ISSWorldTraining

ISS World Washington, DC	ISS World Brasilia, BR	ISS World Prague, CZ	ISS World Dubai, UAE	ISS World Kuala Lumpur, MY

TeleStrategies

ISS World

Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering

More Info | More Info | More Info | More Info | More Info

UpcomingWebinars

Geographic Information Available from Cell Phones

WHEN: January 19, 2012
11:00 - 12:00 (Eastern US)

SPONSORED BY: TeleStrategies

More Info | Register

Investigating Online Social Media Influenced Criminal Flash Mobs

WHEN: February 28, 2012
9:00 - 10:30 AM (Eastern US)

SPONSORED BY: TeleStrategies

More Info | Register

Facebook 201: Tools, Tricks & Techniques Investigators Need to Know

WHEN: March 6, 2012
9:00 - 10:30 AM (Eastern US)

SPONSORED BY: TeleStrategies

More Info | Register

The New Art of Surveillance

While bureaucracies used to keep tabs on activists and often make mistakes, the task of surveillance has now been subcontracted to a variety of companies competing to sell governments across the globe the biggest, shiniest databases... And this isn't just stuff gleaned from your public Facebook...

Think malware and spyware. Think coordinated efforts with your ISP. Twitter had the courtesy to tell users when the US govt asked for a list of Wikileaks followers (and demand a subpoena). Just because Facebook and Google haven't said anything of the sort doesn't mean they aren't in collusion with the authorities.

More info: see Wikileaks SpyFiles ... echelon.project-pm.org .... WSJ Surveillance Catalogue

The Future

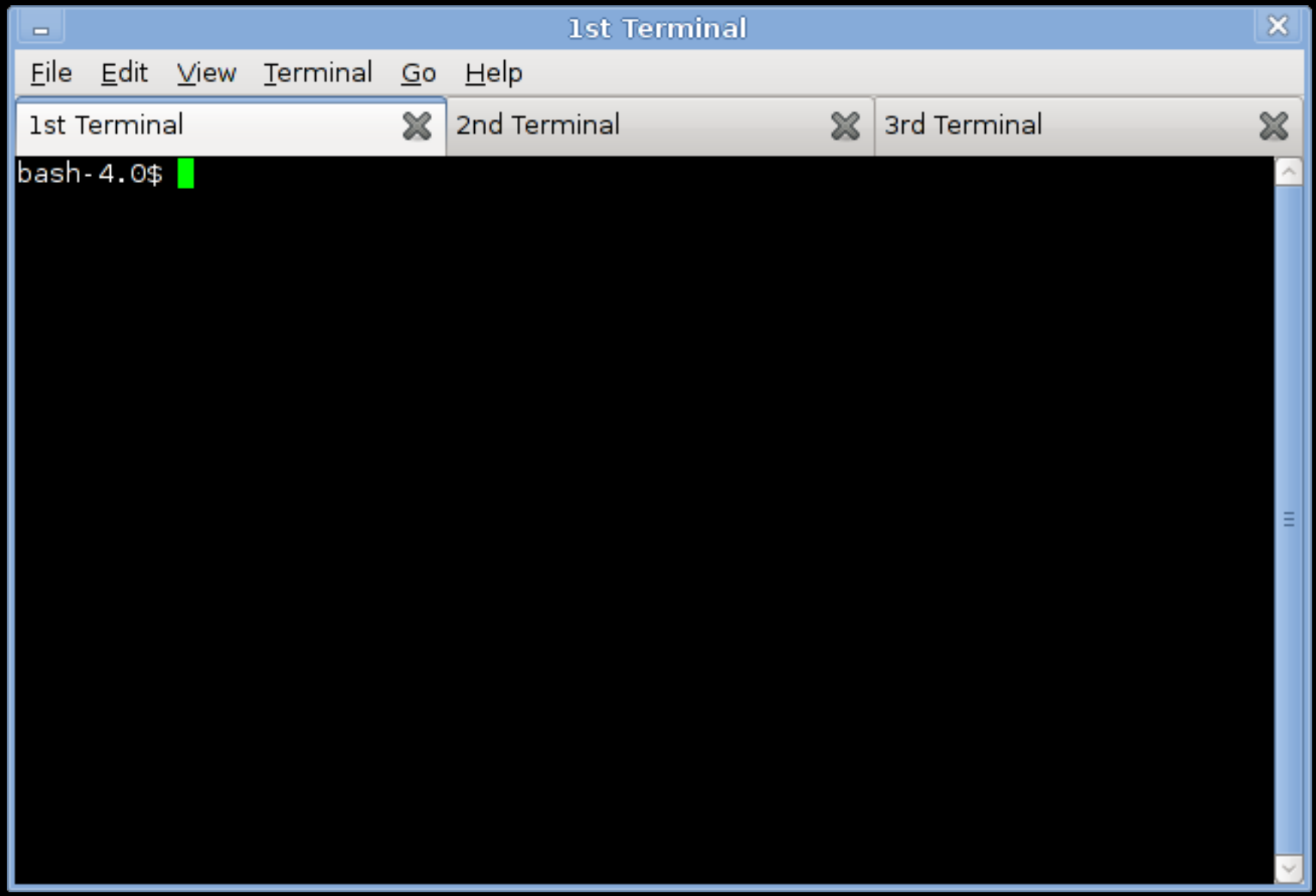
The usefulness of the Internet is always being attacked by people who hate freedom and people who want to turn the entire world into heavily surveiled shopping mall.

Eventually the US govt is going to pass horribly restrictive legislation that will break the back of the Internet; then people will have reason to move to emerging technologies like mesh networks and obsolete ones like BBSes and phone modems.

IN CIPHERSPACE, DREAMS BECOME DARKNETS.


