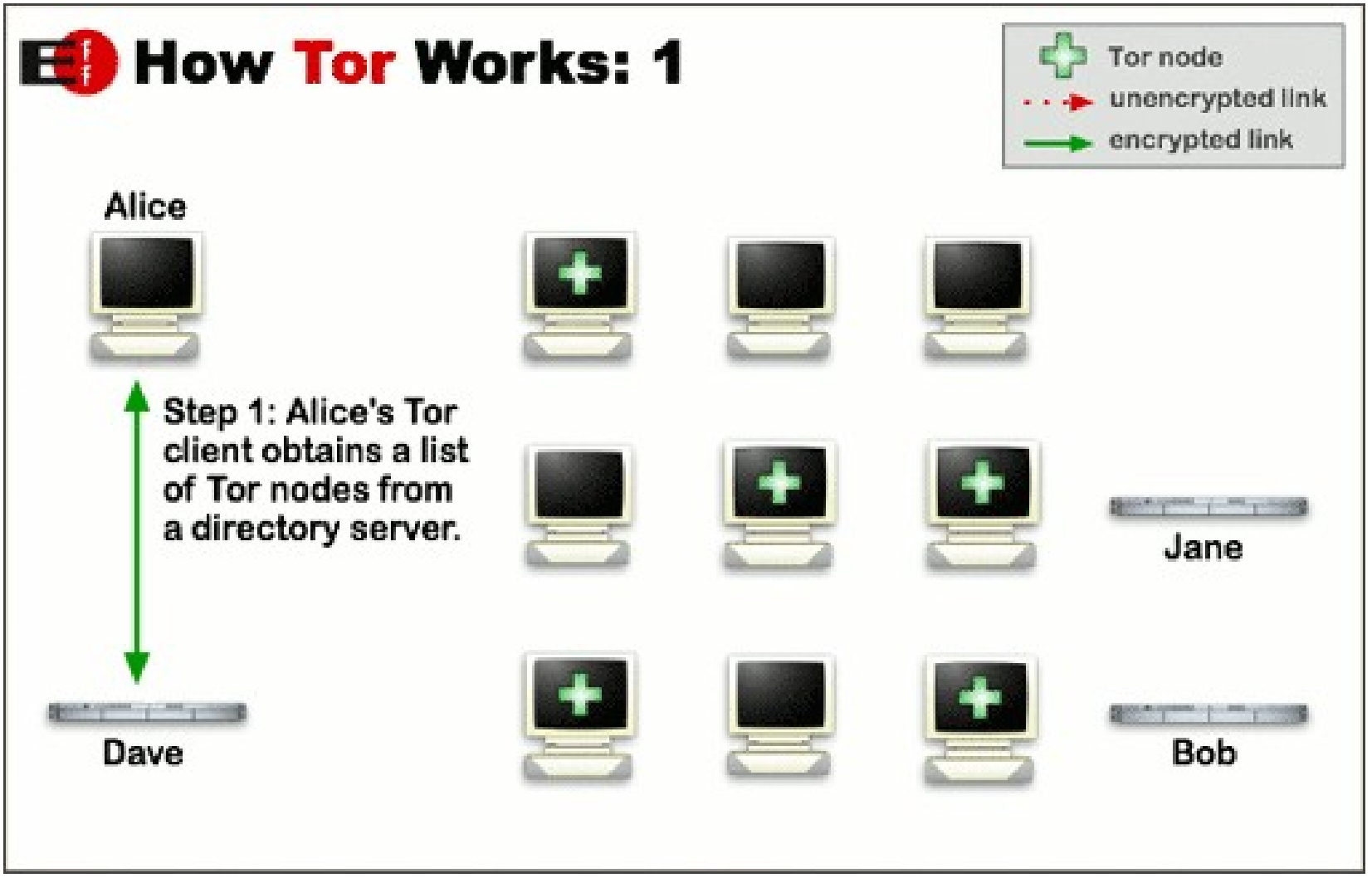


pedofili :?
teroristi :?

pedofili teroristi :?:?

