

Radio Frequency Weapons

Presented to EUROEM 31 May, 2000

Prepared and presented by

Sam Frazier

E³ Division, ¹ Code 5.1.7

Naval Air Warfare Center Aircraft Division

Patuxent River, MD

301-342-3582 Fax: 301-995-0076 e-mail: fraziersj@navair.navy.mil

Approved for Public Release - Distribution Unlimited

•Good _____ Ladies and Gentlemen, today I am going to Discuss the highly debated topic of Radio Frequency Weapons, their threat to the military and civilian infrastructure, and some general RDT&E issues associated with the technology.

J

OVERVIEW



- What are RF Weapons?
- · RF Weapons Effects
- · Applications and Doctrine
- Types of RF Weapons
- Technology Issues
- Status and Future
- RDT&E Issues

As we go through this brief please keep the concept of intent as a key issue.

Intent! The difference between a transmitter and a Death Ray is intent (malice)

Background



Recent Congressional - Joint Economic Committee Hearings Have Brought Public Attention to Radio Frequency (RF) Weapons.

- · Futuristic weapons have always been a popular subject
 - Current interest high
 - Confusion over what is meant by various terminology
- · Briefing is a general discussion of RF weapons
 - From Electromagnetic Environmental Effects perspective
 - Intended to foster thought and encourage discussions
- All technical information discussed can be found in open literature

•On Feb 25, 1998 Congress held Joint Economic Committee Hearings to discuss Radio Frequency Weapons and the impact these weapons could have on our economy. There is growing concern that hostile forces or individuals could attack our national infrastructure with a new class of weapons and cause devastating effects...

The Committee was chaired by Representative Jim Saxton (R-NJ) Panelists included Alan Kehs, Army Research Lab, Jim O' Bryon Director LFT, Dave Shriner, a former employee of China Lake and Ira Merritt of the Army's SMDC.

The panelists all agreed that while no evidence exists to prove that an RF weapon has been used, the emergence of this new class of weapons is just a matter of time.

- •So, these futuristic weapons have made it into the hallowed halls of Congress. Has anything changed to make interest in these threats more than a passing fad? And exactly what is a Radio Frequency Weapon or RFW? Since the evidence to prove these weapons exist isn't available, what are we talking about?
- •This briefing provides a general introduction to RF Weapons. Since my background is Electromagnetic Interference(E3) I will bias this presentation accordingly. Don't plan on walking out of here with the answers, I hope at best to foster some serious thought about the subject, spark some lively discussions and perhaps with luck leave you all a little better educated. Caused by a lot of speculation about RF weapons this brief is intended to provide perspective as it relates to the subject presented at these JEC Committee
- •There is plenty of information available, under a variety of different descriptions. The easiest source of information is the internet. There are many sites, official and unofficial sites. I do not guarantee the validity of that information. You will find a wide range of views on the internet, ranging from the fringe elements and science fiction community to serious scientists and businesses.

RF Weapons Threat



- RF Weapons may pose threat to US Military and Civilian Infrastructure particularly Commercial Off-the-Shelf (COTS) and Non-Developmental Items (NDI).
 - Command and Control
 - Communications
 - Information Systems
 - Navigation
- RF Weapons technology available on open market
 - Buy it, Build it, Open Source Availability
- Most work to date is classified this program makes information available to decision makers

RF Weapons provide potential for Asymmetric Advantage

5/1/2000 12:41:47 PM

The RF Weapons Threat

The concern over RFW threats is increasing. Congress has conducted several hearings into this issue. The increasing reliance on, and leadership in, information technology makes the US particularly vulnerable to potential RF weapons threats. The General civilian and government infrastructure vulnerability may be at risk to future threats.

RFW technology is becoming more and more available to potential adversaries. The Equipment, skills and resources necessary for deploying such a device is no longer limited to large research and development efforts. RF Weapons can readily bought or built. A considerable inventory of devices is available on the open market, which may have applications as a weapon. Most importantly, the performance parameters of such system's continues to expand as advances in all aspects of weapons subsystems improve daily.

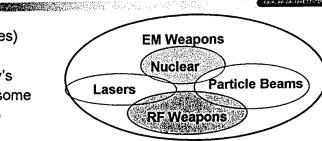
If there is information available on susceptibility / survivability data for systems, it is highly classified. As part of assessing general DOD and National preparedness against such threats, data must be obtained that is non anecdotal, and operationally relevant. Furthermore, this data must be available to decision makers to assist in planning and preparation.

The RFW has the potential for asymmetric advantage. They must be evaluated for effectiveness to help prepare DOD for future Threats.

What are RF Weapons?



