Wireless Systems Security

EE/NiS/TM-584-A/WS

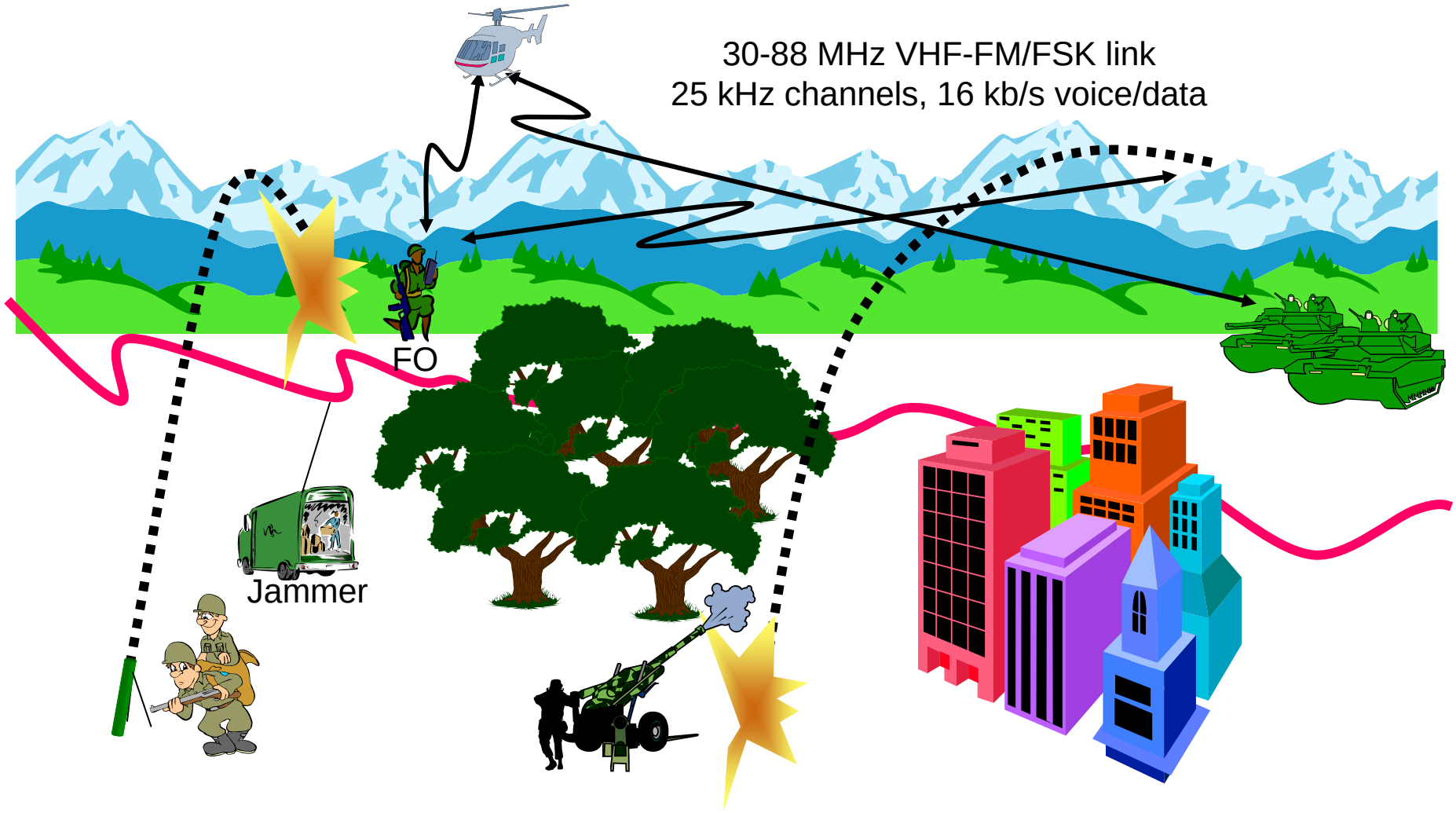
Bruce McNair
