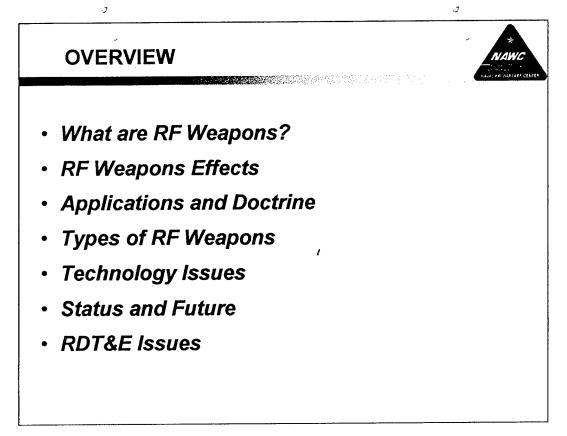


•Good \_\_\_\_\_ Ladies and Gentlemen, today I am going to Discuss the highly debated topic of Radio Frequency Weapons, their threat to the military and civilian infrastructure, and some general RDT&E issues associated with the technology.

# 20000607 022

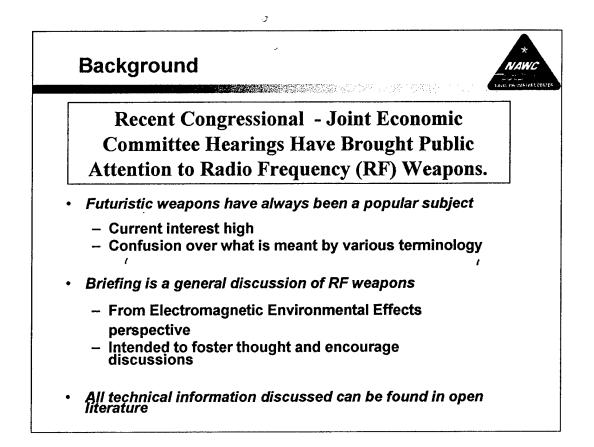
1



,

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)



•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..

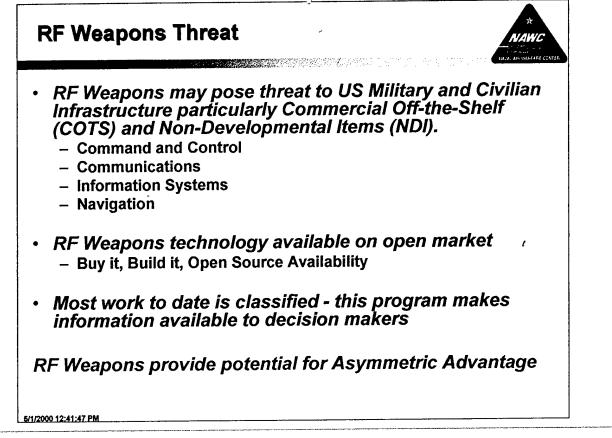
The Committee was chaired by Representative Jim Saxton (R-NJ) Panelists included Alan Kehs, Army Research Lab, Jim O' Bryon Director LFT, Dave Shriner, a former employee of China Lake and Ira Merritt of the Army's SMDC.

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.



#### The RF Weapons Threat

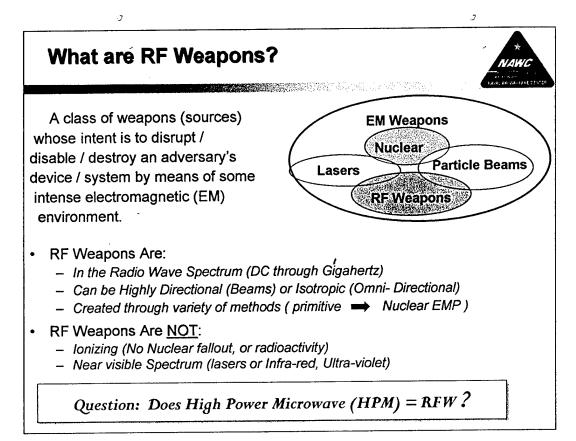
Э

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. 0



•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:

1

•Well, they generate EM signals in the radio wave region which includes power, communications and radar frequencies.

