Cold War Military Technology and You

How the Cold War is Responsible for the Technology You Use Every Day

The Cold War Museum
7142 Lineweaver Rd
Vint Hill Farm
Warrenton, VA 20187

Introduction

The Cold War was a time of incredible international tension, where nuclear armed superpowers with diametrically opposed political systems clashed on the world stage.

The threat of armed conflict, Communist domination of the world, or even catastrophic nuclear destruction drove the development and improvement of multiple technologies for critical military and national security requirements.

This is the story of some of those Cold War technologies that you may use every day without even realizing it.

- Digital Voice Communications
- Spread Spectrum Communications
- Satellite Navigation
- Distributed Adaptive Communications Networks

Digital Voice Communications

Digital Voice Communications

At the beginning of World War II, the U.S. Army Signal Corps had a problem, securely communicating via voice from Washington to commanders around the world.

While offline and online encryption devices and systems existed for written communication, there was no way to provide secure, realtime voice communications with field commanders.

This problem is especially acute in the case of President Roosevelt communicating with British Prime Minister Winston Churchill in London.

Digital Voice Communications

All Transatlantic telephone communications between the United States and Britain had to go via radio. The radiotelephone link was subject to interception by the enemy.

The AT&T Bell Labs had developed the analog A-3 scrambling system to provide privacy on the radio link, but it was only intended to prevent protection from casual radio listeners, not a determined or skilled enemy.

At the end of World War II, the Allies captured a German Reichspost (Nazi Post Office) radio site in Holland where German engineers had built an A-3 descrambler and were decoding monitoring the Allied radiotelephone communications.

Digital Voice Communications

An engineer at Bell Labs, Homer Dudley, had been working on a device known as a VOCODER (VOice CODer and decodER) which could take human speech and convert it into low speed data signals which could be transmitted on a low speed circuit, like the Transatlantic telegraph cable circuit.

In the late 1930s, the Dudley VOCODER was considered more of a laboratory curiosity than a practical telephone instrument, since it was too expensive and produced low quality speech.

Digital Voice Communications

The Dudley VODER (Voice Operation DEmonstratoR) was demonstrated at the 1939 World's Fair in New York City, where specially trained operators used the VODER to produce some of the first synthesized human speech.

Digital Voice Communications

The US Army Signal Corps issued a contract to Bell Labs for the development of a truly secure voice encryption system to secure the Transatlantic telephone link and other strategic radiotelephone links around the world.

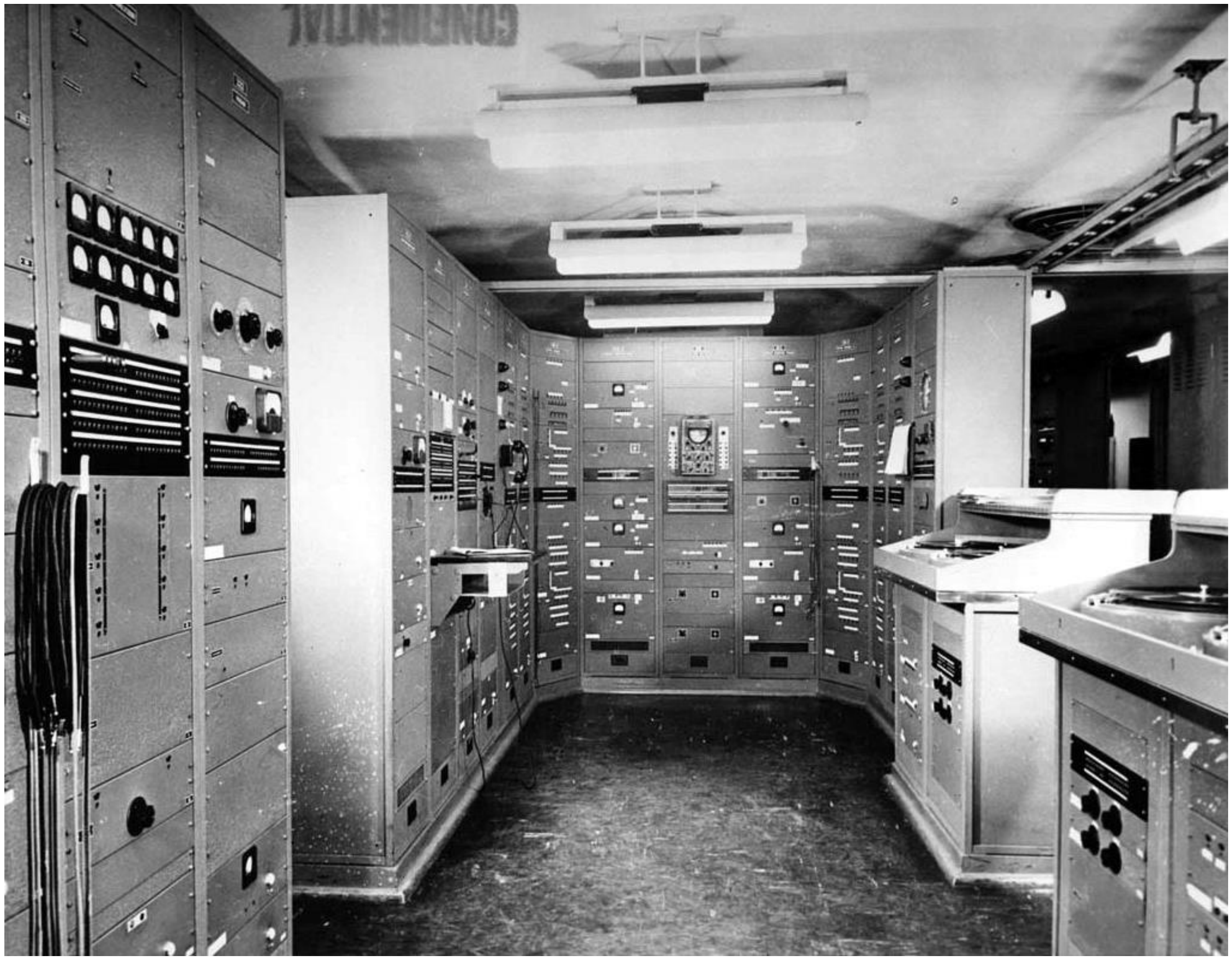
The system used the Dudley VOCODER and a One Time Encryption Key on phonograph records. The output from the twelve VOCODER data channels was added to the random encryption key from the records to create an encrypted signal.

The encrypted signal was then sent to a twelve channel, Six-Frequency Shift Keyed (6-FSK) modem for transmission over the air.

This system was assigned the Signal Corps codename SIGSALY.

Digital Voice Communications (1942)

SIGSALY (System-X) (The Green Hornet)



Forty 7 ½ foot equipment racks
55 tons (80 tons with generators and air conditioners)
Cost $1 Million per terminal

Digital Voice Communications (1942)

