Exploration of Cryptography

Whitfield Diffie

Distinguished Visiting Professor

Zhejiang University

26 November 2020

Dimensions of the Course

- Theory
- Application
- Culture

Cryptographic Theory

Cryptography has not one theory but many and none of them is the theory that is really needed.

Theories of/in Cryptography

- Information theory
- Algebraic theories
- Probabalistic theories
- Complexity theory

Application of Cryptograhy

The essence of real world cryptography is in actual systems and their implementation.

Cryptographic Culture

Cryptography is a difficult subject to learn. Like many subjects it is broad and complex but unlike most of them, although there is a vast amount of public cryptography, there is a vast amount that is secret and that is largely the fraction closest to the real world.

Course Outline

What follows is a general guideline to the lectures. The topics may vary some and may not align precisely with the class boundaries.

1. Why cryptography?

A broad examination of why we need cryptography: communications, the interception and exploration of cryptography. Discussion of communication systems, the vulnerabilities of communication systems and the history of the protection of communication systems.

1. Why cryptography? (Cont'd)

There are many ways to protect communication systems; why is cryptography special?

2. Basic Notions

Definition of cryptographic systems, associated finite mathematics and information theory, symmetric and asymmetric cryptosystems.

3. Key Management

Getting the keys to where you need them. The impact of the organization on key management and the impact of key management on the organization. The role of asymmetric cryptosystems and quantum key distribution. IPSec and TLS.

4. Building cryptosystems

- Stream and block systems
- Linear shift registers, and other known period processes
- Symmetric block cryptosysems
- Asymmetric block systems.

5. Stream Standards

- Known-period sequences
- Linear equivalents
- Function and analysis of A5
- More recent GSM systems

6. 64-bit block ciphers

- U.S. Data Encryption Standard
- Russian GOST-28147-89 (Magma)
- U.S. Skipjack

7. Message Digest Systems

- MD5
- SHA 1, 2, . . .
- Kechak

8. 128-bit Block Ciphers

- U.S./Belgian: Advanced Encryption Standard
- Russian 128-bit block cipher: Kuznyechik
- Chinese 128-bit block-cipher: SM4
- U.S.: Simon and Speck

10. Key Negotiation and Signature Systems

- Diffie-Hellman
- RSA
- Elliptic Curve Systems
- Digital Signature Algorithms

11. Implementation issues

- Random-number generators
- Side channels
- Secure computing

12. Current Problems Prospects, and Policy

- Homomorphic encryption
- Quantum key distribution
- Promotion of cryptography
- Limitation of cryptography

Tentative Homework and Grading

- Two problem sets.
- About five problems each.
- One given out 2020.12.11 and due 2020.12.18
- One given out 2021.01.11 and due 2021.01.18

Any better ideas? Let me know.

Where do you find Information

- At rest (in storage)
- In transit (communication)
- In use (computation)

Information in Storage

- Essentially writing until recently
- Electrical in 20th Century
- Growing explosively at every level

Communication Over Distance

- Transport of writing
- Heliograph
- Telegraph
- Radio and Television

Communication Over Distance (Cont'd)

- Microwave
- Satellite
- Optical Fibre

Information in Use

- Computation by hand
- Calculaters — 20th Century
- Computers circa 1950
- Transistors, IC's, etc.

Gems of 20th Century Intelligence

- Photint (satellites)
- Sigint

Signals Intelligence

World War I

RADIO

- Interception
- Direction Finding
- Traffic Analysis
- Cryptanalysis

The rise of intelligence is the rise of Sigint

David Kahn

Signals Intelligence

All intelligence derived from the study of radio transmissions and other communications

(ASA September 1946)

Signals Intelligence (SIGINT)

- Comint
- Elint
- FISINT
- RADINT
- TELINT

Structure of (SIGINT)

- Access
- Collection
- Processing
- Exploitation

Structure of (SIGINT) (Cont'd)