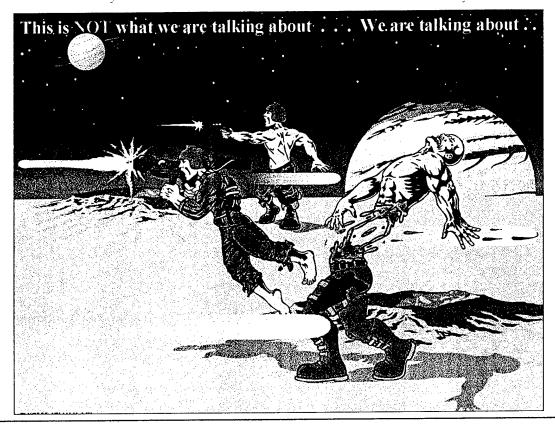
•The energy can be transmitted through a beam, or transmitted in all directions or something in between.

•And the weapon can be as crude as a kids science project or as complex as a nuclear weapon.

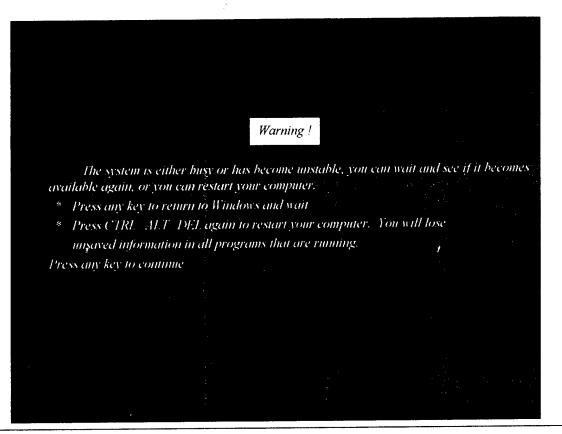
•To understand what these weapons are we must also decide what they are not.

•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.



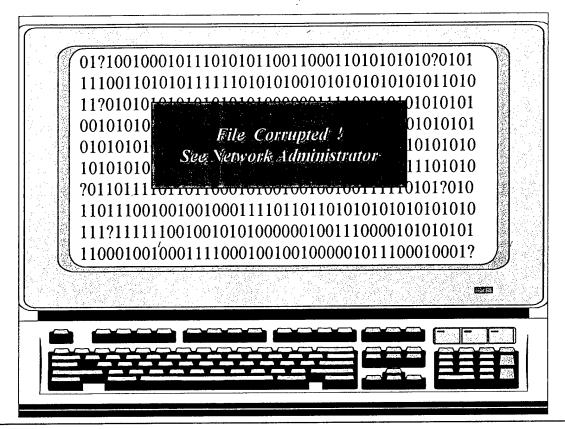
For you Sci-Fi buffs in the audience, I'm sorry to announce we won't be discussing many of the exciting aspects of RF weapons as depicted in the entertainment industry. While its fun to speculate on where science will take us in the distant future, we have some weapons that could be deployed very soon.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



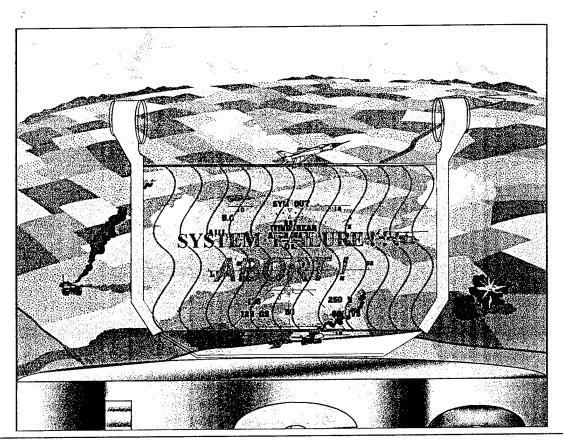
Most of you are familiar with the Bill Gates greeting from Redmond Washington. Many of us have become so numbed to this screen that we would never suspect a criminal, terrorist or military action could be taking place. If it is possible to bring your system back up, it may be too late. Are you oblivious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



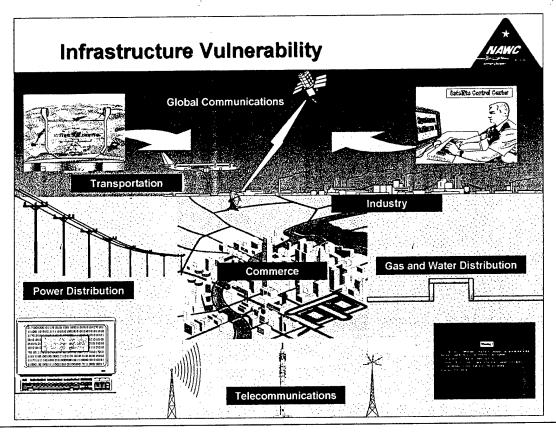
As our small soldier is finding out, the system interruption is neither normal or temporary. An adversary thousands of miles away could have blinded our satellites, seriously degrading our information superiority advantage.



