NYM

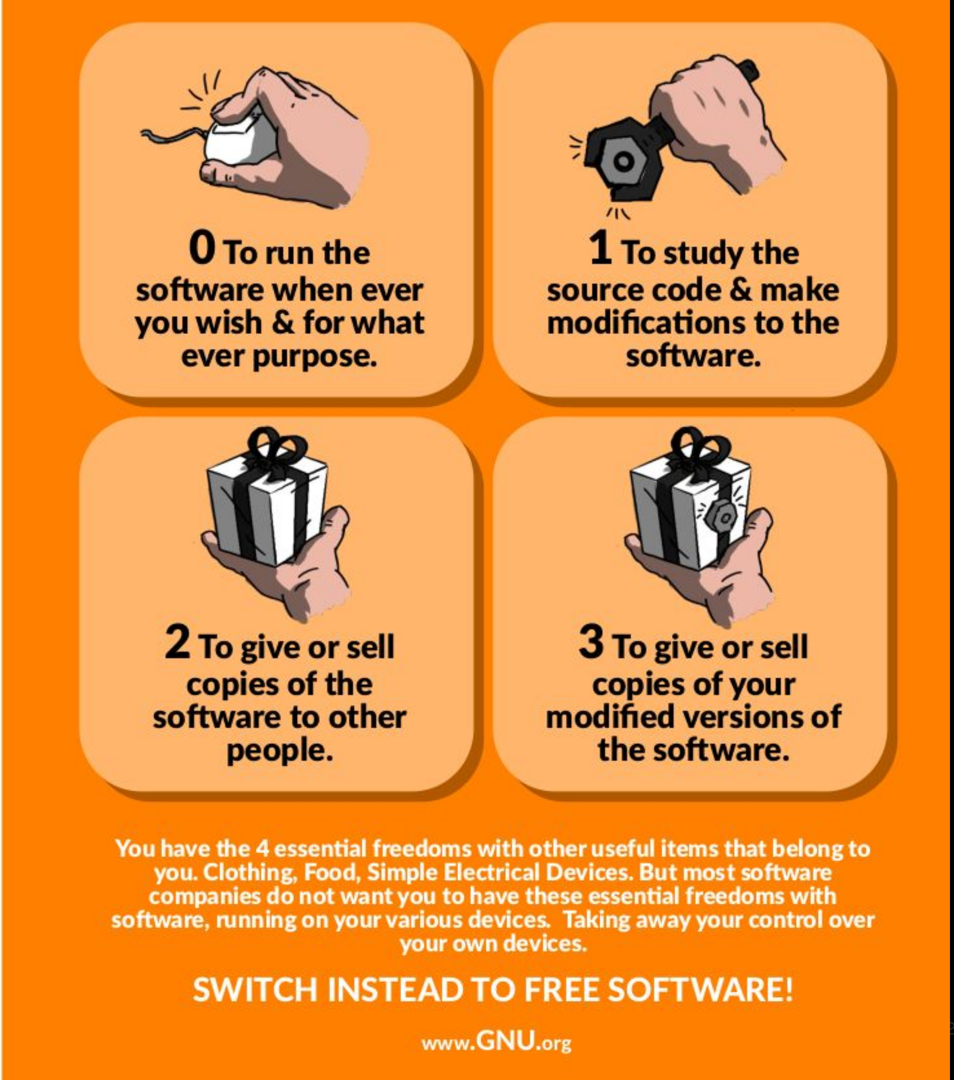
Network-Layer Privacy

Free Software to End Mass Surveillance

Ahmed Ghappour
General Counsel, NYM Technologies

Four Freedoms

…and freedom from surveillance



0 To run the software when ever you wish & for what ever purpose.

1 To study the source code & make modifications to the software.

2 To give or sell copies of the software to other people.

3 To give or sell copies of your modified versions of the software.

You have the 4 essential freedoms with other useful items that belong to you. Clothing, Food, Simple Electrical Devices. But most software companies do not want you to have these essential freedoms with software, running on your various devices. Taking away your control over your own devices.