SIGSALY Block Diagram

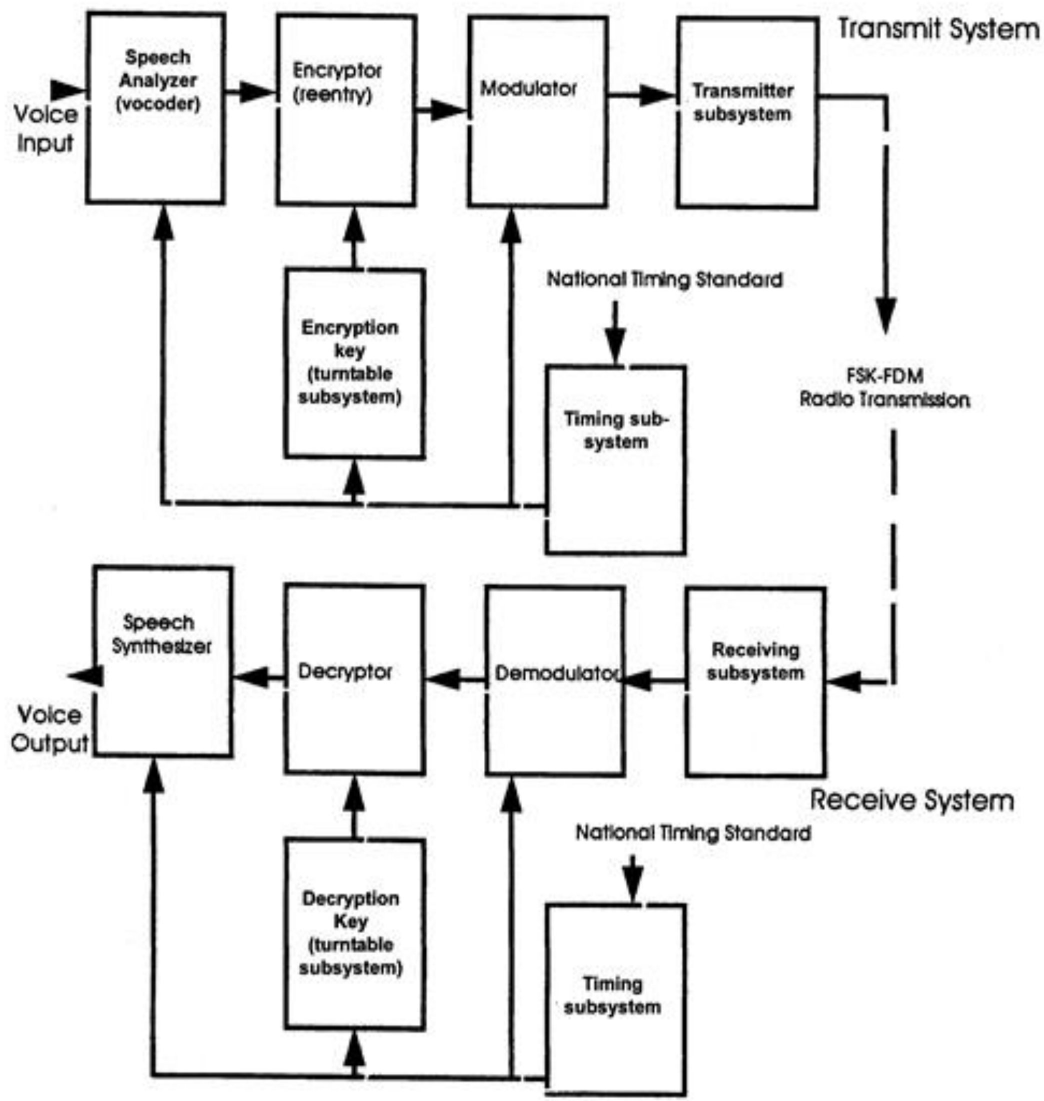


Diagram from
http://jproc.ca/crypto/sigsaly1.htm

Digital Voice Communications (1942)

SIGSALY VOCODER
Encoding/Decoding
Block Diagram

Encryption of the 12
transmission channels
In red is not shown.

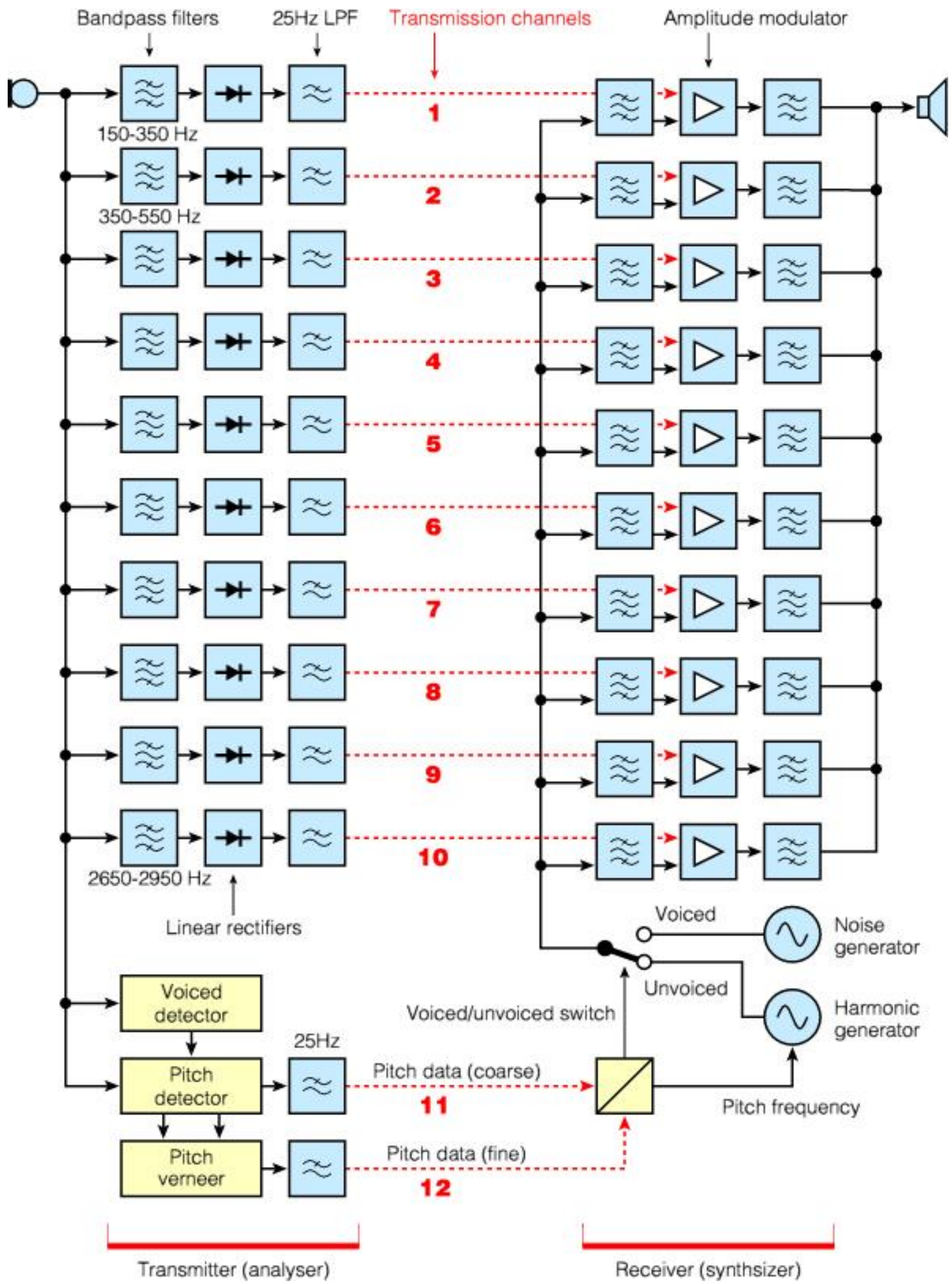


Diagram from
www.cryptomuseum.com

Digital Voice Communications (1942) SIGSALY

SIGSALY Record Turntables

SIGGRUV Master (Gold) and pressed vinyl record

SIGGRUV record compared to a CD

The SIGSALY One Time encryption keys were contained on 16 inch diameter, 78RPM records.

Each record held 12 minutes of encryption key.

The records were used once and then destroyed.

Digital Voice Communications (1942) SIGSALY

“The Green Hornet”

The system was nicknamed the Green Hornet, since the transmitted signal sounded like the opening sequence of the popular Green Hornet radio drama.

Digital Voice Communications (1942)
SIGSALY

This is a multichannel Frequency Shift Keying (FSK) signal similar to the SIGSALY encrypted signal.