CRYPT
MORPHOSIS
FEATURING...
THE CRYPT-KEEPER
THE OLD WITCH
THE VAULT-KEEPER

PART ONE: HACKTIVISM


1st Terminal
File Edit View Terminal Go Help
1st Terminal
2nd Terminal
3rd Terminal
bash-4.0$

hack (v): *to find and exploit uses in a system that were not originally intended to be provided*

Hacktivism, 3 Takes:

1. exposing information to point out misdeeds of a government or corporate entity
2. contributing to software projects relating to e-anonymity and cipherspace to help others unlock and circulate information.
3. shutting down servers and services (and hence, flows of capital) of corrupt corporate and government entities (DDOS, credit card theft)


<3
DATALOVE

Also see #opBlitzkrieg ... leaks on cops in Arizona, Texas, IACP ... Irving Hack, Blood and Honor Hack, Newp hack...

1971: Publication of Pentagon Papers (leaked by Daniel Ellsberg) in NYT forces public & press discourses in a more critical direction.

Wikileaks Timeline

~*~New Media, Classic Reprisals~*~

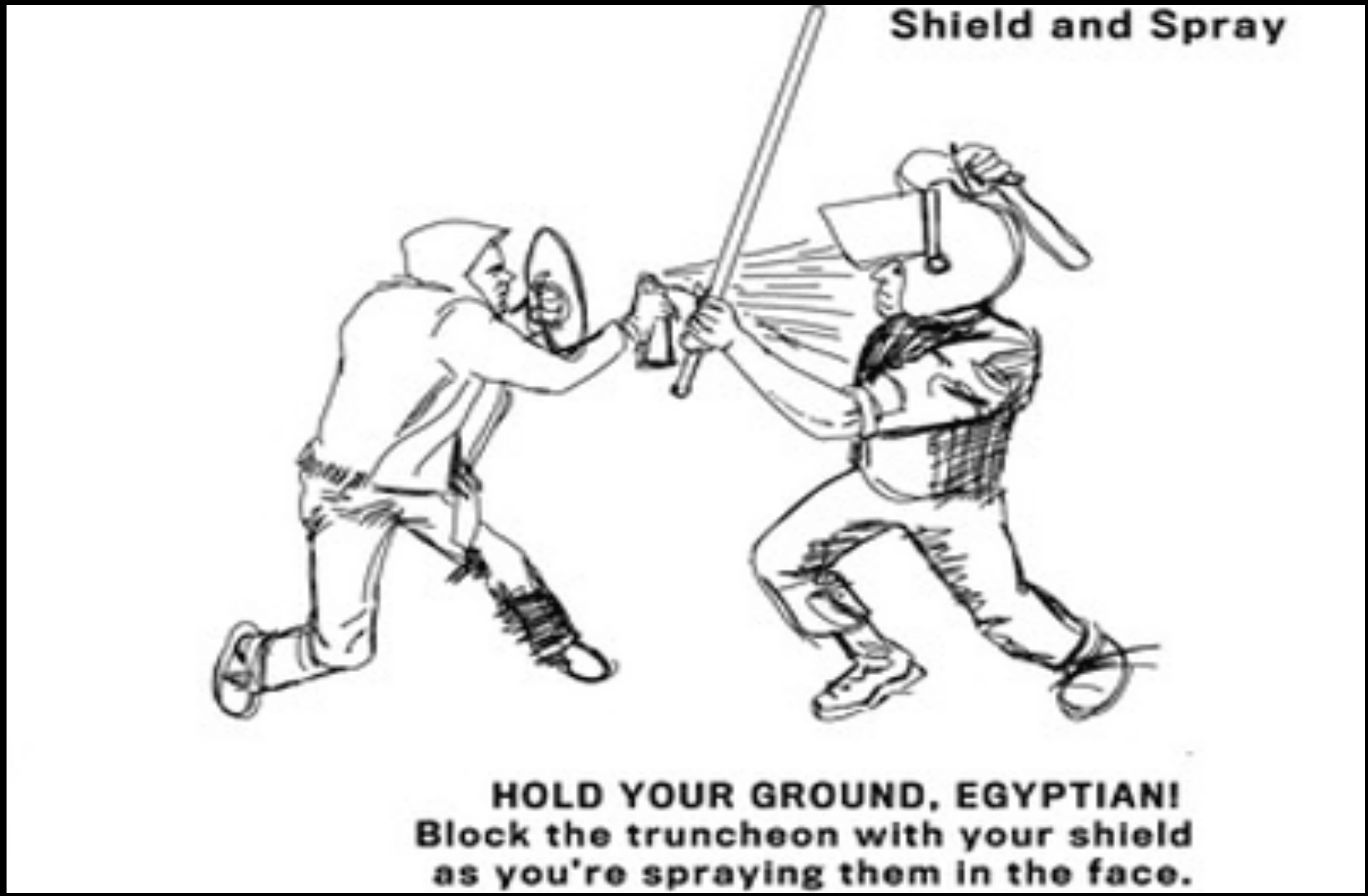
Wikileaks

Detention on arbitrary charges!

Disruption of income!

Police Raids!

...but then came the 'Arab Spring'...