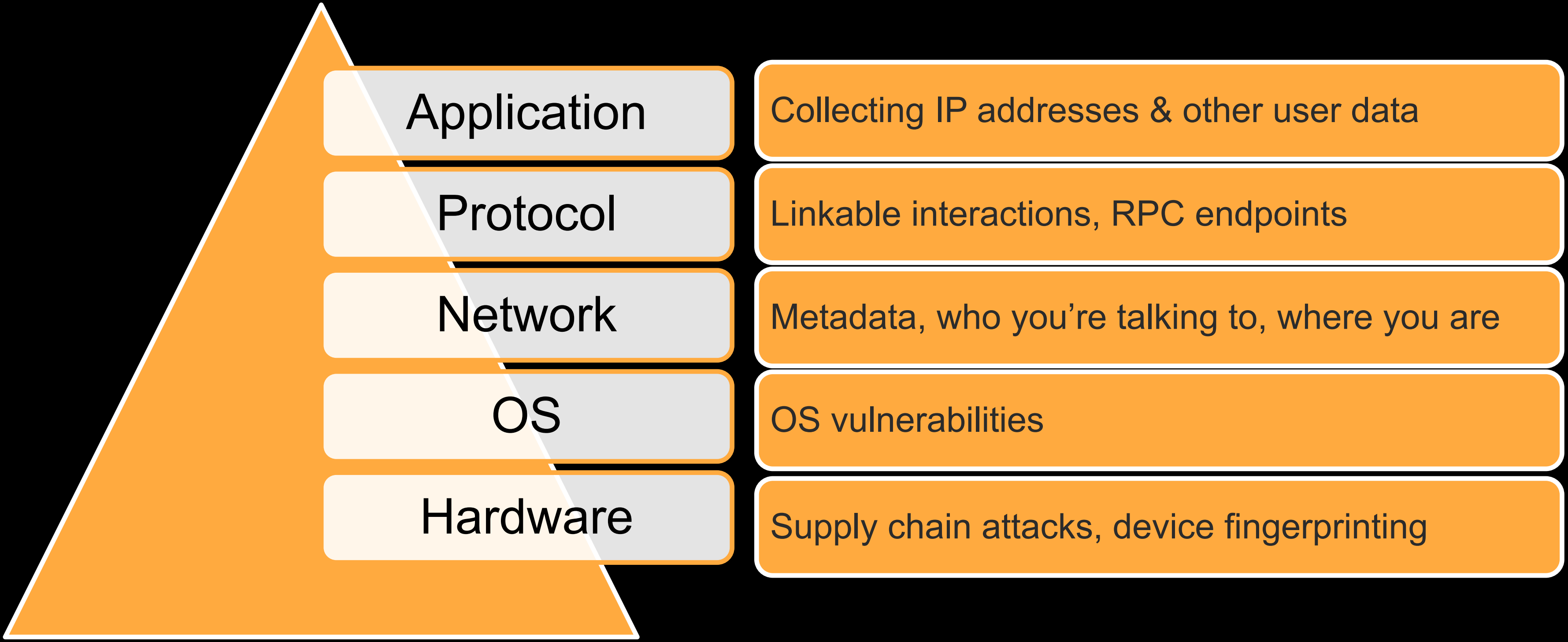
SWITCH INSTEAD TO FREE SOFTWARE!

www.GNU.org

Four Freedoms …and freedom from surveillance

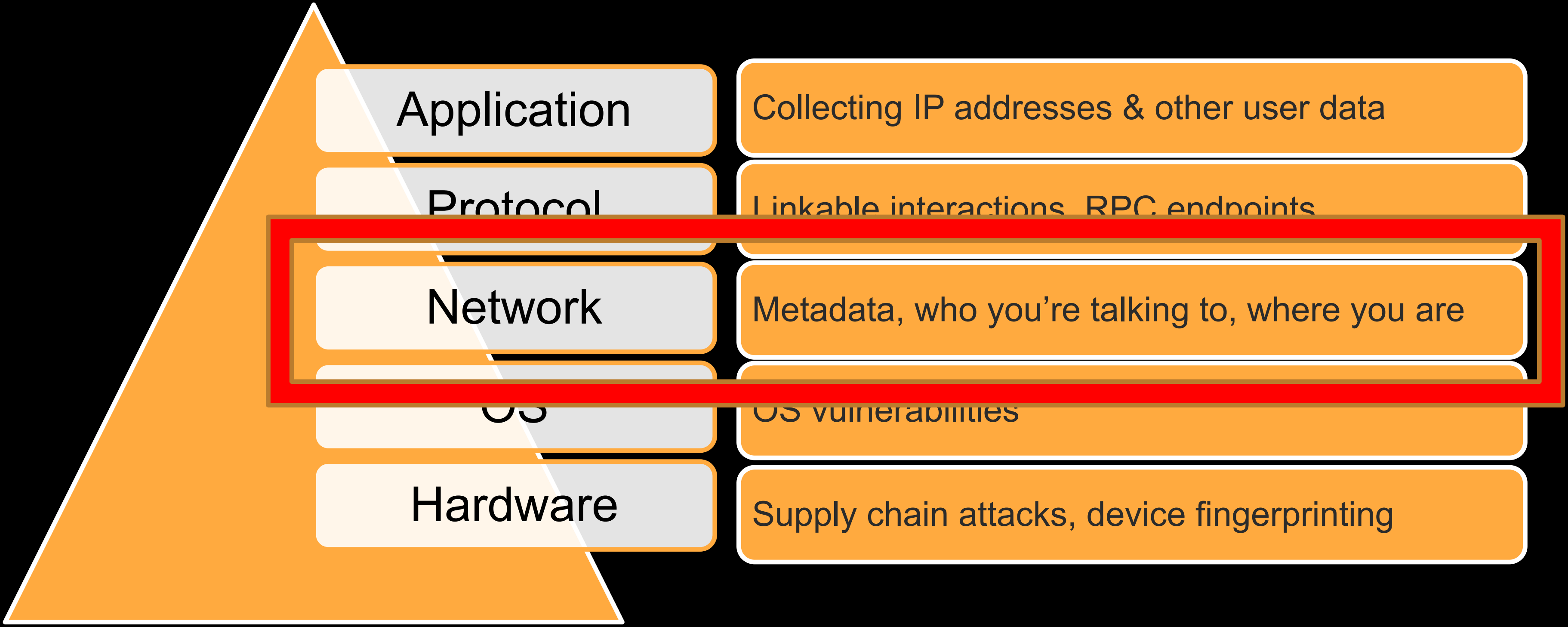
1. The freedom to run the program as you wish, for any purpose.
2. The freedom to study how the program works, and change it so it does your computing as you wish. ...
3. The freedom to redistribute copies so you can help your neighbor.
4. The freedom to distribute copies of your modified versions to others.

