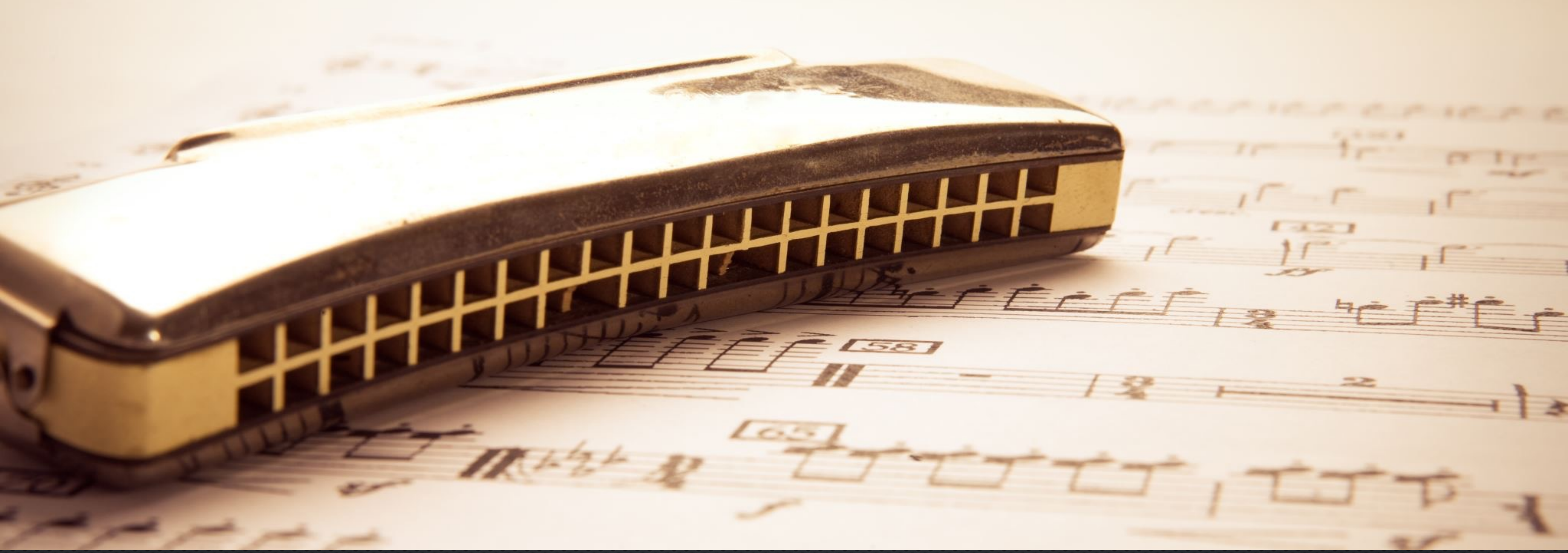


HAM RADIO AND CYBERSECURITY

B. Greg Colburn – N3BYR

OUTLINE

Who is Greg Colburn - N3BYR

What is this world of Cyber Security

How does it relate to Ham Radio as a community

What can Ham Operators do to better prepare

Questions

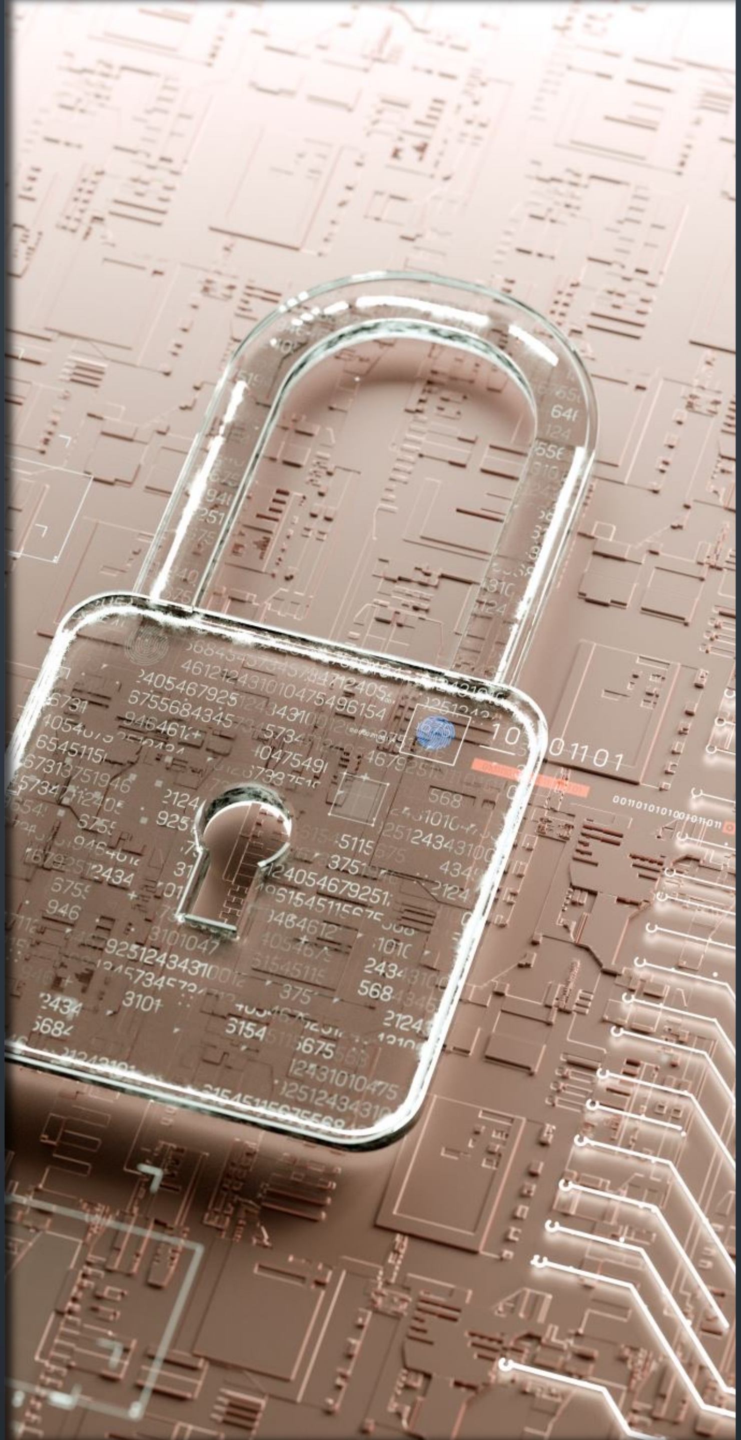
WHAT THIS IS AND IS NOT ABOUT

- This is not anti-Overseas Market – great manufacturers exist both within the US and Overseas
- This is not intended to make you an expert in Cyber Security
- This is not intended as Pro or Con digital communication comparisons
- This IS intended to make you pause and take a minute to analyze your shack/equipment
- This IS intended to make you aware of concerns we should be thinking about as HAMS
- This IS intended to help you understand where Ham Radio and Cybersecurity cross paths and create risks at personal levels and group levels (Clubs, ARES, MARS, etc.)

GREG COLBURN – N3BYR

- +30 Years as a ham operator (Since early 90's… yeah that was 30 years ago)
- Cybersecurity SME and Actively working within IT, Cyber, and Hacking – Experience and Background originates from the 80's – IT, Programmer, Hardware, and SysAdmin – several certifications
- Working with communications that has threat vectors within DoD/DIBS and Cybersecurity Research
- Working with various equipment in Ham Radio including SDR, and Digi Modes
- I really prefer SSB or CW… (this is contrary to pop. belief)

WHAT IS THIS CYBERSECURITY WORLD?



