# So, you want to compute post-apocalypse...

## Rebuilding the internet at the end of the world

Hack3rcon^3
Doomsday Eve 2012

# About me

- Security Consultant with NWN Corporation
- Former network guy
- PaulDotCom crew
- Ham radio operator (KB1TNF)
- Credit to Darren Wigley @Razmus21

# Our expertise

- I'm a pro at "Internet Uptime Testing"
- I love gadgets
- I'm an "amateur" preppers
- The security community has made me paranoid
- survivalnerds.com

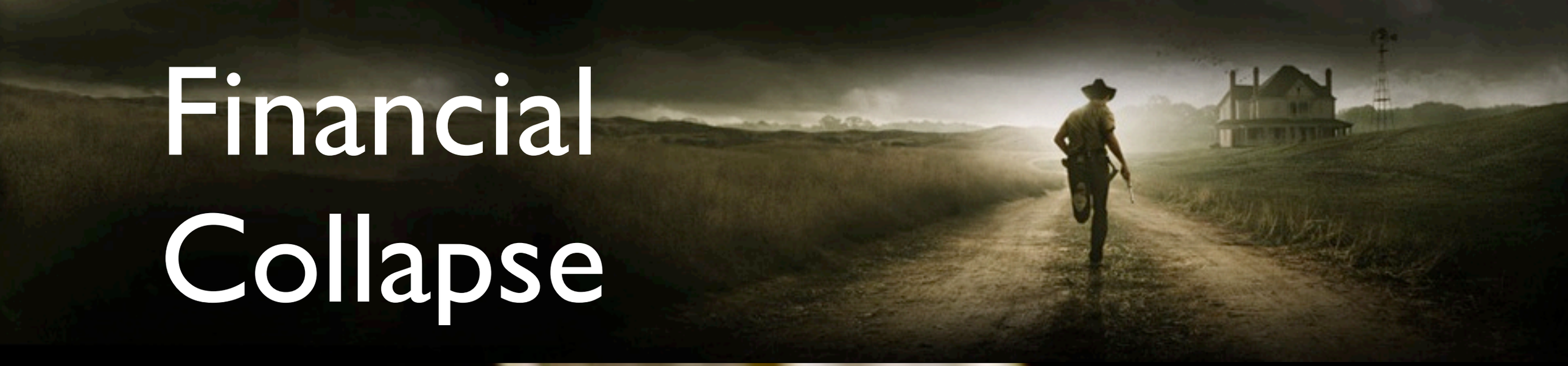
# The End of the World As We Know It

- There are a whole range of scenarios
- It really doesn't matter which one you believe in
- I'll pick the last on the list as a likely, most encompassing scenario
- Let's discuss some favorites