Privacy Across the Stack



Application	Collecting IP addresses & other user data
Protocol	Linkable interactions, RPC endpoints
Network	Metadata, who you’re talking to, where you are
OS	OS vulnerabilities
Hardware	Supply chain attacks, device fingerprinting

Privacy Across the Stack



Application – Collecting IP addresses & other user data

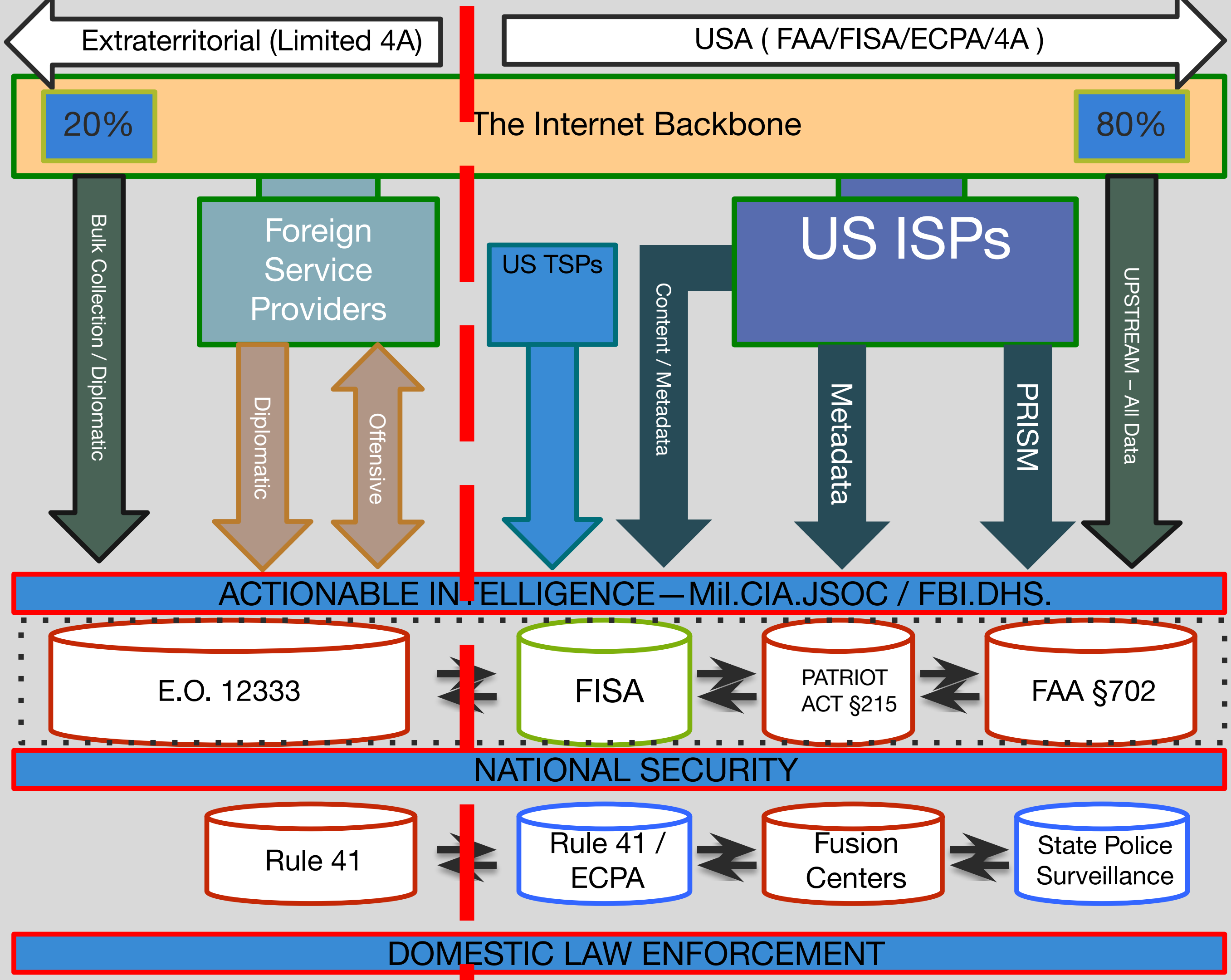
Protocol – Linkable interactions, RPC endpoints