bmcnair@stevens.edu

Week 7 - Wrapup

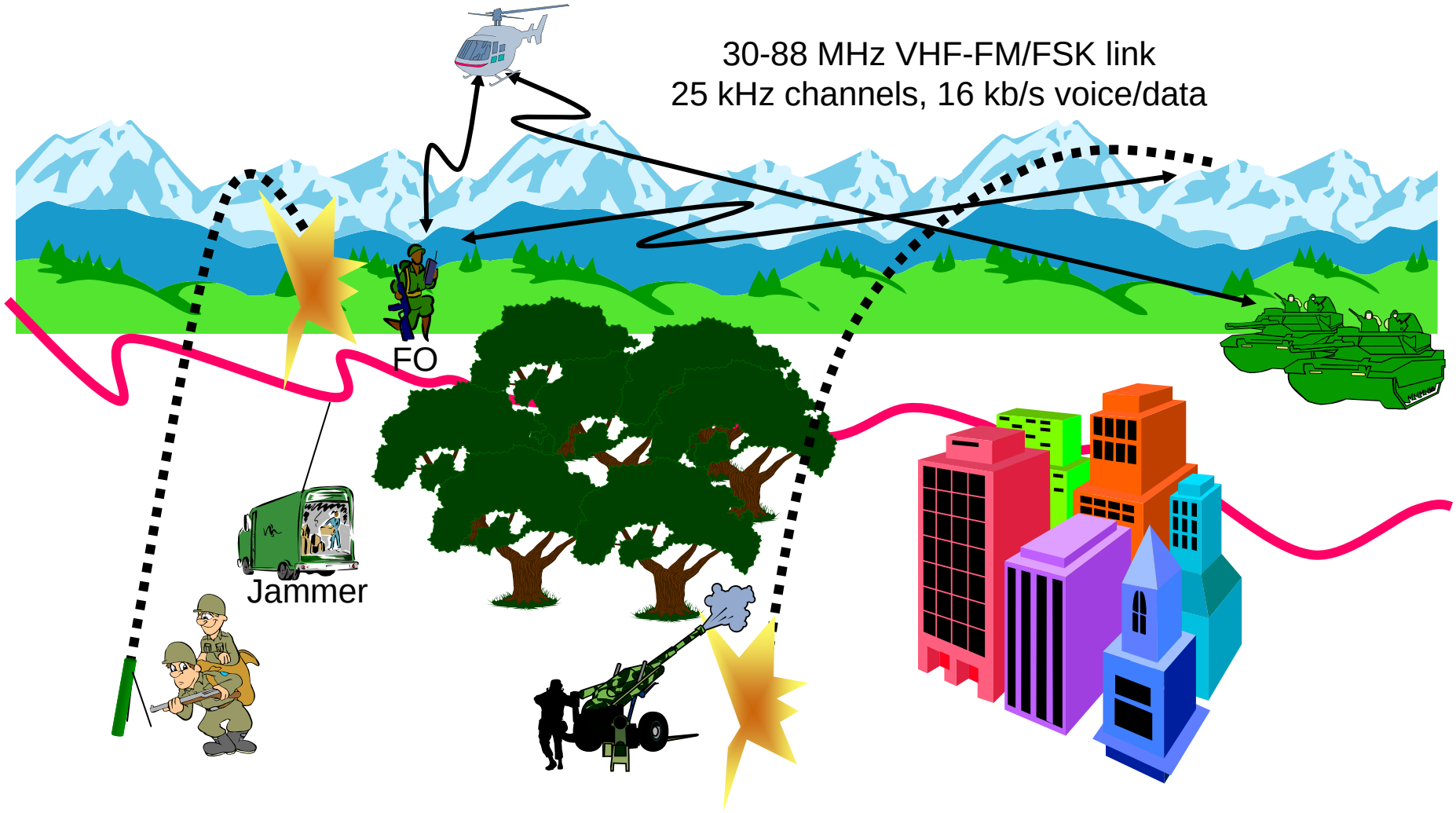
Case Study 3