WHAT IS CYBERSECURITY

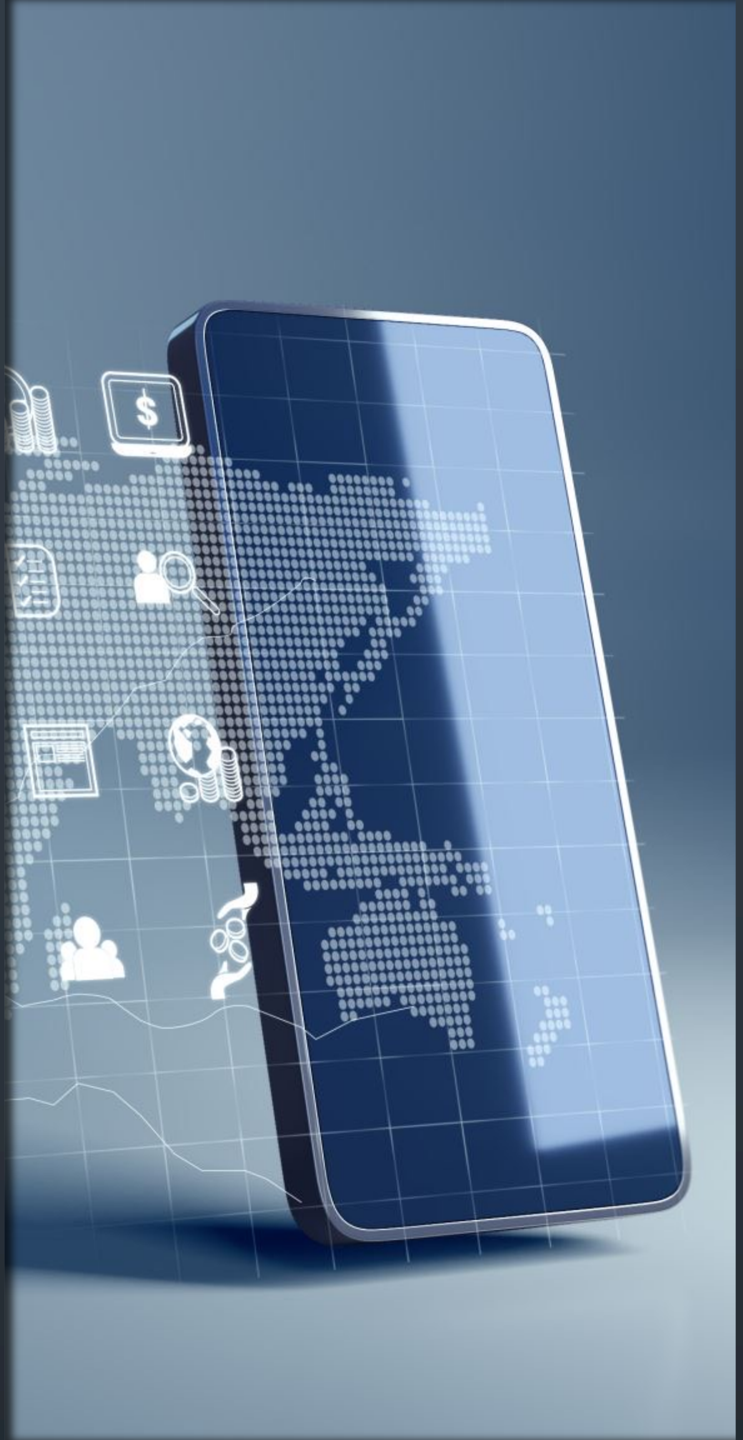
- Cybersecurity is the art or practice of protecting digital/computing resources through cryptography, hardware, software, and physical restrictions to networks, computers, and hardware that may be vulnerable to exploitation. Proactively defending these resources helps maintain their availability, integrity, and functionality.

JUST HOW MANY HACKS OCCUR ANNUALLY???

- Depending on the reporting source between 800,000 to 1,200,000 compromises occurred in 2022 (Businesses & Personal – actual reported cases in the U.S.)
  - Equates to roughly 100,000 per month or ~3500 per day! (US 331M Pop.)
  - This data is INCOMPLETE – Not every compromise is reported – OR known!
  - This also does not account for companies that "Monitor" your activities and may share that meta data as anonymous information to third parties or store it.
- An est. 10.2B USD ($10,200,000,000.00) in losses in 2022 (Likely Higher)
  - This is a huge increase from $6.9B est. in 2021 losses
  - Many of these losses are from outdated software or lack of an Anti-virus program
  - Losses include ransom ware, bank scams, and recovery costs