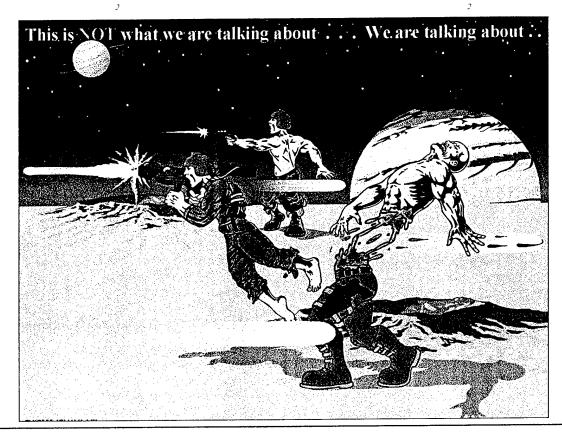
A class of weapons (sources) whose intent is to disrupt / disable / destroy an adversary's device / system by means of some intense electromagnetic (EM) environment.



- RF Weapons Are:
 - In the Radio Wave Spectrum (DC through Gigahertz)
 - Can be Highly Directional (Beams) or Isotropic (Omni- Directional)
 - Created through variety of methods (primitive → Nuclear EMP)
- RF Weapons Are <u>NOT</u>:
 - Ionizing (No Nuclear fallout, or radioactivity)
 - Near visible Spectrum (lasers or Infra-red, Ultra-violet)

Question: Does High Power Microwave (HPM) = RFW?

- •We should begin with definitions. What exactly are RF Weapons? "A class of weapons (sources) whose intent is to disrupt / disable / destroy an adversary's device / system by means of some intense electromagnetic (EM) environment.."
- •RF weapons are part of the larger family we can call EM weapons, Lasers, Particle Beams, and Nuclear Weapons are familiar examples. Since all EM weapons are related the separation and distinction is somewhat arbitrary. However, for our discussion RF Weapons are easily defined.
- •What are some of the attribute of an RF Weapon:
 - •Well, they generate EM signals in the radio wave region which includes power, communications and radar frequencies.
 - •The energy can be transmitted through a beam, or transmitted in all directions or something in between.
 - •And the weapon can be as crude as a kids science project or as complex as a nuclear weapon.
- •To understand what these weapons are we must also decide what they are not.
 - •They are not ionizing. There is no lingering radiation, or fallout or radioactive residues to contend with.
 - •They are Not lasers, or similar systems which operate in the or around the visible part of the spectrum.



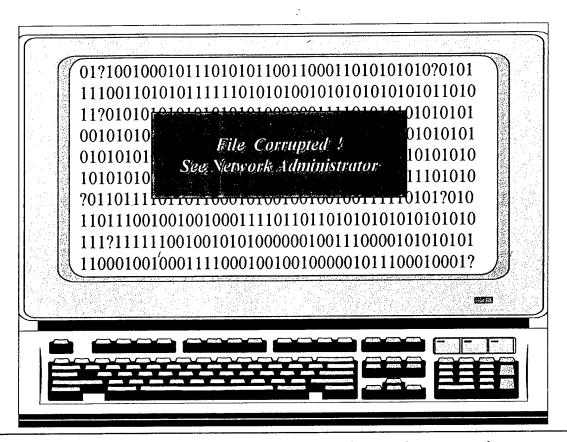
For you Sci-Fi buffs in the audience, I'm sorry to announce we won't be discussing many of the exciting aspects of RF weapons as depicted in the entertainment industry. While its fun to speculate on where science will take us in the distant future, we have some weapons that could be deployed very soon. For example:

Warning! The system is either busy or has become unstable, you can wait and see if it becomes available again, or you can restart your computer. * Press any key to return to Windows and wait * Press CTRL ALT DEL again to restart your computer. You will lose unsaved information in all programs that are running. Press any key to commite

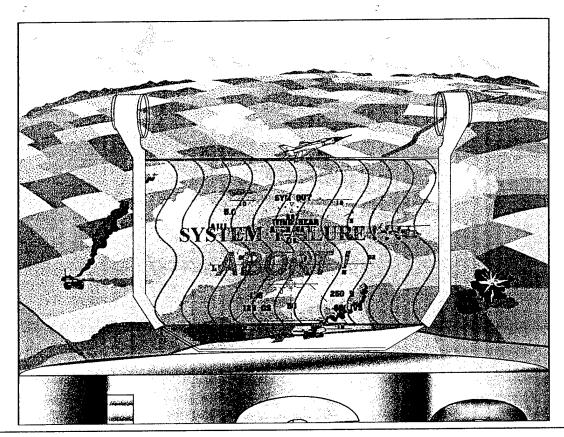
Most of you are familiar with the Bill Gates greeting from Redmond Washington. Many of us have become so numbed to this screen that we would never suspect a criminal, terrorist or military action could be taking place. If it is possible to bring your system back up, it may be too late. Are you oblivious to sinister forces at work, or is this just another harmless gremlin?



