Deep Vs. Dark web demystifying differences

Jurica Čular, M.Sc, MBA, CISA, CISSP
jcular@zsis.hr

Is there rally a confusion?

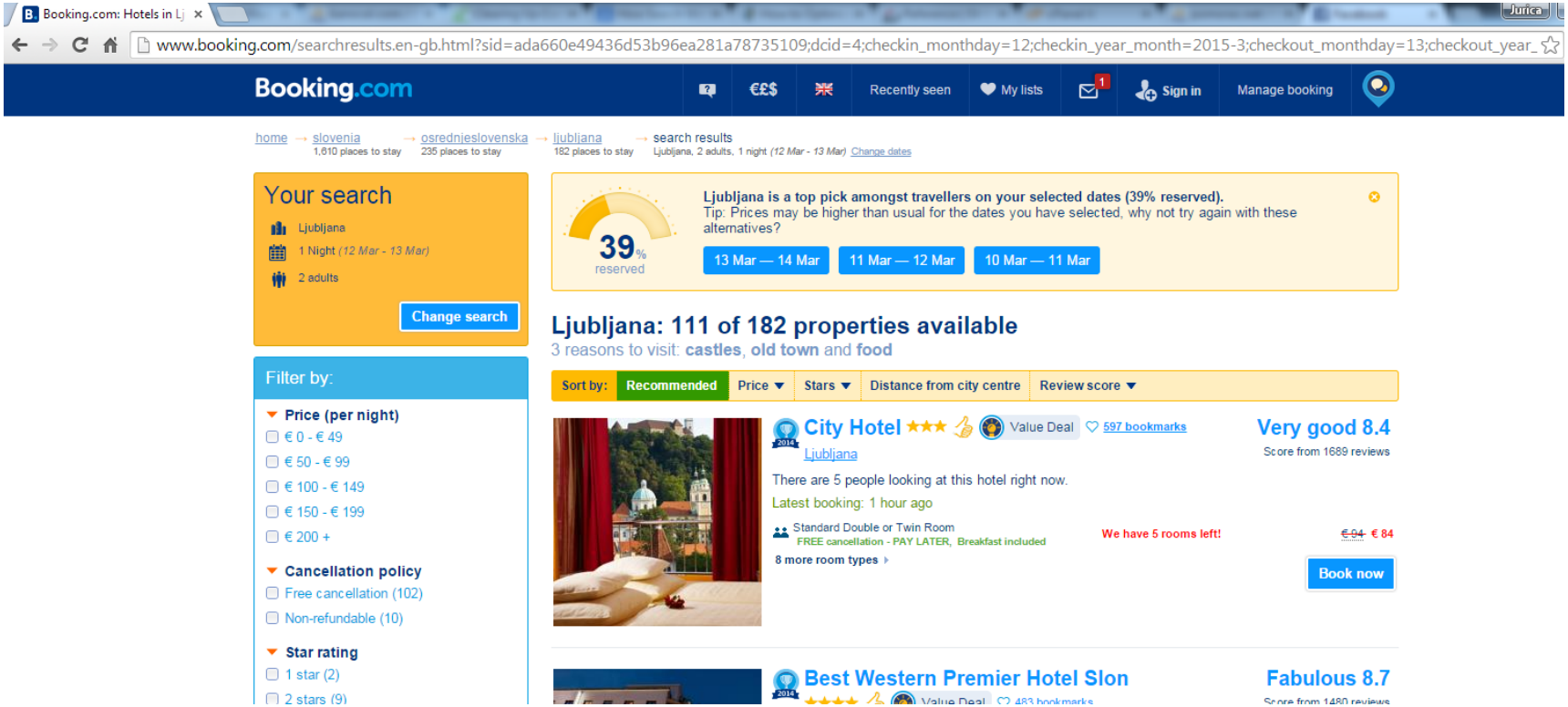
- Ooh YES!

Defs.

- Surface web – anything that can be indexed by a typical search engine like Google...

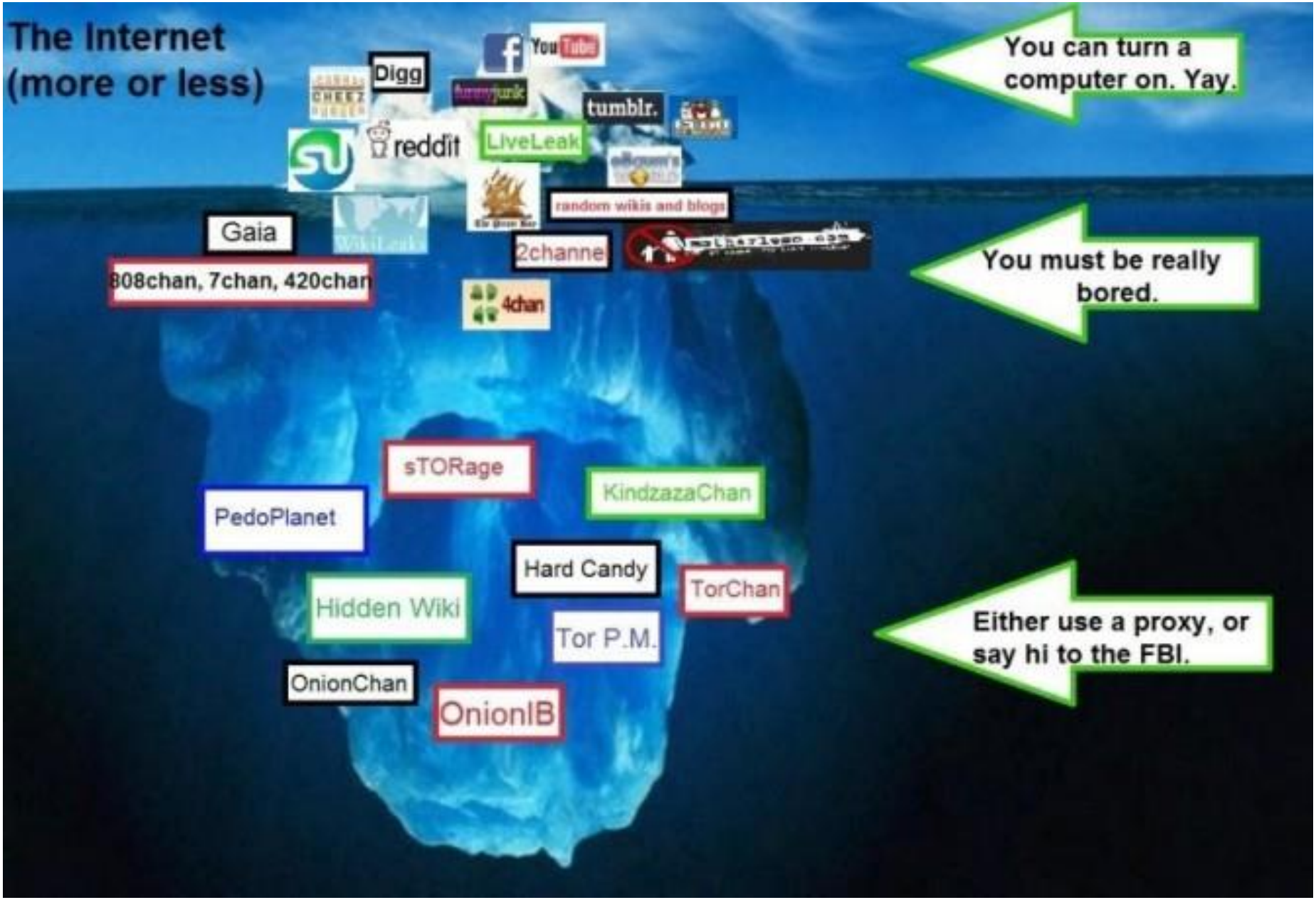
Defs.

- Deep web – anything that CANNOT be found by search engine (purist)



Defs.