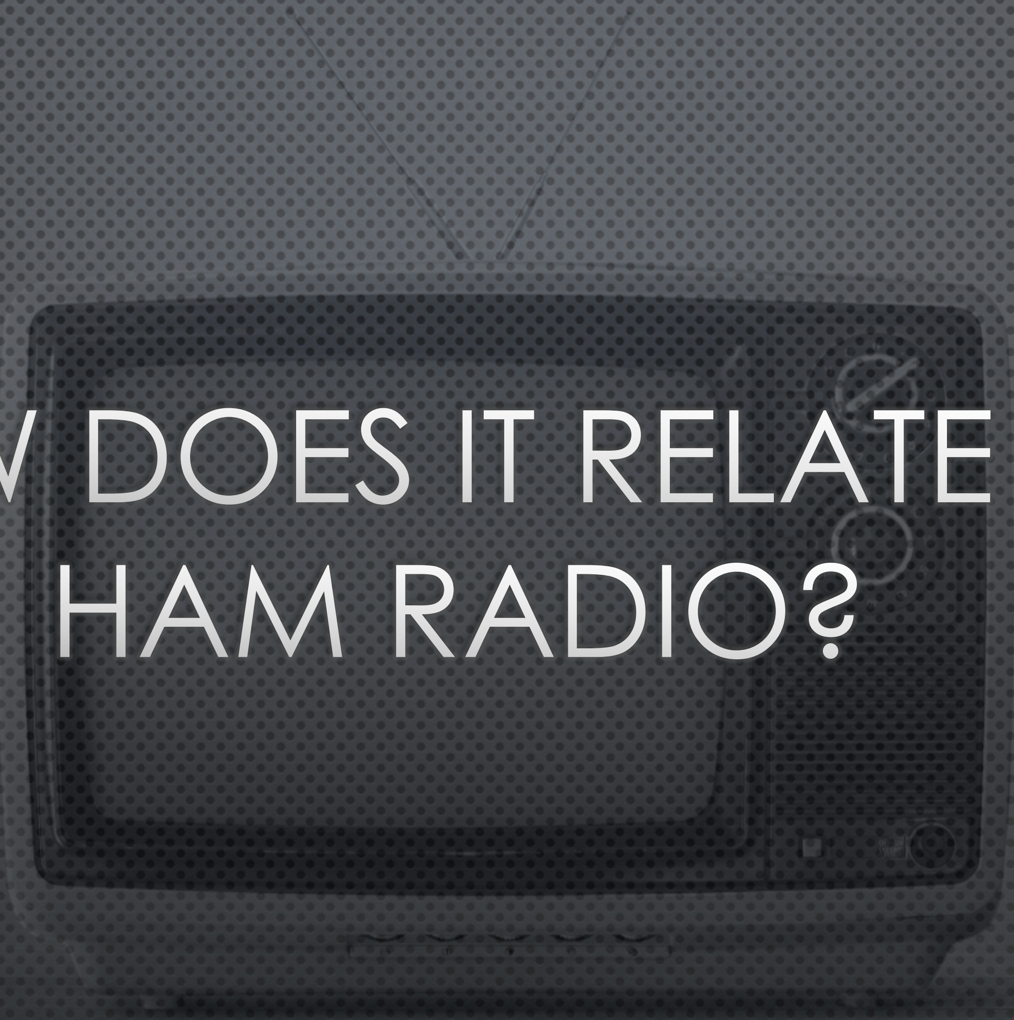
HOW LONG HAS CYBER SECURITY EXISTED

- Many principals and precautions originate from the concerns in the 1970's – Yes that's 50 years ago…
- My first taste and understanding of those concerns was in the early 80's – most considerations were based on physical access or telephone dial-in access
- While the technology has changed dramatically in 50 years, tactics are still primarily based on initial compromise (Trojan) and lateral propagation
- In the 70s and 80s defenders were taught where weaknesses reside within systems, today with so many moving parts the focus is on general detection methods
- Many companies specialize in "White Hat Hacking" to find potential flaws and improperly configured baseline settings and report the findings to manufacturers for "bounty" rewards