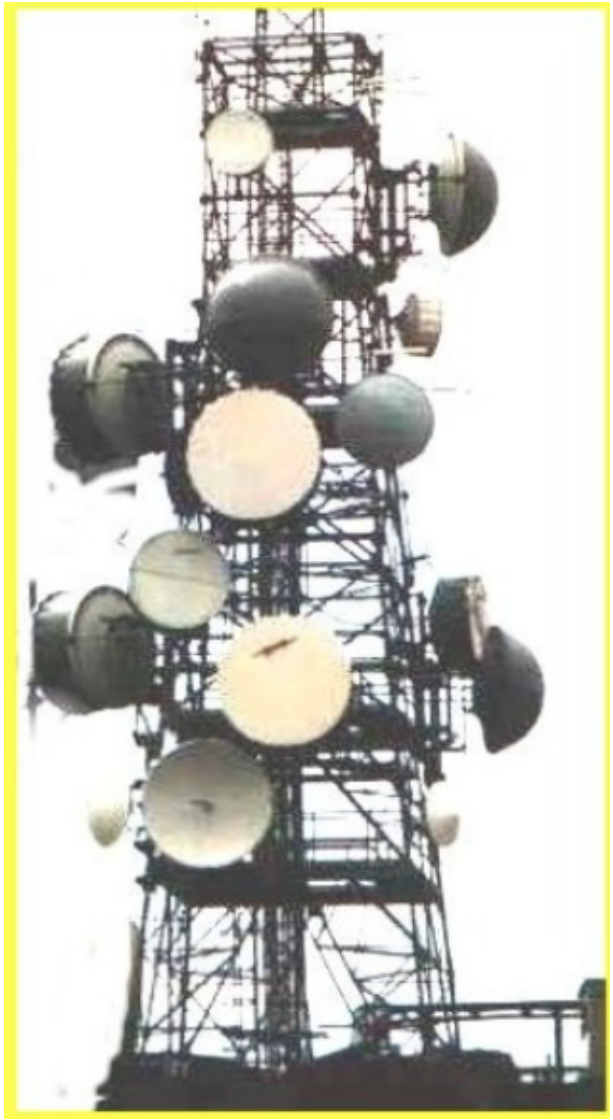
- Analysis
- Reporting
- Dissemination

Access
(pretty pictures)