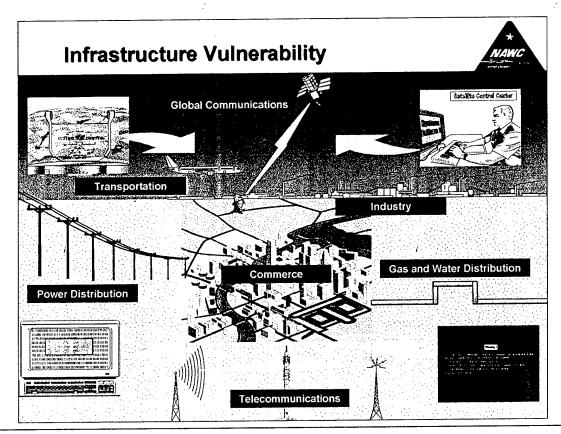
As our small soldier is finding out, the system interruption is neither normal or temporary. An adversary thousands of miles away could have blinded our satellites, seriously degrading our information superiority advantage.



Not just a file is being destroyed, the majority of your data repository. Meanwhile at your remote archive site many miles away, your backup data is being irrecoverably destroyed. The culprits could have made off with millions of dollars and used this to cover up their tracks. The data was priceless. Next time your management will take extortion demands seriously.



Sometimes, rebooting is not an option, As shown here, External Radio Frequency signals are affecting the pilots Heads up display, The signals may also be affecting the aircraft's digital flight control systems of this fly by wire aircraft. In this futuristic scenario, the computer operators day is completely ruined.



There are certainly plenty of examples of how RF Weapons COULD be used today or in the near future. But the point is that IF RF Weapons aren't real today, they will be tomorrow. We as a nation are extremely dependent on information and potentially vulnerable to the effects of hostile attacks on our infrastructure. The concerns which prompted congress to establish committees to address this issue are not military. It is the National Infrastructure. Utilities, communication, transportation, commerce, all are vulnerable. In fact, Few activities are prepared to cope with even some of the more amateur devices which could be fielded. The economic losses from coordinated assaults could be enormous. Finding the culprits could be difficult and serious incidents may go undetermined as to both cause and effect. RF Weapons create RF Interference, but create it on demand and with destructive power, this disrupts the flow of information; and information is money and time and perhaps, lives.

RF Weapons in Information Warfare



- U.S. leads the world in information technology
- Although militarily mighty, our nation relies on information superiority
- We're most vulnerable in terms of potential effects
- Speed of decision making increasing
- · RF considered a critical battle area in IW
- To maintain Information Superiority we must protect our information and Infrastructure
- Information is the new "high ground"

5/1/2000 12:41:47 PM

We possess the majority of the worlds computers.

89% of internet content
protect our information while denying the enemy his
situational awareness
The more you rely on information, the more critical it becomes
Increasing complexity and interconnectivity
Even the American foot soldier of tomorrow will be a walking console

Applications and Doctrine



- What are the benefits of RF Weapons?
- How would you use them?
- Will it work?
- How will you know it worked?