DEFINITION – THREAT VECTOR

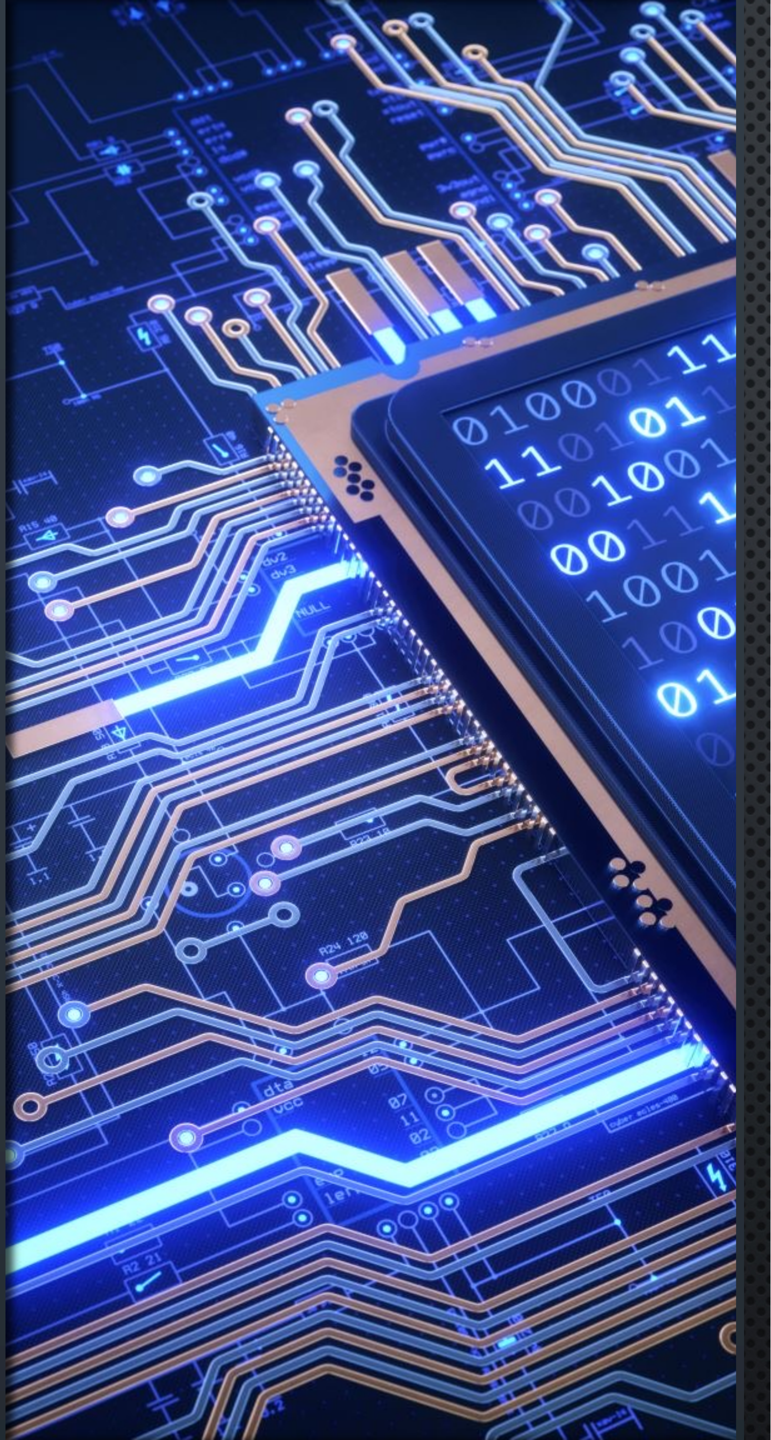
- A threat vector (or attack surface) is a path or means for a hacker to compromise, threaten, or make a resource unavailable. Threat vectors can be computers, networks, applications, users, email, software/firmware, mobile devices, and more.



HOW DOES IT RELATE TO HAM RADIO?

WHY SHOULD CYBERSECURITY BE A CONCERN FOR HAM RADIO?