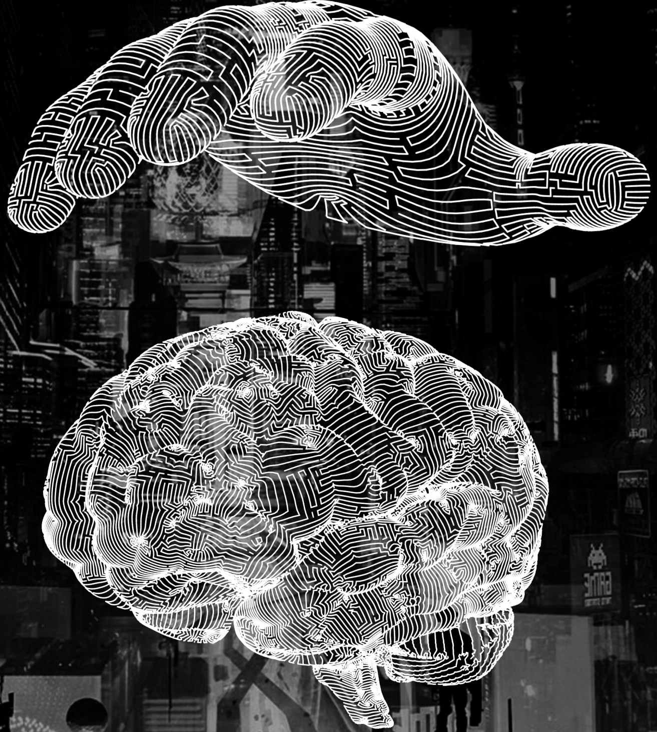
Network – Metadata, who you're talking to, where you are

OS – OS vulnerabilities

Hardware – Supply chain attacks, device fingerprinting

[The internet is broken]


Extraterritorial (Limited 4A)
USA (FAA/FISA/ECPA/4A)
20%
The Internet Backbone
80%
Bulk Collection / Diplomatic
Foreign Service Providers
Diplomatic
Offensive
US TSPs
Content / Metadata
US ISPs
Metadata
PRISM
UPSTREAM – All Data
ACTIONABLE INTELLIGENCE—Mil.CIA.JSOC / FBI.DHS.
E.O. 12333
FISA
PATRIOT ACT §215
FAA §702
NATIONAL SECURITY
Rule 41
Rule 41 / ECPA
Fusion Centers
State Police Surveillance
DOMESTIC LAW ENFORCEMENT

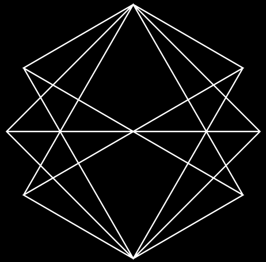


No existing solution can defend against the NSA and private companies

Metadata leaks at the network level, even with encrypted messages apps like Signal or zero-knowledge cryptocurrencies like ZCash

VPNs (including dVPNs) provide no actual anonymity. Centralized VPNs just move trust.

Tor doesn’t provide anonymity against adversaries that can monitor the whole network. Obfuscates only the IP address.



SOLUTION PART 1

Nym mixnet

Scalable, tunable latency, and generic: As fast and private as required by any app

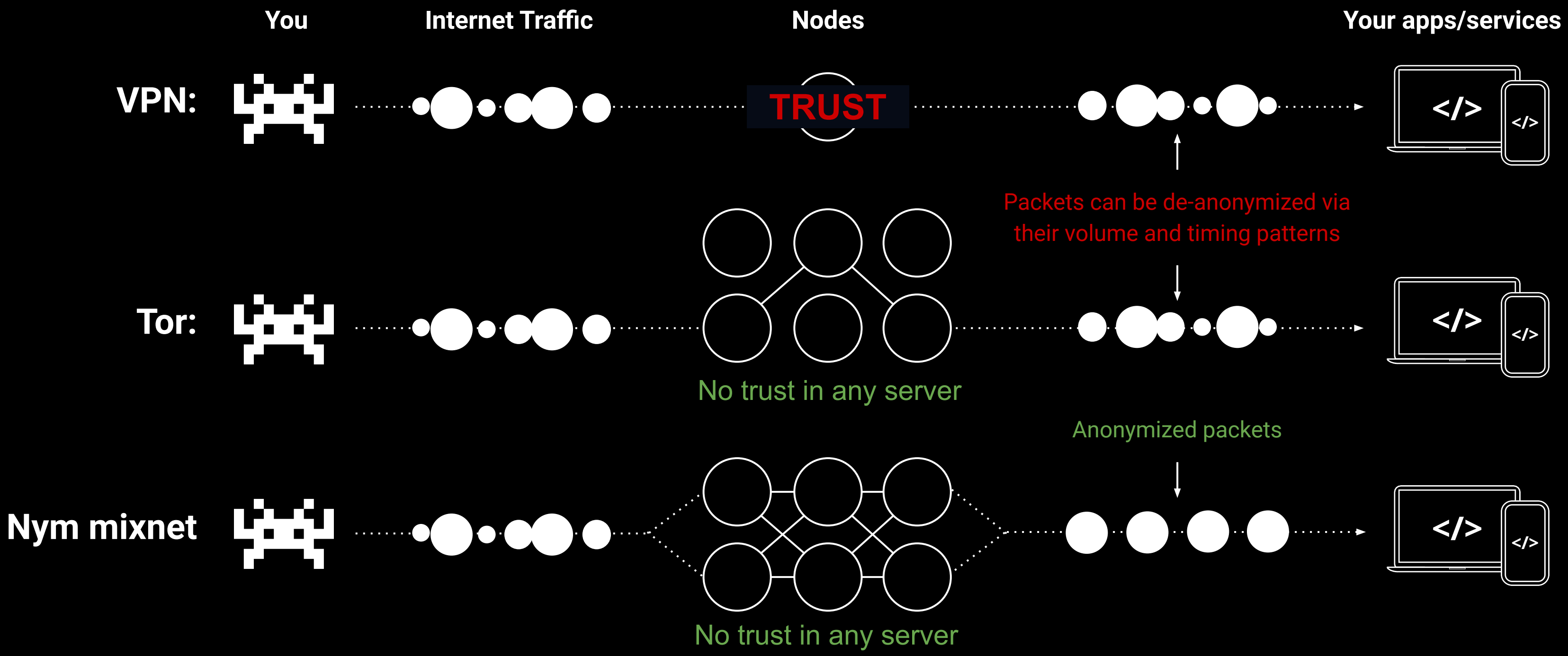
1. **Multiple hops**
   Traffic routed through multiple nodes to unlink origin and destination (IP address), like Tor.

