- I’m here to render some perspectives on cyber defense & offense, based on about 40 years in the field
    - I’ll keep it unclassified
- 40 years ago we were protecting mainframes. Personal computers were not quite around yet.
- Biggest national threat was the Soviet Union stealing national level information
- Computers were expensive and used by many
- Rainbow series had not yet come out (TCSEC 1983).

- Late 70s/early 80s had proofs showing that testing could never find all flaws, so government funding switch to formal methods away from testing

- 1980s saw proliferation of PCs and workstations, early Ethernet and Internet.
    - C2 by 92 mantra

- 1988 was the Morris worm —
    - Big shock to the system — number of non-certified systems, speed of problem, range of sites hit

- 1989 formation of the CERT/cc (DOE CIAC was there first)

- early 1990s, focus on intrusion detection

- my early conversations with Bill Black, Brian Snow, Becky Bace, Jim Anderson and others. Bill left the agency in 1997 and returned in 2000 as deputy director.

- Need for something beyond individual systems — network centric, tactical awareness

- NTOC was created in 2004, inspired in part by the NSOC

- I was working with Air Intelligence Agency in 1990s. They developed the virtual honey net, had developed signal capture envelopes to test new items

- As I told Bill, I expected AF to be first, Navy second, and Army 3rd. (Talk about spheres of operation, 2d, 3d, EWF). Ware and Anderson reports (1967 DARPA, 1972 for AF)

- History of cavalry in the Army: 1778 to 1950 (armor)

    - The last horse-mounted cavalry charge by a U.S. Cavalry unit took place on the Bataan Peninsula, in the Philippines in early 1942. (had to eat the horses.)

    - 10th Mountain Division non-calvary charge any Army organization while engaged in Austria in 1945.[9] An impromptu pistol charge by the Third Platoon 14–23 April 1945.

    - Chief, the last surviving tactical horse of the United States Cavalry, died in 1968, at the age of 36.

    - 1st Calvary Division has ceremonial 40 horses

- Space Command, then Evolution into Cybercommand

- Still not quite where it should be as individual service leaders tend to see the capability as supporting their own areas rather than as independent operations. Also, the Title 10/Title 50 conflicts throw some off.

- 20 years ago it was mostly O1s and O2s, plus warrant officers. Now seeing maturation, with talent up and down the ranks.

- Future: We perhaps need a new service? Cyber is here to stay. Also need to include psyops (consider Russian meddling)

- Some other topics….

- What is security? (History of the C-I-A model). Robert Courtney first recipient of the National Computer Systems Security Award. Died about a decade ago

  - Nothing useful can be said about the security of a mechanism except in the context of a specific application and environment.

  - Never spend more mitigating a risk than tolerating it will cost you.

  - There are management solutions to technical problems but no technical solutions to management problems.

- Donn B. Parker’s Hexad (add authenticity, possession/control and utility)
- Absolute security is not achievable
    - Against hackers, probably
    - Against organized crime, probably
    - Against malware, less certain
    - Against nation state actors, more difficult
    - Against UFO invasion — what?
    - Against Extinction Level event?
    - Maybe move out to a colony on Mars, but then death of the sun will consume all the inner planets so time is a factor

- I will define it as “trust” and “awareness” — trust in people/technology, awareness of threat/technology possibilities, cost, lifespan

- We use assurance methods to gain higher levels of trust. This include formal methods and testing — neither is sufficient by itself

- Management has to understand these things! Also, speed is not conducive to getting things right

- We need to have trust in supply chain and 3rd parties
- That also means trust in data provenance
- Target attacked via HVAC systems in 2013
- Casino attacked via fish tank controls, 2016
- Android games online
- Ccleaner software
- Taiwan translation

- Supply chain is both a vulnerability and an opportunity.
    - Lowest bid is not our friend, nor is unduly tight scheduling
    - Thinking about long maintenance tails may give an interesting possibility for attack.

- Farewell Dossier, 1981-1982, Colonel Vladimir Vetrov
    - Handled by French intelligence
- Unit Line X
- Mitterand gave to Reagan
- trans-Siberian pipeline disaster in 1982
- Vetrov executed in 1985 after love triangle

- Kaspersky

- Phoning home with virus data. Not unusual, although most use some kind of encoding. (Symantec, Norton)

- Apparently, Israel was monitoring the traffic and saw US classified material from NSA

- Kaspersky offered open source viewing

- Now, it appears CIA was using Kaspersky's identity to hide their own exfiltration

- Design vs adhockery
- A program that has not been specified cannot be incorrect; it can only be surprising. Earl Bobert 1985
- Adding on afterwards leaves you in an uncertain state. Patching is not securing

- Understanding the art of the possible, and how far technology can be pushed is part of awareness

- Spycraft by Robert Wallace and Keith Melton (Bob was Director of CIA's Technical Services Branch)

- Glomar Explorer, Project Azorian, 1973-1974, depth of 3 miles. Glomar Challenger for drilling

    - Soviet submarine, K-129, March of 1968

    - Equivalent of $1.7 billion

- Enigma machine
- Venona papers, 1943-1980
  - part of a project that discovered the Cambridge 5 and Manhatten spies
  - Reuse of one-time pads, and employment of computer algorithms

Summing up

- It is worth studying the past, both to understand failures, and to get a proper perspective on time

- It is important to understand who and what we trust, and why. Then DOCUMENT it!

- Understand context

- The old “Fast, good, or cheap — pick 2” is true, and may only be just 1.

- Understand you are defining a field of endeavor, for the military and for the nation. Do what you can to make choices wisely.