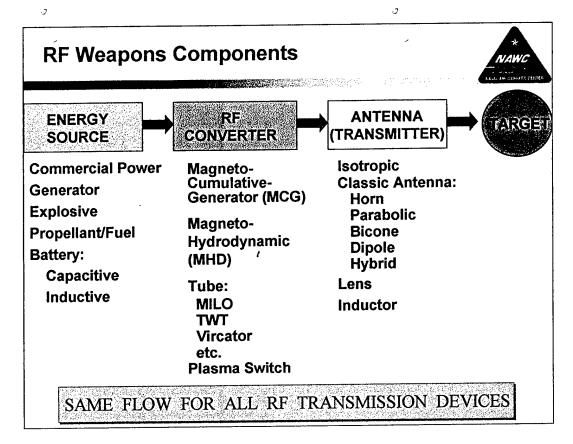
Are RF weapons worth pressing

Are they better than throwing lead of more classical devices at your adversary

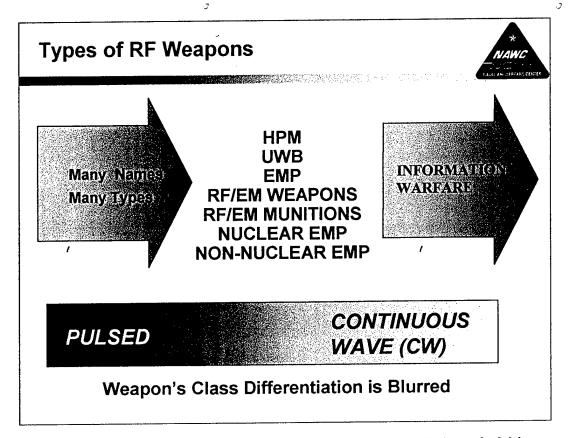
What are the Likely scenarios

How would a terrorist / vandal / extortionist use them

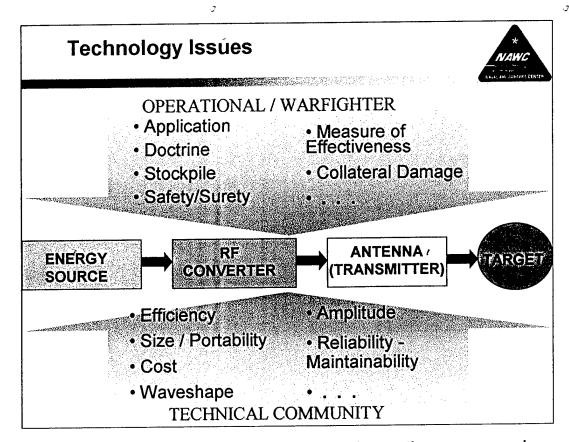
The hardest question is how can you be sure your weapon worked May not be any visible signs of effects



Same for RF Comm etc



CW Emitters can send out pulse trains and can have high bandwidth Pulsed systems can have any number of waveforms a munitions could conceivably send out multiple pulse trains before expanding its power



Many issues associated with EM Weapons apply to other areas such as EW, Radar Communications, E3, System safety etc.

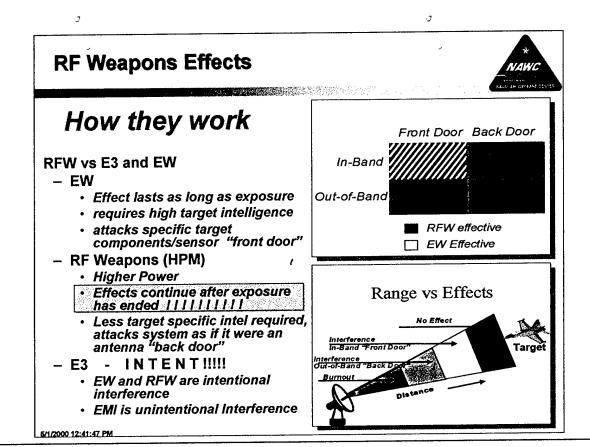
Applications (Benefits)



- Offensive
- Defensive
- Reduced Collateral Damage
- Speed of Light / Line-of-Sight
- Rapid Firing and Retargeting
- Deep Magazines (Infinite Ammo)

•

Won't go into too much detail here the internet is full of speculation!!!!!



What are RF Weapons

A class of weapons (sources) whose intent is to disrupt / disable / destroy an adversary's device / system by means of some intense Radio Frequency RF environment.

Lets put RF weapons into perspective as an E3 / EMI issue.

Regardless of the form a weapon may take, as long as it is in the frequency range and bandwidth of other EM environments. we will use the same E3 tools to protect our system.

In many scenarios the only difference between RF Weapons and RADARS and Comm Equipment is INTENT! Maxwell's equation are applies uniformly.

RFW is Different from classic Electronic Warfare (EW)

EW

Effect lasts as long as exposure requires high target intelligence attacks specific target components/sensor "front door"

RFW

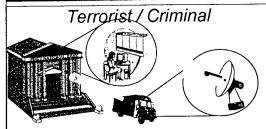
Higher Power

Effects continue after exposure has ended

Less target specific knowledge required, attacks system as if it were an antenna "back door"

RF Weapon Uses



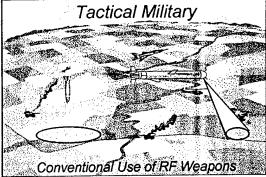


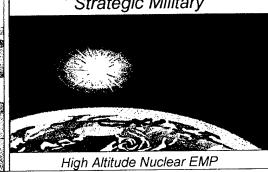
Excess Military Equipment or "Radio Shack" Technology