# Act of FSM

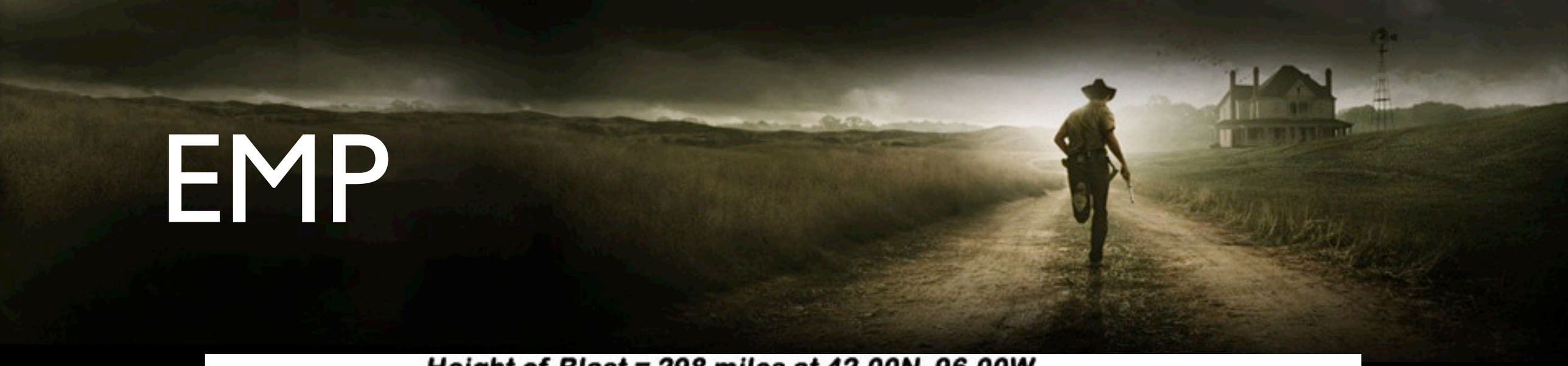
# Zombies

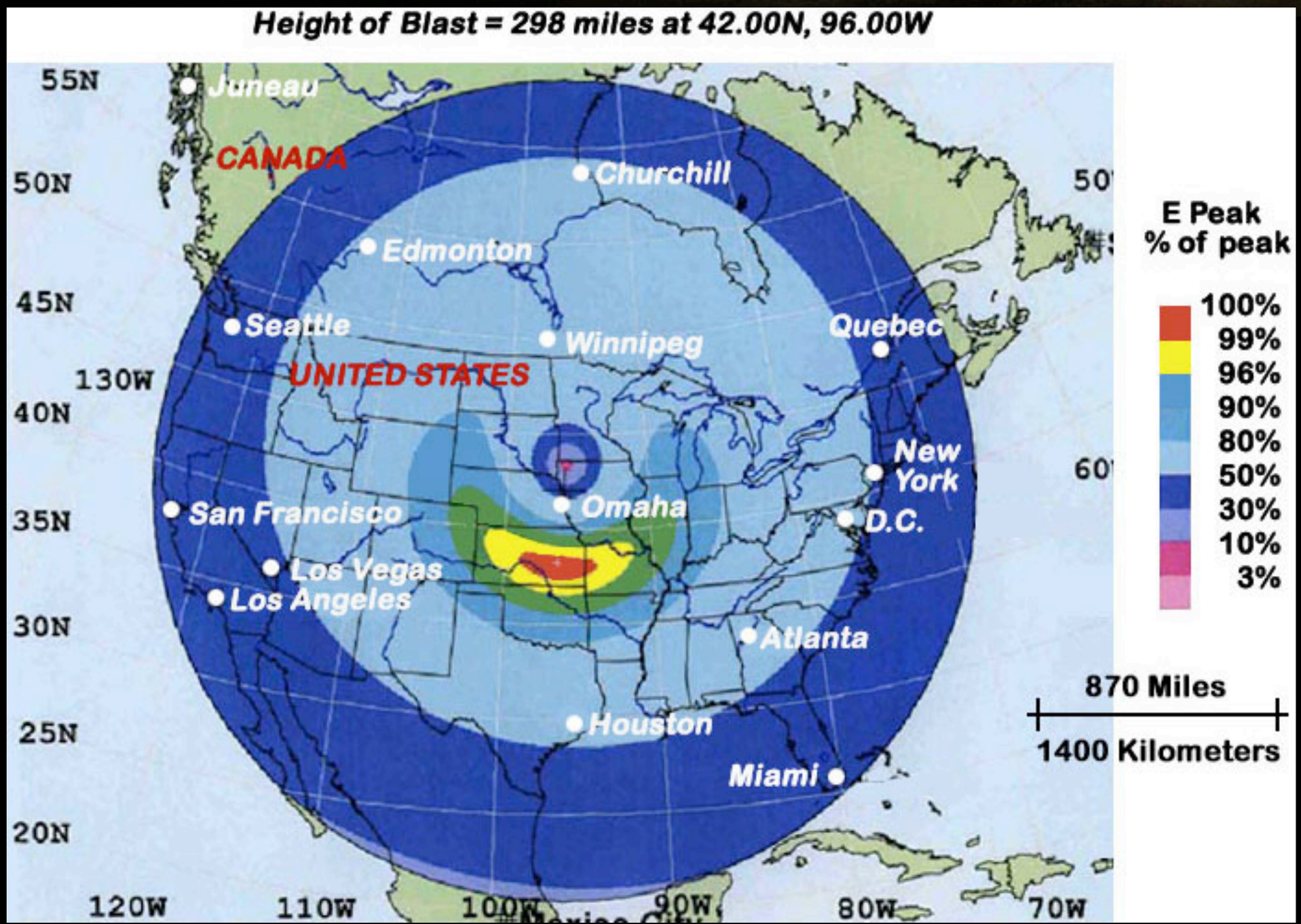
# Financial Collapse



# Government Failure

# EMP




Height of Blast = 298 miles at 42.00N, 96.00W
55N
50N
45N
40N
35N
30N
25N
20N
130W
120W
110W
100W
90W
80W
70W
60
Juneau
CANADA
Churchill
Edmonton
Seattle
Winnipeg
Quebec
UNITED STATES
New York
San Francisco
Omaha
D.C.
Los Vegas
Los Angeles
Atlanta
Houston
Miami
E Peak
% of peak
100%
99%
96%
90%
80%
50%
30%
10%
3%
870 Miles
1400 Kilometers

# The End Goal

- Multiple stages
  - Reduce our burden on Emergency Services
  - Be prepared should they never respond
  - Find ways to improve/protect life/ family

# A Hacker's Perspective

- There are a few tenets of preparedness
  - Two is One, One is None
  - Do more with less
  - The haves vs. the have nots
- How can technology help us with the end game and the preparedness


HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are

...& blow your family to smithereens!