2. **Cover traffic**
   Prevents traffic analysis via adding cover (‘dummy’) traffic, with less needed as more real traffic enters the network, unlike Tor.

3. **Timing obfuscation**
   Packets re-ordered at each hop prevents traffic de-anonymization.

4. **Horizontal scalability**
   Nym mixnet can expand to allow for more traffic by adding nodes dynamically

Nym mixnet comparison



Mixnet clients

There are numerous different scenarios in which developers can integrate Nym software to privacy-enhance their applications - and there are different Nym Clients to choose from for each

1. **Websockets Client**
   Standalone binary that runs on desktop or server machines. Can always compile it yourself! You can also do a **native integration in your codebase**!

2. **WebAssembly Client**
   Useful for browser applications. Packaged via NPM for import into Typescript or Javascript apps.

3. **SOCKS5 Client**
   Useful for allowing existing applications to use the mixnet without any code changes. All that's necessary is that they can use a SOCKS5 proxy - **integrates on anything that works with Tor!**

SOCKS5 client

Support for SOCKS5 is fairly standard - using this client is the best way to quickly begin to send application traffic through the mixnet without needing to do any code changes.

Anything that works on Tor should work on Nym!

1. **Application to proxy**
   Any application that has support for Socks5 (IRC, Signal, Telegram, crypto wallets, email clients, etc). Send traffic to your local nym-socks5-client instance for proxying through the mixnet.

2. **Local SOCKS5 client instance**
   The binary that will accept application traffic and send this traffic to a Network Requester on the 'other side' of the mixnet.

3. **Network Requester**
   Run alongside a Nym client on a VPS. Allows for private network requests to be made outside the mixnet from your Desktop machine. *Not* an open proxy. Like Tor **exit node.**

Integration components

So you want to start running app traffic through the mixnet - what components do you have to think about when planning?

1. **Local Client (e.g. NymConnect)**
   Your application requires a Nym client in order to send traffic through the mixnet to the recipient. Packets are all made same size and converted to Sphinx packet format.

2. **(Optional) Service Provider**
   Some code on the ‘other side’ of the mixnet that you are sending messages to: file storage, something to make outbound network requests, etc.

3. **(Optional) Gateway**
   The “first hop” into the mixnet. Although you could use any other public gateway, running your own makes sure your app has better uptime and reliability. Like Tor **entry node**.

Licensing

Used Apache 2.0 to make integration easier because anonymity loves company, and we need more users - not just free software. Yet core components are licensed using GPL/AGPL.

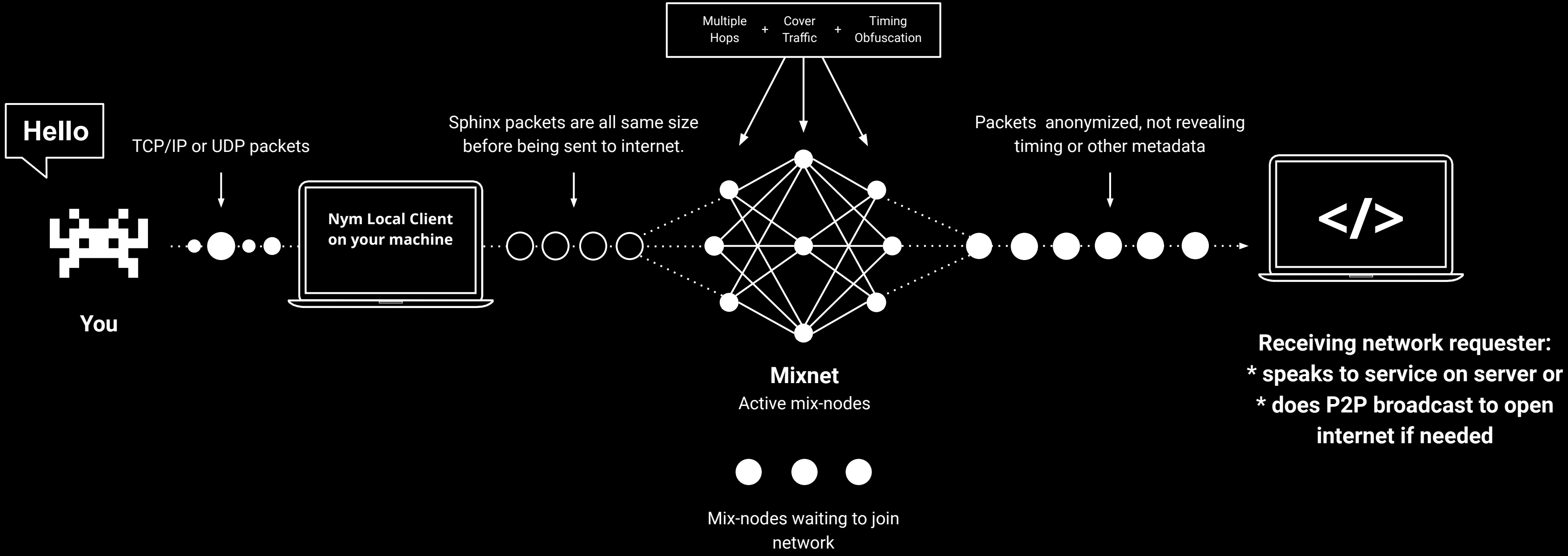
1. **Apache 2.0**
   (best of the rest – integration)
2. **GPL3/AGPL 2.0**
   (core)