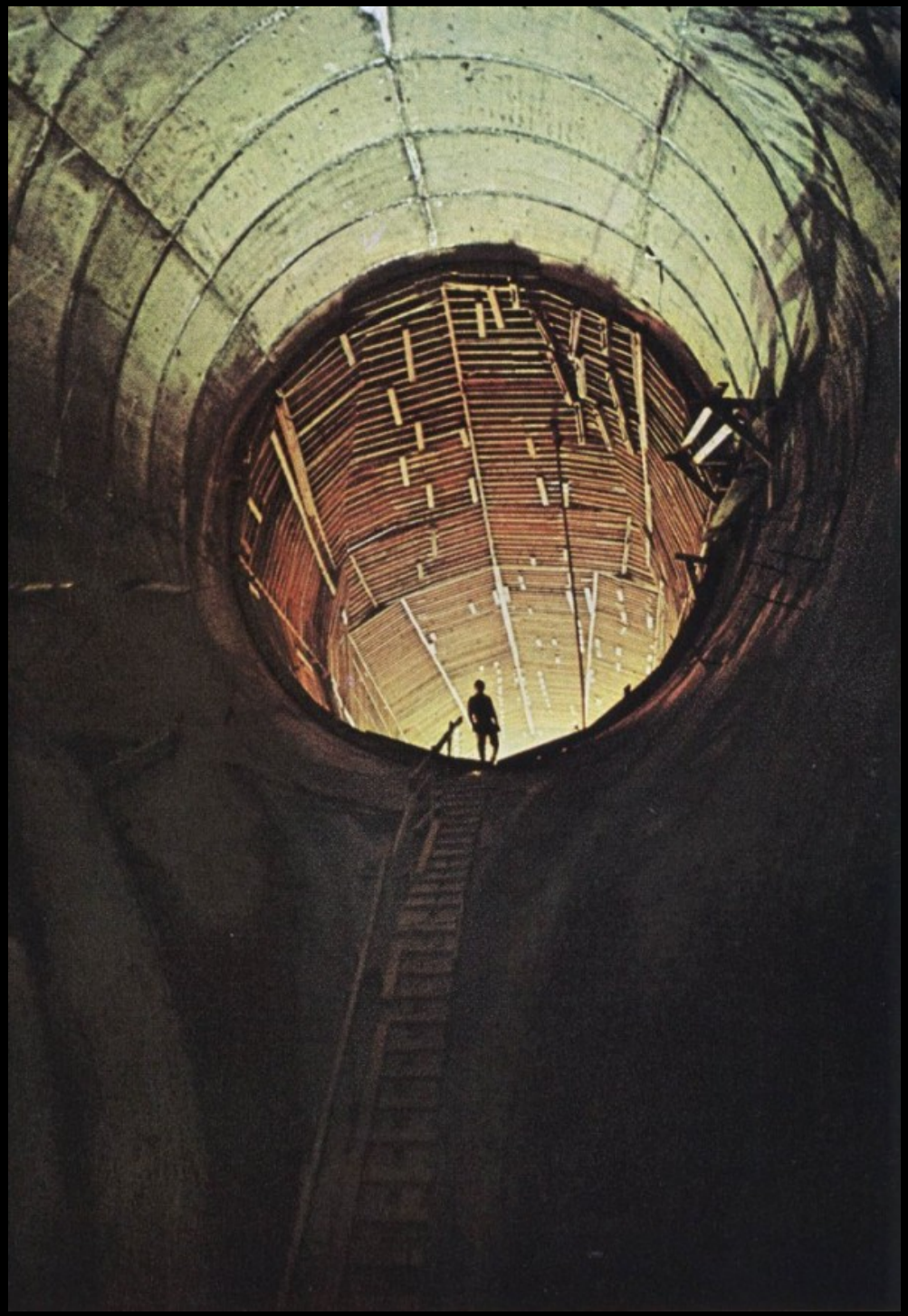


II. Open Source / Linux

Linux refers to a collection of free operating systems, forming a backbone of the open source movement, with deep roots in pre-commercial software.

Many distributions of Linux are packaged to run from CDs or USB drives; you can run them on any computer without touching the data stored on the hard drive.

Several specialized versions of Linux exist for people with security concerns, including Security Enhanced Linux and TAILS.