German radio intercept operators intercepted and recorded the SIGSALY signals but since it does not sound like scrambled voice transmissions, they did not recognize that these signals were actually encrypted voice.

The German operators assumed that it was some type of multichannel teletype transmission.

Digital Voice Communications (1942) SIGSALY

- The audio quality on the SIGSALY system wasn't particularly good, but it met military operational needs.
- With the use of the One Time random encryption key from special 16 inch, 78RPM phonograph records, and the digital encoding, encryption, and transmission of the voice signals, it was a truly secure system.
- This allowed classified conversations to be conducted via telephone and radio connections throughout the world.
- Eventually a dozen SIGSALY units are constructed and deployed.

“The AFSAY KO-6 was operated over the radio circuits from San Francisco to Washington DC.”

Digital Voice Communications (1950s)

KO-6 PHOEBE (1955)

Weighs 2400 pounds
Size of three refrigerators

Digital Voice Communications (1960s)

KY-3 Wideband

250 Pounds

KY-9 Narrowband

565
Pounds

First generation transistorized equipment

Significant reduction in size and weight from
the older vacuum tube equipment like the KO-6

Digital Voice Communications (1960s)

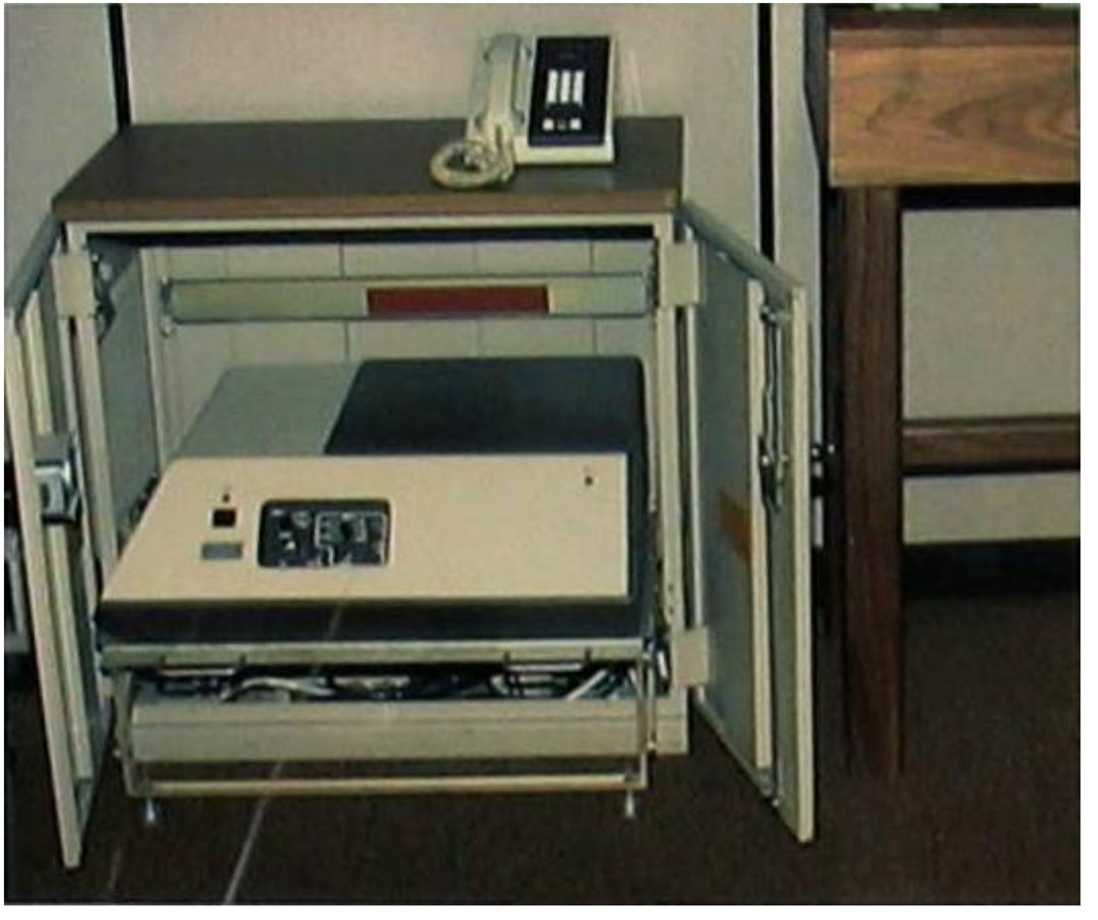
KY-38 NESTOR
Portable

PRC-77 radio
(25 pounds)

KY-38 NESTOR
encryption unit
(35 pounds)

Digital Voice Communications (1970s)

Secure Telephone Unit (STU-II)   KY-71



Size of a microwave oven
(60 pounds)

Integrated circuit technology

Digital Voice Communications (Mid 1980s)

STU-III

Desktop phone
(8-10 pounds)

Digital Voice Communications (2000s)

SECTERA Terminal

10 ounces

Digital Voice Communications

Until the late 1980s, the primary force driving the development and improvement of narrowband digital voice communications was the military and government need for secure voice communications.

Today's digital VOCODERS are all descendants of the the original Dudley SIGSALY VOCODER.

Spread Spectrum Communications

Spread Spectrum Communications

In the 1950s, the Direct Sequence Spread Spectrum (DSSS) communications was developed to provide virtually undetectable, jam resistant communications.

DSSS involves the use of mixing high speed, wideband, Pseudorandom Noise (Pseudo Noise (PN)), signal with a normal narrowband signal in order to produce a wideband, noiselike transmitted signal with low power density.

Direct Sequence Spread Spectrum Communications offers several advantages over conventional modulation;

- Low Probability of Detection/Intercept (LPD/LPI)
- Anti-Jamming (AJ)
- Enhanced Ranging and Navigation Performance
- Multipath propagation resistance
- Code Division Multiple Access (CDMA)

Spread Spectrum Communications

DSSS involves the use of mixing high speed, wideband, Pseudorandom Noise (Pseudo Noise (PN)), signal with a normal narrowband signal in order to produce a wideband, noiselike transmitted signal with low power density.