@notrustverif

Demo: IRC over Nym Network

1. LimeChat IRC Client
2. Socks 5 Proxy Configuration
3. Nym Connect Local Client
4. Service Provider in Open Proxy Mode

Thanks @NoTrustVerif !



Multiple Hops + Cover Traffic + Timing Obfuscation

Hello

TCP/IP or UDP packets

You

Nym Local Client on your machine

Sphinx packets are all same size before being sent to internet.

Mixnet

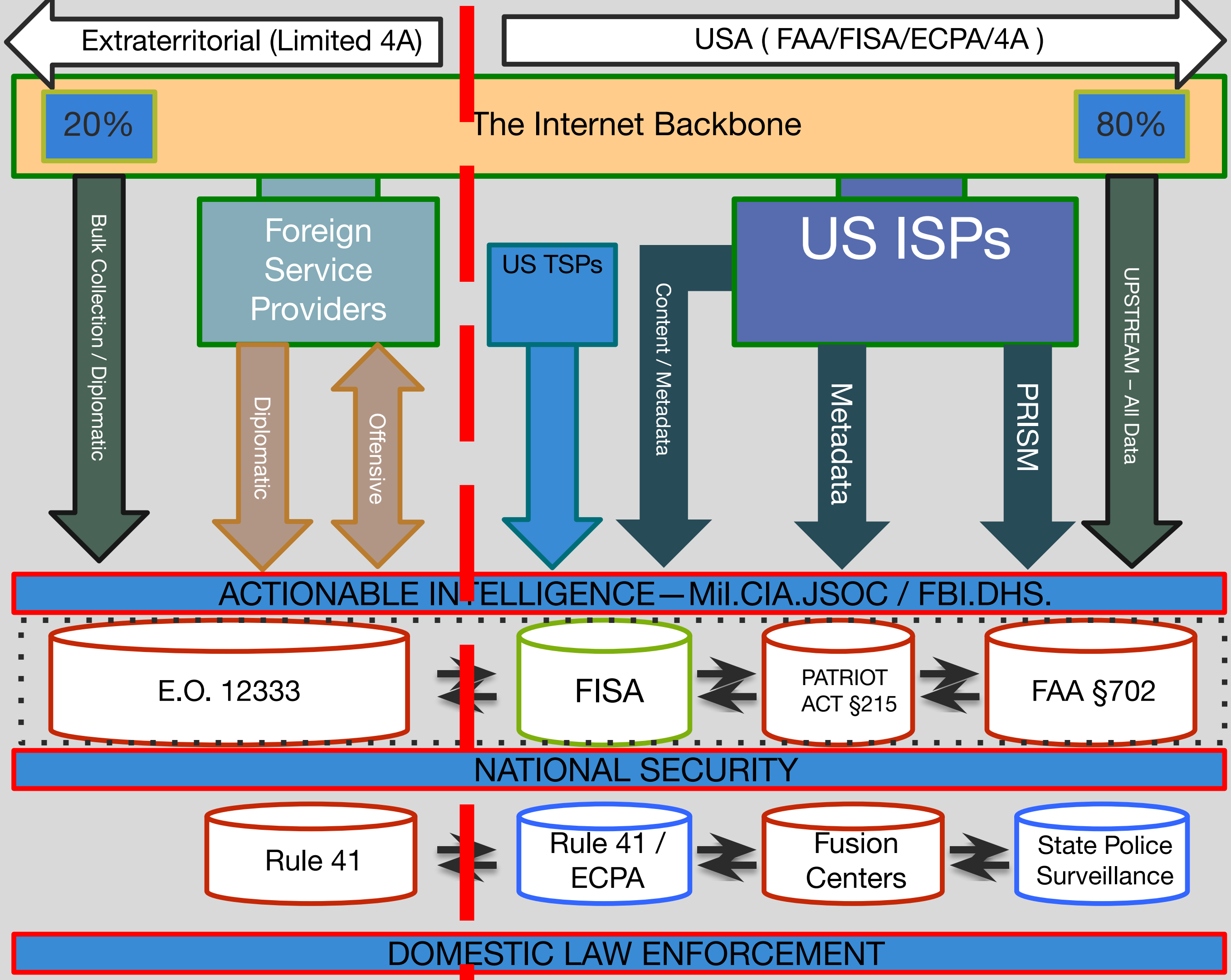
Active mix-nodes

Mix-nodes waiting to join network

Packets anonymized, not revealing timing or other metadata

</>

Receiving network requester:
*** speaks to service on server or**
*** does P2P broadcast to open internet if needed**