- Dark web – small portion of deep web that has been intentionally hidden (...)


The Internet
(more or less)
Digg
You Tube
tumblr.
reddit
LiveLeak
random wikis and blogs
Gaia
2channel
808chan, 7chan, 420chan
4chan
You can turn a computer on. Yay.
You must be really bored.
sTORage
KindzazaChan
PedoPlanet
Hard Candy
TorChan
Hidden Wiki
Tor P.M.
OnionChan
OnionIB
Either use a proxy, or say hi to the FBI.

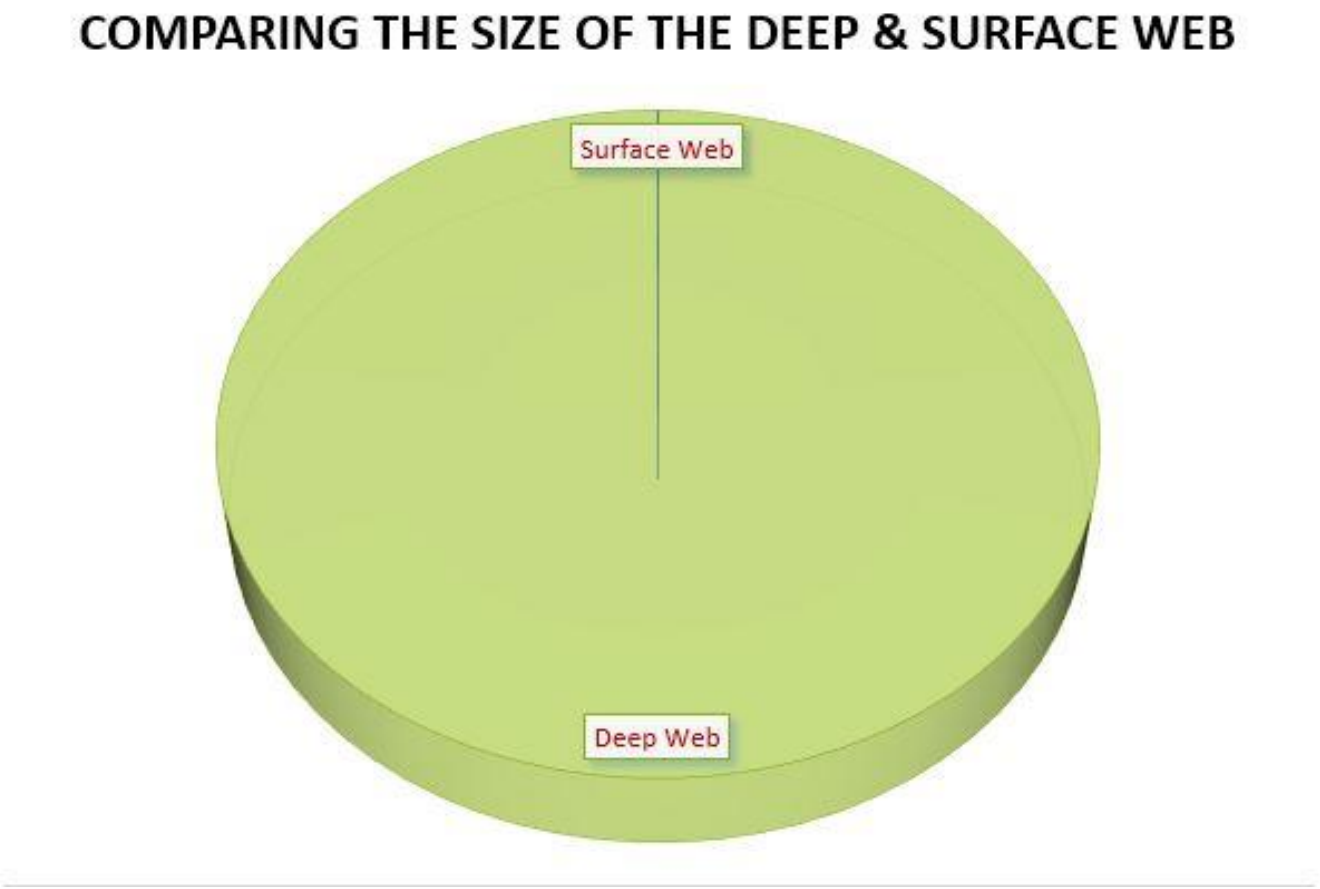
Search engine Vs. Deep Web Harvesting

- Search engine(s)
- „What time does McDonalds close?”
- 90’s
- Non comercial - research purpose

Search engine Vs. Deep Web Harvesting

- „What new info has been published on my competitors web site today?”
- Amount of data – metadata Vs. Full content
- BI or InfoSec?

Search engine Vs. Deep Web Harvesting



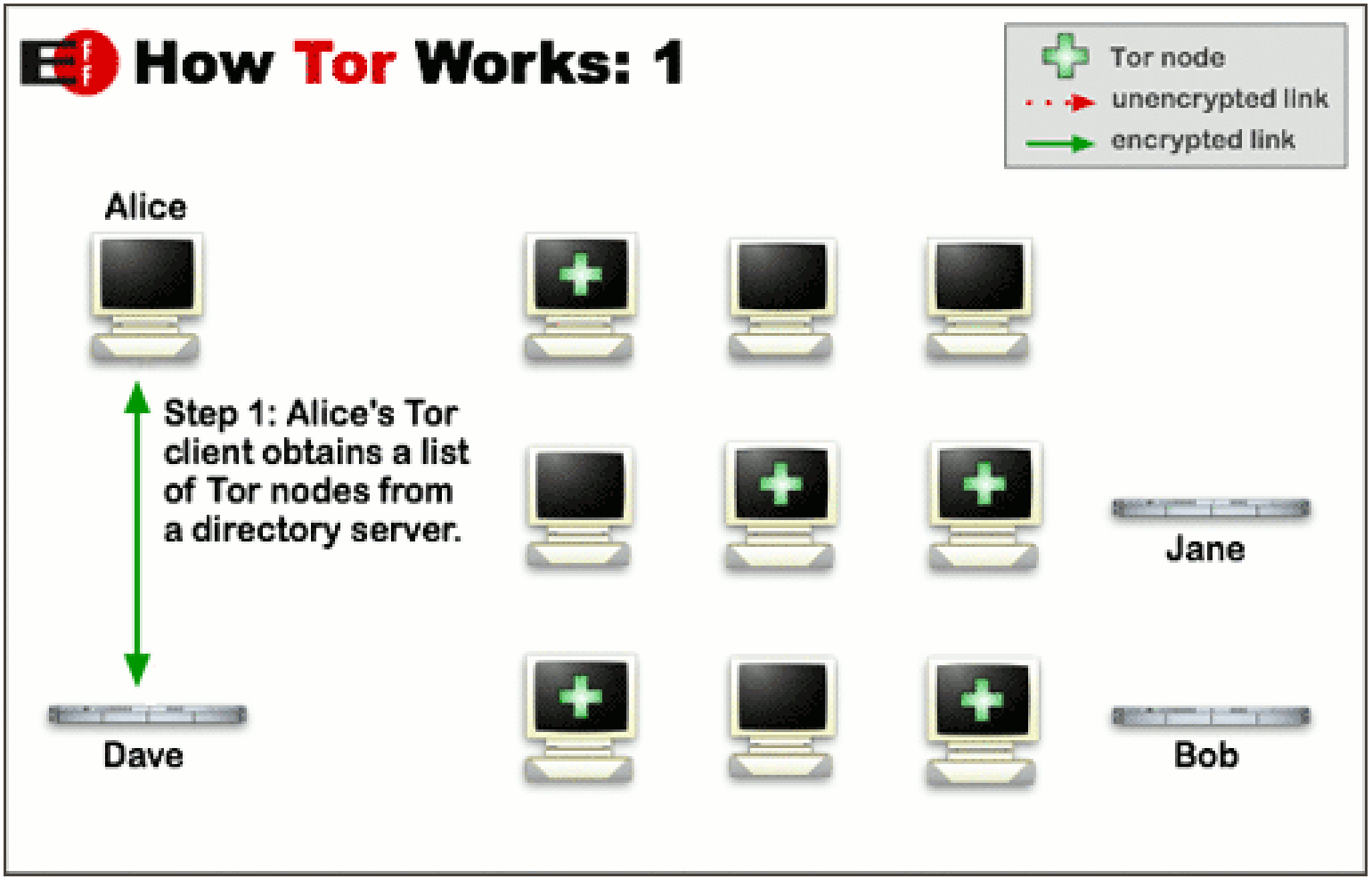
Anonimity

- Anonimity...why?
- Def. – „unidentifiablilty within a set of subjects”
- New rules
- Many researches