Police / Military Operations

Covert Missions and Special Tactics







- •The scenarios in which RF Weapons can be deployed is only limited by the imagination.
- •Although many may argue whether the technology exists. If it does exist, it is not yet practical or affordable for most.
- •As this chart shows, the terrorist attacks on "soft" targets on of the most primitive forms of RF Warfare. Such an attack could be carried out with the victim unaware that an attack has occurred. The equipment used could be excess military components, a home brewed RF transmitter, or a fairly sophisticated military grade4 weapon.
- •For Police and Military operations there are many non-violent applications such as zapping vehicles or defeating security systems.
- •For the tactical Military Application RF Weapons can be considered an extension of classic Electronic Warfare New Electronic attack weapons will yield higher powers at longer ranges and disrupt systems in ways today's EW systems cannot.
- •The ultimate RF Weapon for the foreseeable future is High-altitude EMP, were an intense RF environment is generated aver large areas of the earth when a nuclear weapon is detonated in the upper atmosphere. Many military systems are protected against this threat which is estimated by some to be 50,00 V/m over large geographic areas.

Program Overview - RF Threat



Hostile use of RF sources [High Power Microwave (HPM)/ Radiofrequency Weapons (RFW)] may pose threat to US Military and Civilian Infrastructure particularly Commercial Off-the-Shelf (COTS) and Non-Developmental Items (NDI).

- Command and Control
- Communications
- Information Systems
- Navigation
- RF Weapons technology available on open market
 - Buy it, Build it, Open Source Availability /
- DOT&E (LFT&E) Concerned about emerging non-traditional non-ballistic RF threats.
 - Terrorist
 - Rogue Nations
 - Asymmetric Warfare

RF Threats Provide Potential for Asymmetric Advantage

and Could Result in "Technological Surprise"

20

Doctrine

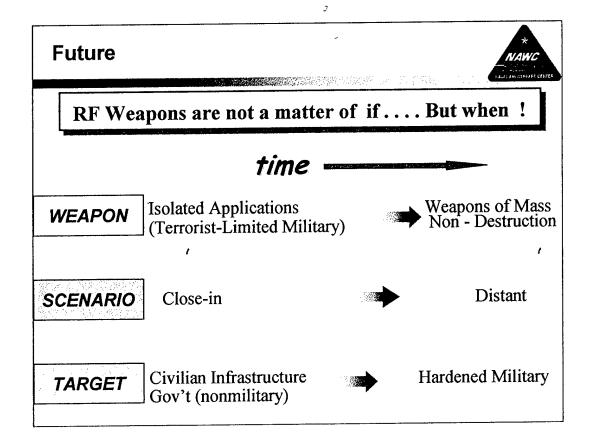


- · Great Terrorist Weapon!
- EM Weapons Crucial to Information Warfare (IW)
 - Controlling information while denying the enemy his
 C3I is the cornerstone of IW
 - Information superiority is the high ground of the modern battlefield
- Valuable in Both Full Conflict and Operations Other Than War.
- · Examples:

Golf War - CNN reported continuously

EM weapons attacking C3I nodes in city centers would have decapitated leadership without collateral damage (would have wiped out CNN as well) While still defeating the soldiers in the field the old fashioned way.

At EUROEM in Bordeaux France a Russian General Lobarev made statements about a beer can sized RF munition. While in Albuquerque in 1996 the general discussed the threat of RF terrorism and cave 4-case scenarios.



CNN will have the most survivable equipment in theatre
Scenario most dangerous
JEC Capital Hill
COTS
EM Weapons since 30's

Summary and Conclusions



- · RF Weapons are Coming!
 - Not if, ... But when
 - Will evolve from limited device (terrorism & extortion) into a weapon of mass non-destruction

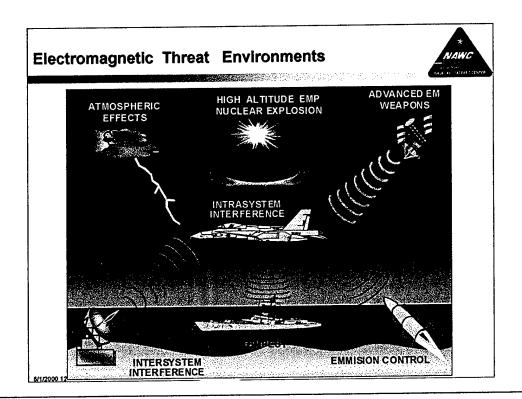
- · Planners need IW weapon
 - Strong doctrine requirements
 - C3I decapitation with minimal casualties
- Prepare to Protect Against RF Weapons!
 - Environment is nothing more than intense/intentional EMI
 - Ability exists in E3 EW and survivability community