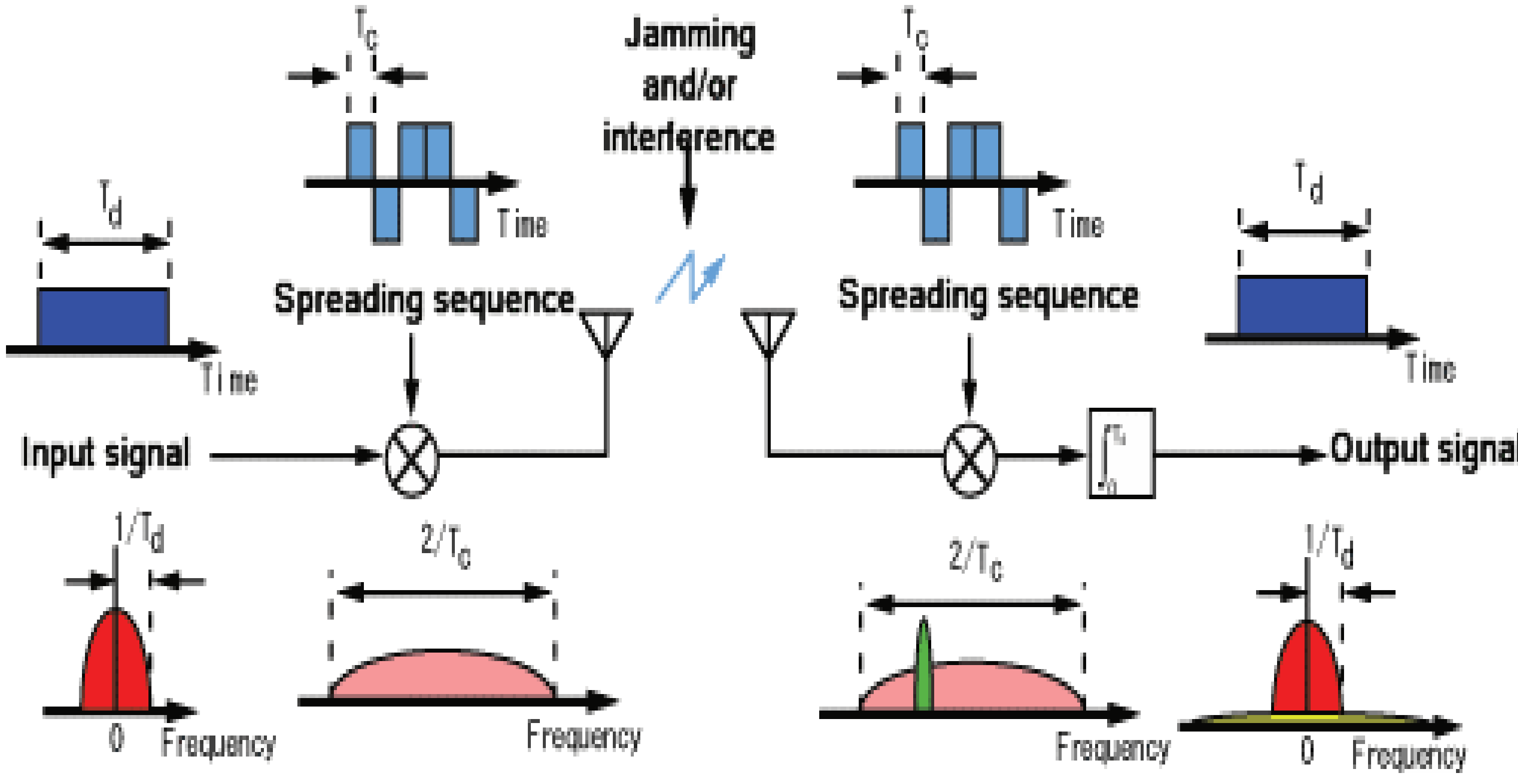


Diagram from Tachikawa Laboratory http://www.nagaoka-ct.ac.jp/ec/labo/info/eng.html

Spread Spectrum Communications

Direct Sequence Spread Spectrum was first applied to military communications, navigation, and radar systems in the early 1950s.

Most of these systems were classified at the time.

In the 1970s, spread spectrum was used in a number of unclassified applications, mostly in NASA space applications, such as deep space probes, and later in the NASA Tracking and Data Relay Satellite System (TDRSS).

Spread Spectrum Communications

The wideband, low density, noiselike signal is difficult to detect, especially since it can blend into the naturally occurring background noise making it virtually impossible to detect and intercept (Low Probability of Detection (LPI)/Low Probability of Intercept (LPI)).

Direct Sequence systems can even be used on radio bands where other narrowband signals are being used at the same time, since the spread spectrum signals won't interfere with the narrowband signals, and the narrowband signals won't interfere with the spread spectrum communications.

Spread Spectrum Communications

The receiving stations have an identical PN noise signal generator to the transmitting station. When the locally generated PN noise is exactly synchronized to, and mixed with the incoming signal, the noise modulation is canceled out and the original signal is recovered. This is known as **Correlation Detection.**

Any received signal which is not encoded with the same PN code gets spread out in the receiver and appears to the receiver as an increase in background noise against any properly encoded signal. This is the key to the Anti-Jamming (AJ) performance of a spread spectrum system.

The spreading of the narrowband original signal into a spread, wideband signal results in a Process Gain which is responsible for the jamming resistance of spread spectrum signals.

Spread Spectrum Communications

Another added benefit of spread spectrum correlation detection is that different users can be assigned different PN codes.

Each user can use their unique PN code for communications without causing interference to, or receiving interference from other users using different PN codes, even if the users are all using the exact same radio frequency.

This process is known as **Code Division Multiple Access (CDMA).**

While early military use of spread spectrum concentrated on the Low Probability of Detection/Intercept (LPI/LPD) and Anti-Jam (AJ) benefits, later military, and virtually all commercial/civilian uses exploit the CDMA benefits to increase communications system capacity.

Spread Spectrum Communications (1950s)

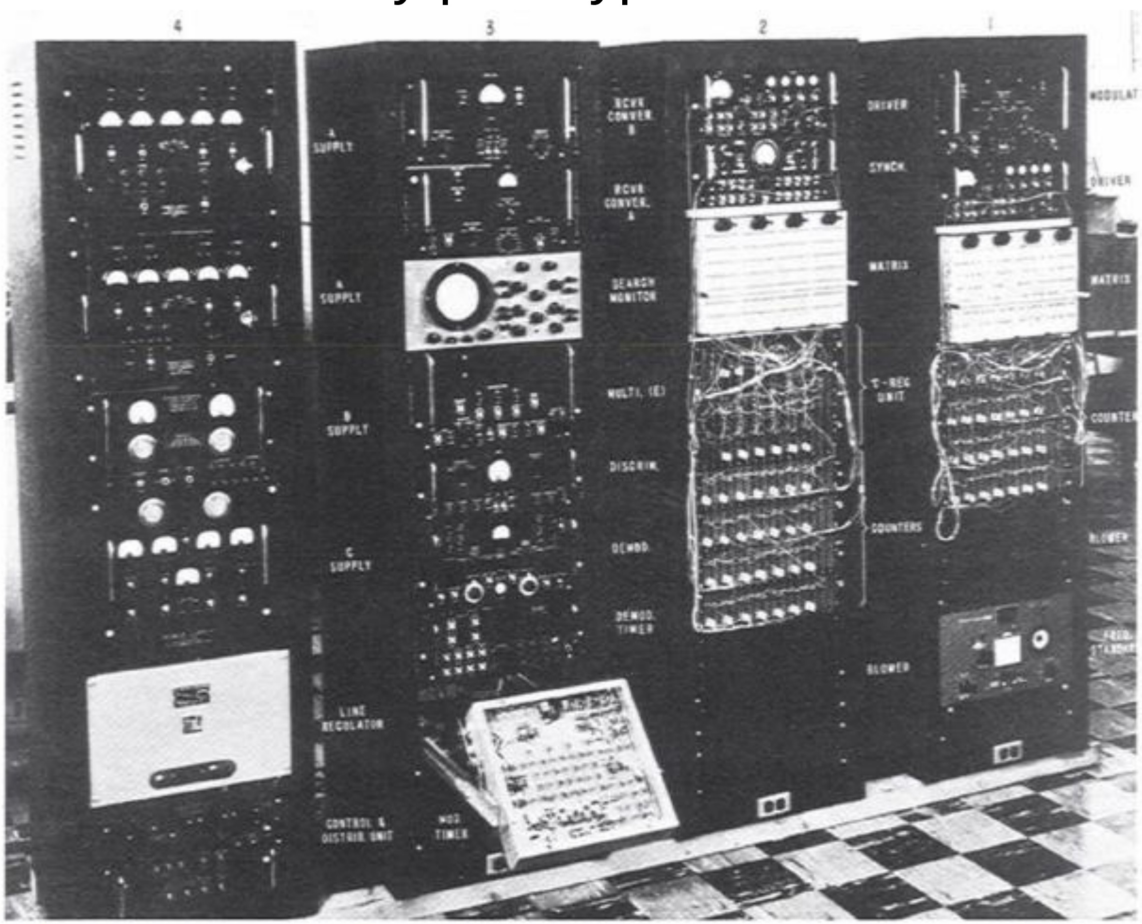
In the 1950s, Sylvania Corporation built the F9C Spread Spectrum Modem for the U.S Army Signal Corps. The F9C modem transmitted a narrowband teletype signal via shortwave radio as a 10Khz wideband, noiselike signal. The spreading of the signal provided approximately 23 Decibels (23db) of Process Gain for the signal.