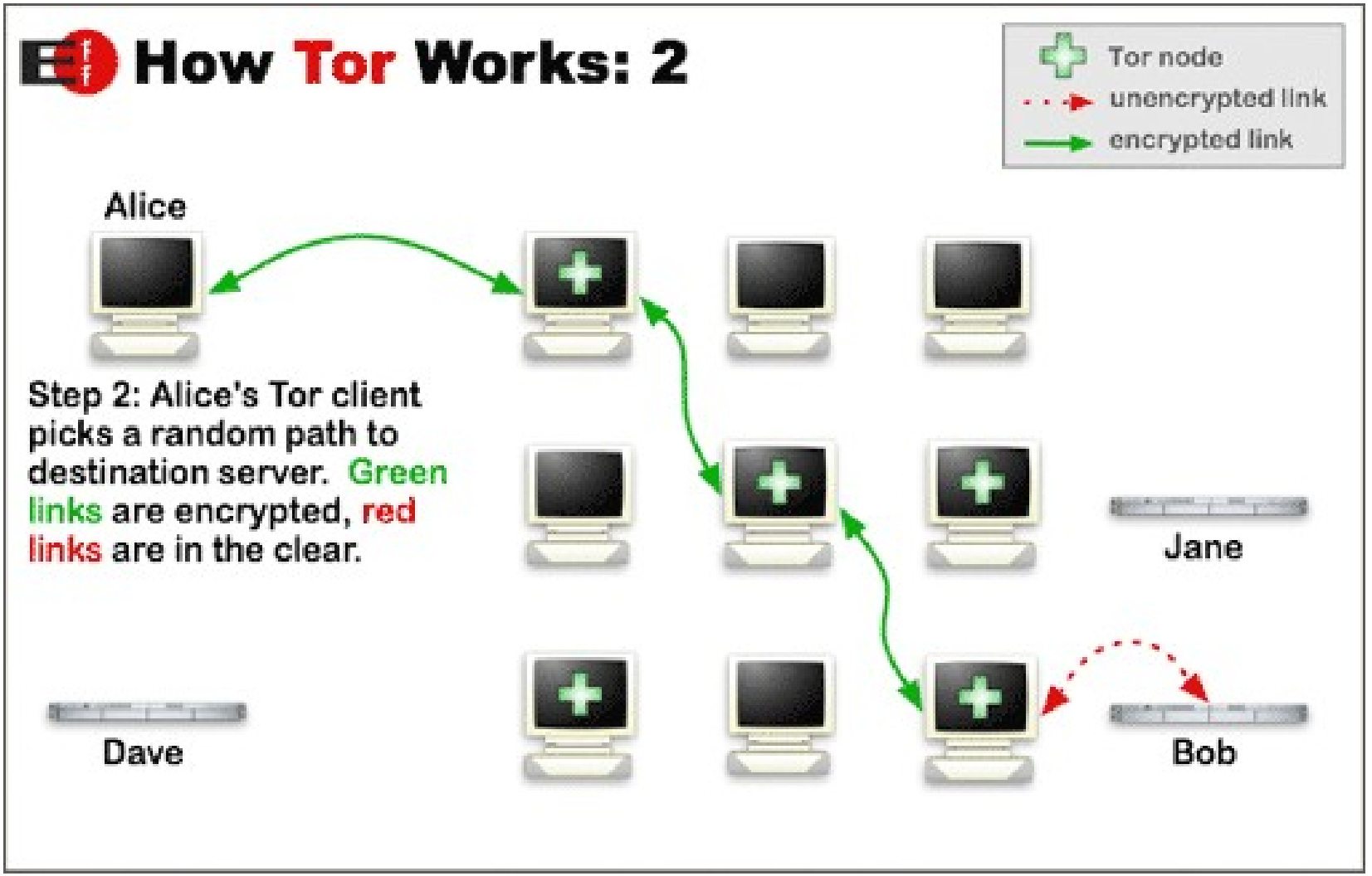
42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Kako radi Tor [1]



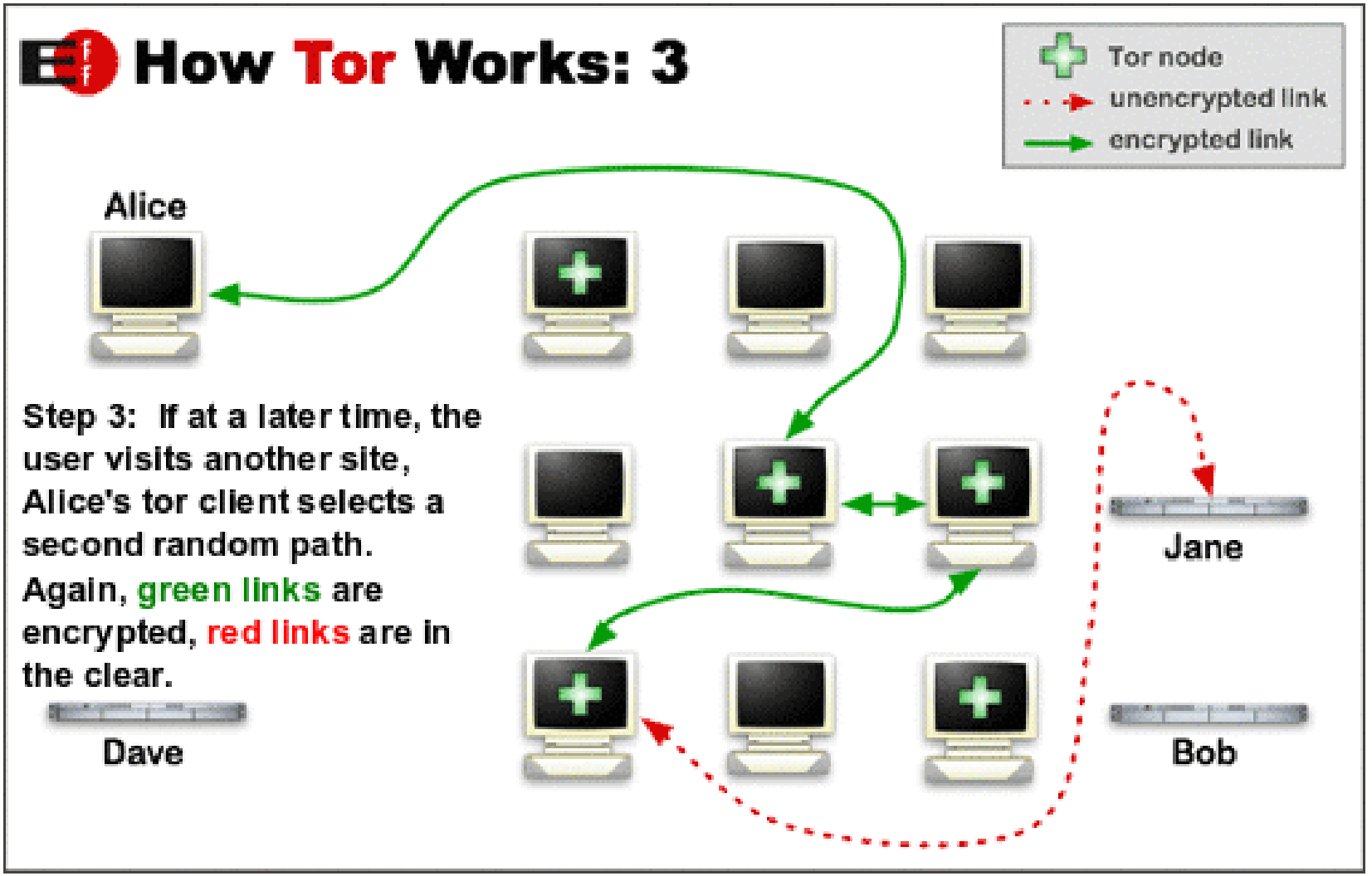
42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Kako radi Tor [2]