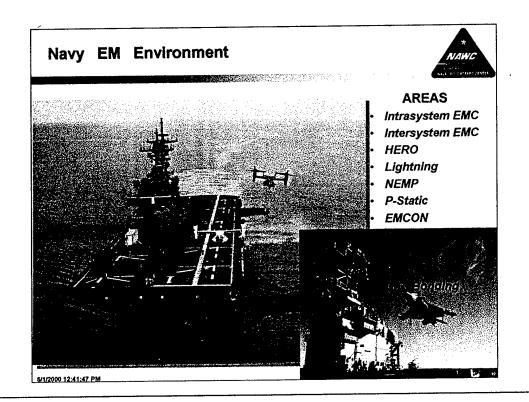
23

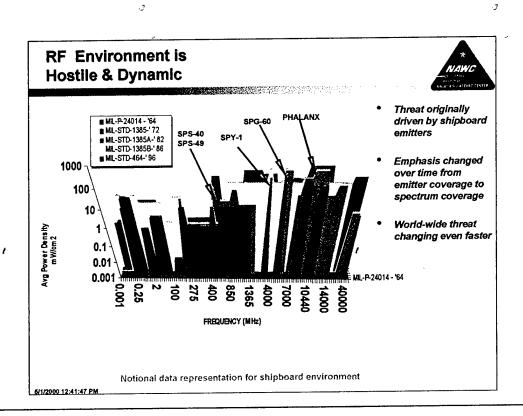


RFW RDT&E TECHNOLOGY ISSUES

5/1/2000 12:41:47 PM







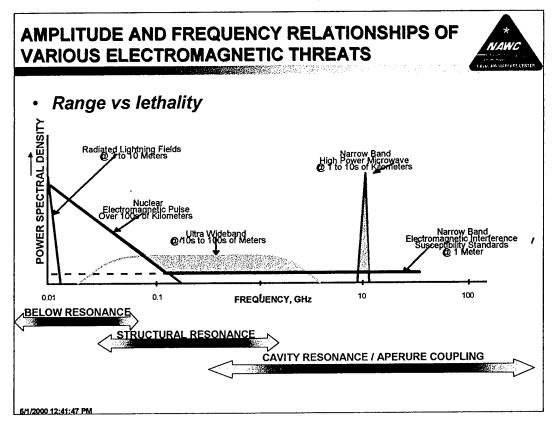
Naval Air Approach to E³, EMP & RFW

5/1/2000 12:41:47 PM



Navy/NAVAIR embraced EMP (and will Embrace RFW) as a critical element of E³

- Seamlessly integrated EMP into E³ as an Electromagnetic Transient (EMT)
- Leverage EMP and RFW S&T thrusts as a technology base for general E³ RDT&E
- EMP and RFW as a balanced part of E³



This slide reminds us that since most notional RF weapons could have higher frequency content. we may become concerned about different coupling modes.

If you compare an RF weapon with a non RF weapon with similar characteristics the coupling modes should be similar.

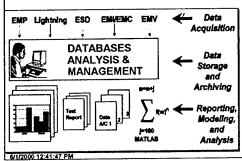
This slide also highlights the issue of intent. The difference between a radar and a weapon could easily be whether malice is involved, the system under assault is an antenna.

E³ RDT&E Process



Approach

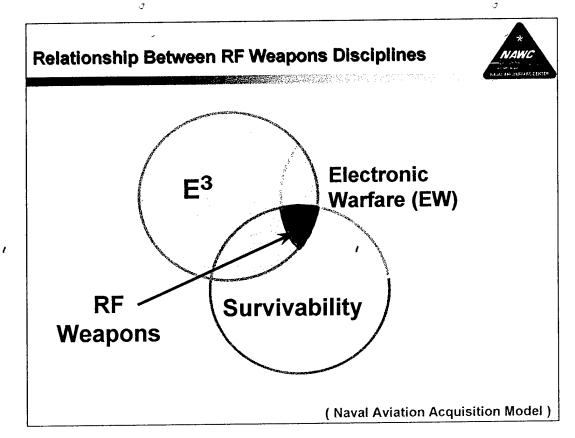
- Enormous # of E³ Issues, a very complex test object, and limited resources (time, \$)
- Source-Victim (Qualitative) Assessments for most EMC/EMI
- Margin (Quantitative) Assessments for HERO & EMP
- In house capability and technology to perform research, investigations and troubleshooting





- EM Modeling and Simulation capability
- Extensive Data Acquisition and Processing Capability (EM Transients)

 Over 100 Test Points Instrumented
 - simultaneously
 - 100's of unique measurements per day real-time processing and Data Mgmt
- Full suite of E3 instrumentation



EW traditionally in-band and requires knowledge of systems being assaulted EM Weapons more Brute force and out-of-band

EW effects stop when EW emitter is turned off RF weapons effects remain

Other services or agencies may use another model for example the army may have a large ordnance area for RF munitions

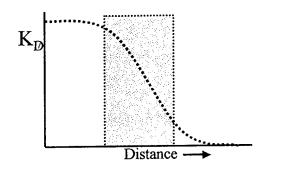
Both Offensive and Defensive

E3 is concerned with Protection, lethality, fratricide

System Survivability



- Determining Survivability/Vulnerability
- Estimation of Meaningful Distance for Likely vs. Unlikely Effects



5/1/2000 12:41:47 PM

Include Theory of System Survivability

Describe difference between LTF Survivability (P $_{\rm k}$ x P $_{\rm k/h}$ and EM Survivability.