Because of the Process Gain, a potential jammer would have to transmit a jamming signal 23db (200 times) stronger than than the F9C signal in order to successfully jam it.

The technique used in the F9C system was referred to as NOise Modulation And Correlation (NOMAC)

Spread Spectrum Communications (1950s)

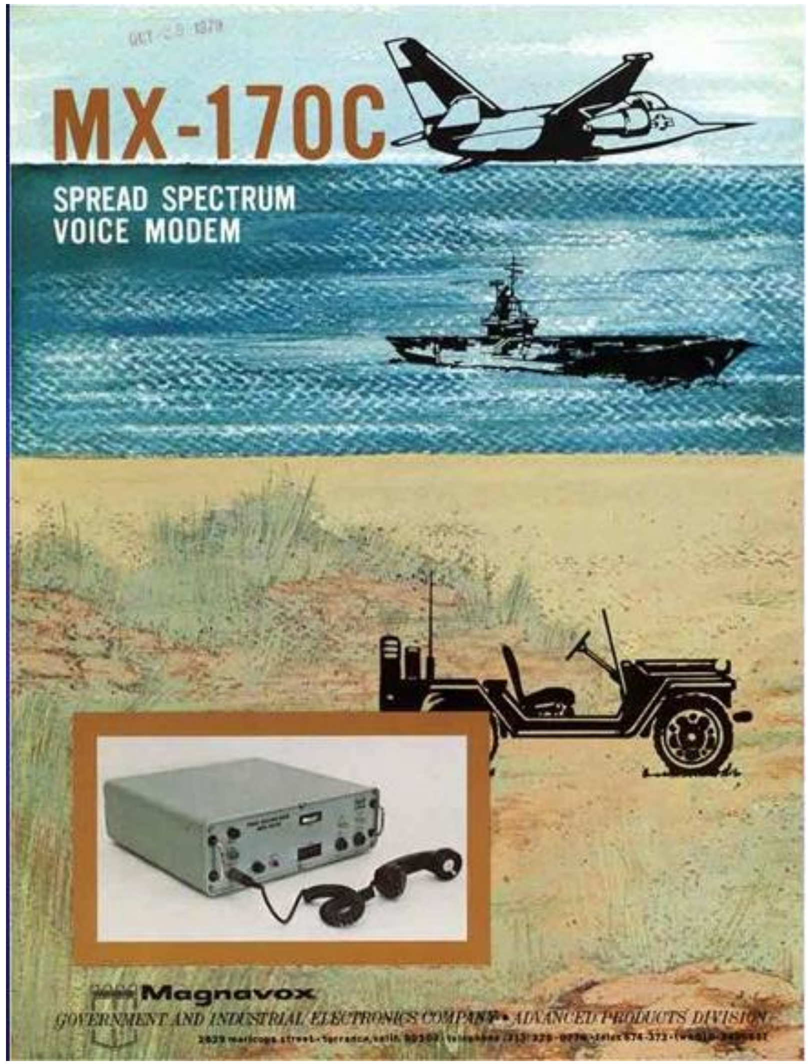
Laboratory prototype F9C Modem



Four 7 ½ foot tall, 19 inch rackmount cabinets
Approximately 2000 pounds

Spread Spectrum Communications (1970s)

By the late 1970s, Magnavox Corporation is producing the MX-170 Spread Spectrum Voice Modem for use on military radios.



Weight 40 pounds

Spread Spectrum Communications (1980s)

By the 1980s, commercial satellite companies begin using Direct Sequence CDMA modulation to increase the capacity of their communications satellite systems.

Boeing Wideband Global Satcom(WGS) Satellite (Picture by Boeing Corp.)

Spread Spectrum Communications (1990s)

In the 1990s, with the availability of high speed, low cost digital electronics, and Digital Signal Processing (DSP), Spread Spectrum Communications techniques are introduced into a wide variety of commercial and consumer products.

Direct Sequence Spread Spectrum (DSSS) modulation is a core technology in multiple types of consumer electronic devices;

- 2G, 3G, 4G Cellular telephones
- 802.11 WiFi
- GPS
- Radio control systems (models and drones)

Satellite Navigation

Satellite Navigation

In the 1960s, the US Navy developed and fielded the TRANSIT satellite navigation system.

This system allowed ships and submarines to determine their position on the earth at any time and in any weather conditions without the need for celestial navigation techniques.

Satellite navigation provided a continuous correction capability to Shipboard Inertial Navigation Systems (SINS) to compensate for the long term precession drift in mechanical gyroscope based systems.

Satellite Navigation

The TRANSIT system had several significant shortcomings;

- It only provided Longitude and Latitude information.
- For accurate position information you needed to know your Altitude and Speed.
- TRANSIT was only for stationary receivers, or slow moving vehicles, like a ship or submarine (No aircraft)
- In the early days, your position could only be determined once every 30 to 120 minutes.
- Determining your position during a satellite pass would take 10-15 minutes.

Satellite Navigation

In 1973, the US Air Force and the US Navy Naval Research Lab (NRL) got together to discuss a future satellite navigation system.

As a result of this cooperative effort, the Air Force and Navy combined their work on their different system proposals, the Air Force 621B Program and the Navy Timation (Time Navigation) program, picking the best aspects from each program to produce what became the NAVSTAR-GPS system.

After testing with an experimental Navigation Technology Satellite (NTS-2) in 1977, the first GPS satellites were launched in 1978.

Satellite Navigation

GPS was a dramatic improvement over the TRANSIT system;

- Provides 3 Dimensional (3D) information (Latitude, Longitude, and Altitude)
- Provides precision Time and Frequency information.
- Supports fixed, mobile, high speed aircraft, and even Low Earth Orbit (LEO) satellites.
- Rapid and continuous position information.
- Anti-Jam/Anti-Spoof (AJ/AS) security.
- Selective Availability (SA) to deny enemy use of GPS on the battlefield.

Satellite Navigation

The GPS satellites use Direct Sequence Spread Spectrum (DSSS)-Code Division Multiple Access **(CDMA)** transmission to send navigation signals to GPS receivers.

Spread Spectrum provides Anti-Jam capabilities for GPS receivers.

The use of CDMA allows up to 32 different GPS satellites to operate on exactly the same radio frequency at the same time.

CDMA also permits each satellite to transmit two different signals, a **Coarse/Acquisition (C/A)** signal and a **Precision/Y (Encrypted) (P/Y)** signal on the same L1 carrier frequency.

The 1.023 MHz C/A signal is used for rapid acquisition and synchronization to the satellite, and provides accuracy to about 10 meters.

The 10.23Mhz P/Y signal is an encrypted signal with an accuracy of about 1 meter, for military use only.

Satellite Navigation (1970s)

Early 1978-1979 GPS test system for use on the ground or in cargo aircraft.