42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Kako radi Tor [3]



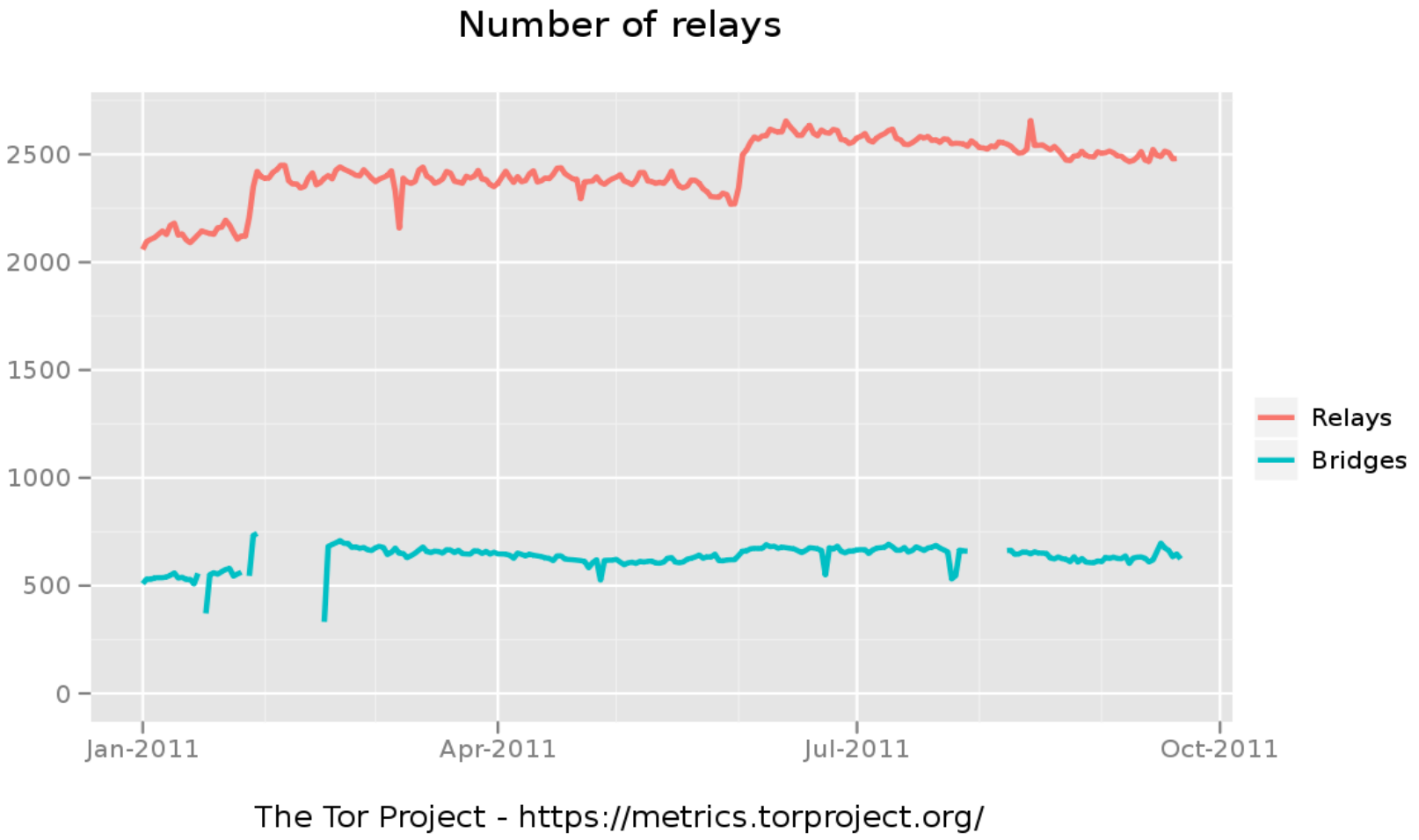
42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Prijenosnici (eng. relays)

- (srednji) prijenosnik [eng. (middle) relay]
- Izlazni prijenosnik [eng. exit relay]
- Most [eng. bridge]