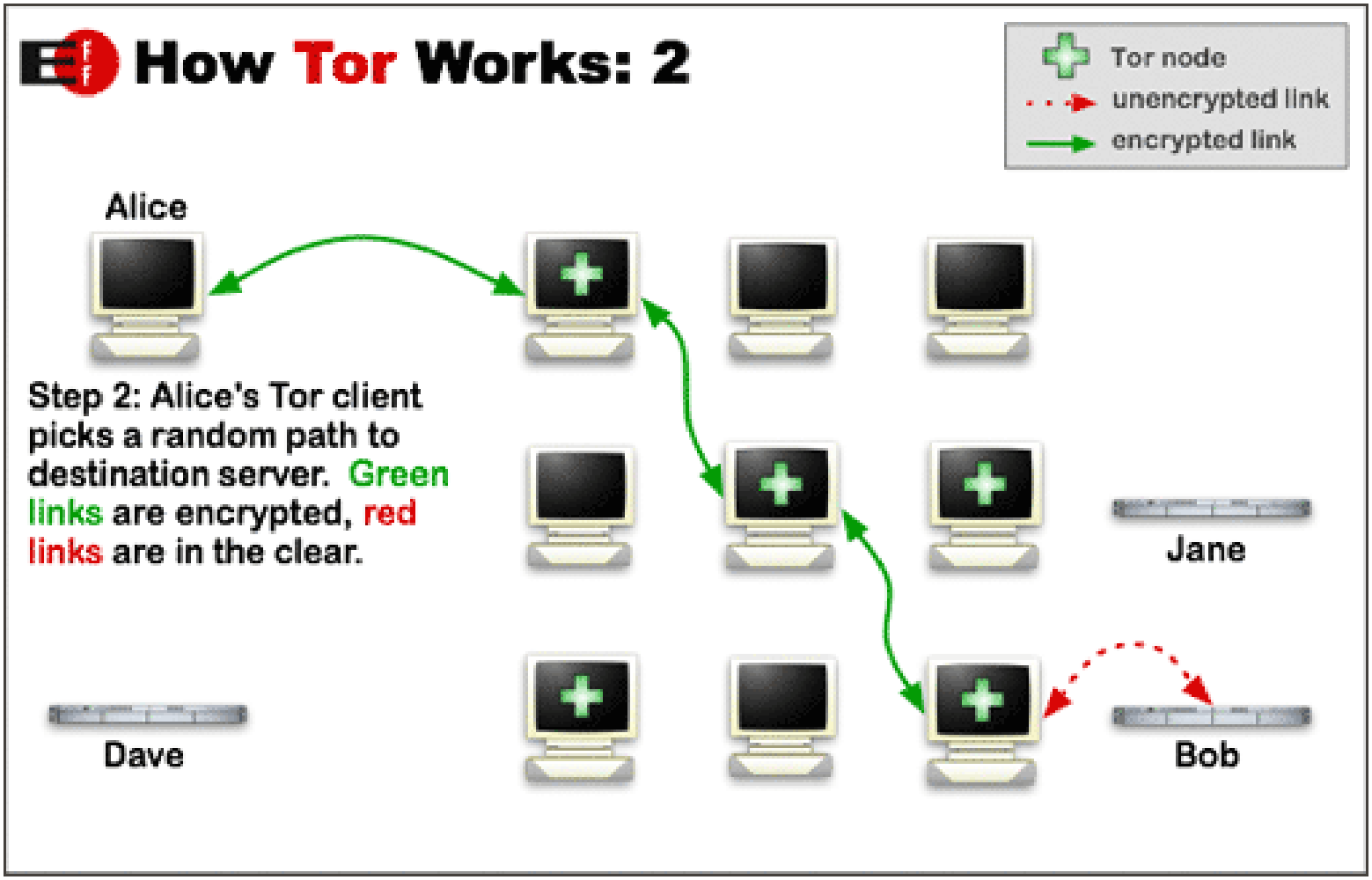
Tor

- Encrypted content
- Encrypted content and routing info
- Reley networks

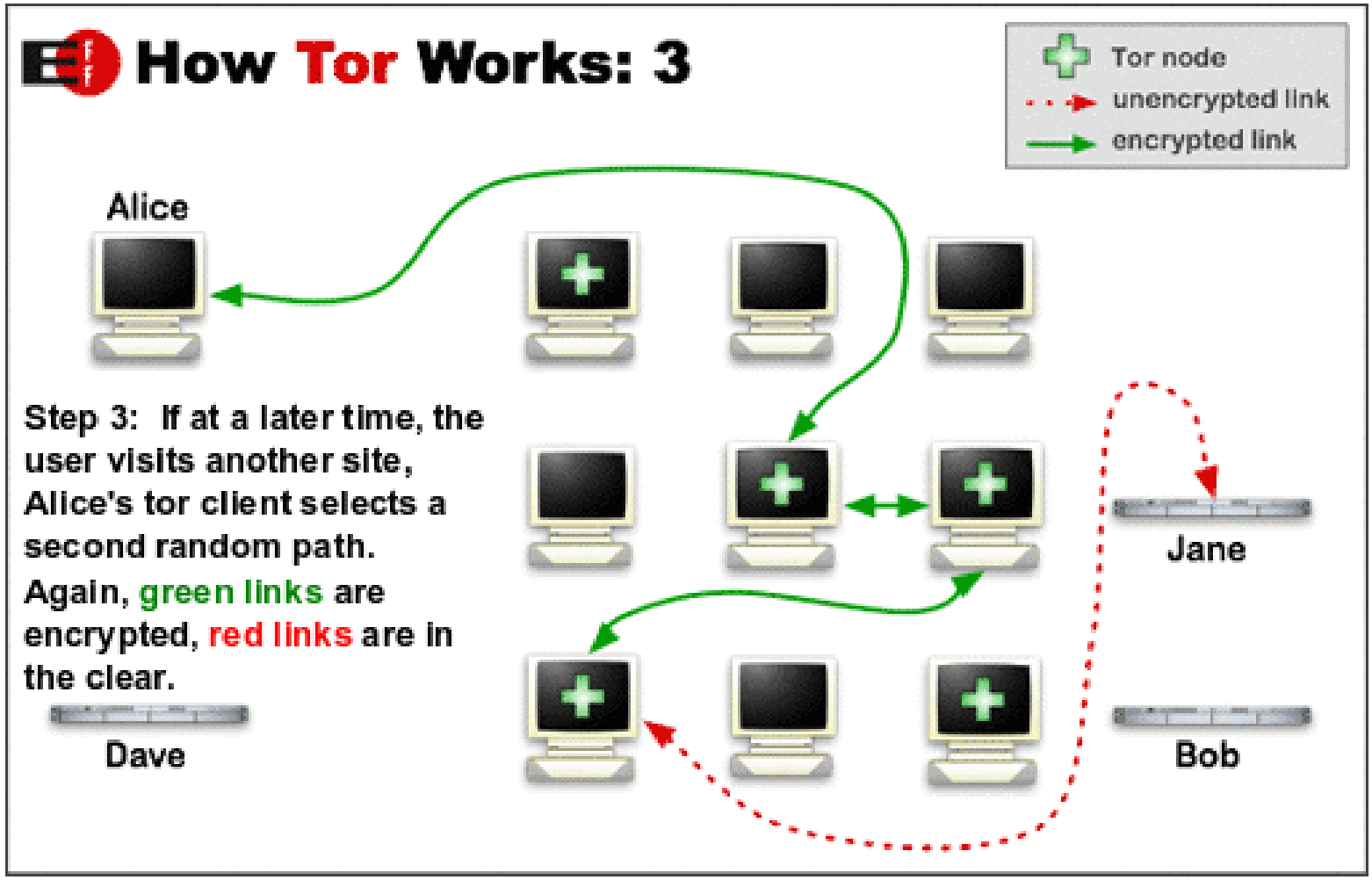
Tor – how Tor works?