Extraterritorial (Limited 4A)

USA (FAA/FISA/ECPA/4A)

20%

The Internet Backbone

80%

Bulk Collection / Diplomatic

Foreign Service Providers

Diplomatic

Offensive

US TSPs

Content / Metadata

US ISPs

Metadata

PRISM

UPSTREAM – All Data

ACTIONABLE INTELLIGENCE—Mil.CIA.JSOC / FBI.DHS.

E.O. 12333

FISA

PATRIOT ACT §215

FAA §702

NATIONAL SECURITY

Rule 41

Rule 41 / ECPA

Fusion Centers

State Police Surveillance

DOMESTIC LAW ENFORCEMENT

NYM

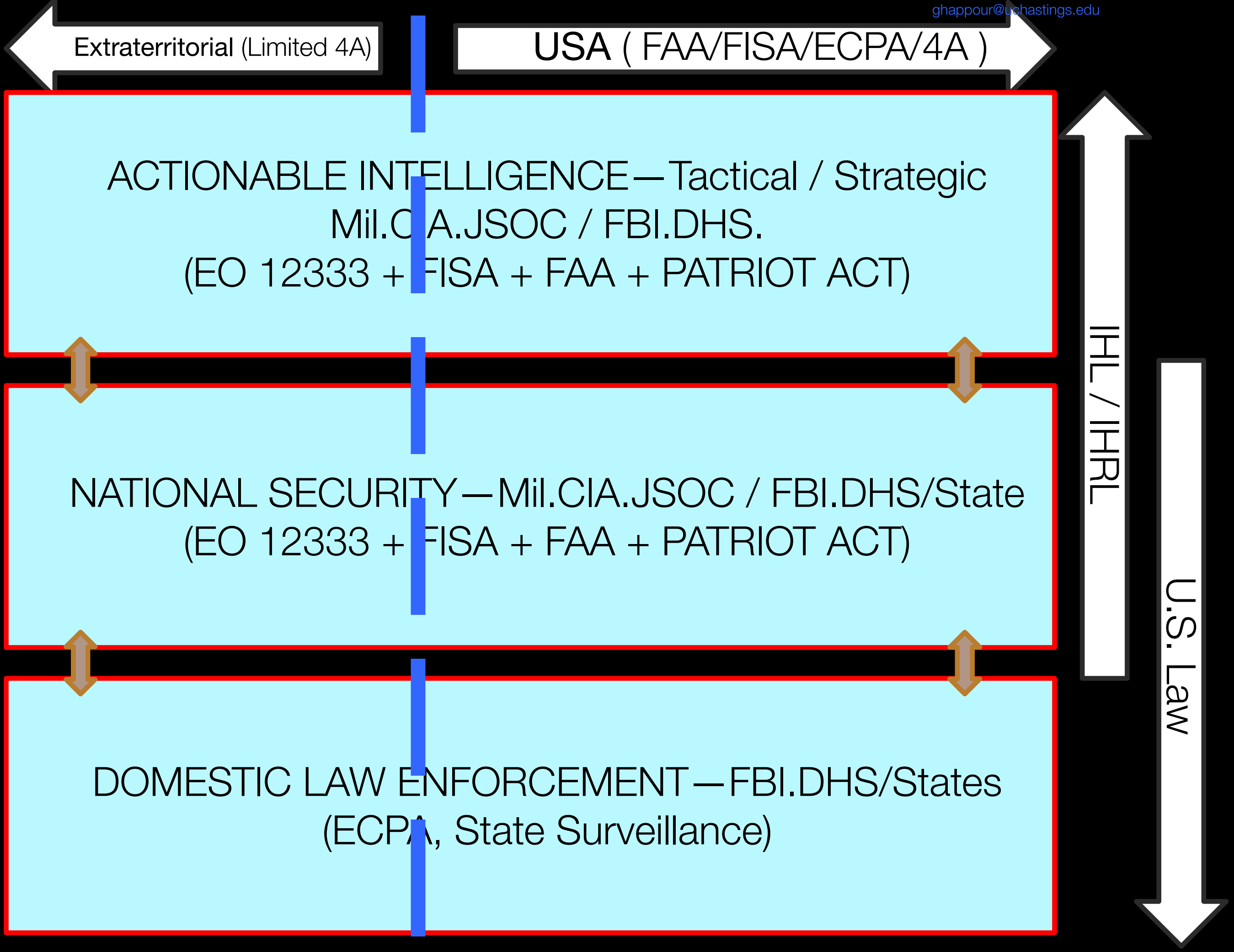
THANK YOU!