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

# Two is one, One is none

- Have more than one of each item that can fail
  - That means, two radios, two laptops, two antennas...
    - Do this BEFORE, not scrounging afterwards
      - Keep in mind possible community spares and community “consensus”
    - Do not always need to be expensive
- Store them appropriately
  - See EMP
- TEST THEM!


# Technology Saving Lives

- The obvious
  - Beans, Bullets and Bandaids
- Saving lives?
  - Short distance comms
  - Long distance comms for tactical communication
  - Disruptive technology - pink P25 jammer
  - Data exchange
    - e-books, medical training, survival education


# Protecting Electronics

- EMP?
  - EMP cabinet! (or two or three)
  - “Sealed” metal enclosure
    - Be careful of insides
  - Keep any unused survival electronics here...
  - 18 inches of wire
- Weather?
  - Some will be on the move, think weather resistant
  - Fixed installation, research and stock enclosures and silicone (two is one, one is none)

# On Having Power...

- Generator?
  - What fuel type and how much?
  - How loud?
- Wind?
  - How windy is it?
  - Lots of moving parts to break
  - Comparatively expensive startup costs
- Solar
  - Quiet, but how sunny?
  - Portable?
  - Batteries
  - Relatively inexpensive startup costs
  - Don’t forget spare charge controllers in your EMP cabinet

# ...batteries

- Flexible charge controller
  - Find one that can charge various battery types
    - Or DIY with voltage converters, but beware efficiency
    - Barter for charging others' batteries
- Various battery types
- Sealed lead acid, automotive, marine gel, deep cycle, lithium
  - All various charging methods needed
  - Again, community spares and consensus
  - Also, think multi-purpose and portability

# Rebuild?

- Ok, so we know why...
- We know how to power it
- (We'll leave opsec up to you, but...)
- We'll need to start small, potential to get bigger.
  - Defending your home, block, city

# Wires

- Sure, there are all of these wires on the poles...
  - Likely fiber...
  - LOTS of old copper
- This is good, but...
  - Old, not maintained
  - Those that know the cables and systems are likely unable to help

# Phone Patch?

- When times START to get tough
- Local phone service might not work
- How about a radio phone patch?
  - Send telecom outside of local area
  - Likely not far enough
- Just a matter of finding a “public” one
- Set one up?
  - Decent expense at little return

# Who Needs Wires?

- Well, maybe we don't...
- Wireless technology!
  - Specifically we're talking ham radio
  - Also, commodity gear, aka WiFi

# Ham Radio

- Yup, requires a license to transmit
- Several license types grant different privileges
  - Go get your tech -> general at least!
  - Tests are easy...
  - ...FCC requires a valid mailing address made public
- We’re not here to preach, just educate and enable
- Ham radio is...
  - Incredibly diverse and powerful
  - Entrenched in the EMCOMM community
  - As complicated/expensive as you want to make it
- With great power comes great responsibility

# Practice Makes Perfect

- Ok, so here's the deal: the FCC
  - Or other governmental agency
- We have to work within their rules
- These rules set the stage for understanding the limits, use cases and technologies
- Some rules?
  - No amateur service encrypted comms
  - Limited encoded comms
- What happens when there are no rules?
  - Think about the application now
  - We'll already have practice when there are no rules

# Gear (1)

- This is the part that can get expensive...
  - Think swap meets, ebay and craigslist
  - New is not always better
    - More buttons to break
- Of course 1 is none, 2 is one
  - Make sure you USE and maintain both
- Don't discount "boat anchors"
  - Will definitely need some going over
    - Capacitors and tubes
    - Don't forget the spare tubes
  - Be aware of duty cycle
  - Not easy to move
- Guess what? Tubes are allegedly EMP proof!
  - Good, I don't want to have to move 'em out of the EMP cabinet

# Gear (2)

- More radios == more toys
  - Want comms with someone else? LPOP?
  - Tactical position, even at long distance?
  - You might be finding more radios and add ons...
- Or build a community (survivalnerds.com, arrl.com, linkedin.com)
- Don't forget the extra parts too (we'll get to those)
  - Other commodity gear as well...
  - ...stock up now!