How do we protect against RF Weapons



- Bonding
- Grounding
- Shielding
- Filtering
- Circumvention
- Good EMI Practices, use holistic approach
- Consider RFW, EW and E3 as interrelated areas

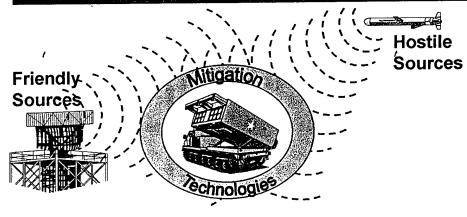
5/1/2000 12:41:47 PM

RADIO FREQUENCY INTERFERENCE MITIGATION



Development of Radio Frequency Interference Mitigation Technologies is driven by both friendly and hostile sources of interference.

ATD is developing technologies to allow COTS and military electronics to operate in all RF environments.



5/1/2000 12:41:47 PM

Categorization of Effects



Test System Effects

Any Upsets and/or Anomalies observed and recorded for systems/subsystems will be assigned a specific effect level.

Effects Level	Response
0	No Observable Effets
1	Effects Present only During Illumination
2	Residual Effects Requireing user intervention- system function reset
3	Residual Effects Requireing user intervention- system Power recycle
4	Effects Requiring system maintenance Action
5	Physical Damage

Operational Impact

How will the aggregate individual effects from the various systems/subsystems impact/ affect the

Mission Category	Operational Impact of Effects
IV	None
111	Nuisance - Does Not Degrade Impact Mission Performance
11	Degraded - Requires Operator/Maintenance Intervention resulting in reduced effectiveness (Improved performance desireable)
ı	Abort / Disabled - Serious Safety or mission Impact (Improved Performance required).

5/1/2000 12:41:47 PM

mission.

35

Program Approach - Objectives



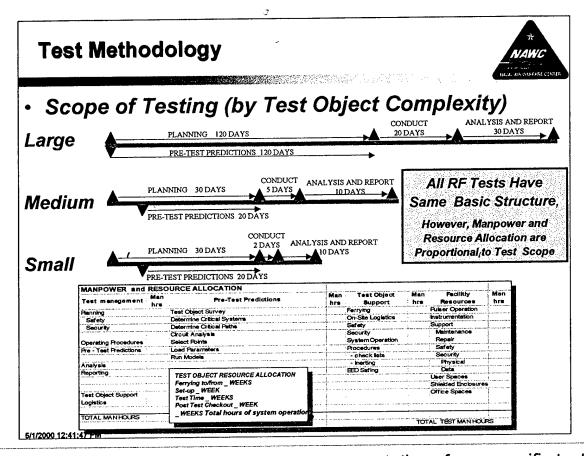
- Assess broad range of Military, COTS and NDI systems
 - From simple electronic devices
 - To complex Integrated Weapons Systems
- Use straightforward classic Operational T&E approach
- Restrict assessments to operationally relevant scenarios for Ultrawideband terrorist threats

This is a Test Program, NOT a Research Program

5/1/2000 12:41:47 PM

Program Approach

This program will assess the survivability of a broad range of Military, Commercial Off-The-Shelf and Non-developmental systems. The intended test objects will range from small hand held devices such as cellular phones and handheld GPS to large complex integrated weapons systems.



This table is intended to be generic and not representative of any specific test. Mike Grothous and Sam Frazier agree in principle that the scope of each type of assessment is proportionally adequate to foster discussion.