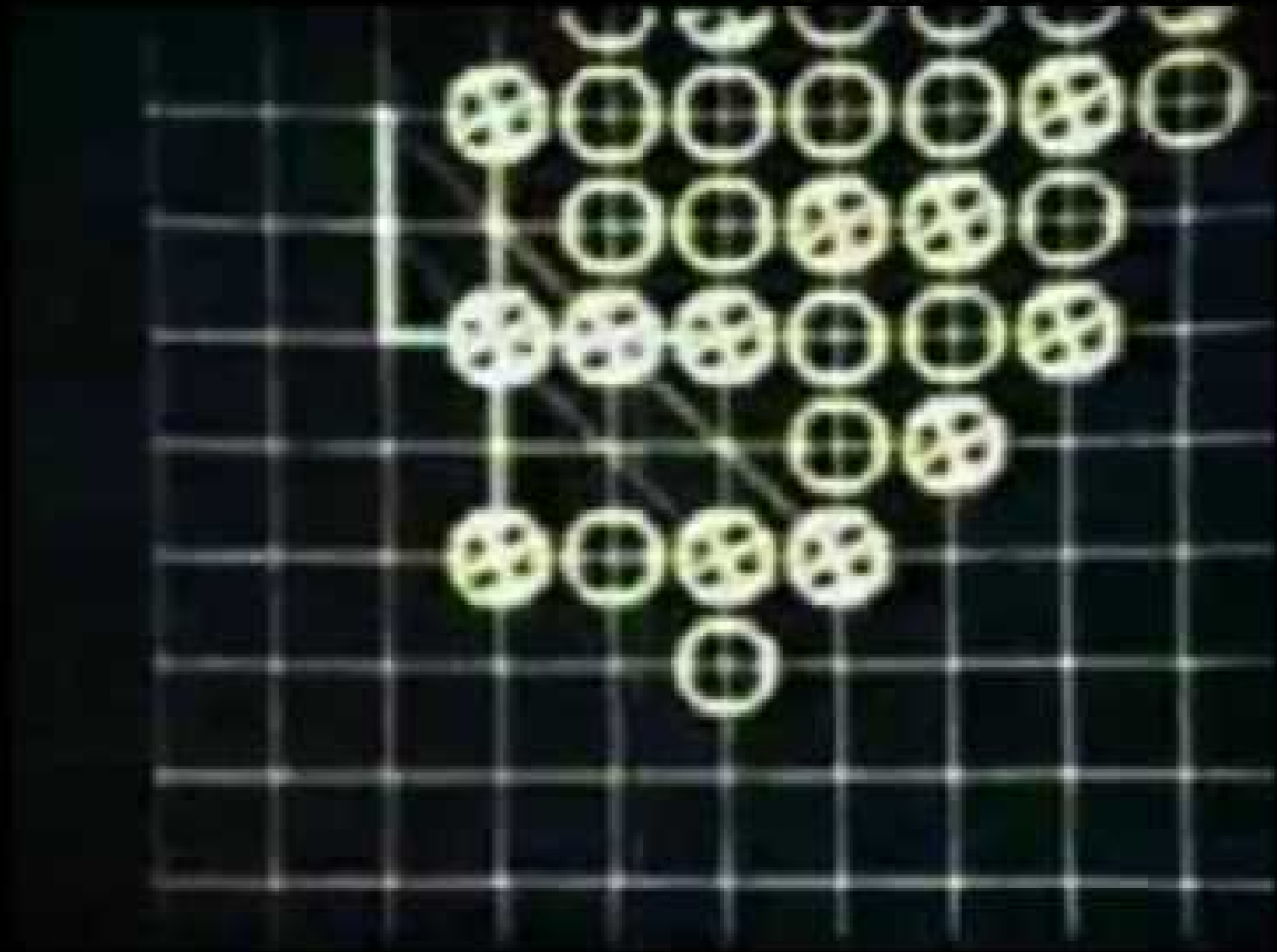


Open Source is...

- software that is collaboratively coded, publicly licensed, open to see/improve/fork.
- updated when a programmer needs a change badly enough to implement it. Much commercial software is changed for thousands of man-hours a week regardless of what's going on.

III.

The Beginnings of Cipherspace



Full-Disk Encryption

Full-disk encryption is the only surefire way to make sure data on your computer is not seized by the authorities. What encrypting your hard drive with a passphrase does is make it so that only a 200-500 MB boot sector of your hard drive is unencrypted/exposed prior to you entering in a passphrase that is hopefully 20 or so characters long. (A good strategy is to take a phrase from a book and sandwich it between two identical four digit numbers.)

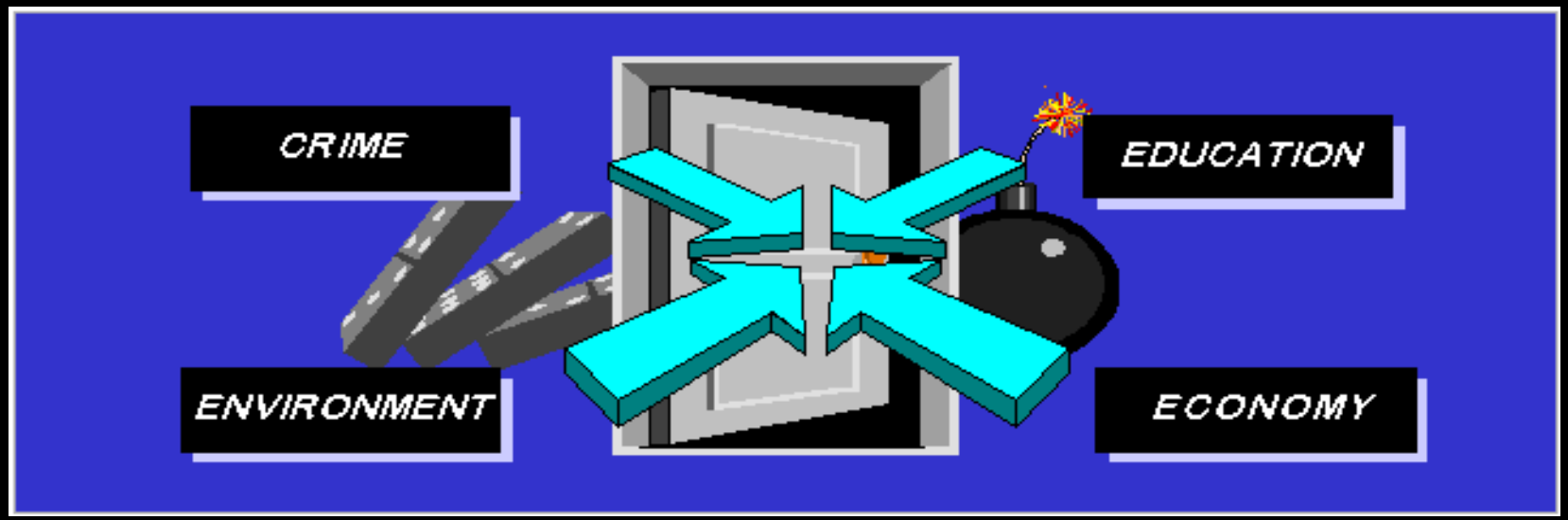
Mac:
Full-disk encryption only supported by OS 10.7 ... You will have to reinstall your OS to get this, however. Also be sure your swap drive is encrypted and Spotlight is off.

Ubuntu: (Re)install whatever flavor of Ubuntu you prefer. When the partition manager comes up, select that you would like to set up a disk with encrypted LVM.

IP Addresses / Routing

IP addresses tell routing equipment where to forward your messages. They are assigned to you from a pool owned by your ISP. Anyone can resolve your IP address into an approximate location, and law enforcement can resolve it into your real name and address by requesting information from your ISP.