# Again, More Practice

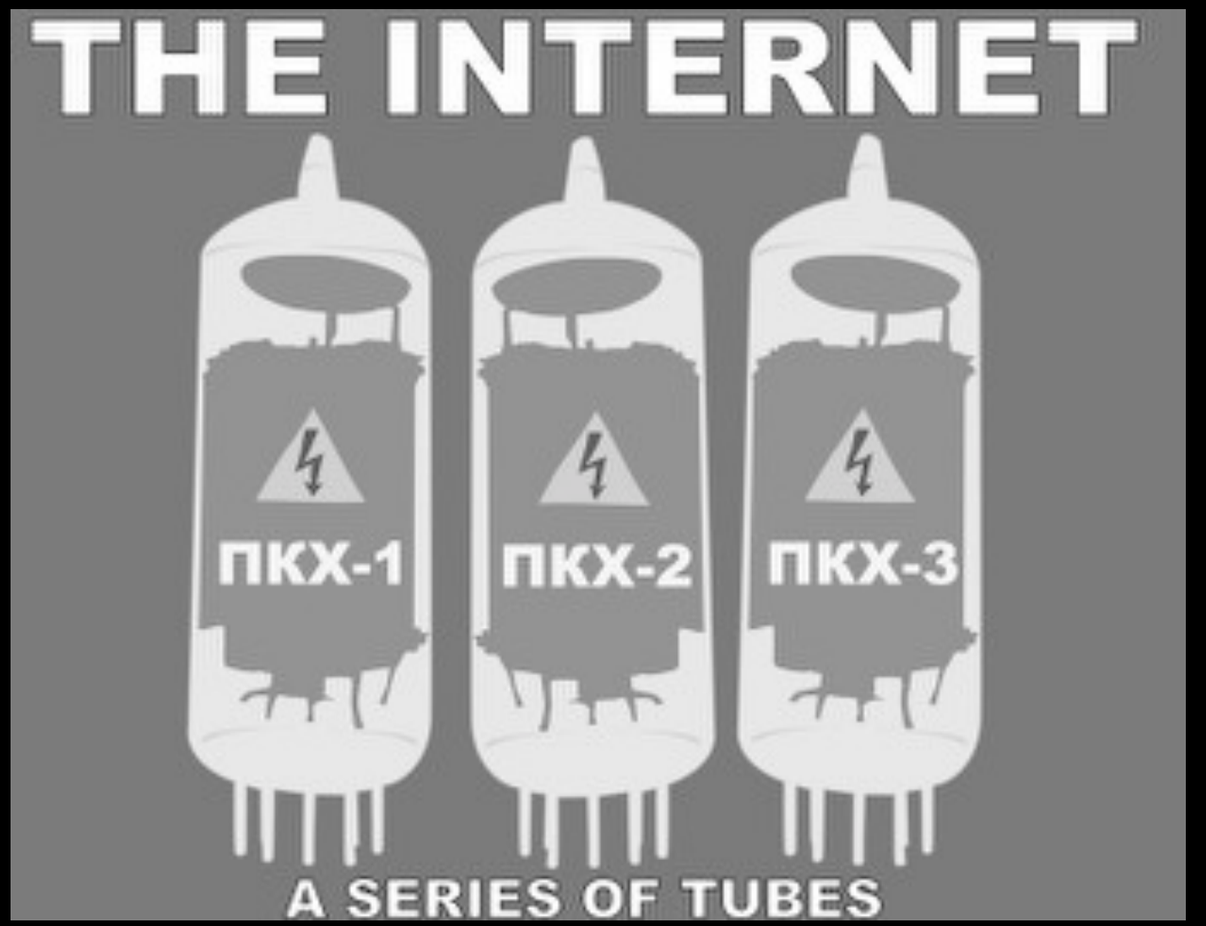
- Having the gear is great, but knowing how to use it before you need to is better
- The digital modes require more gear
  - You better know how to use it
  - ...and set it up with a few moments notice
- Be sure to rotate in and out gear....

# Protecting Gear Redux

- Yes, you'll need to rotate...
  - One in use for practice
  - The other stored in your EMP cabinet
  - Remember to disconnect antennas when not in use
    - Remember to reconnect them during use!
- Depending on where these are you may want waterproofing

# Where Are the Tubez?

- Ok, we've preached about
  - Radio tech
  - Gear
  - Survival goodies
- But, how in the heck does this help me rebuild the internet?
- Let's start figuring out how to use this stuff to transfer data...