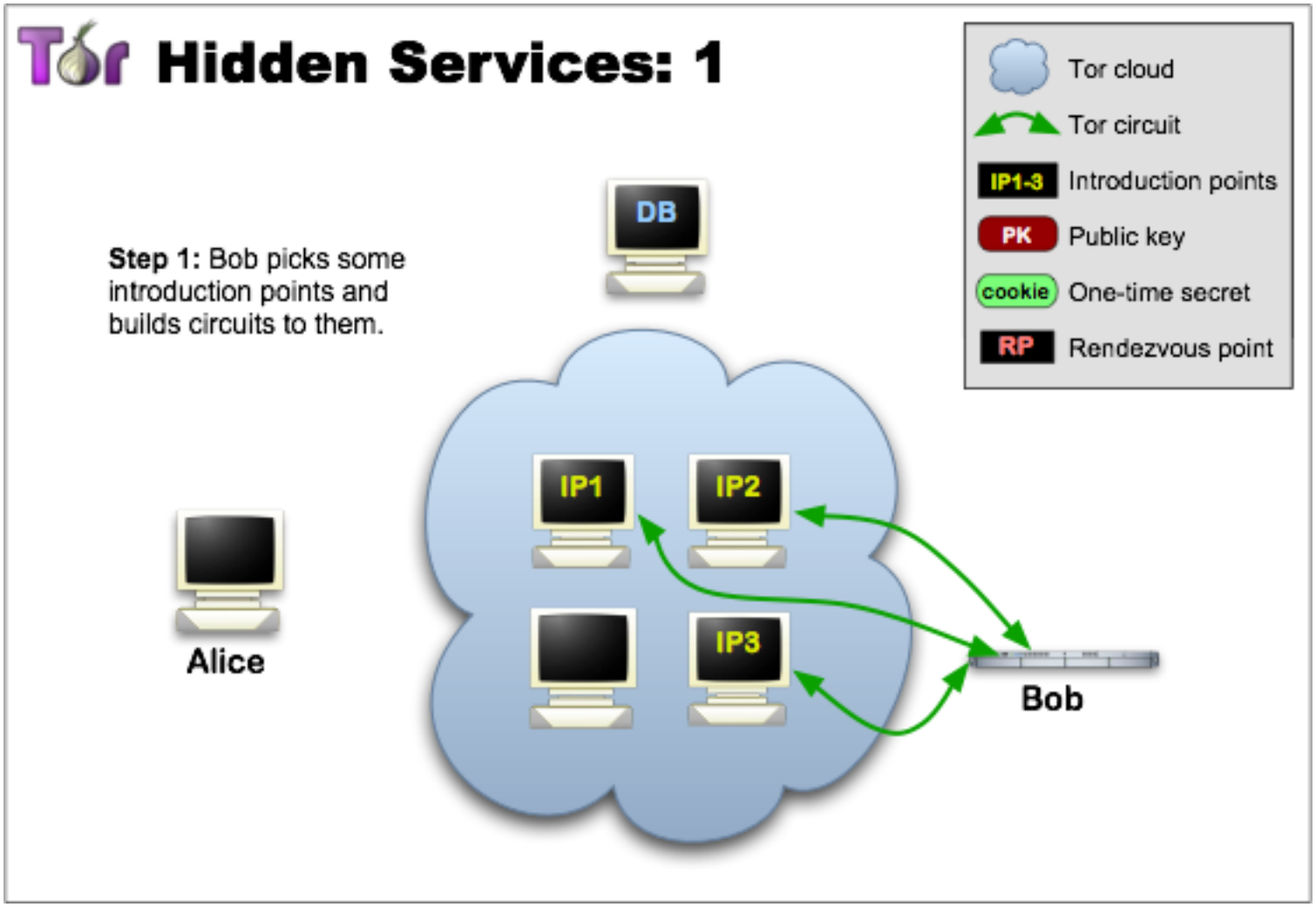
Tor – how Tor works?



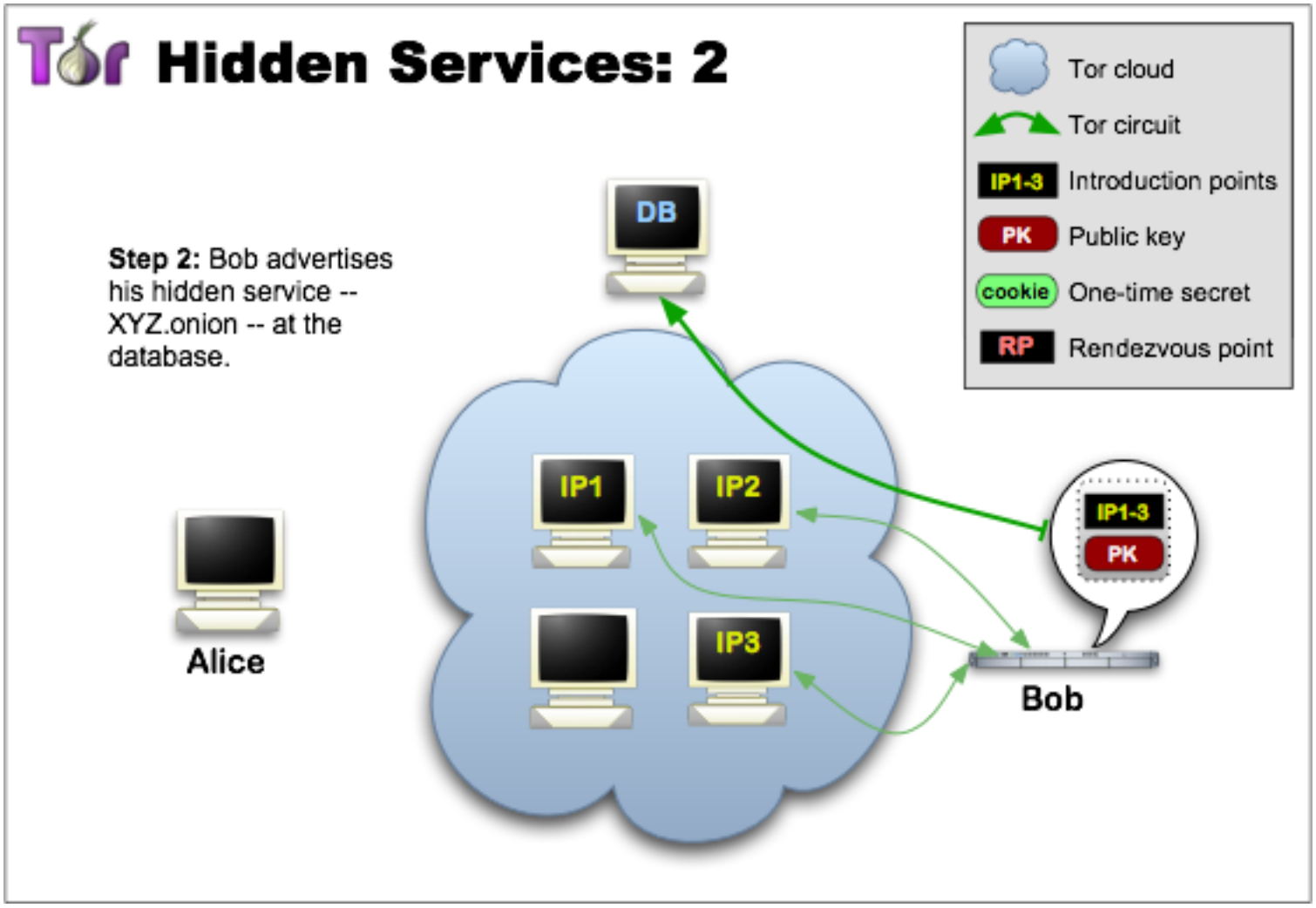
Tor – how Tor works?