37

Test Setup

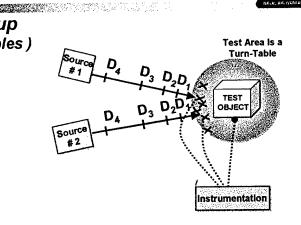
Typical RFW Test Setup Scenarios (Controlled Variables)

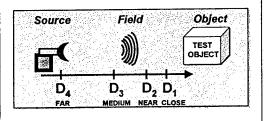
- Source Output
 - Field Strength (Distance)
 - Rep Rate / Burst Rate
- Scenario
 - Polarization
 - · Aspect Angle / Elevation
- Test Object Modes

Instrumentation

- Source Parameters
- Field Characteristics
- Test Object response
 - Visual Response
 - · Electromagnetic Response

SOURCE Waveform(s)	RANGE (Distance)	AZIMUTH (Turntable Rotation)
S1	D1	A1`
S2	D2	A2
S3	D3	A3





Nwwd to create MATRIX which shows general scope of test through phases Sources

Intensity

5/1/2000 12:41:47 PM

Waveform

Rep rate

Test Object

Modes

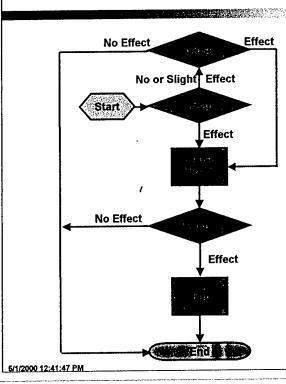
Scenario

Polarization

Angle of Incidence

Test Object Exposure Protocol





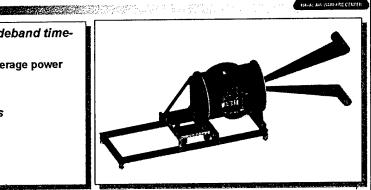
- Standard Test Object Exposure Protocol
 - Start Exposure at Near
 - If little or no effect move to Close
 - If no Effect, End
 - If Effects, Reduce exposure parameters set (η) based on optimum coupling/effects
 - Move to Medium
 - If Effects, End
 - If no effects move to Far
 - After Far, End Test Sequence

39

Typical Ultrawideband RF Threat Source



- ALL Sources are Ultrawideband timedomain radiators
 - high peak power low average power
 - fast-rise pulse shape
 - high repetition rates
- Each has unique features
 - waveform attributes
 - tunability
 - etc

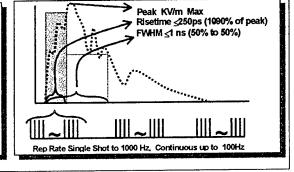


Performance Parameters

- Electric Field is the Parameter usually Measured
- Output can be 100's KV/m close to antenna
- Rise-time 100's of Picosecs. (10 to 90 % of peak)
- Full Width Half Max (FWHM) Peak to 50%~ less than a nanosec.
- Rep-rate Single-shot to KiloHerttz
- Continuous operation up to 100 of Hertz

No single system May possess all above attributes

No single system way possess an above da



5/1/2000 1:42:22 PM

Other Systems



COTS/NDI under consideration

- Computer
- GPS
- Medical Life Support (pacemaker)
- · Wireless / Cellular
- Civilian Emergency Communications NET
- Physical Security Devices
- Pagers
- Digital Phones
- A/C Flight Controller
- Video Conf. Equip

5/1/2000 1:49:21 PM

REPORT DOCUM	MENTATION PAGE	Form Approved
		OMB No. 0704-0188
and maintaining the data needed, and comple information, including suggestions for reducing 1215 Jefferson Davis Highway, Suite 1204, A	ting and reviewing this collection of information. So this burden, to Department of Defense, Washington rlington, VA 22202-4302. Respondents should be a	, including the time for reviewing instructions, searching existing data sources, gathering end comments regarding this burden estimate or any other aspect of this collection of Headquarters Services, Directorate for Information Operations and Reports (0704-0188), ware that notwithstanding any other provision of law, no person shall be subject to any DMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE
1. REPORT DATE	2. REPORT TYPE Viewgraphs	3. DATES COVERED
4. TITLE AND SUBTITLE		5a. CONTRACT NUMBER
Radio Frequency Weapons		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
Sam Frazier		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATIO	ON NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Naval Air Warfare Center Aircraft	Division	
22347 Cedar Point Road, Unit #6		
Patuxent River, Maryland 20670-1		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
Naval Air Systems Command		
47123 Buse Road Unit IPT Patuxent River, Maryland 20670-1:	547	
12. DISTRIBUTION/AVAILABIL		
12. Digitalborioiwa valibabib	III GIZIZZIVIZZIVI	
Approved for public release; distrib	oution is unlimited.	
13. SUPPLEMENTARY NOTES		
14. ABSTRACT		
	•	
		•
	•	
15. SUBJECT TERMS		

17. LIMITATION

OF ABSTRACT

Unclassified

18. NUMBER

41

OF PAGES

Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std. Z39-18

19a. NAME OF RESPONSIBLE PERSON

19b. TELEPHONE NUMBER (include area

Sam Frazier

code) (301) 342-3582

b. ABSTRACT

Unclassified

c. THIS PAGE

Unclassified

16. SECURITY CLASSIFICATION OF:

a. REPORT

Unclassified