# THE COMPUTER!

- Yea, great I use it to surf the tubes that don't exist...
- How about using it to
  - "Surf" the "new tubes"
  - Control the hardware to run you radio gear to enable data transfer
- Ham radio rig control with software
  - Tune frequencies, log contacts
  - Convert and send encoded data via audio and PTT interfaces
- Think of the old days of external modems
  - Instead of phone lines, we are using radio
  - Instead of computer and modem, the computer IS the modem

# Sending Data

- Again with the modem analogy...
- We need to convert data to tones for transmission - same with the modem
  - Some of the same issues apply
  - Interfacing and audio bandwidth
  - Fidelity and distance
- We'll talk about a few digital modes and their application


# CW (1)

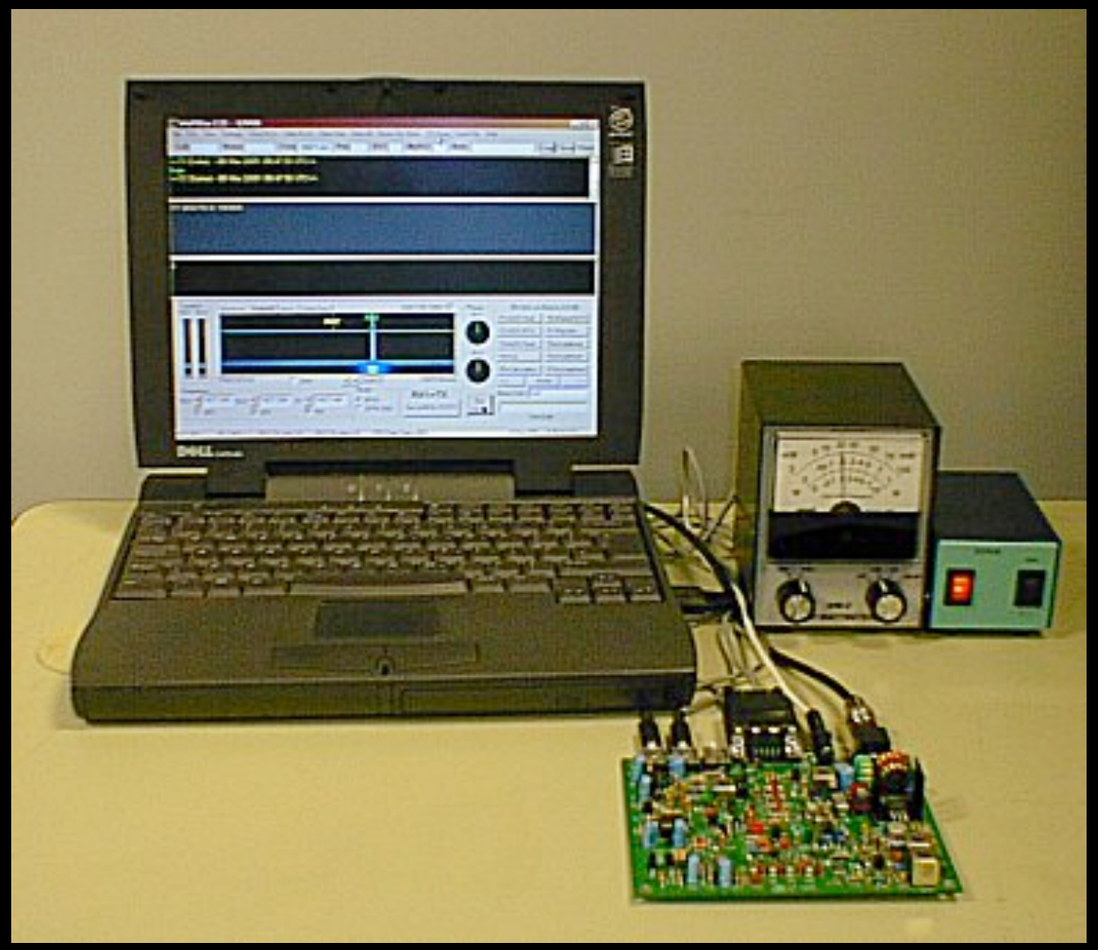
- Yes, good old morse code!
- No, we don't have to type all this stuff out by hand
  - We'll let he computer receive and decode and send!
  - All we do is read and type!
- Problem is...
  - SLOW? You thought 300bps was slow...
  - 20 WPM =~ 16.5 baud (that's no typo)
  - limited character set for binary data
  - How about Base64
    - No case designation
  - How about UUENCODEing
    - No [, ], and ^ in character set...