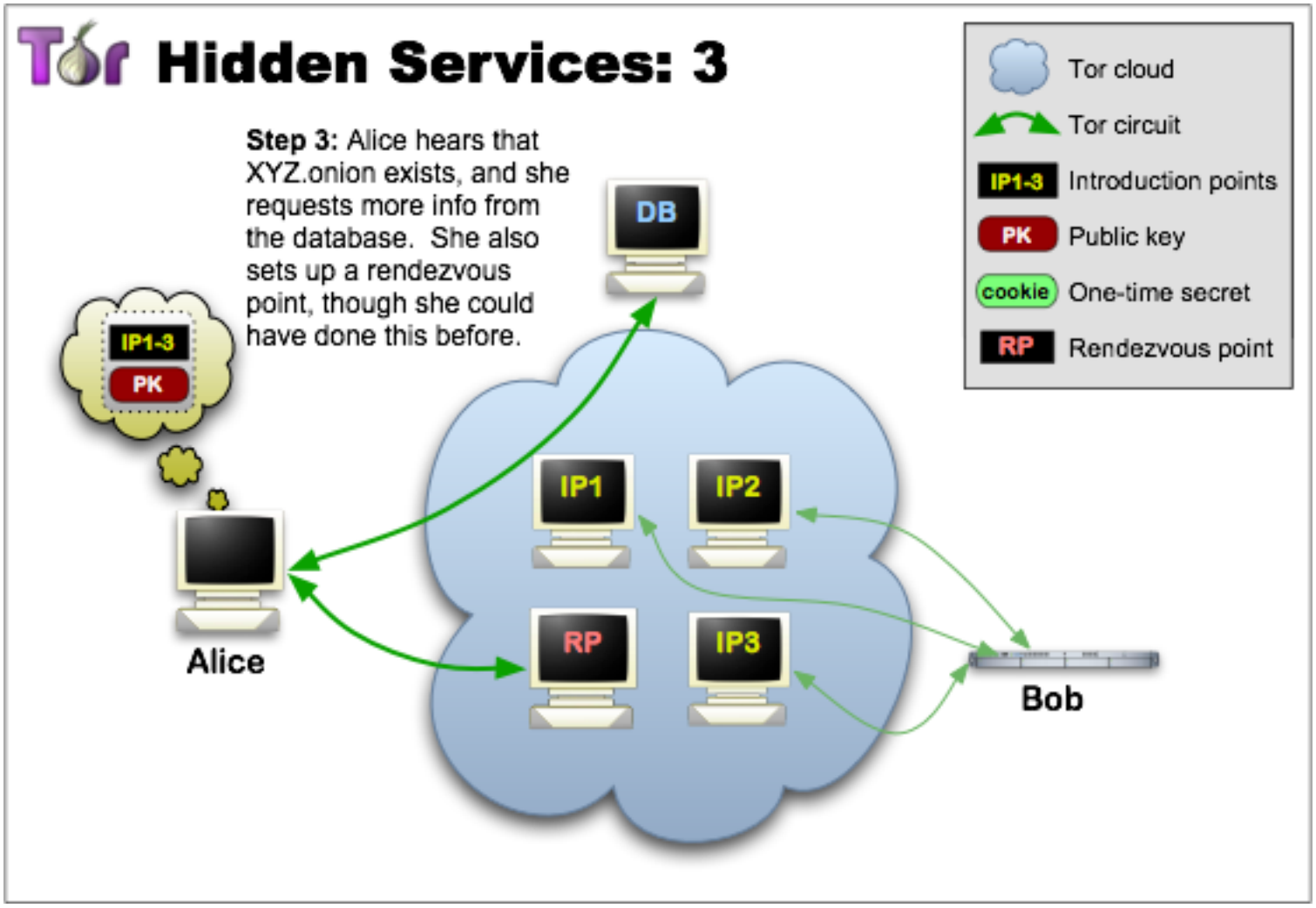
Tor – hidden services



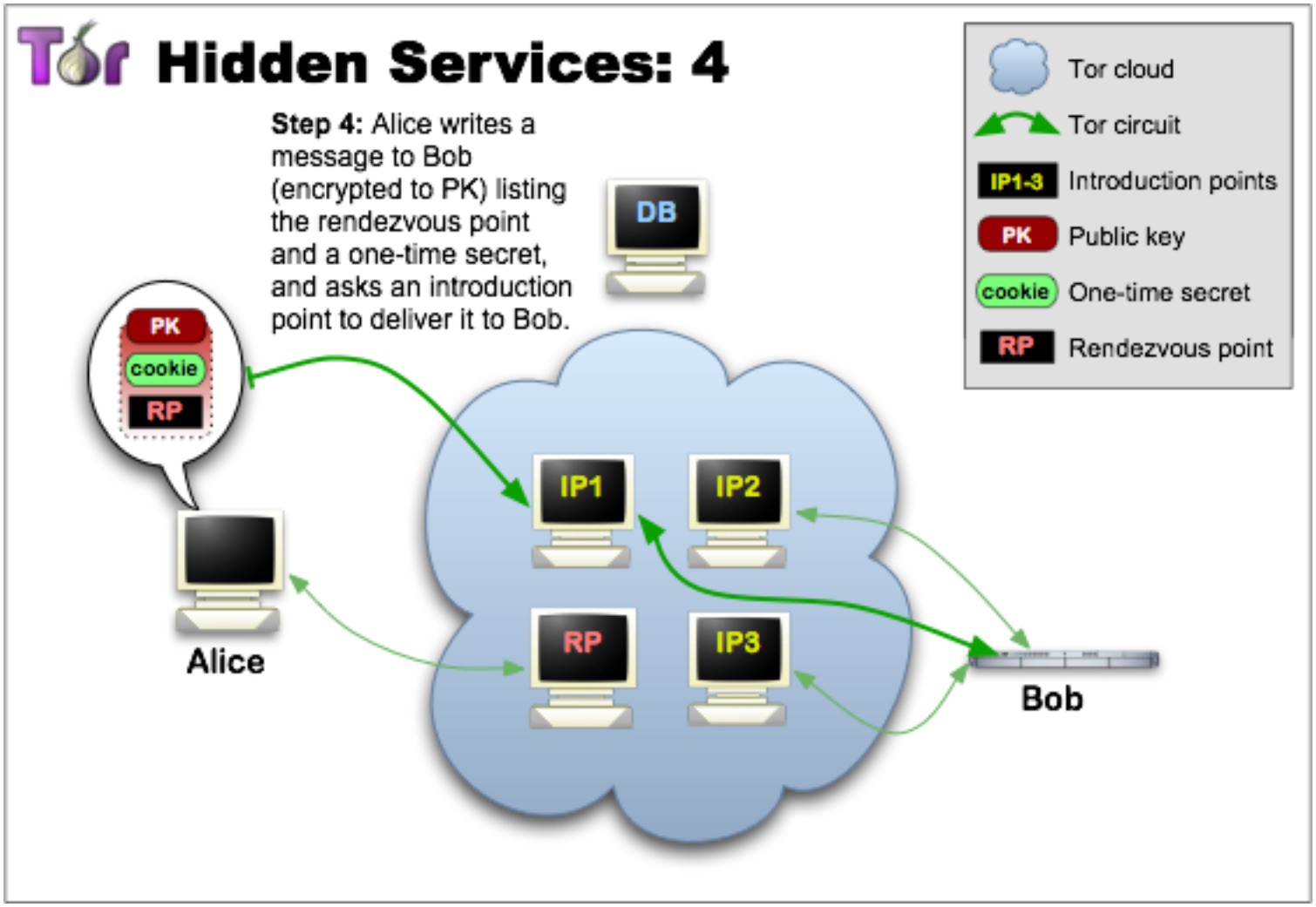
Tor – hidden services



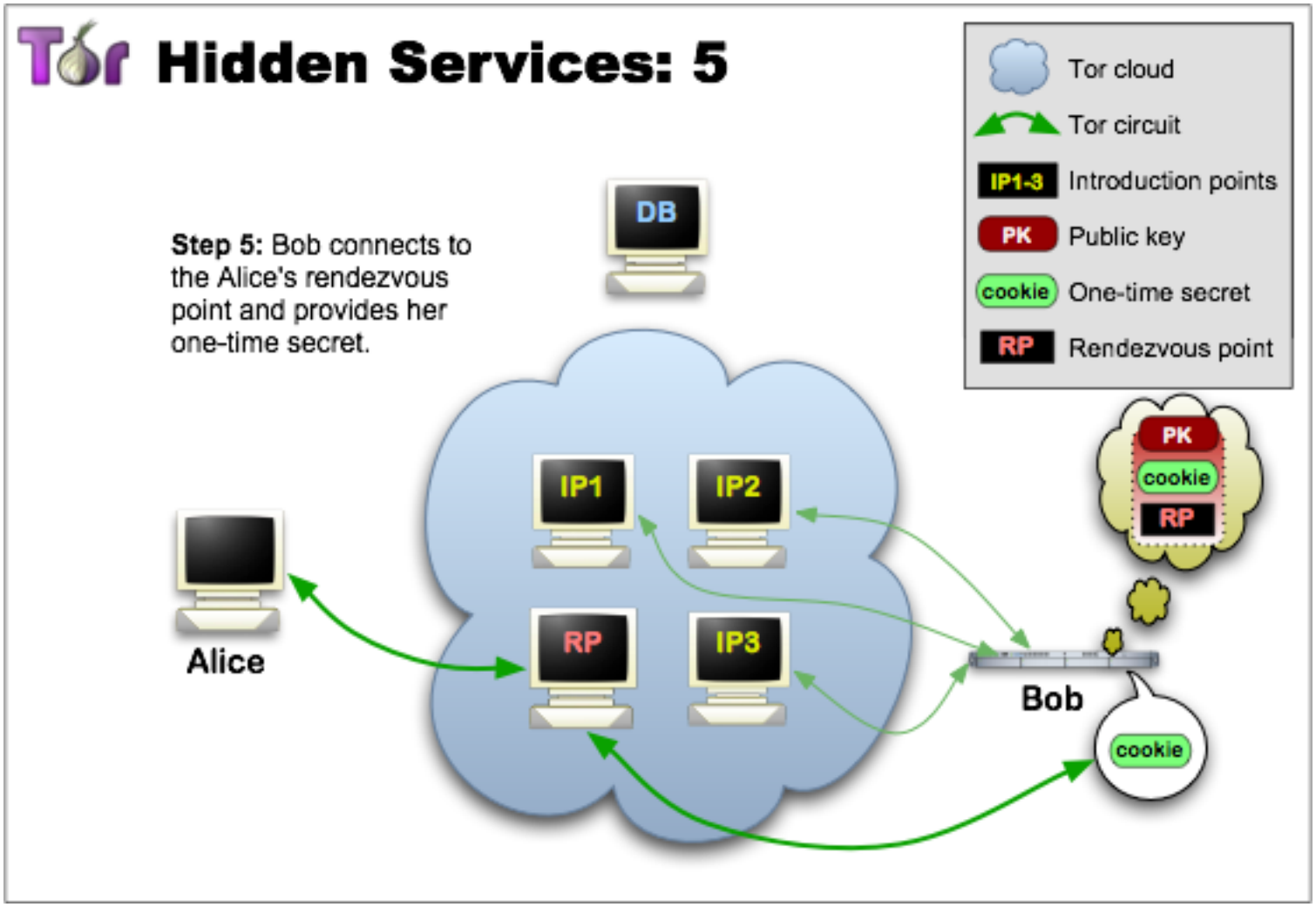
Tor – hidden services



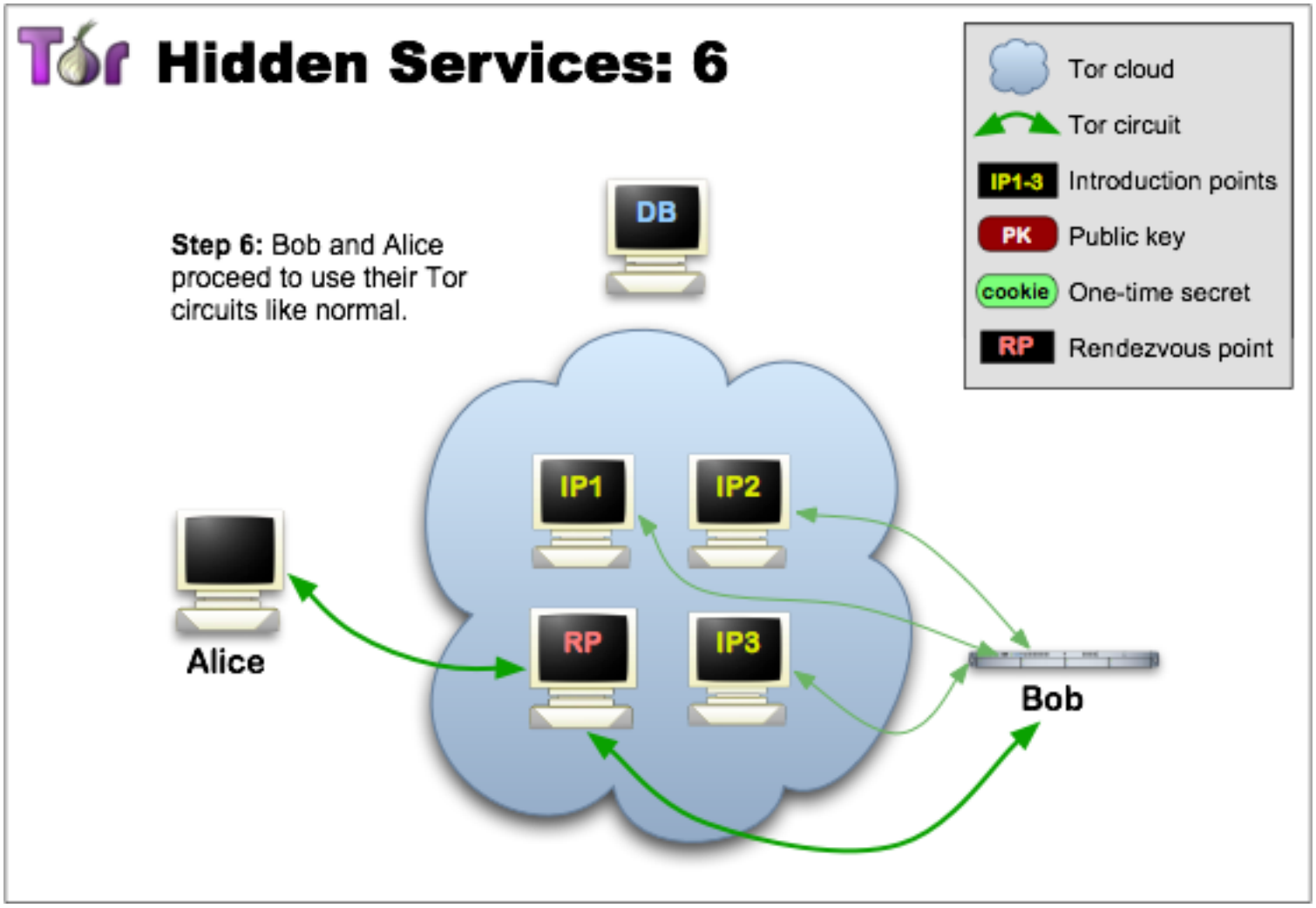
Tor – hidden services



Tor – hidden services



Tor – hidden services



Tor – users

Social Media

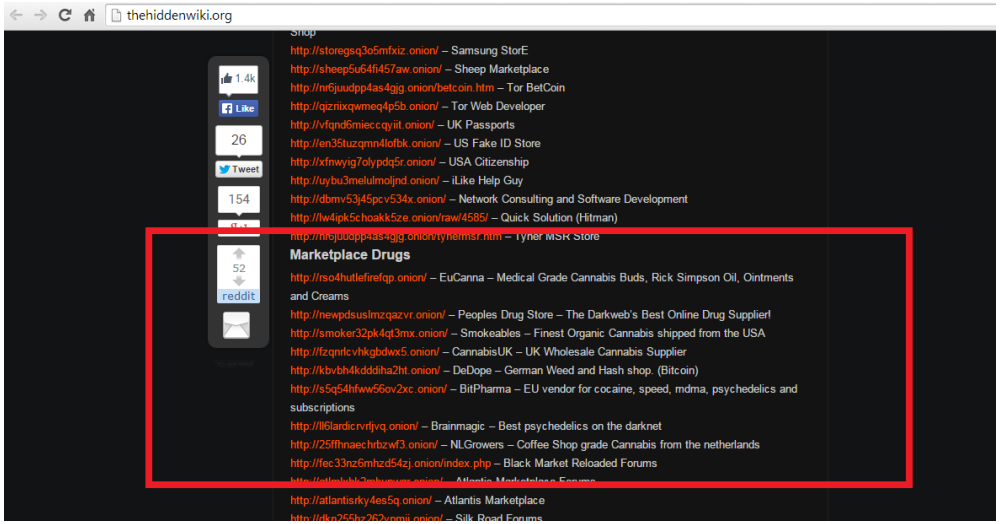
FOLLOW MASHABLE >

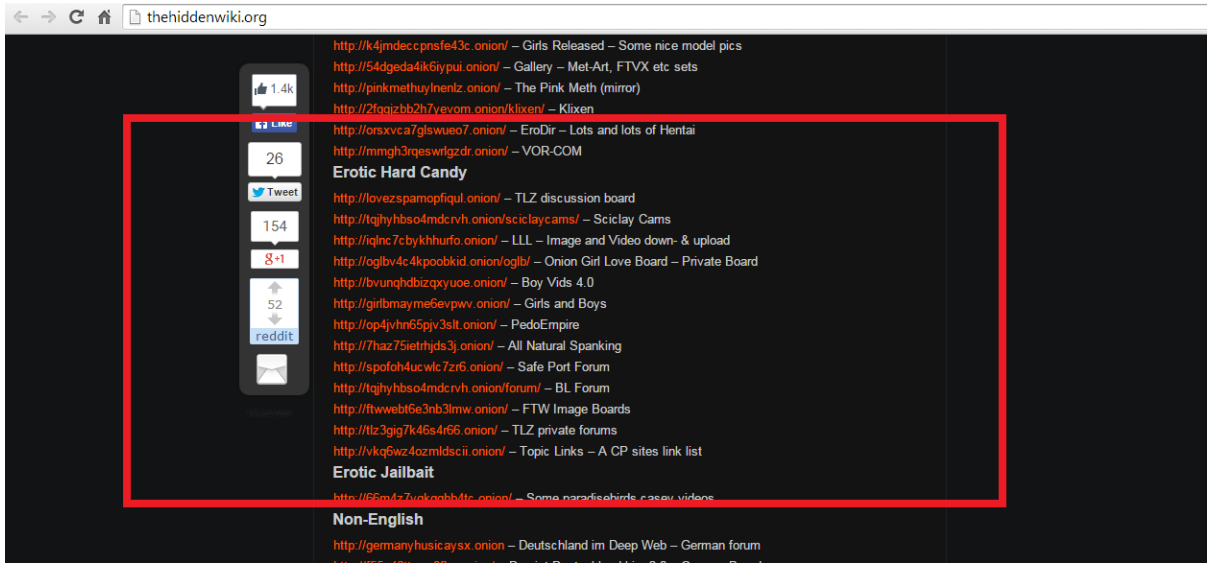
Tor Project Wins Award for Role in Middle East Revolutions

2.4k
SHARES

Share on Facebook | Share on Twitter | +

Tor – users


thehiddenwiki.org
http://storegsq3o5mfxiz.onion/ – Samsung StorE
http://sheep5u64fi457aw.onion/ – Sheep Marketplace
http://nr6juudpp4as4gjg.onion/betcoin.htm – Tor BetCoin
http://qiznixqwmeq4p5b.onion/ – Tor Web Developer
http://vfqnd6mieccqyiit.onion/ – UK Passports
http://en35tuzqmn4lofbk.onion/ – US Fake ID Store
http://xfnwyig7olypdq5r.onion/ – USA Citizenship
http://uybu3melulmoljnd.onion/ – iLike Help Guy
http://dbmv53j45pcv534x.onion/ – Network Consulting and Software Development
http://lw4ipk5choakk5ze.onion/raw/4585/ – Quick Solution (Hitman)