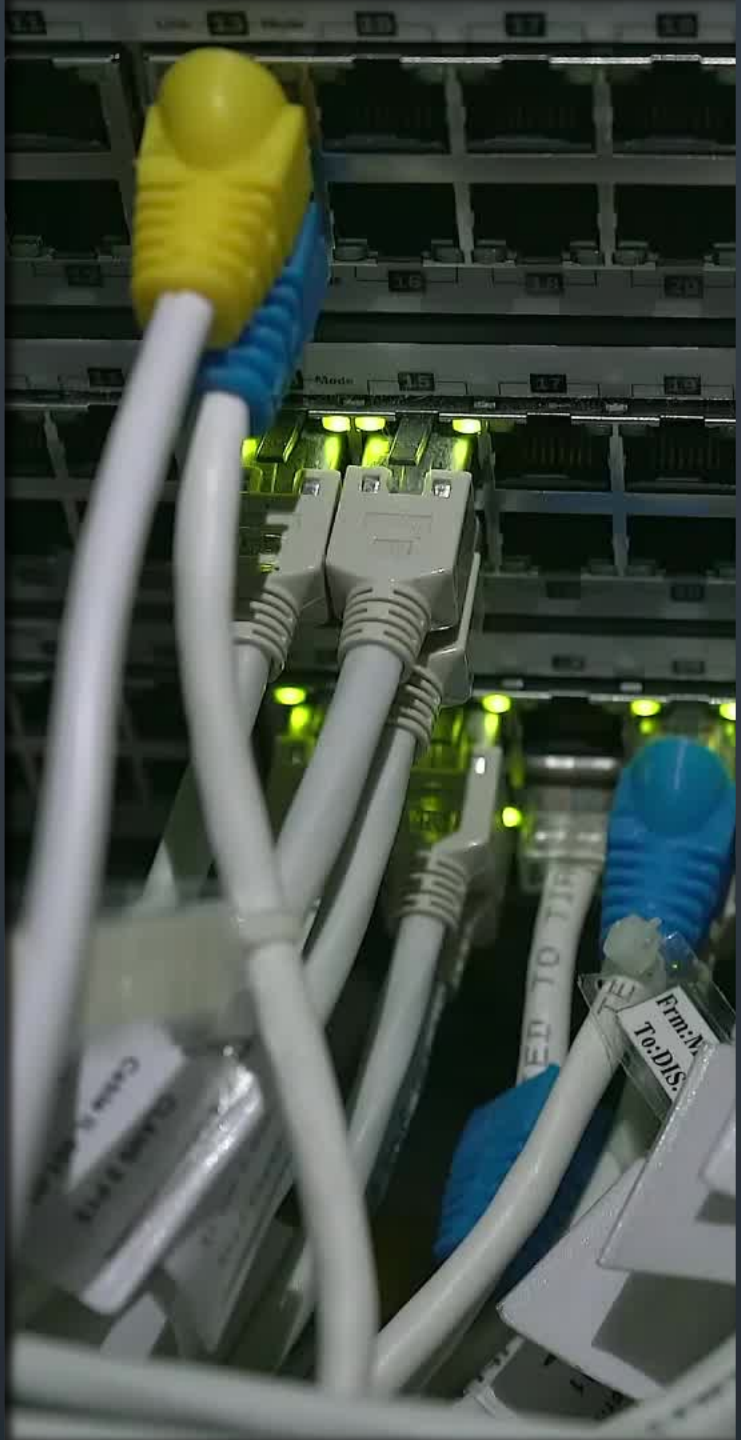
- Ham Radio Is Not Just A Hobby – We are an Infrastructure that can be called upon during disasters to support communications!
- Almost all equipment being produced now is firmware driven or requires software for interfacing various other features
- The Personal Computer now resides in almost every radio shack around the globe
- 90% or better of the components, software, and devices as a whole are manufactured/created overseas and are not monitored or screened the way other critical infrastructures are…
- Many countries, organizations, hacktivists, and individuals present a real threat to any infrastructure they may view as an easy target – Ham Radio is an Infrastructure!



Where does this apply to Hams??