Satellite Navigation (1970s)

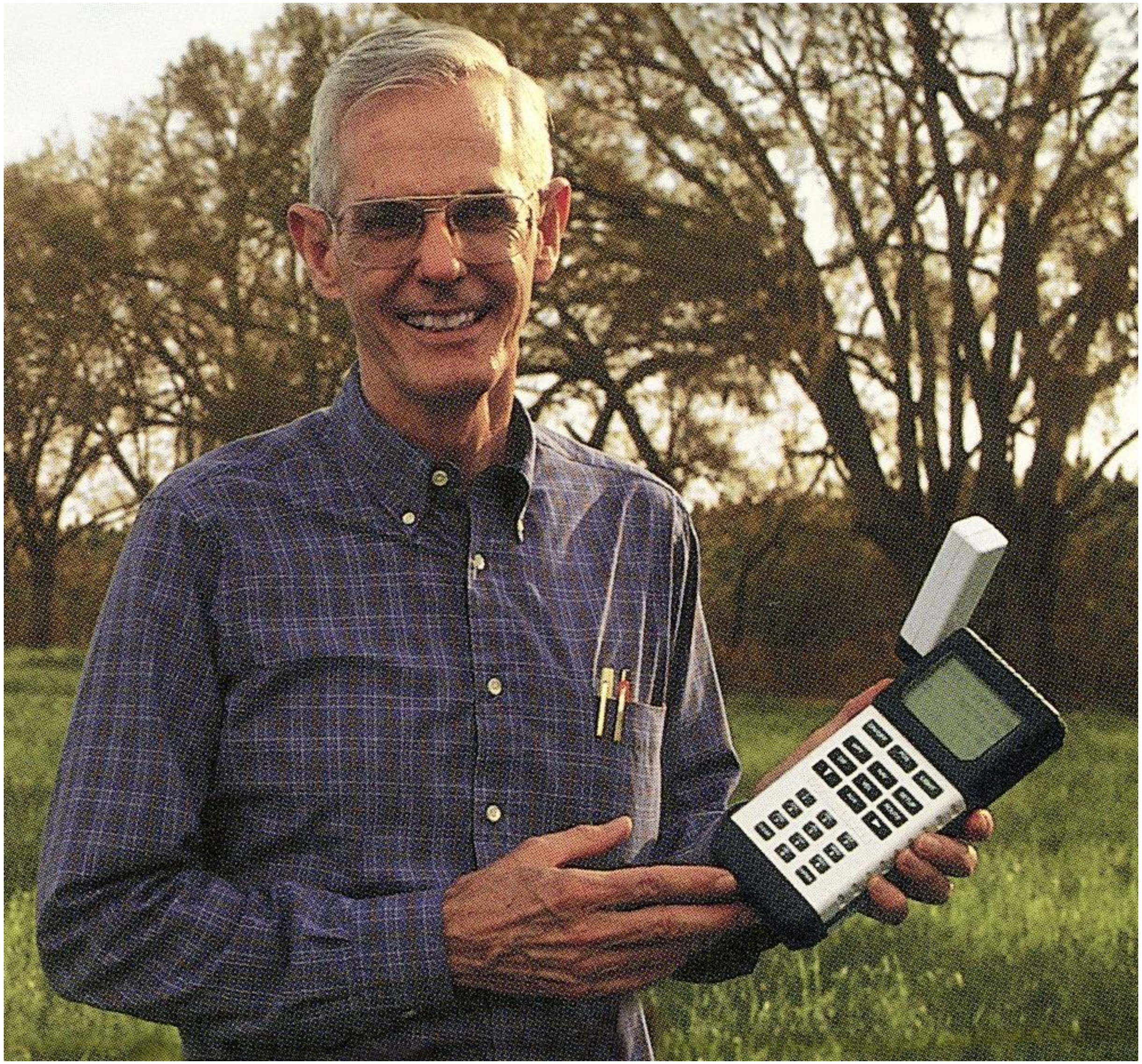
Magnavox System-X   GPS Test system for aircraft and ground use.

Satellite Navigation (1980s)

Early portable, manpack GPS receivers.
Weight 25-30 pounds

Receivers only provide Latitude/Longitude or Military Grid Reference System (MGRS) coordinates. **(Bring your own paper maps)**

Satellite Navigation (1988)



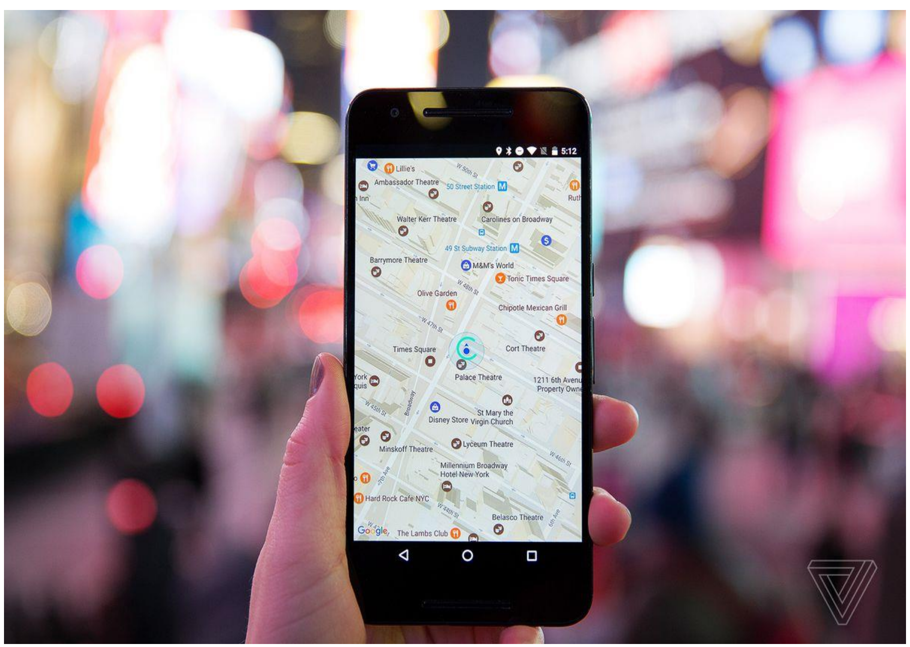
Magellan 1000. The first handheld GPS receiver available to the public.
Weight 30 ounces

Satellite Navigation (1994)

Garmin GPS 45
Weight 10 ounces

Limited internal digital maps

Satellite Navigation (Today)



Distributed Communications Networks

Distributed Communications Networks

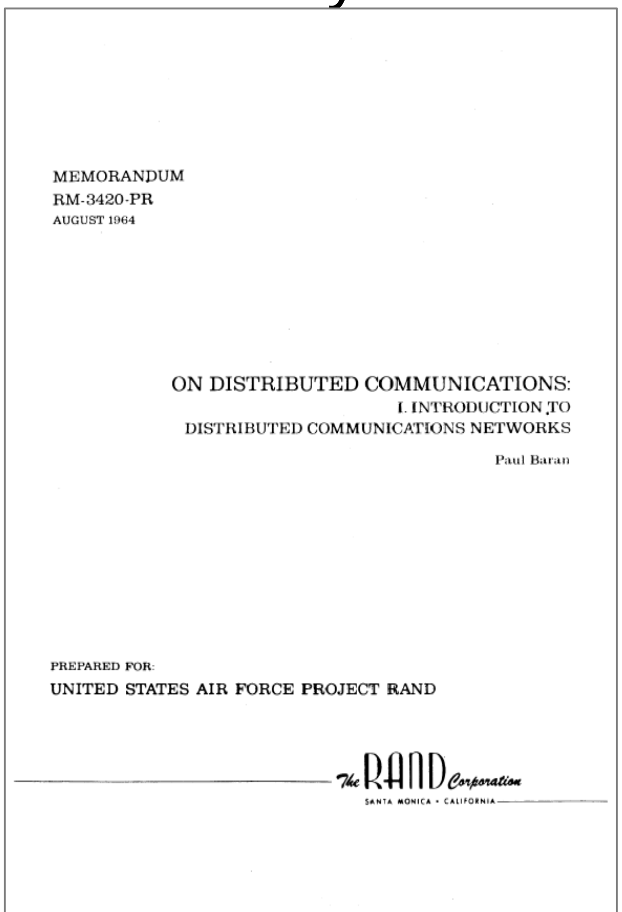
In 1960, the US Air Force tasked RAND Corporation with studying methods of building a survivable communications network which could survive a nuclear attack.