Encryption hides your information;
pseudonyms and proxy servers hide your identity.



Tracking by Law Enforcement

The NSA works with ISPs to try to pick dangerous terrorist communiques out of unencrypted internet traffic.

It is anyone's guess as to how effective this is and what exactly they're reading!

ODDS ARE THEY ARE BEING IRRESPONSIBLE

Web Browsers:

Firefox has a lot of sweet extensions for privacy/encryption so no one can intercept your data:

AdBlock Plus -- BetterPrivacy -- Certificate Patrol -- CipherFox -- HTTPS-Everywhere -- ipFuck -- Safe -- ShareMeNot -- SSLGuard --- NoScript --- TorButton

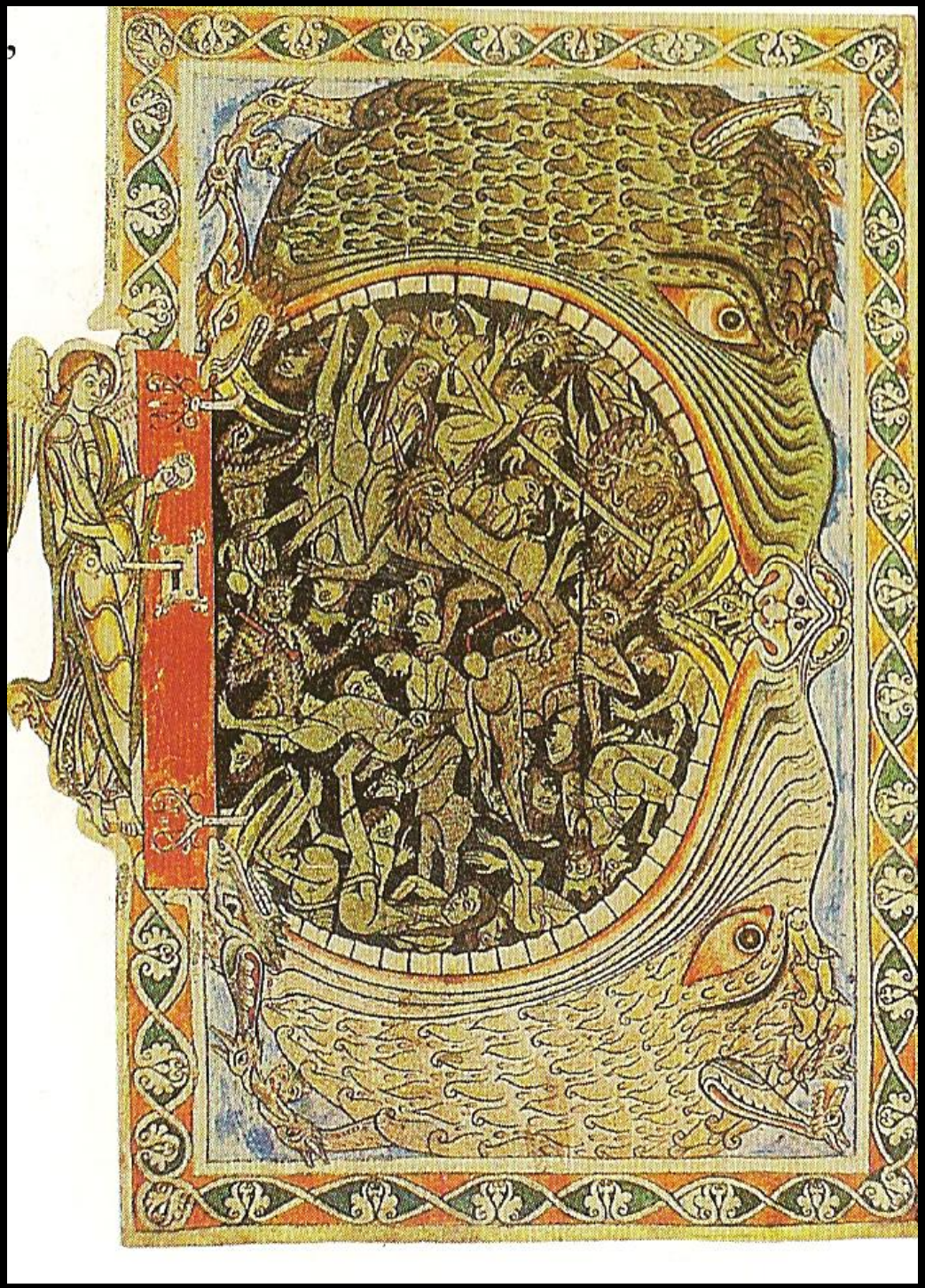
Other Useful Firefox Extensions:

DownloadHelper -- Download Statusbar -- FlashBlock -- Hide Menubar -- Omni Bar -- FXChrome (Theme)

End-to-End Encryption

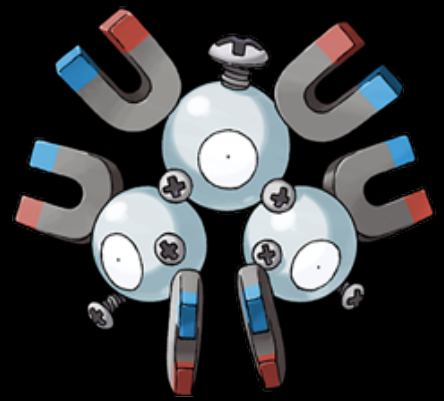
Enciphered Messages - keys are often stored in a file on your computer, meaning that the message is probably unreadable unless your computer is compromised / seized.

VPN's
Encypher all traffic that goes through them; used by governments and corporates to create secure networks.