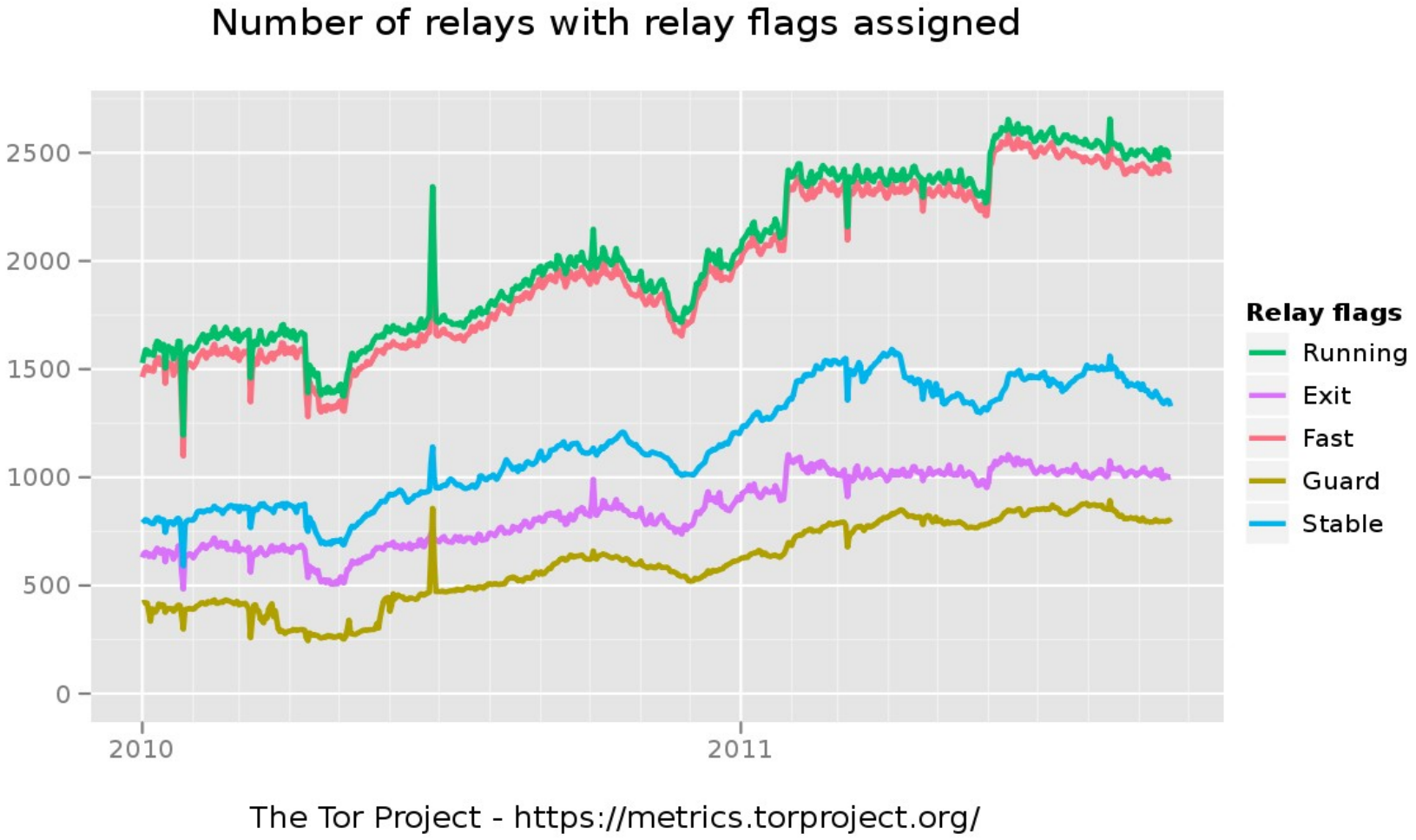
- ExitNodes $fingerprint,$fingerprint,... :?

Prijenosnici (eng. relays)



42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Prijenosnici (eng. relay)



Enkripcija

- AES 128-bit stream cipher (CTR)
- RSA 1024-bit signing keys
- Diffie-Hellman...

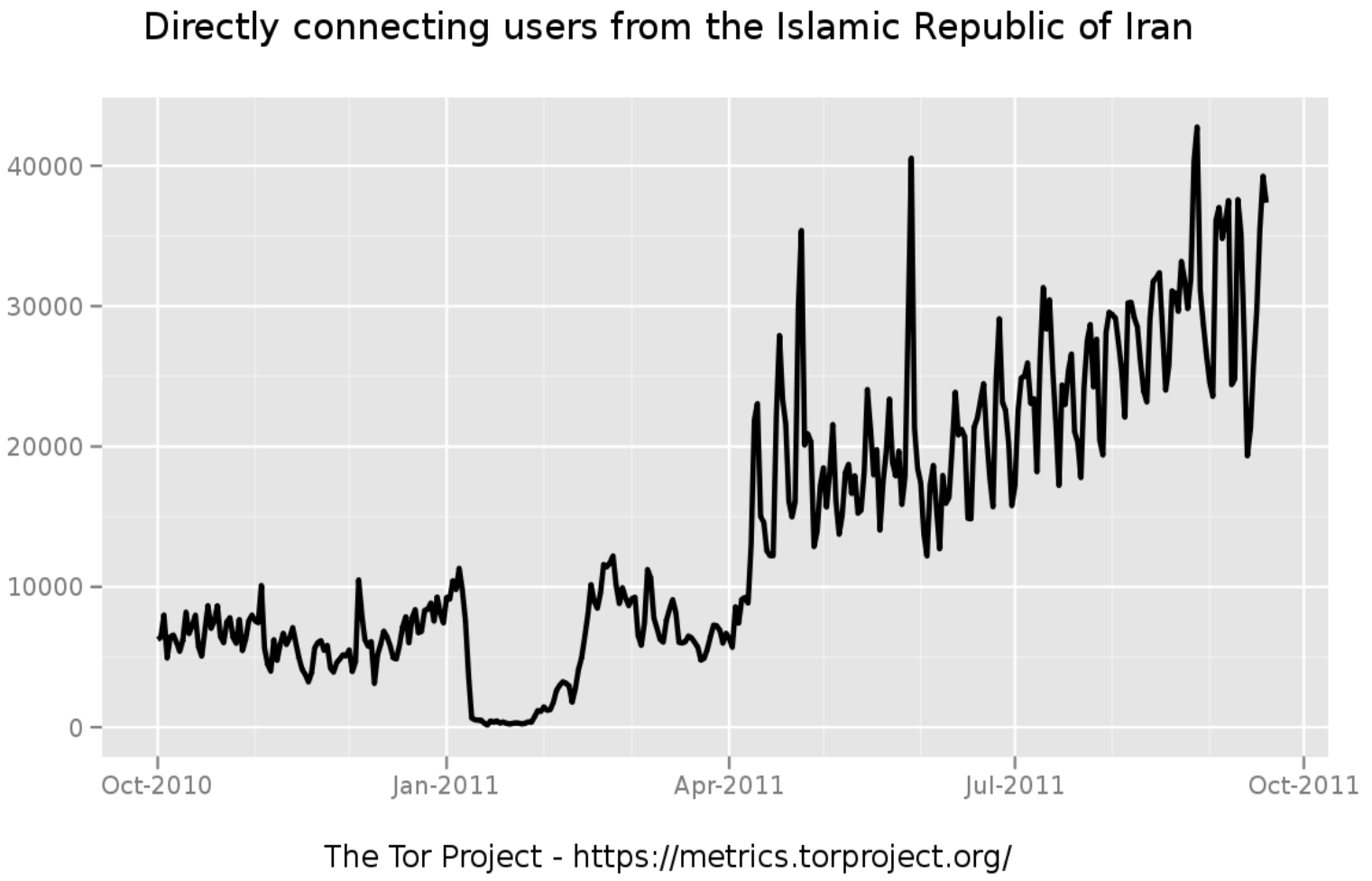
  ... prije se koristio 1024-bit safe prime iz RFCa (2409, 6.2)