Paul Baran, an engineer at RAND Corporation proposed the construction of a distributed, adaptive communications network with no centralized switching facilities.

By constructing the network as a distributed system with intelligent, adaptive switching nodes, and connecting nodes with multiple links, such a network could remain operational even if individual nodes or communications links were damaged or destroyed in an attack.

Distributed Communications Networks

In 1964, RAND delivered an 11 Volume report “On Distributed Communications” to the Air Force. The Baran report was a study of the design concepts, feasibility, and estimated survivability of such an intelligent network.



MEMORANDUM
RM-3420-PR
AUGUST 1964

ON DISTRIBUTED COMMUNICATIONS:
I. INTRODUCTION TO
DISTRIBUTED COMMUNICATIONS NETWORKS

Paul Baran

PREPARED FOR:
UNITED STATES AIR FORCE PROJECT RAND

The RAND Corporation
SANTA MONICA • CALIFORNIA

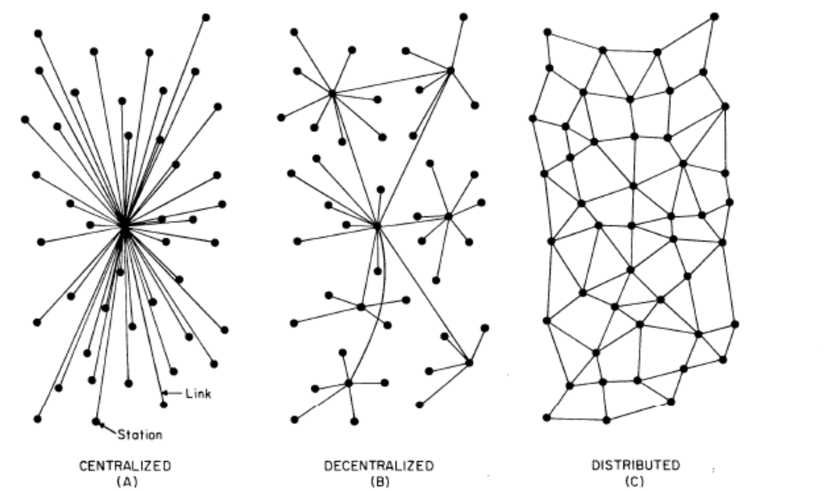


FIG. I — Centralized, Decentralized and Distributed Networks

Distributed network conceptual diagram

https://www.rand.org/about/history/baran.html

Distributed Communications Networks

In the proposed network, all traffic, voice, text, and data would be transmitted in digital form between the intelligent switching nodes.

The switching nodes would constantly monitor the connections to the other nodes in the network and develop routing paths to allow data to be sent between nodes.

As the network changed, or as links, or nodes failed, the remaining nodes would dynamically update their route to insure connectivity to the remaining nodes.

The multiple links between nodes, and the intelligent, adaptive routing of data around failed links and nodes, gives the network its' survivability and reliability.

Distributed Communications Networks

In 1967, the Department of Defense Advanced Research and Projects Agency (ARPA) begins construction of a distributed computer network ARPA Network (ARPANET). The first ARPANET node is installed at UCLA in 1969.

The goal was to allow different types and brands of computers to be connected together. At the time, computers from a manufacturer could only easily talk to other computers and equipment from that manufacturer.

ARPANET was intended to provide a common network communications standard to allow widely separated computers from different manufacturers to communicate with each other.

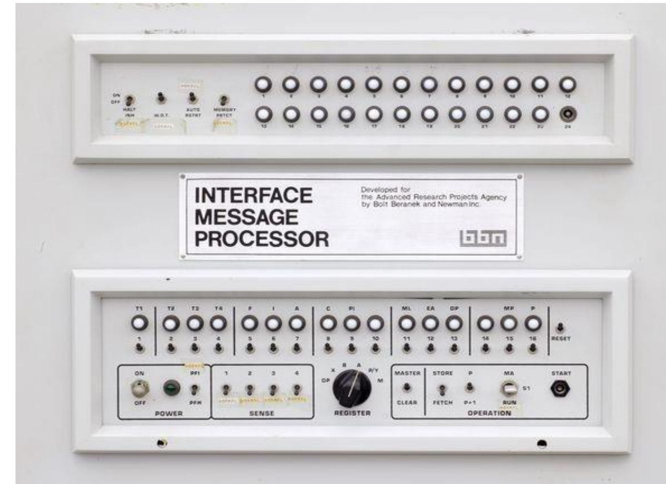
Distributed Communications Networks

The ARPANET concept involved the use of a device, the Interface Message Processor (IMP), containing a dedicated minicomputer, between the computers and the network, and IMPs in the network as switching devices.

The IMP would translate between the user computer interface and the common network communications language, the Network Control Protocol (NCP).

The IMPs were built by Bolt Beranek and Newman (BBN) in Cambridge, Massachusetts.

Distributed Communications Networks



IMP Control Panel

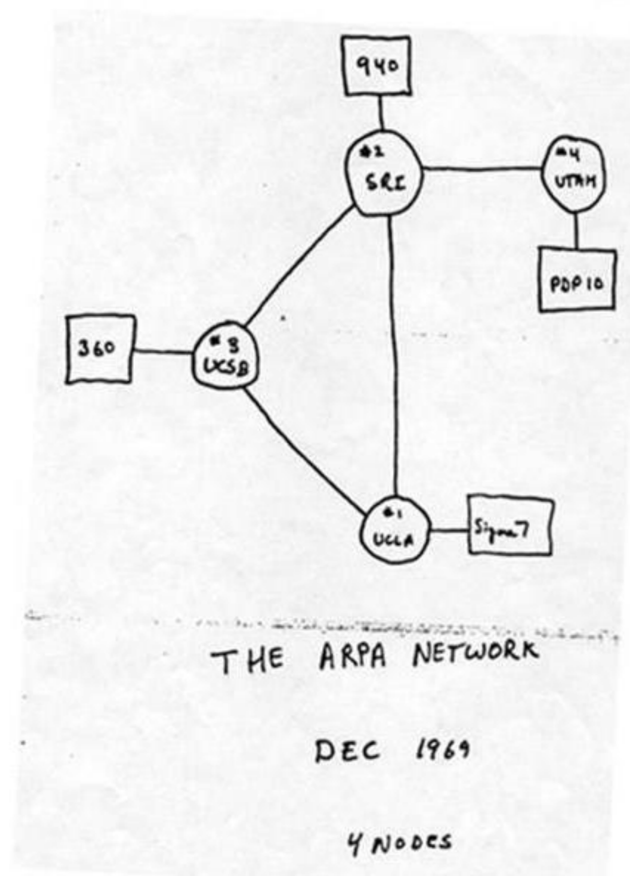
ARPANET IMP Cabinet

IMP Interior View

Distributed Communications Networks

The Birthplace of the Internet

First ARPANET IMP Node
Room 3420 Boelter Hall UCLA



The ARPANET
December 1969

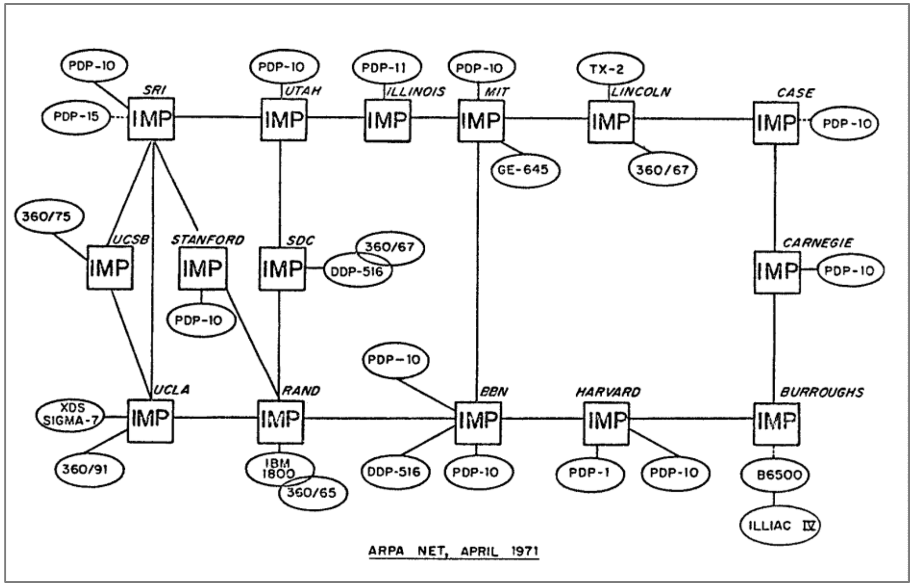
Distributed Communications Networks

In 1972, two BBN computer scientists, Robert Kahn and Vint Cerf develop the Transmission Control Protocol (TCP) and the Internet Protocol (IP) to replace the original ARPANET Network Communications Protocol (NCP).