VPNs (Virtual Private Networks):

- Be careful. Use VPN's that don't log data. The police can and have raided VPN server sites in North America and abroad and arrests have been made.
- The best way to know if a VPN actually keeps no logs is if it HAS been raided by the police and arrests haven't been made.
- AIRVPN does not log so far there have been no arrests. They also offer free accounts to activists, but don't bog down their generosity by using a VPN for everything.



Hiding your IP Address: Open Proxies

There aren't many of these right now and they tend to get shit-flooded by hackers. There is also no guarantee that they won't keep records that record a user's identity.

Botnets

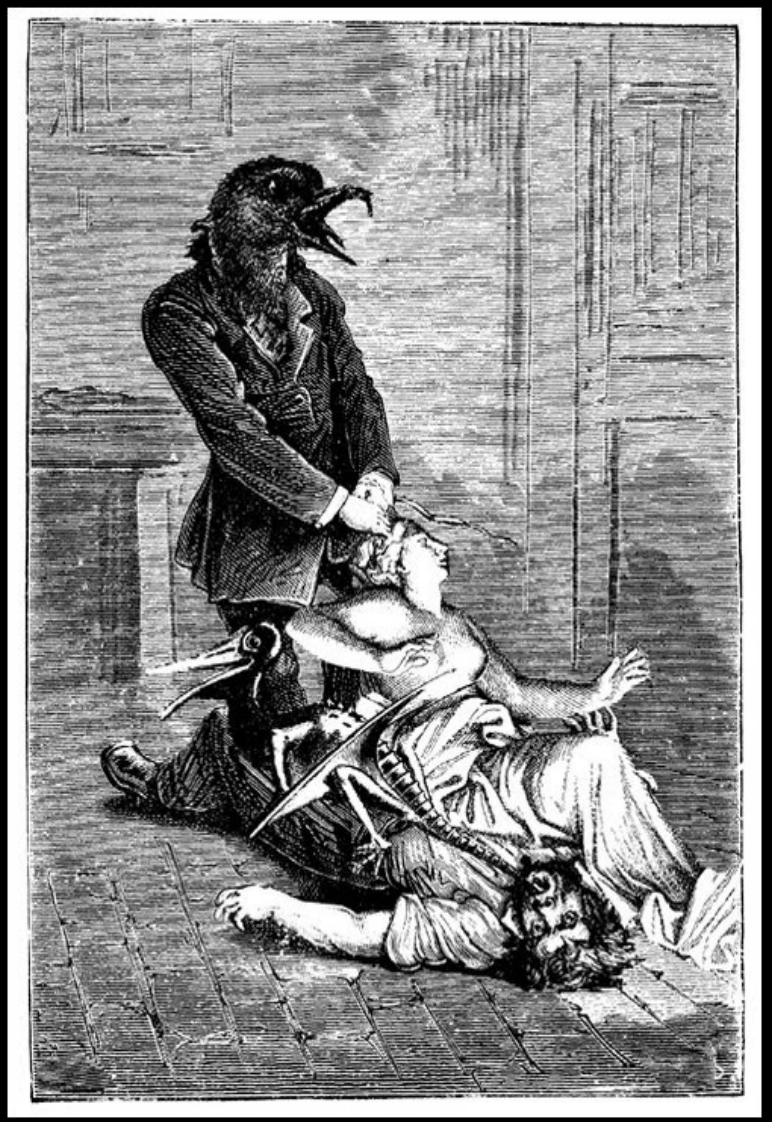
These are shadow networks that run in the background of thousands of compromised home computers. They can provide perfect anonymity but are illegal and hard to get access to.

She's the happiest because her internet is reconfiguring her IMMORTALITY

http://physical-immortality.com/

Handles:

- Pick a random 'handle' (username) which you can consistently for email, IM, IRC, and other services. Tell trusted friends what your handle is, but nobody else.
- Your handle should be a random word or phrase -- perhaps from a book. Don't choose 'your favorite' something-or-other. Make it detached and totally random.



Email:

- To bypass email verification in the short term visit 10minutemail.com (works through TOR).
- Longer-term A: Hushmail - free secure mail
- But hushmail cooperates with court orders : (
- http://www.wired.com/threatlevel/2007/11/hushmail-to-war/
- http://www.wired.com/threatlevel/2007/11/encrypted-e-mai/

- Longer-term B (extreme): Use TOR to set up a PrivacyBox.de account. (PrivacyBox is run by the German Privacy Foundation).
- Generate S/MIME .key and .pem files with: openssl req -new -x509 -days 200 -keyout ca.key -out cas.pem
- Upload to Account Settings on PrivacyBox.de

x

Email:

To send mail to a privacybox email anonymously visit any one of these depending on what device you are using and what degree of anonymity you need:

- https://privacybox.de/pseudonym.msg
- https://privacybox.de/pseudonym.mobi (mobile access)
- http://c4wcxidkfhvmzhw6.onion/pseudonym.msg (Tor)
- http://privacybox.i2p/pseudonym.msg (I2P)

That does not require a privacybox account.

You will NOT be able to send messages FROM your privacybox account.

- Generate PKCS12 file to give to Thunderbird with:
  openssl pkcs12 -export -in cas.pem -inkey ca.key -out my.p12
  - Upload to Edit --> Prefs -->Advanced --> Certificates --> View Certificates
- Configuration Settings:
  --Pop3.. privacybox.de .. port 995 (SSL)
  --Outgoing/SMTP mail will not work so map SMTP to a .onion site.

IM:

- Install Pidgin and enable the Off-the-Record (OTR) plugin, which you may need to separately download.
- Disable logging for OTR and/or all conversations.
- Set up a new account through 'Manage Accounts' --> 'Add Account' --> 'XMPP' --> Server = jabber.ccc.de
- Click the checkbox for 'create a new account.'