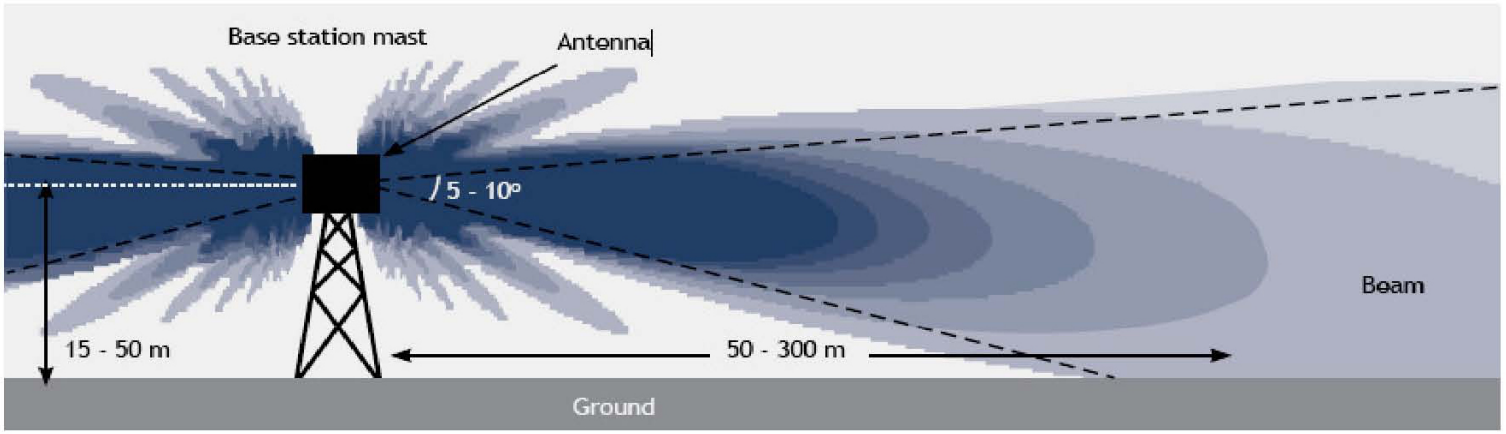
Elephant Cage I

Elephant Cage II

Microwave Tower



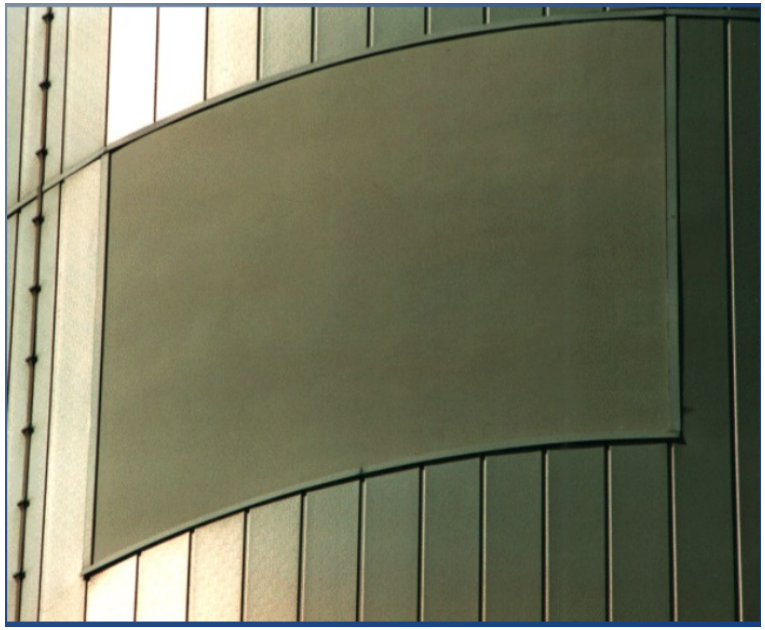