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

Ĵ

- 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

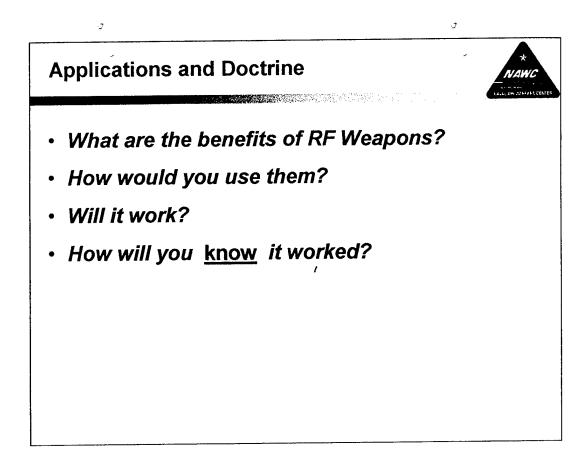
protect our information while denying the enemy his

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



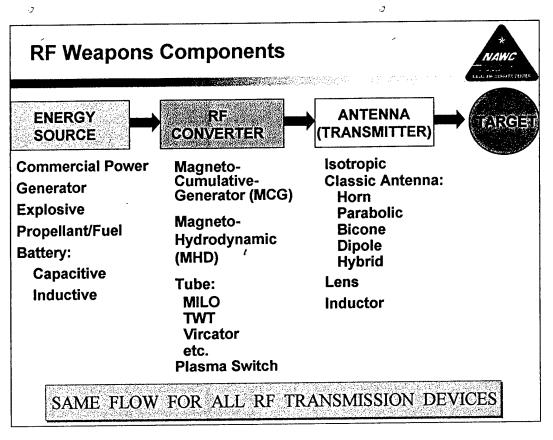
Are RF weapons worth pressing

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

What are the Likely scenarios

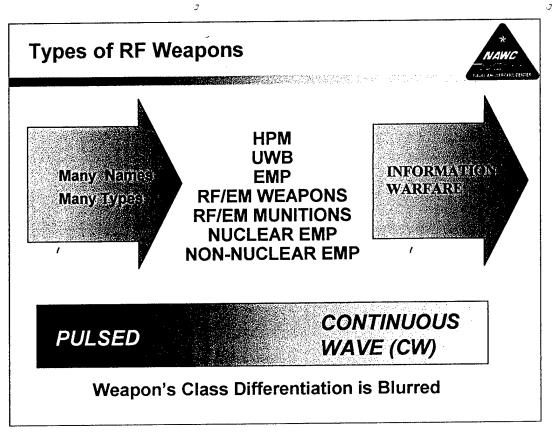
How would a terrorist / vandal / extortionist use them