Summary and observations

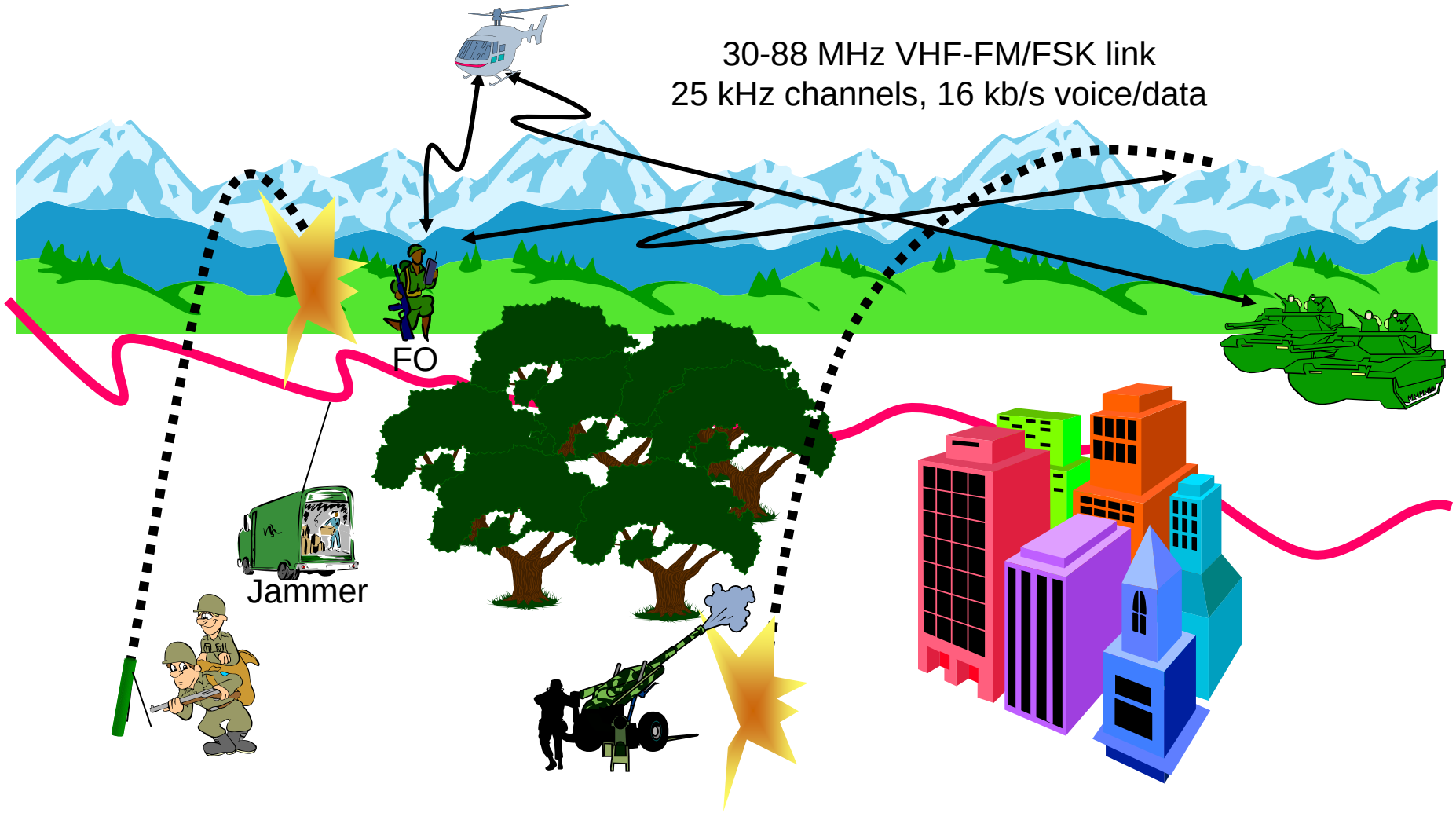
Case 3 – Military Tactical Radio Systems