  ... 1.2011. dogodio se Iran :D

  ... sada se koristi mod_ssl-ov

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Iran 1.2011.



Ključevi

- Long-term signing (“identity”) keys
  Router descriptor

  Directory authorities have more keys
  Regular identity key
  3-12 month “Authority Signing key”
  Super-secret long-term “Authority Identity Key”
- Medium-term “onion skin” keys
  Decrypts onion skins when accepting circuit extend attempts
  Lasts for a week
- Short-term “connection key”
  Negotiates TLS connections
  Rotates periodically and independently
  Ephemeral (2 hours)

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

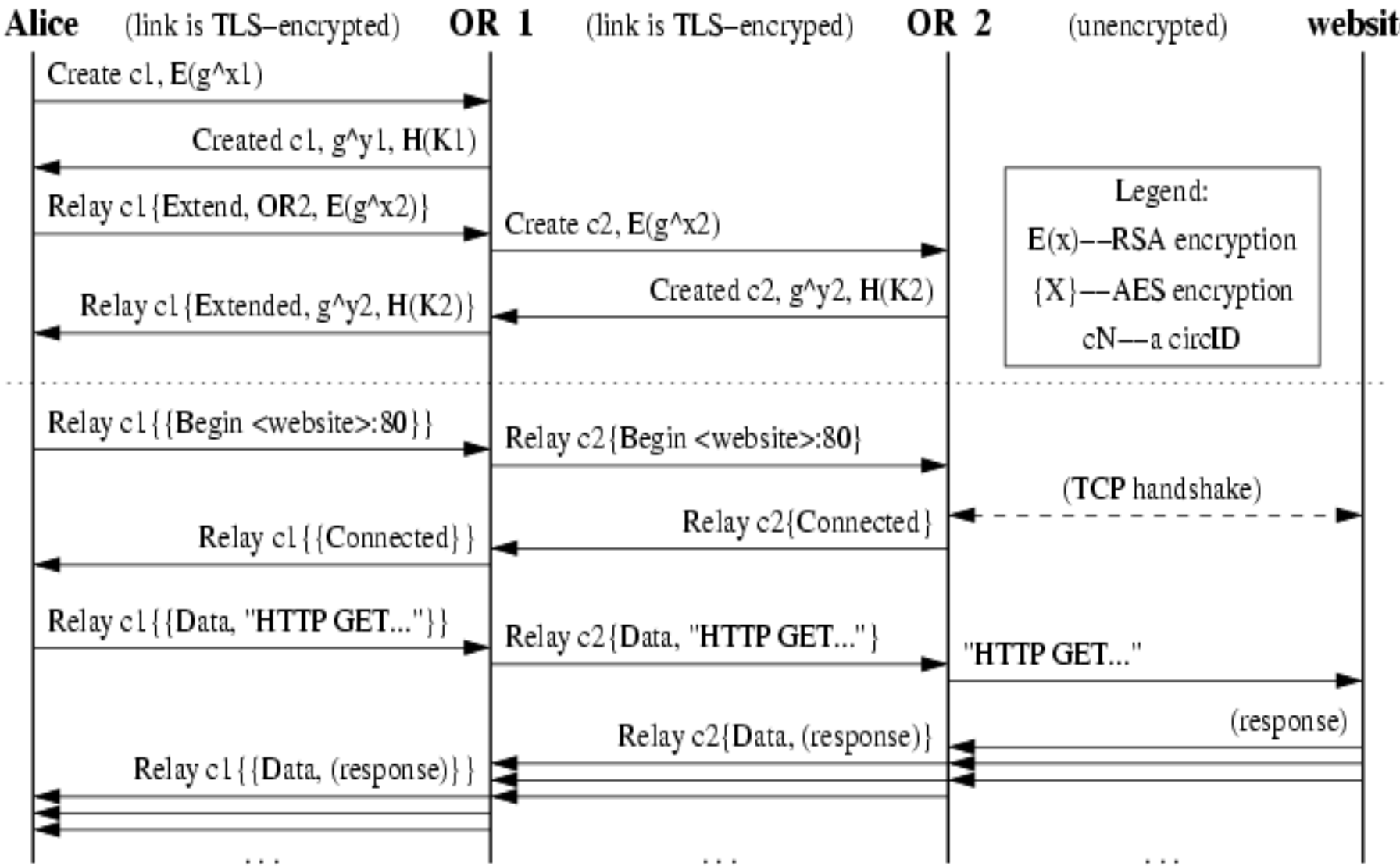
Ključevi

- Long-term signing (“identity”) keys
  Router descriptor

  Directory authorities have more keys
  Regular identity key
  3-12 month “Authority Signing key”
  Super-secret long-term “Authority Identity Key”
- Medium-term “onion skin” keys
  Decrypts onion skins when accepting circuit extend attempts
  Lasts for a week
- Short-term “connection key”
  Negotiates TLS connections
  Rotates periodically and independently
  ~~Ephemeral (2 hours)~~ !!! Iran 9.2011.