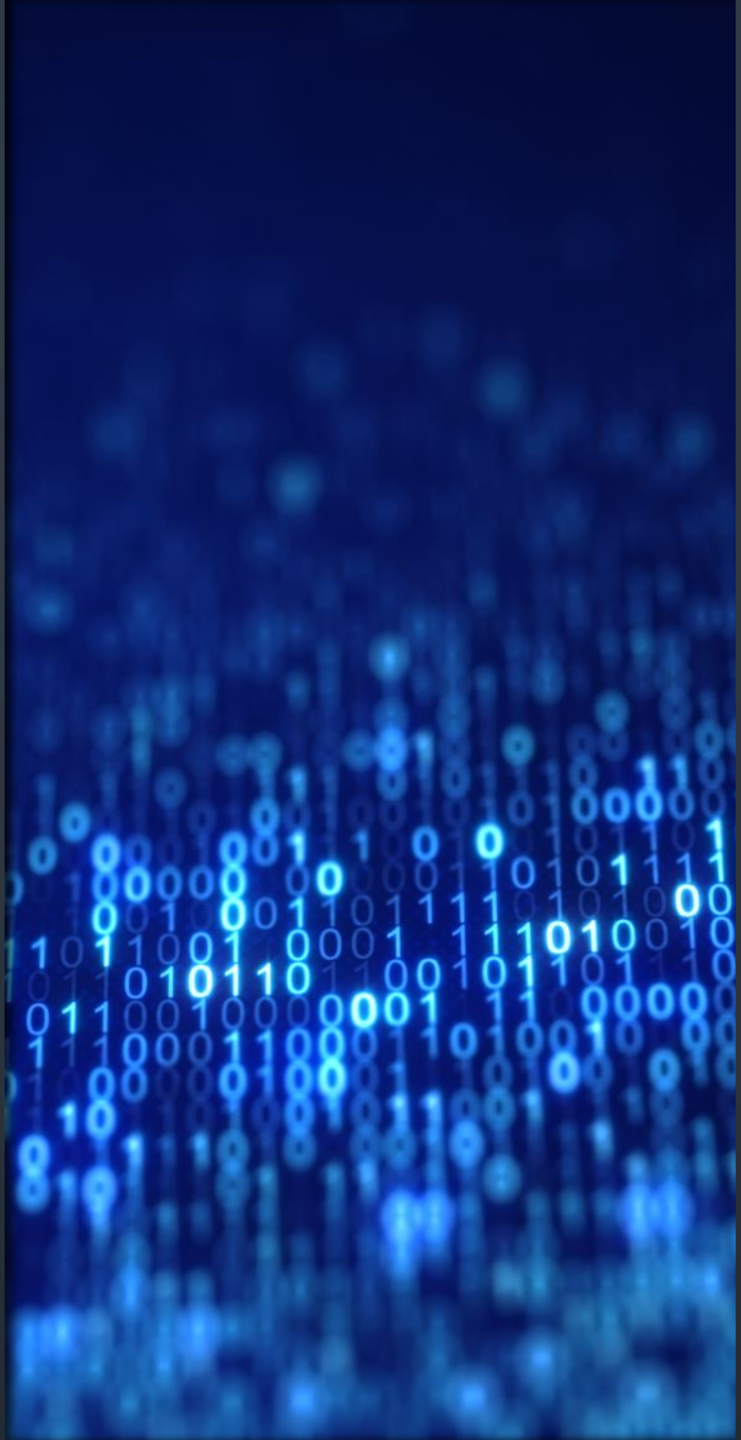
- Firmware updates – Radios and Equipment now use Bluetooth, Ethernet, Wi-Fi, Remote Access Software, and other advanced features.
- Software Control – Programming HTs/Mobiles, Digital Control (CAT/CI-V), Radio Sound Interfacing, Setting up remote access
- Computer Software – Operating Systems, Digital Modes, Rotor Control
- Email – This is the number one threat vector no matter who you are!

THINGS WE SHOULD TAKE SERIOUSLY AS HAM OPERATORS…



Home Networks

- Most modems (Cable, Fiber, etc.) have a built-in firewall – Is It Turned On?
- What Anti-virus are you using – Microsoft Defender is ‘ok’ but not a solution
- Ever shared your Wi-Fi password? Change it once in a while…
- Are all the devices on your home Network Protected? Lateral movement is a thing!