Marketplace Drugs
http://rso4hutlefirefqp.onion/ – EuCanna – Medical Grade Cannabis Buds, Rick Simpson Oil, Ointments and Creams
http://newpdsuslmzqazvr.onion/ – Peoples Drug Store – The Darkweb's Best Online Drug Supplier!
http://smoker32pk4qt3mx.onion/ – Smokeables – Finest Organic Cannabis shipped from the USA
http://fzqnrlcvhkgbdwx5.onion/ – CannabisUK – UK Wholesale Cannabis Supplier
http://kbvbh4kdddiha2ht.onion/ – DeDope – German Weed and Hash shop. (Bitcoin)
http://s5q54hfww56ov2xc.onion/ – BitPharma – EU vendor for cocaine, speed, mdma, psychedelics and subscriptions
http://ll6lardicvrljvq.onion/ – Brainmagic – Best psychedelics on the darknet
http://25ffhnaechrbzwf3.onion/ – NLGrowers – Coffee Shop grade Cannabis from the netherlands
http://fec33nz6mhzd54zj.onion/index.php – Black Market Reloaded Forums
http://atlantisrky4es5q.onion/ – Atlantis Marketplace
1.4k
Like
26
Tweet
154
52
reddit


thehiddenwiki.org
http://k4jmdeccpnsfe43c.onion/ – Girls Released – Some nice model pics
http://54dgeda4ik6iypui.onion/ – Gallery – Met-Art, FTVX etc sets