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

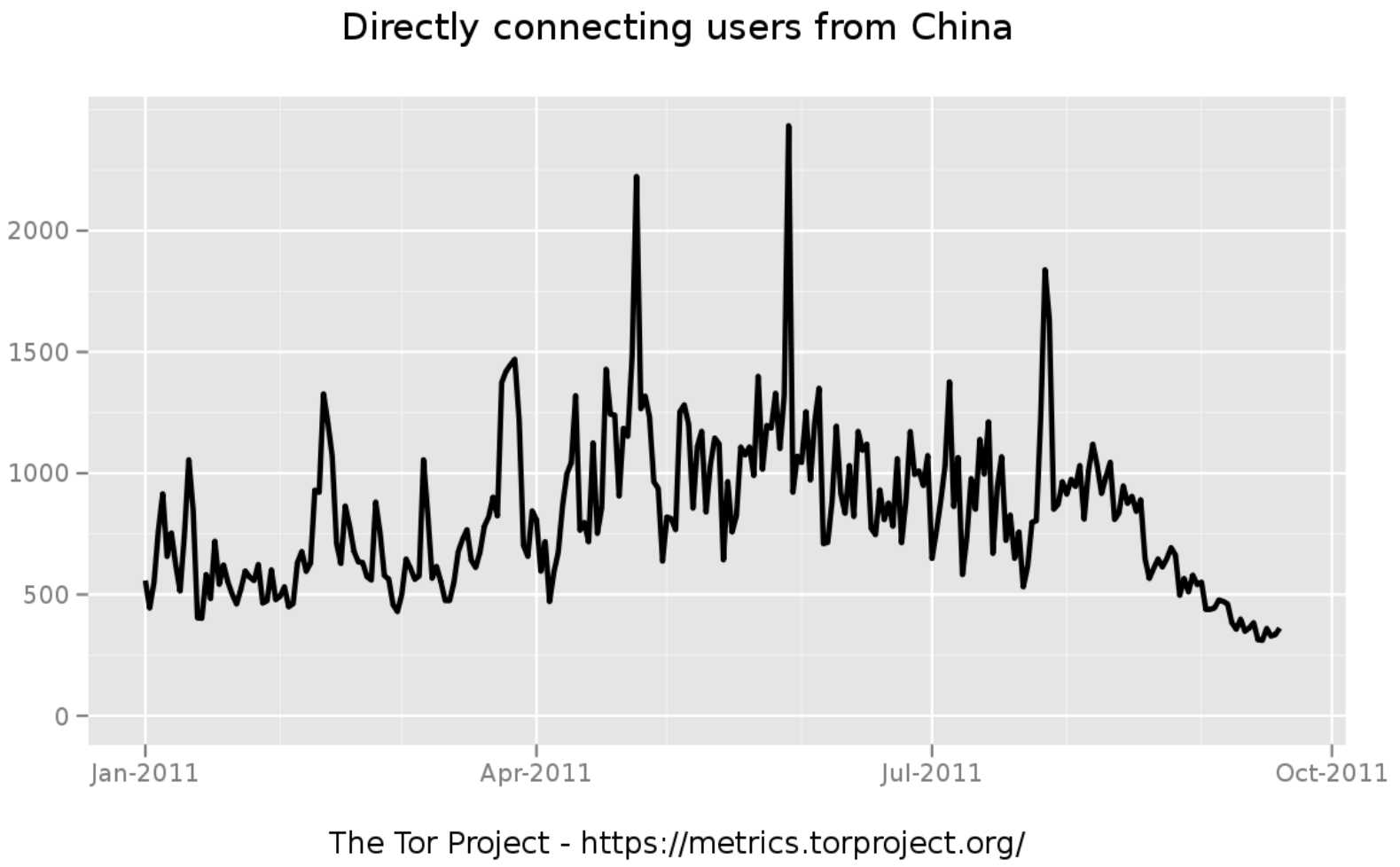
Kako radi Tor [4]



Kako blokirati Tor?