# CW (2)

- Still great for simple text transfers
  - Think ~~telegraph~~ e-mail
- Also easy to implement repeating, cyclical and scheduled broadcasts
- Can do long distance with little power
  - Working DX with 5 W
  - Build in a tuna can with few parts

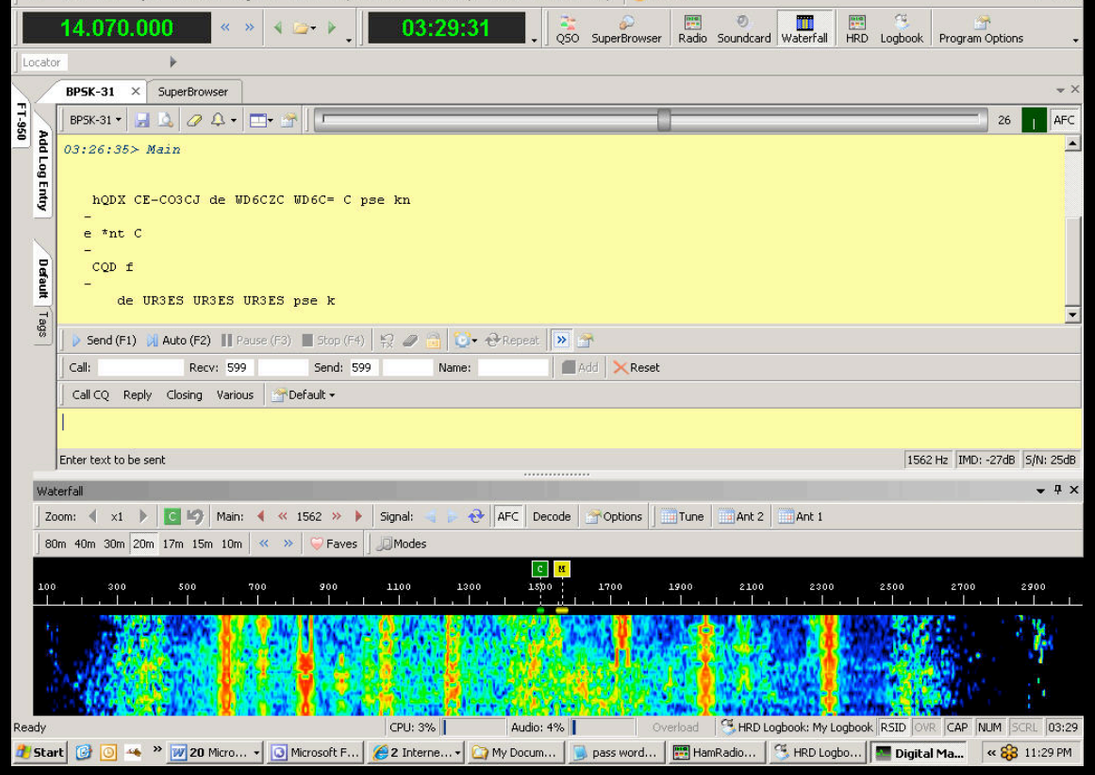

# PSK31 (1)

- Yet another digital mode
  - A little newer -1998
  - Whistle with a slight warble, low bandwidth requirements
- Again, all we do is read and type
- Problem is...
  - SLOW? 31 baud (again, also not a typo)
  - No error control/correction
  - Unusual byte order/length



# PSK31 (2)

- 128 character ascii set
  - How about Base64 - SURE!
  - How about UUENCODEing - SURE!
  - Not great for critical, large blocks
  - We just need some method for converting
    - Might be useful for some limited encoding/pseudo-encryption
- Can do long distance with little power
  - Working DX with 5 W
  - Very resistant to poor conditions
- Little equipment needs - low power cpu, sound card, cables and a resistor
  - RasPi anyone?
- Error correction with the QPSK variant




# Winlink 2000

- Want to do e-mail with attachments? This is your protocol!
- Intended for "remote internet"
  - Boats, remote residences, etc
- Based on AX.25 plus others (D-Star, Wifi)
- Community based network
- Can cover long distances
- Store and forward, and can sent to Internet
- Client/Server Architecture
  - Servers hard to establish
  - Need to be up 24/7/365 and connected to the internet
- But...