http://pinkmethuylnenlz.onion/ – The Pink Meth (mirror)
http://2fqqjzbb2h7yevom.onion/klixen/ – Klixen
http://orsxvca7glswueo7.onion/ – EroDir – Lots and lots of Hentai
http://mmgh3rqeswrlgzdr.onion/ – VOR-COM
Erotic Hard Candy
http://lovezspamopfiqul.onion/ – TLZ discussion board
http://tqjhyhbso4mdcrvh.onion/sciclaycams/ – Sciclay Cams
http://iqlnc7cbykhhurfo.onion/ – LLL – Image and Video down- & upload
http://oglbv4c4kpoobkid.onion/oglb/ – Onion Girl Love Board – Private Board
http://bvunqhdbizqxyuoe.onion/ – Boy Vids 4.0
http://girlbmayme6evpwv.onion/ – Girls and Boys
http://op4jvhn65pjv3slt.onion/ – PedoEmpire
http://7haz75ietrhjds3j.onion/ – All Natural Spanking
http://spofoh4ucwlc7zr6.onion/ – Safe Port Forum
http://tqjhyhbso4mdcrvh.onion/forum/ – BL Forum
http://ftwwebt6e3nb3lmw.onion/ – FTW Image Boards
http://tlz3gig7k46s4r66.onion/ – TLZ private forums
http://vkq6wz4ozmldscii.onion/ – Topic Links – A CP sites link list
Erotic Jailbait
Non-English
http://germanyhusicaysx.onion – Deutschland im Deep Web – German forum
1.4k
Like
26
Tweet
154
+1
52
reddit

Tor [background]

1995.