Microwave Antenna Splash Pattern



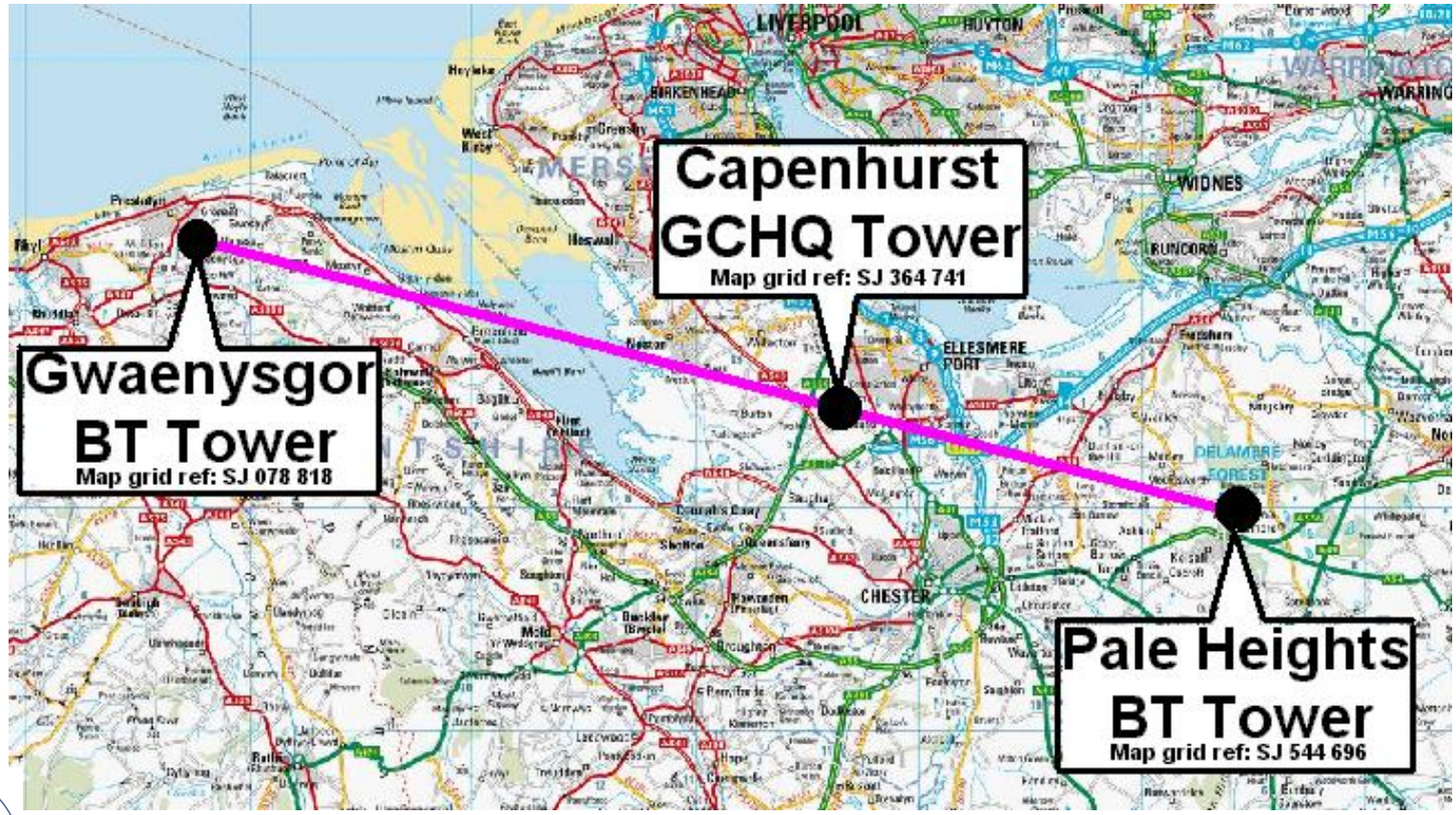
Teufelsberg

Capenhurst Tower

Capenhurst Tower (windows)