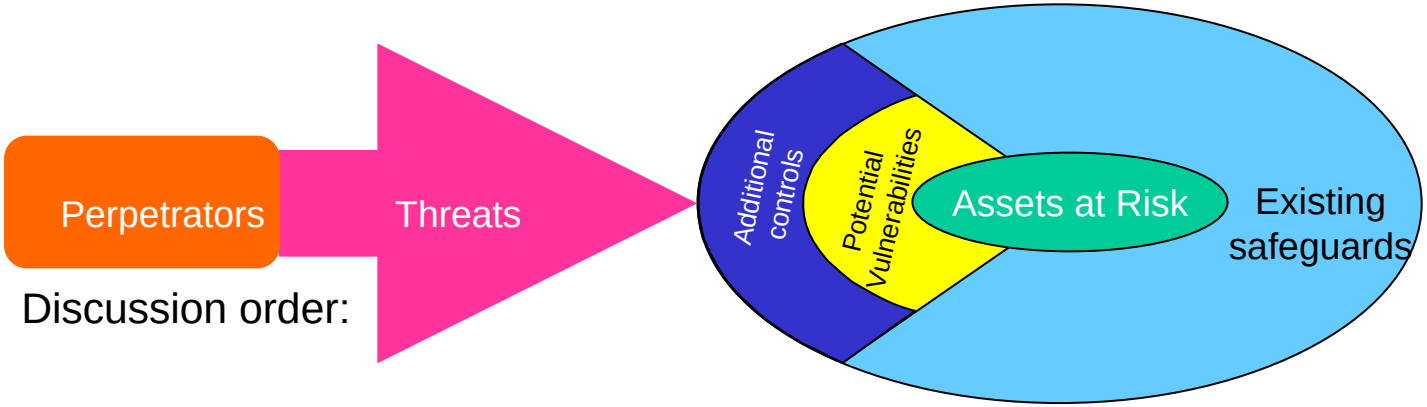


Case 3 – Military Tactical Radio Systems



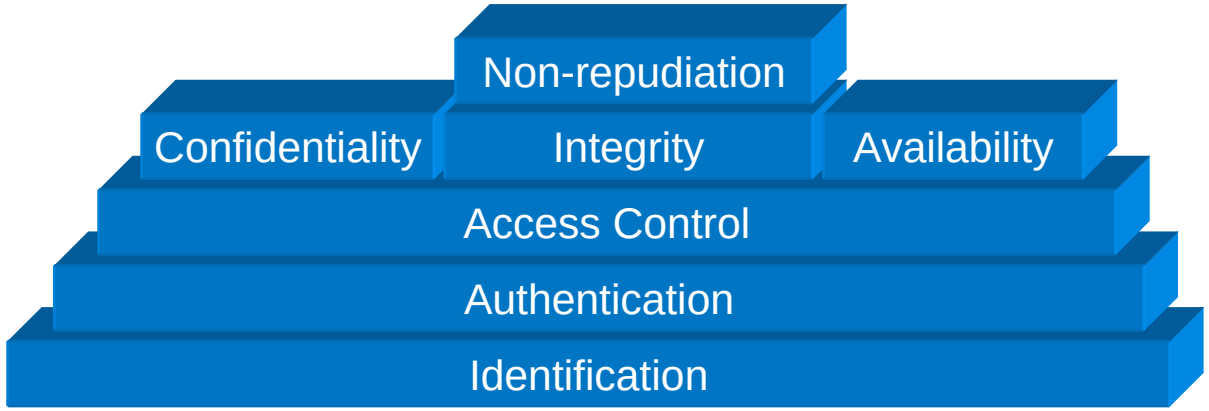
Case 3 – Military Tactical Radio Systems





Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls



Assets

Equipment
- Crypto key

Soldier's life
Operations
- Frequencies
- Procedures

Equipment shelters
Command center
Information transmitted
Other physical assets (tanks, vehicles)
Outcome of engagement
- And therefore national security and ultimately freedom

Codes, security procedures
Tactical advantage
- Surprise
- System technologies

System design
Perceived strengths (2-ways)
Fear factor

Communications bandwidth
Operating frequency
- hopping pattern
- DSSS – spreading sequence

Crypto
ECCM
Command center – and location
Forward Observer – and location
All communications system elements
All soldiers lives
Vehicles, aircraft, weapons, artillery
Power
Voice/data content
Tactical advantage
Traffic flow/load

Perpetrators

Spy
Enemy
Traitor
Double agent
Terrorists
Nature
Foreign government
Fun seeking hackers
Thieves
Black market
Organized crime
Russian mob
FMP'ed AT&T employees
EE/TM584 students looking for more income
Program competitors

Enemy – intel, jammer operators, direction finder operators
Turncoat/traitor
Enemy supporters
Press
Terrorists
Equipment competitors

Threats

Jamming
Spoofing – fraudulent information
DF'ing – bearing and distance
    To attack location
    To track movements
Destroy radio link
Kill the FO
Detecting transmitted information
"Friendly" disclosure of information
Inclement weather
Damage to equipment
    Lightning strike
    Driven over by tank
    Bombed
    Exploding battery
Exploit knowledge of POWs about system, operational procedures
Exploit designers
EMP
Replay transmissions

Jamming
Interception
Kill the Forward Observer
Physical destruction of equipment
Cause waste of power
Observe connectivity
observe traffic flow
    to identify operations
    to identify command structure
Spoofing/replay
Traitor sells: content, keys, eccm settings, operation al plan
Equipment manu sells info, equipment
Exposure of operational data that compromises location
Upload virus to CC computer
Attacker tries to steal /compromise crypto/keys
Stealing bandwidth
Enemy attacks communication link to cause segmentation of communication network
Enemy captures radio and operations on network

Existing Safeguards

Air superiority
Technical advantage
Hiding equipment in trees
Crypto
Frequency range limits accessibility to signal due to propagation
Encryption
Frequency hopping
Antijam – Direct Sequence Spread Spectrum
EMP protection
No tone squelch
Access to wide variety of data, etc., services
Physical construction of radio
Training/intelligence of operator
Crypto/ECCM – zeroize
FH
DSSS
Crypto
Power control
Physical security protecting radio operator, Forward Observer

Vulnerabilities

- Wireless nature of system
- Potential for interference
- Finite fuel source – battery
- Portable
- Fixed design elements
  - Protocol
  - Crypto algorithms
- Human operators – human error, wrong mode of operation
- Frequency range is limited
- Physical construction – fragility
- Operating environment
  - Heat
  - Sand
  - Rain/water
- Budget restrictions
- System complexity leads to systems failures
- Loss of power
- Lack of environmental controls
- Design flaws
- Misconfiguration
- Size/weight of equipment
- Battery power
- Exploding batteries
- Centralize C3 structure
- No user authorization on communications link
- Broadcast, not addressable radio

Additional Controls

Augment batteries with solar power
Remote maintenance
Software defined radio
Biometric user ID
Self-destruct (zeroize)
Peace
Position reporting capability to track captured systems
Physical hiding/protection of equipment
Sprint picture phone
Beamforming/smart antennas