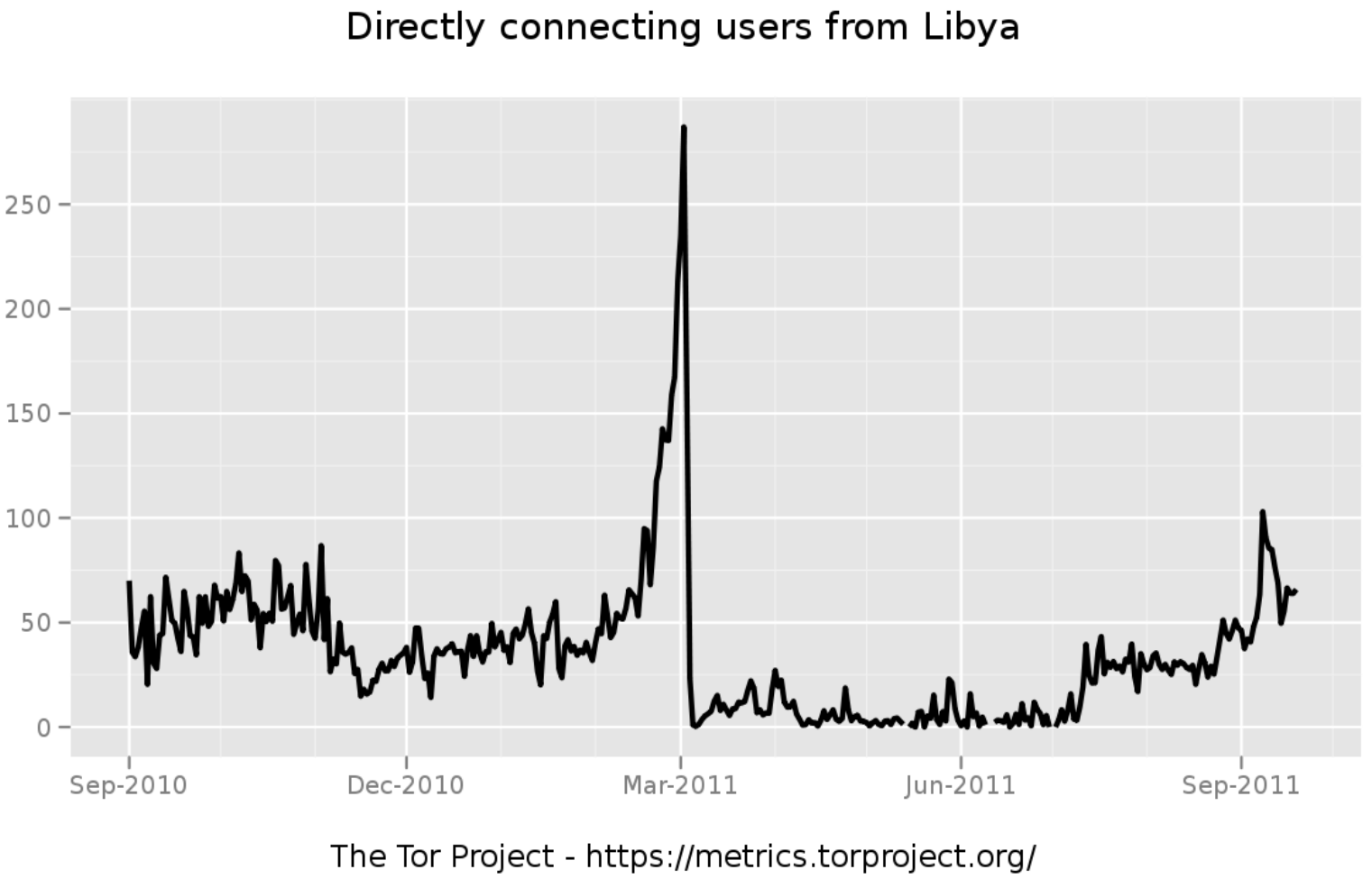
- Blokirajući *directory* autoritete [Veliki kineski vatrozid]
- Blokirajući sve prijenosnike na razini IP adrese (podaci iz *directory* autoriteta) [Veliki kineski vatrozid]
- Filtrirajući po Torovom mrežnom *fingerprint*u [Iran 1.2011.]
- Onemogučujući korisnicima da pronađu Tor
- Statističkom analizom ključeva [Iran 9.2011.]
- ???

Kina



42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Libija



Projekti

- Tails - Live CD/USB distribucija prekonfigurirana za sigurno korištenje Tora
- Orbot - Tor za Google Android uređaje
- !Torbutton - ekstenzija za Firefox korisnike koja omogućava surfanje WWW-om preko Tor mreže
- Check – jednostavna i brza provjera surfate li preko Tor mreže
- Tor Browser – preglednik prekonfiguriran za sigurno korištenje Tora
- IPv6 :(

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Fijasko == DigiNotar

- 12 *.torproject.org certifikata
- Problem s preuzimanjem softvera
- Ne utječe na Tor mrežu :?

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Problemi za vlasnike prijenosnika

- Mail blackliste
- IRC blackliste
- DMCA [Europa?]
- ISP
- Država (zapljena računala) !!!

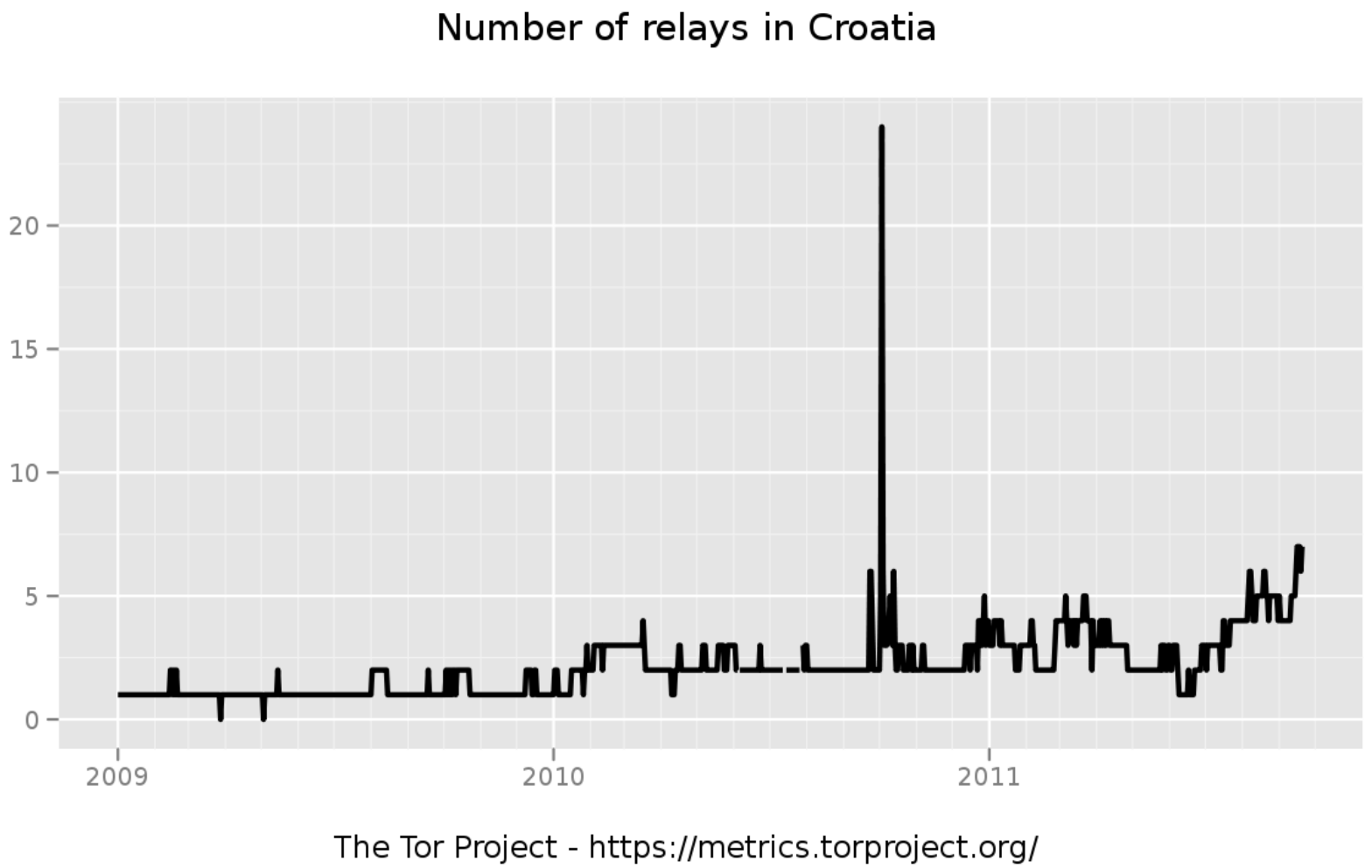
42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Kako izbjeći poteškoće s/sa ...