- When you IM someone, click 'NOT PRIVATE' just below the chat window. Select 'start private conversation.' If the status changes to 'unverified,' you're good. (This will require the recipient to also have OTR installed.)
- You can't use Jabber to IM other services like Gchat, AIM, or Facebook, but it's not a good idea to use an anonymized IM account to contact accounts obviously linked to your friends anyways. That makes it easier to figure out who you are.

IRC: The standard chat room protocol since 1988. It actually predates the http internet we are so used to. Sometimes, when govts disable the internet, IRC still works.

It is very simple to set up a private encrypted IRC server in cypherspace, using TOR or I2P. Telecomix made excellent use of IRC during the "Arab Spring" and IRC rooms are still popular gathering places for hackers and nerds of every stripe.

You can open new rooms on existing networks as well, such as Freenode, efnet, Undernet, etc.

Chat rooms are made for Idling.

Anonymous Collaboration

http://piratepad.net - compose and edit public documents anonymously, as a group. It runs off of open source software called EtherPad, so you could run your own copy somewhere (like inside of TOR) if you really wanted to.

Publishing & Sharing:

- To share text using client-side aes encryption:
  cryptobin.org
  bin.defuse.ca
- Use multiupload or mirrorcreator.com w/ TOR to upload a file to lots of mirror uploader/downloader sites quickly.

Circulating Files:

Torrent:
Create a .torrent file using a Torrent client and...

- if sharing to the public-at-large:
  upload it to a tracker site like ThePirateBay or isoHunt through TOR.
- if sharing to the darknet:
  you can seed it through an I2P torrent client -- the default one that comes with I2P is I2PSnark -- and upload it to an I2P torrent tracker like _____

Mediafire:

- Use TOR to connect to mediafire and upload a file. Share the link however you want--just not in a way that makes it obvious you created/obtained the file.
- Other people will not have to go through TOR to download the file you anonymously uploaded.