Computers and Devices

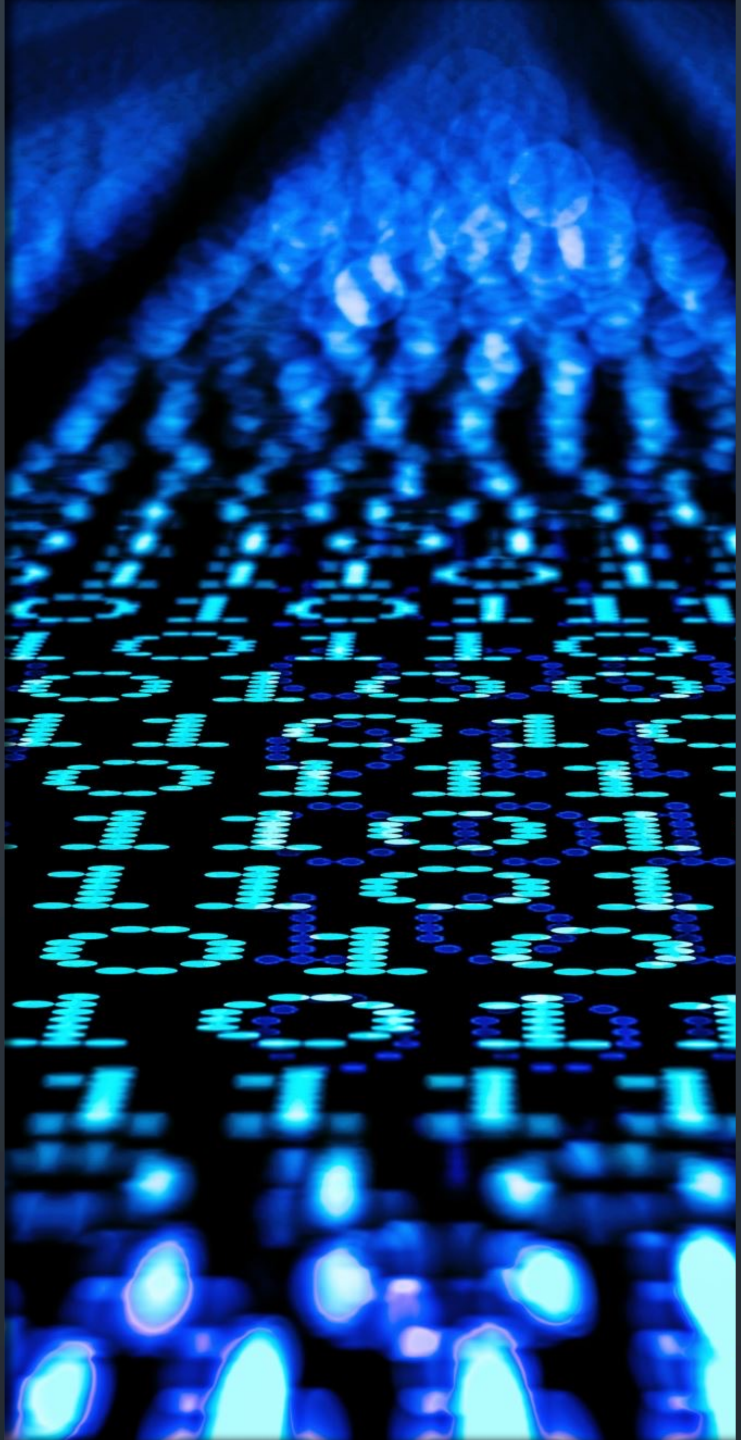
- How up-to-date is your operating system? Are you still running Windows 7? Vista? XP? – they are "End of Life" OS's with hundreds of vulnerabilities!!
- What Anti-virus software are you running – Does it provide "whole system" protection to include web browsing, auto-updates, etc.?
- Are all your computers protected?
- Do you verify that software you install is directly from the vendor/manufacturer or an actual "OEM" copy?
- Do you scan your computer or new thumb drives?

THINK BEFORE YOU SURF FOR SOME MANUAL OR DOWNLOAD SOMETHING!

- Some of the overseas manufactured radios have obscure sites to download updates from – double check what you are downloading.
- This special firmware update I found automagically unlocks MARS – it means I won’t have to cut the red wire and crush diode 4927 – Careful!!
- I can’t find a manual for this 1992 obscure import transceiver, I can google it! – Some sites are programmed to echo your search to lure you in, Be careful!

Ham Radio is not a Huge Target – Yet…

- As we advance our ham shack and our club or group stations – the risk will increase. Cyber-warfare is now part of tactics used by other countries to disrupt communications.
- Any chance a scammer gets, they will take… it pays well for them to risk targeting a new user, club, or platform
- We, as Amateur Radio Operators, are programmed to experiment – just use caution when it involves technology.
- As the numbers grow, we are more likely to see these threats increase



USE THE RIGHT RESOURCES…

- Use an anti-virus *SUITE* (Malware Bytes, Sophos, Bitdefender, etc.)
- Keep software up to date – especially you’re AV and OS
- If something looks strange – don’t click it, think or ask someone that knows
- Feel free to reach out to me – I will answer as time permits

QUESTIONS

- My email is N3BYR@ARRL.NET (My response will be from a yahoo or special domain email)
- I use Winlink and Packet for mail messages though this time of year my response my be delayed

THANK YOU