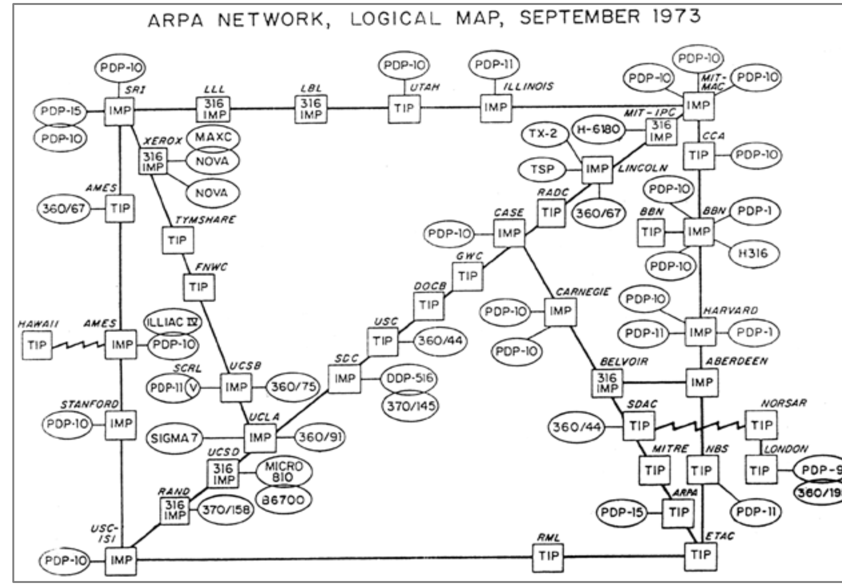
The TCP/IP protocols, with improvements and modifications over the years are the fundamental protocols for the operation of the Internet today.

Distributed Communications Networks

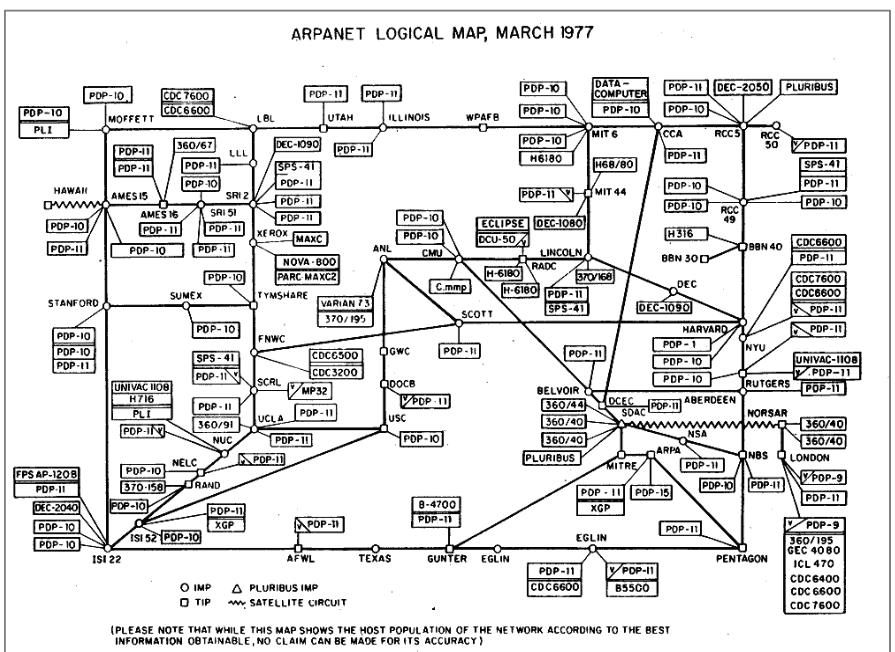
1971



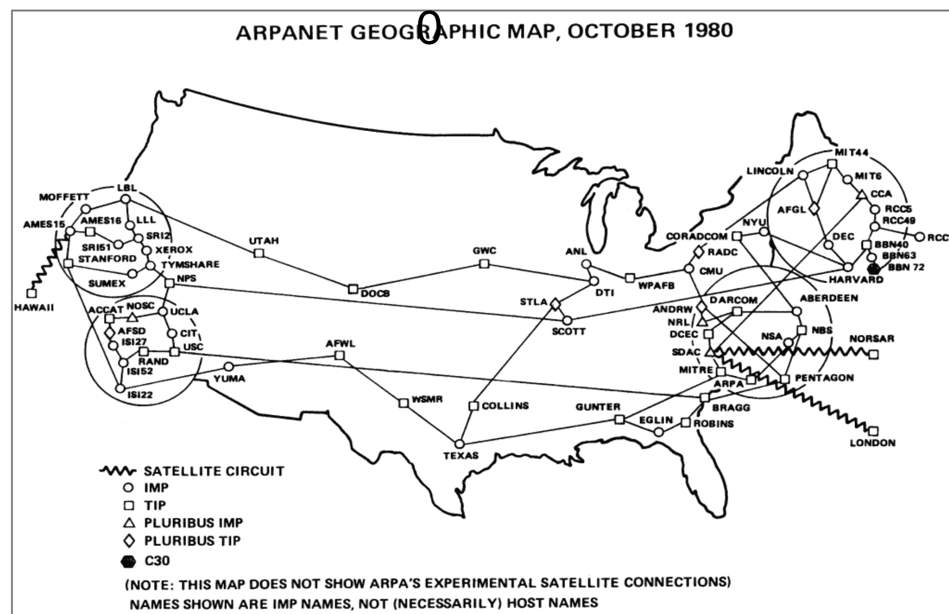
1973



1977



1980



ARPANET to the Internet

ARPA eventually turns over the civilian and educational portion of ARAPENET to the National Science Foundation (NSF) in 1989, while the military part of the ARPANET became MILNET.

The NSF subsequently privatized the network in the 1990s and renamed it the Internet.

As a publicly accessible network backbone, the Internet rapidly becomes the nationwide and then worldwide communications system it is today.

Bringing it all Together

We now have four families of Cold War military technology;

- Digital Voice Communications
- Direct Sequence Spread Spectrum
- GPS
- The Internet

All coming together

Cold War Military Technology in Your Hand

Weight 5 to 6 ounces

Digital Vocoders Direct descendants of SIGSALY and military narrowband VOCODERS

Direct Sequence Spread Spectrum radios 2G,3G,4G cellular standards
802.11 WiFi
GPS receive

GPS US Military worldwide navigation system

Internet Internet network architecture and protocols conceived in the 1964 RAND Corp. Baran Report and implemented in 1969 in the ARPANET

The Cold War Museum

7142 Lineweaver Road
Vint Hill Farm
Warrenton, VA 20187
(540) 341-2008