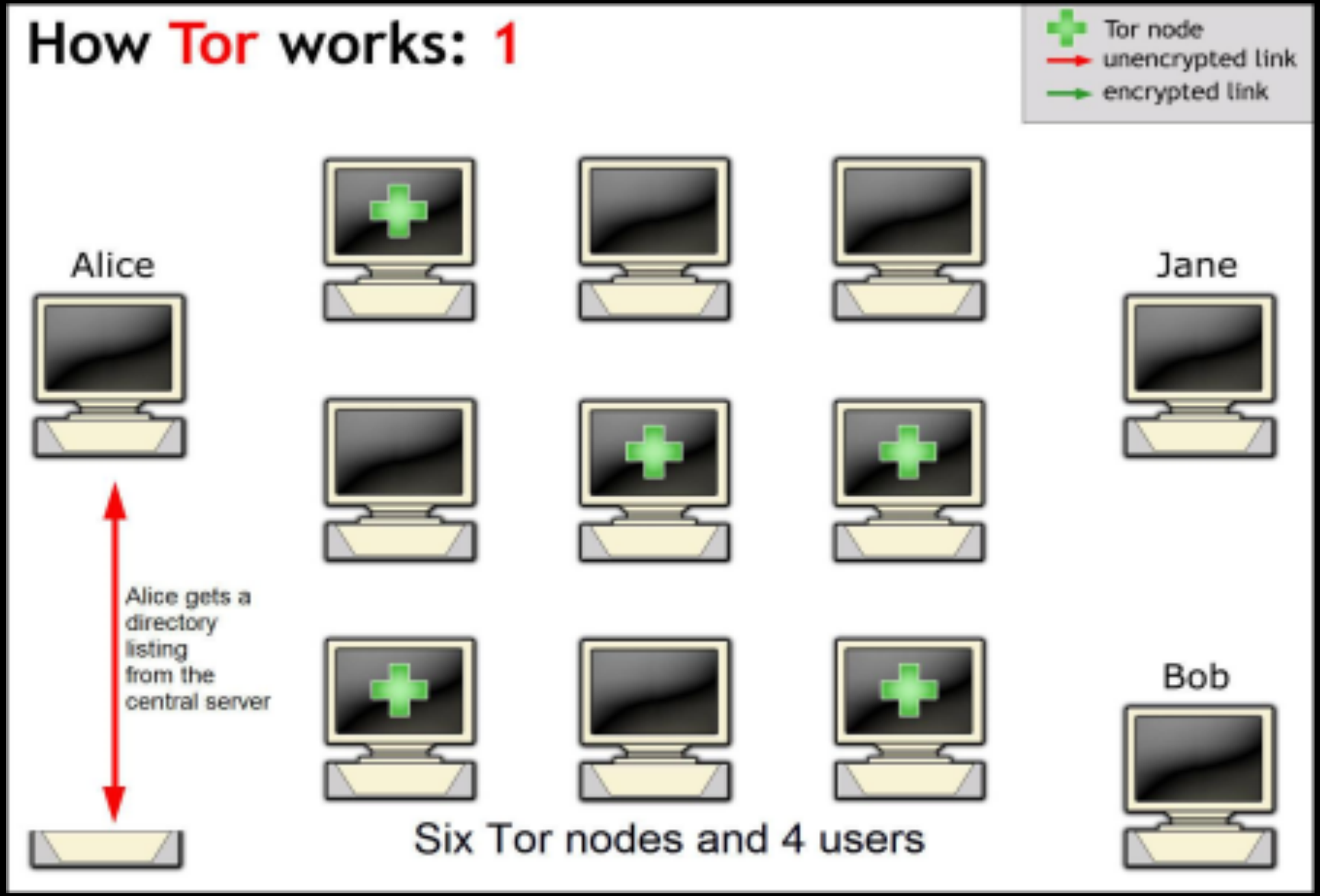
IV. DARKNETS

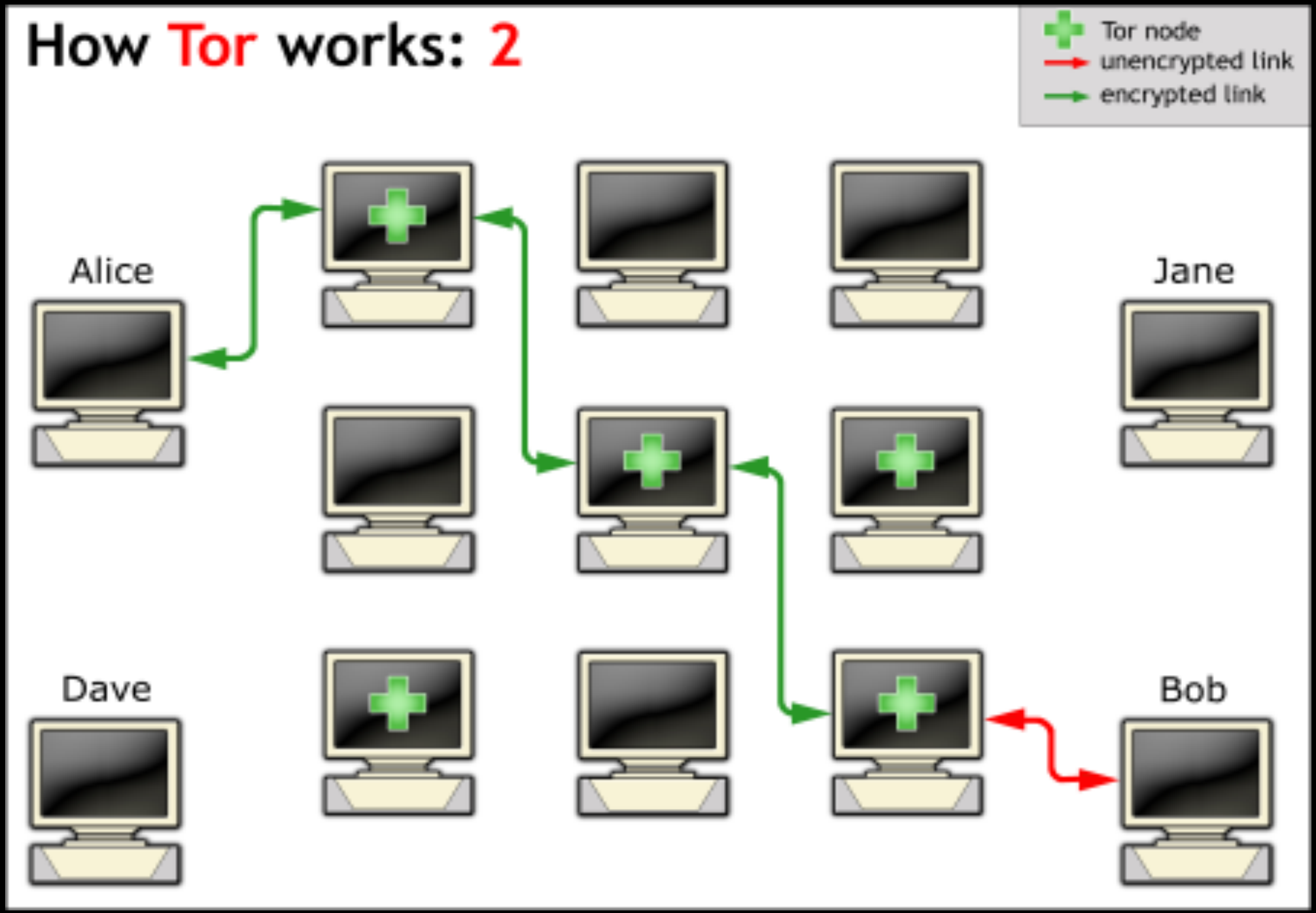
What is a darknet?

Anonymizing networks: Tor & I2P -- Distributed Proxies

Communication coming from these networks can only be tracked to the network as a whole, not to any individual user.


Tor
tor.eff.org


How Tor works: 1
Tor node
unencrypted link
encrypted link
Alice
Jane
Bob
Alice gets a directory listing from the central server
Six Tor nodes and 4 users


How Tor works: 2
Tor node
unencrypted link
encrypted link
Alice
Jane
Dave
Bob

TOR and I2P are each useful for different things, however.
With TOR, one can:

- visit regular web sites anonymously (including file uploaders and torrent tracker sites)
- visit .onion sites
- connect to IRC through a TOR port (but many IRC servers block this due to abuse ... less so with I2P
- visit sites without relaying any data to others

With TOR, one can't:

- torrent fies (compromises anonymity and slows down the tor network)
- visit i2p sites (derp)

- In general, Tor is easier to use than I2P, but there are demonstrated security risks in its architecture; a group of French researchers found a way of revealing the identities of Tor users through "bad apple" attacks.
- There is a Linux distribution called Tails that routes all of your internet traffic through Tor.


BURGER KING
GETTY IMAGES/FILE


i2P

With I2P, one can:

- visit .I2P sites (eepsites). There are a couple I2P search sites (unlike TOR) and also message boards and forums. Many I2P sites are also mirrored somewhere outside the darknet.
- You can get 'real words' before your .i2p site like chaos.i2p ... TOR just generates a random prefix like knvlsdfl334.onion for you.
- connect to IRC through an I2P port
- torrent files
- connect to the outside web

With I2P, one can't:

- surf the darknet without relaying data for other people which takes up hella CPU and bandwidth
- visit .onion's

I2P also takes 30 minutes to an hour to integrate.

TOR also uses a lot less CPU, but it's much less clear how much data is being relayed etc. when compared to I2P.