# P2P

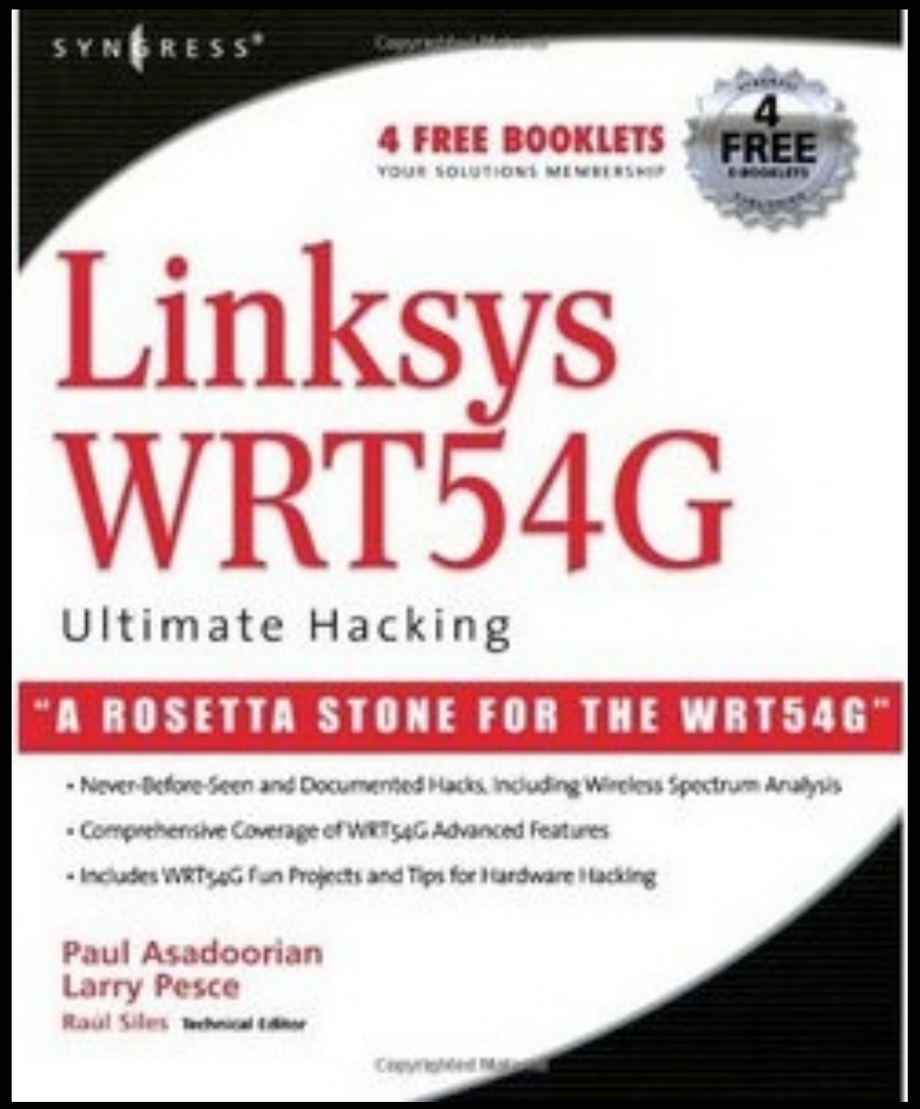
- Winlink can be set up in P2P mode
- Set up your own server under windows
  - Does not need to connect to the Internet
  - Need to schedule transfer
- Does not require special hardware modem
  - and open source protocol
- No long distance relay
  - Unless you build your own network
- One could use the proprietary protocol...
  - Requires expensive modem for each station
  - Proprietary protocol
- Firmly entrenched with Military EMCOMM
  - MARS (Military Affiliate Radio System)

# Packet Radio

- We're going to skip this one for the most part
- Expensive hardware to implement each node
- Limited bandwidth
  - 9600 - 19200 bps
- Based on only AX.25
- We can do better...


# Commodity Gear

- Readily available
- Inexpensive
- Plenty of antennas, amplifiers and cables
- Technology everyone understands
- Specifically the Linksys WRT54G(L)
  - This is relevant to my interests



# HSMM-MESH

- Custom Firmware based on OpenWRT Kamikaze 7.09
- Self healing, self routing mesh network
- Power, install, small config
  - Auto joins mesh, and you're off
  - local computing resources connect via (short) ethernet
- Carries native IP traffic
  - All the rules of the internet apply...
  - ...but without wires




# A Bit On the WiFi...

- HSMM-MESH shows up with that SSID
  - Ad-hoc
  - Mesh nodes with same SSID auto join
  - Uses OSLR for mesh routing
- But guys, 1W indoor 4W outdoor!
- So, install them outdoors!
  - Remember the weatherproofing?
  - Use additional antennas
- WEP/WPA allegedly ok by FCC
  - Not obscuring, but securing messages
  - Not supported without some tinkering with HSMM-MESH

# Moar Power

- With great responsibility comes great power!
- Ham radio operators can have increased power
  - All you need is a Technician license
- Some channels fall within Amateur band allocations
  - 802.11b Ch 1-6, 10W (DSSS)
  - 802.11g all Ch, 1500W (OFDM)
  - 802.11a all Ch, 1500W (OFDM)
- Distance? 802.11b with antennas and amplifiers...
  - 10 miles in urban areas
  - 79-134 miles with clear line of sight
    - Get your towers ready...
    - Now do that for 802.11g...
    - Oh, and be sure to practice OPSEC
- That will get us pas the end of the block for sure