- Ne vrtite izlazne prijenosnike od kuće
- Upoznajte ISPa s namjerama
- ExitPolicy !!!

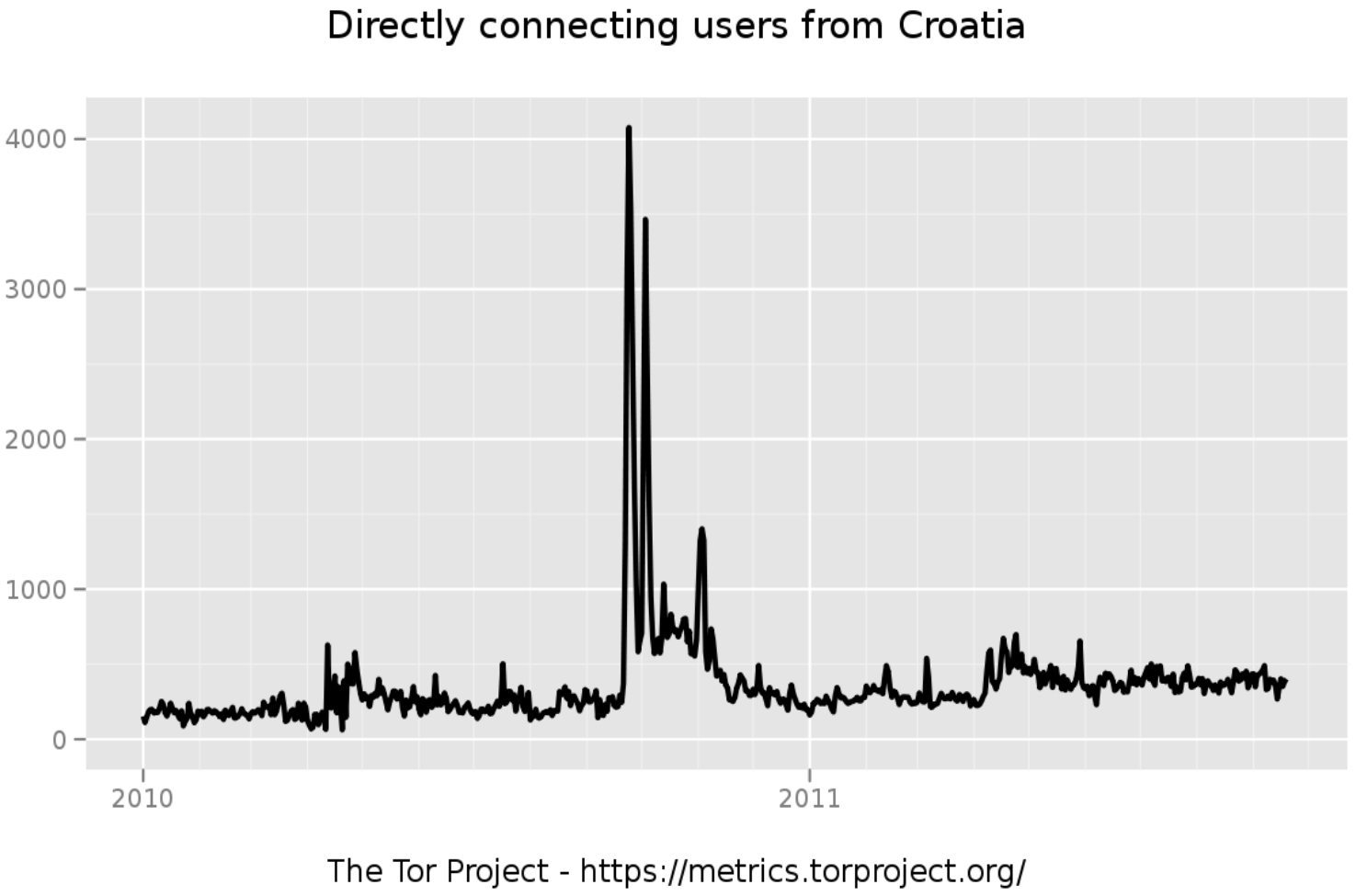
42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70

Stanje u HR



42:72:61:76:6f:21:20:55:73 :70:6a:65:6c:69:20:73:74:6 5:20:70:72:6f:63:69:74:61: 74:69:20:6f:76:6f:20:3a:70

Stanje u HR



Poveznice

- www.torproject.org
- metrics.torproject.org
- #tor @ irc.oftc.net

42:72:61:76:6f:21:20:55:73
:70:6a:65:6c:69:20:73:74:6
5:20:70:72:6f:63:69:74:61:
74:69:20:6f:76:6f:20:3a:70