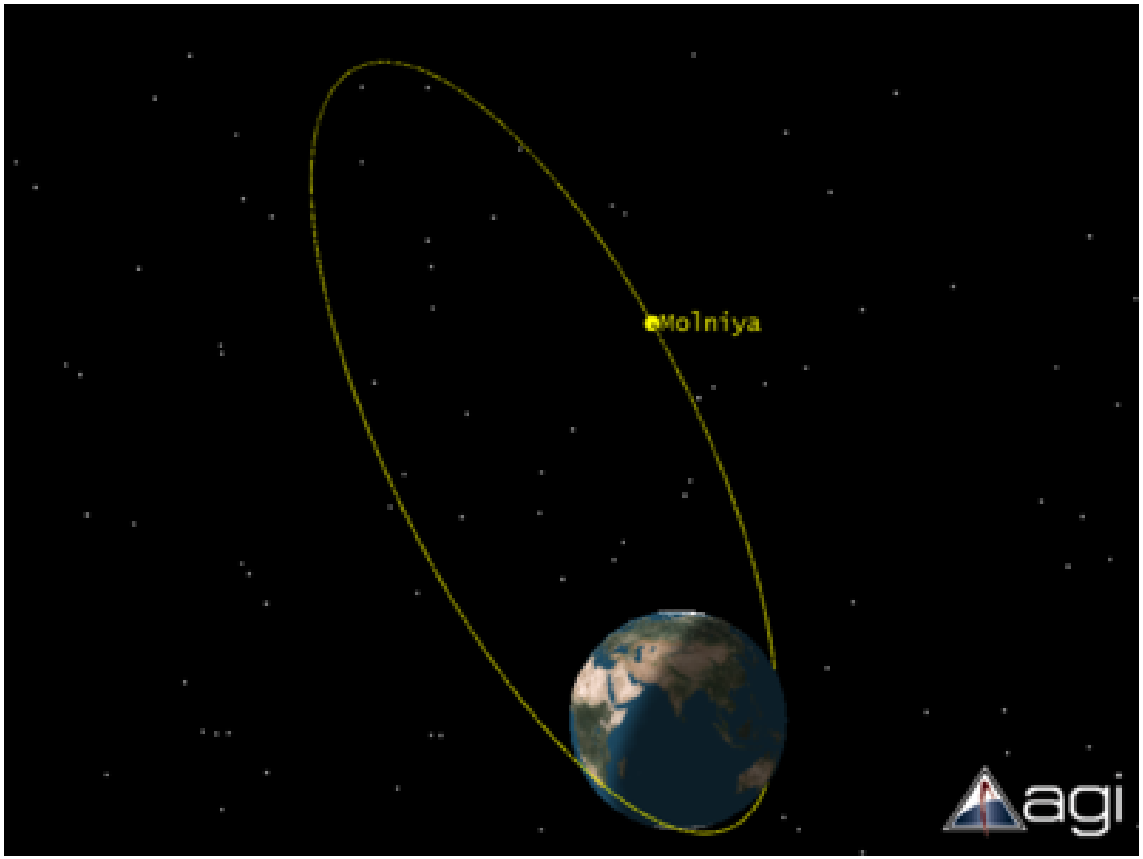


Capenhurst Tower Location

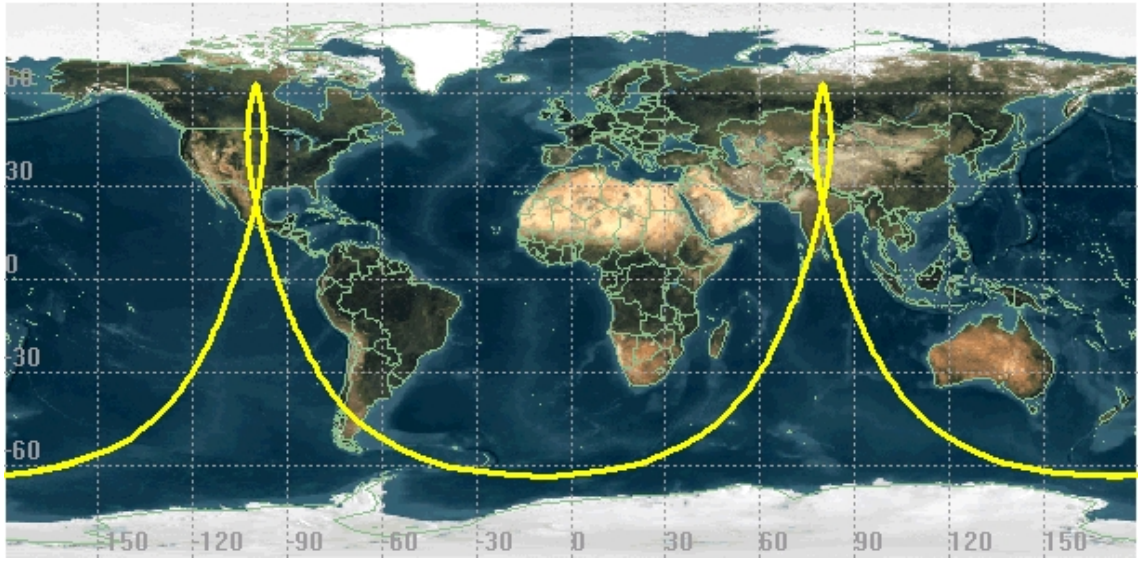


Sugar Grove

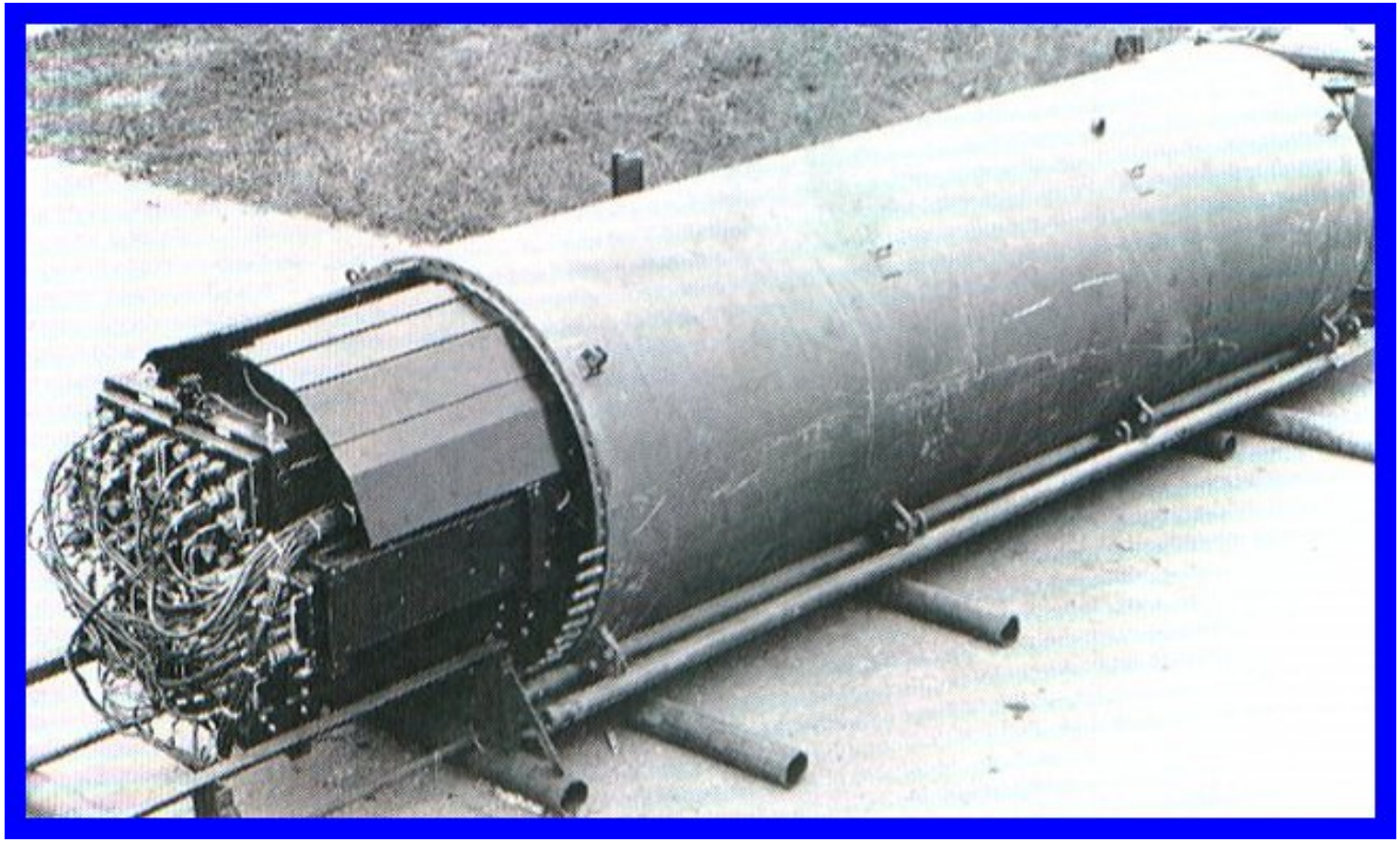
Molniya Satellites



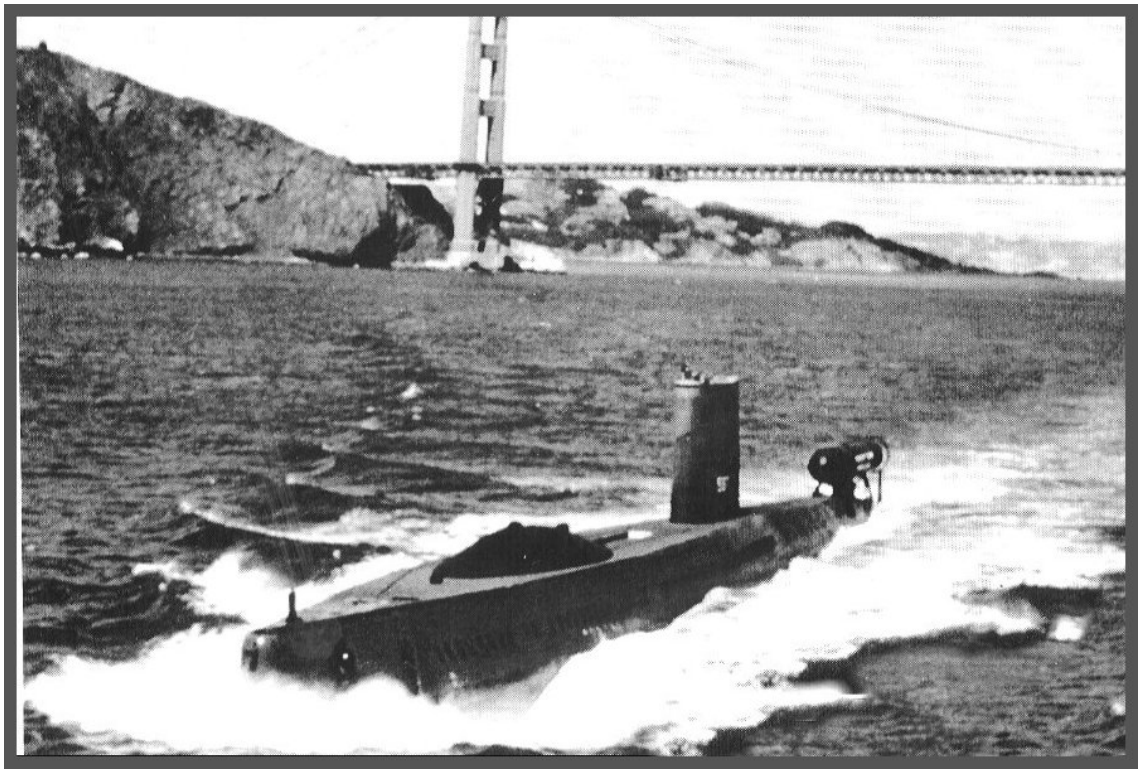
Molniya Orbit



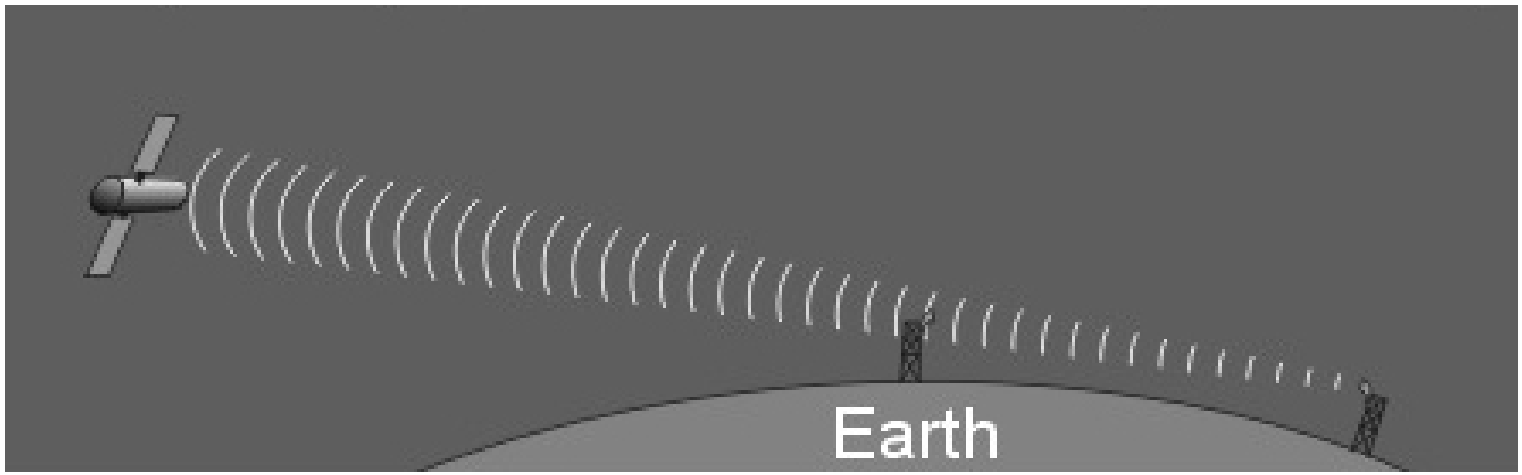
Ivy Bells Pod



USS Halibut



Satellite Microwave Pickup

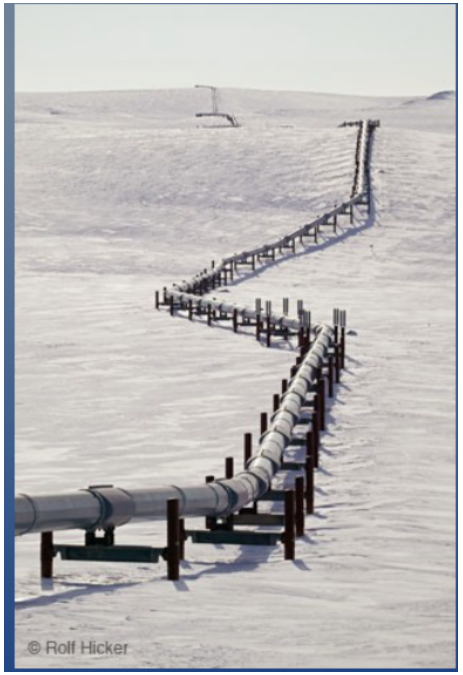


Some Less Obvious Antennas

Arecibo Radio Telescope

Allen Telescope Array

Pipelines



Hainan Island Incident

Sometimes it doesn't go so well.

Collection

Recording, storage, and management of signals

Processing

- Select what you want.
- Filter out what you don't.

Exploitation

Mostly Cryptanalysis

Analysis

Intelligence analysis.

Reporting (report writing)

We intercepted this signal at this time in this direction and this is what we think it means.

Dissemination

Delivering finished intelligence to the customers.

SIGINT Trends I

From nuggest to low-grade ore

SIGINT Trends II

Toward real-time targeting

SIGINT Trends III

Away from vertical integration and toward shared resources

SIGINT Trends IV

From passive to active

Protection of Information

- At rest
- In transit
- In use

Protection of Storage

- Mostly locking it up in a safe

- Crypto only comes into play in recent years

Protection of Data in Transit

- Trusted courier or system
- Guarded wires
- Restricted routing
- Oxygen absorption band
- Narrow-beam laser
- Cryptography

Protection of Data in Use

- Mostly guarding the computer
- Partly homomorphic encryption
- Fully homomorphic encryption

Why cryptography?

- When cryptography is applicable, it is typically the best solution.
- An encrypted message is no longer sensitive.
- Can choose to send it fast, reliably, or cheaply.