# Get Extras

- Start stocking up on routers now
  - Sure, there will me thousands available post crash
    - You'll be searching house by house
    - ...and will not have been in your EMP cabinet
- Those antennas and amplifiers will be REALY hard to come by post crash


# More On Extras

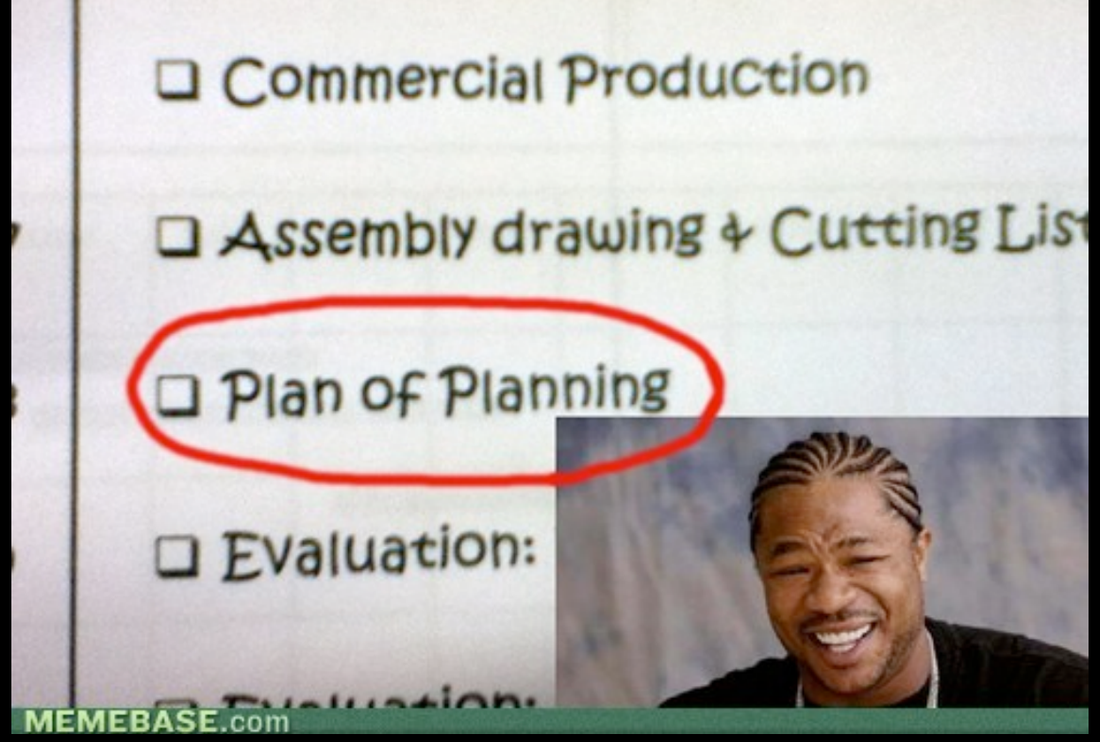
- We've talked a lot about a computer attached to
  - Radios
  - WRT54G's for sharing info
- What do you pick?
  - Netbook?
    - Small, moderate power
    - Battery power for some period
    - Good for charging off battery, solar
- Each station needs 2 or 3
  - In an EMP cabinet
  - This is where community comes in on cutting costs

# Software

- Oh, and don't for get EVERY piece of software that you'll ever need
  - OS, patches, supporting software
  - Remember that software that requires a dependency and the whole no internet thing?
  - Yeah, good luck installing .net or mirroring repositories
- Back it up. Twice. And then 6 times again
  - ...and then find ways to make backup post crash
  - Yeah, several spinning disks fail (and EMP)
  - Have copies on DVD that get scratched
  - Thumbdrive/Flash that get lost, broken, fail (also EMP)

# We Have A Plan

- We know what we need to do to rebuild
- Now is the time to get started!
  - Acquire some licenses
  - Acquire some gear
  - Acquire some practice
    - Use
    - Setup
    - SOP pre- and post- crash




# Help?

- We potentially have lots of work to do
  - Finding deals on gear
  - Configuration issues
  - Testing
- Finding like minded folks for this work
- We'd love your help in building community
  - http://survivalnerds.freeforums.net
  - Suggestions are welcome
- Guest posts are great too!
- survivalnerds.com

http://www.survivalnerds.com
http://survivalnerds.freeforums.net
@survivalnerds

# SurvivalNerds

A techie's approach to survival post-apocalypse

Larry Pesce
@haxorthematrix
larry@survivalnerds.com