"As military grade communication devices increasingly depend on the public communications infrastructure, it is important to use that infrastructure in ways that are resistant to traffic analysis. It may also be useful to communicate anonymously, for example when gathering intelligence from public databases"

Naval Research Labs Review,1997

Tor [background]

- Techincal solution not enough

“The United States government can’t simply run an anonymity system for everybody and then use it themselves only. Because then every time a connection came from it people would say, ‘Oh, it’s another CIA agent.’ If those are the only people using the network.”

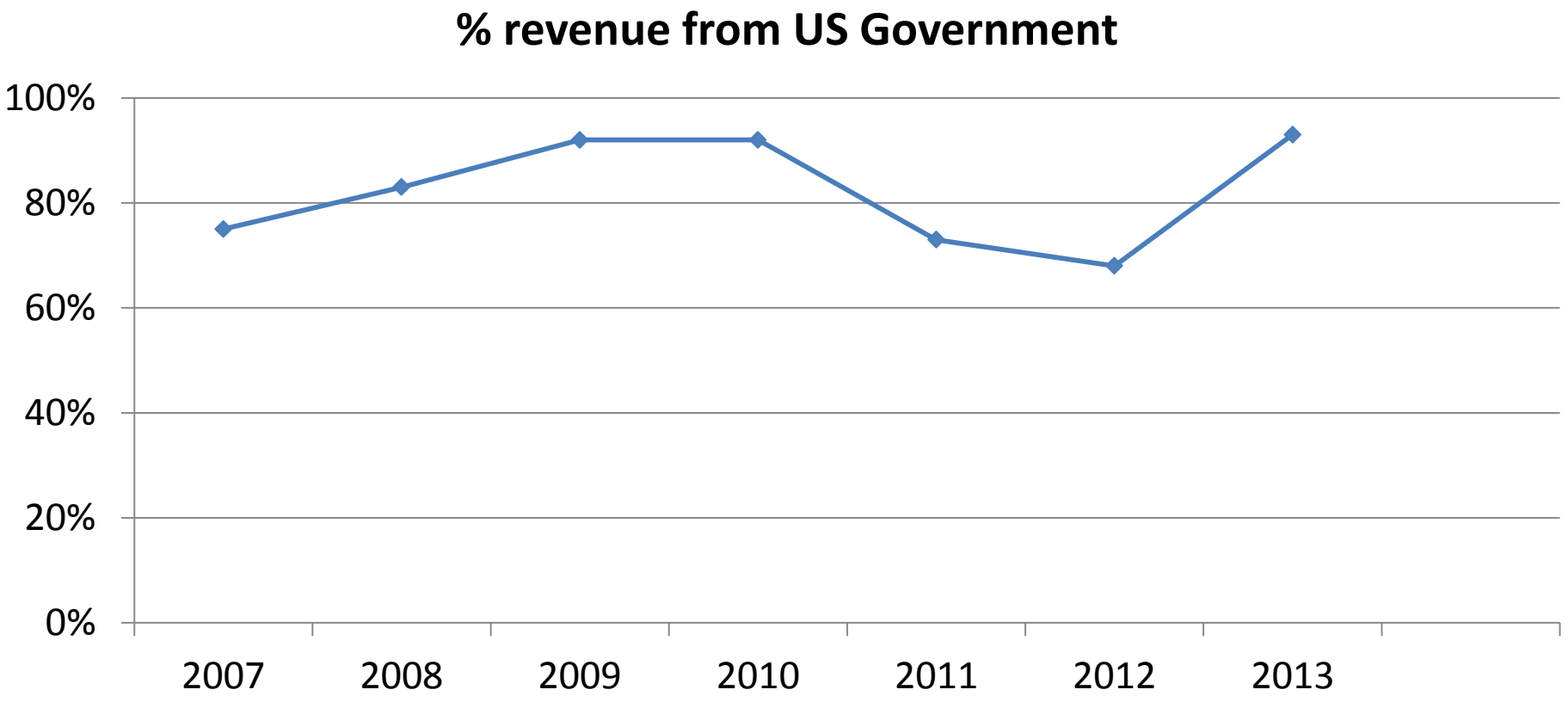
Tor [background]

2004.

- TOR ready for deployment
- Relased as Open Source
- Electronic Frontier Foundation

Tor [background]

2004.---



Tor [background]

- Using, trying to „crack” and fund – at the same time!

- Runing an exit node
- Big (expensive) nodes
- Washington DC

Tor [background]

- Fast nodes first
- 2005. „tricky design question”
- 2012. explanation

„(...) *if we want to end up with a fast safe network, do we get there by having a slow safe network and hoping it'll get faster, or by having a fast less-safe network and hoping it'll get safer? We opted for the "if we don't stay relevant to the world, Tor will never grow enough" route.*”

Famous takedowns

- Botnets /Adult sites /Black markets
- 2013.Freedom Hosting
- JavaScript & Firefox
- „One purpose” based malware

Famous takedowns

- 2013.Silk Road
- On-line store
- Island IP
- Surface web CAPTCHA
- Not likely!
- „economic” impacts

Famous takedowns

- 2015.Ulbricht convicted
- Lessons learned
  - just a platform
    - "*Silk Road was specifically and intentionally designed for the purpose of facilitating unlawful transactions*,"
  - money laundering
    - „Is BitCoin Money? Yes!"
  - Crack House Statute
    - „*This is not an ordinary dwelling, but a drug dealer's 'dream house.*"

Famous takedowns

- Investigation legit?
  - Island teritory
  - Ulbricht not owner
  - „*systems may be monitored for all lawful purposes, including to ensure that use is authorized*.”

- „Fourth Amendment”
  - “Because the SR Server was located outside the United States, the Fourth Amendment would not have required a warrant to search the server, whether for its IP address or otherwise,,”
- Catch 22
  - No possesion, no privacy

Take aways

- Just to raise some questions
- Internet of things
- Popcorn and the front row!


THANK
YOU
GRACIAS
ARIGATO
SHUKURIA
JUSPAXAR
BOLZÏN
MERCI
BÏYAN
SHUKRIA
DANKSCHEEN
TASHAKKUR ATU
YAQHANYELAY
TINGKI
SUKSAMA
EKHMET
MEHRBANI
GRAZIE
MAAKE
KOMAPSUMNIDA
GOZAIMASHITA
EFCHARISTO
PALDIES
SPASSIBO
NUHUN
SNACHALHUYA
CHALTU
WABEEJA
MAITEKA
YUSPAGARÀTAM
HUI
GUI
HATUR
DHANYABAAD
AHHIA
ATTO
MERSI
SPASIBO
DENKAUJA
NENACHALHYA
UNALCHÉESH
EKOJU
SIKOMO
MAKETAI
MINMONCHAR
SANCO
MERASTAWHY
GAEJTHO
LAH
TAVTAPUCH
MEDAWAGSE
AGUYJE
FAKAAUE
BAJIKA