Ahmed Ghappour

General Counsel, Nym Technologies

@ghappour ((Twitter, Telegram, Mastodon, etc.))
ahmed@nymtech.net (Email)

@nymproject
@nymtech (Github)



Extraterritorial (Limited 4A)

USA (FAA/FISA/ECPA/4A)

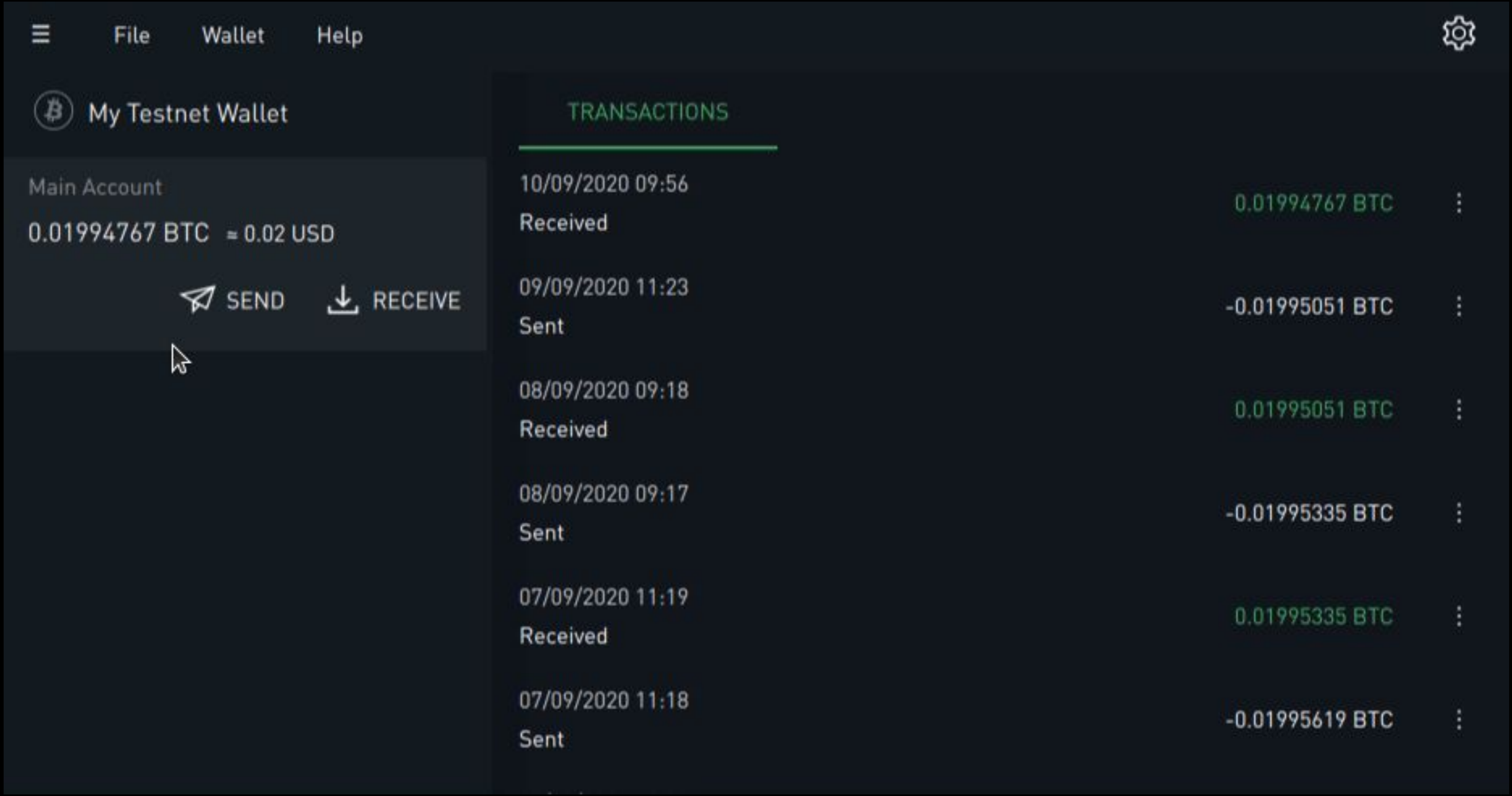
ACTIONABLE INTELLIGENCE—Tactical / Strategic
Mil.CIA.JSOC / FBI.DHS.
(EO 12333 + FISA + FAA + PATRIOT ACT)

NATIONAL SECURITY—Mil.CIA.JSOC / FBI.DHS/State
(EO 12333 + FISA + FAA + PATRIOT ACT)

DOMESTIC LAW ENFORCEMENT—FBI.DHS/States
(ECPA, State Surveillance)

IHL / IHRL

U.S. Law



My Testnet Wallet

Main Account

0.01994767 BTC ≈ 0.02 USD

10/09/2020 09:56 Received	0.01994767 BTC	⋮
09/09/2020 11:23 Sent	-0.01995051 BTC	⋮
08/09/2020 09:18 Received	0.01995051 BTC	⋮
08/09/2020 09:17 Sent	-0.01995335 BTC	⋮
07/09/2020 11:19 Received	0.01995335 BTC	⋮
07/09/2020 11:18 Sent	-0.01995619 BTC	⋮