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



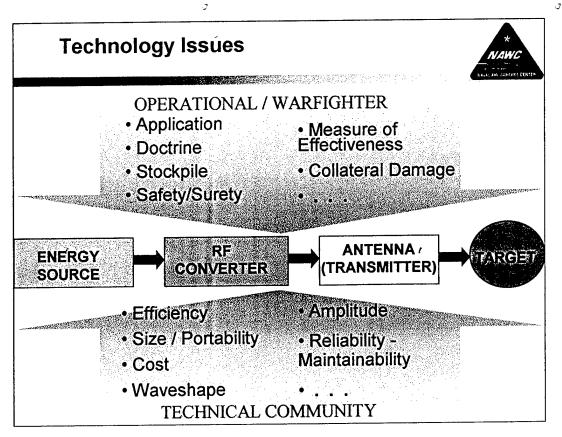
Same for RF Comm etc

t

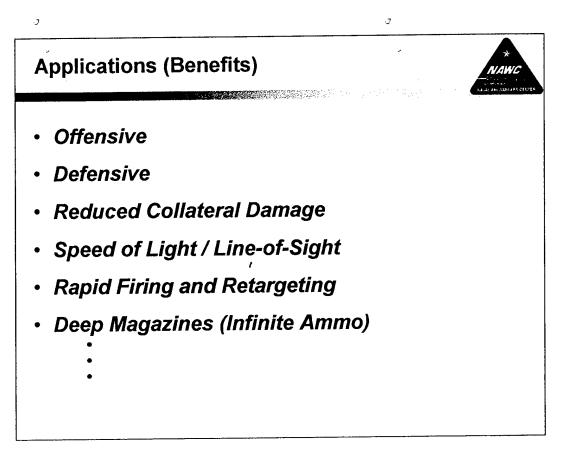


CW Emitters can send out pulse trains and can have high bandwidth

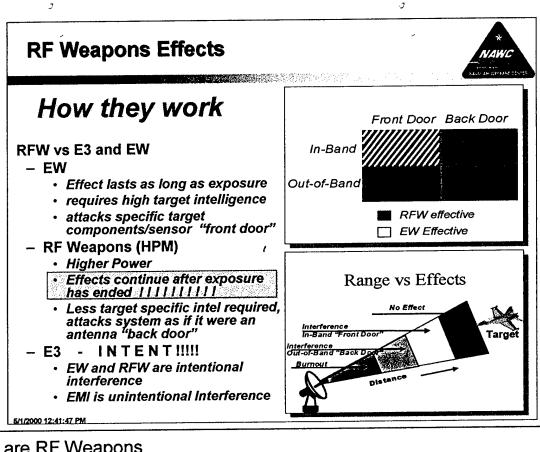
Pulsed systems can have any number of waveforms a munitions could conceivably send out multiple pulse trains before expanding its power



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



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.

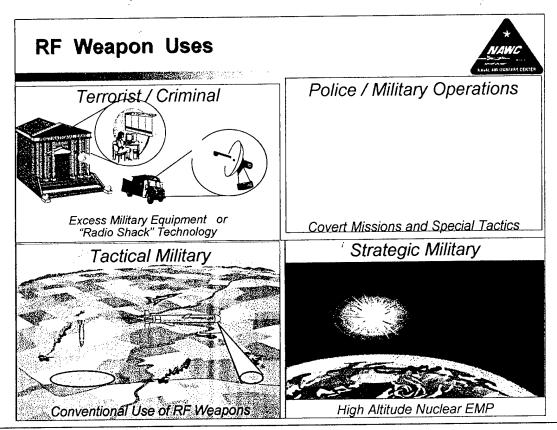
Lets put RF weapons into perspective as an E3 / EMI issue.

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"



•The scenarios in which RF Weapons can be deployed is only limited by the imagination.

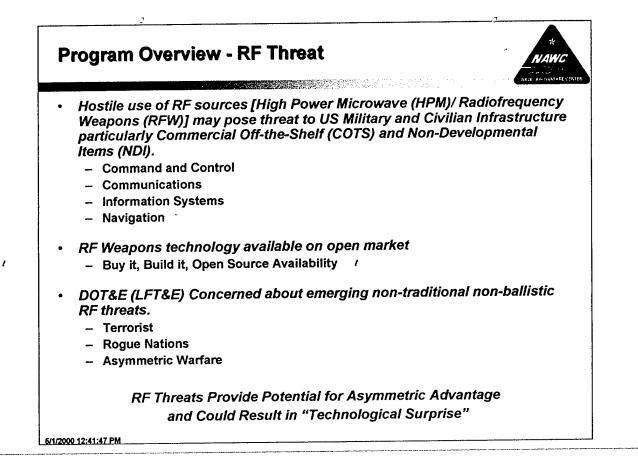
•Although many may argue whether the technology exists. If it does exist, it is not yet practical or affordable for most.

•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.

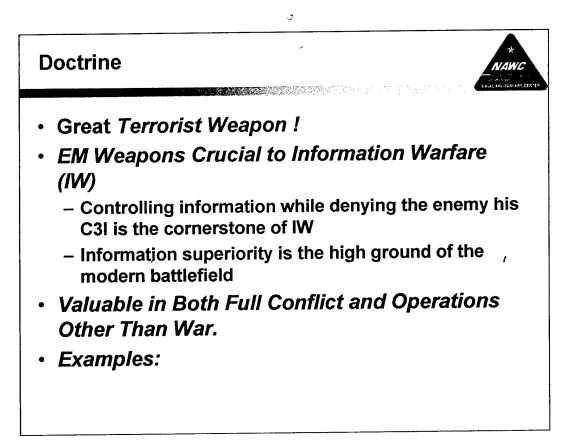
•For the tactical Military Application RF Weapons can be considered an extension of classic Electronic Warfare.New Electronic attack weapons will yield higher powers at longer ranges and disrupt systems in ways today's EW systems cannot.

•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.



20

ł



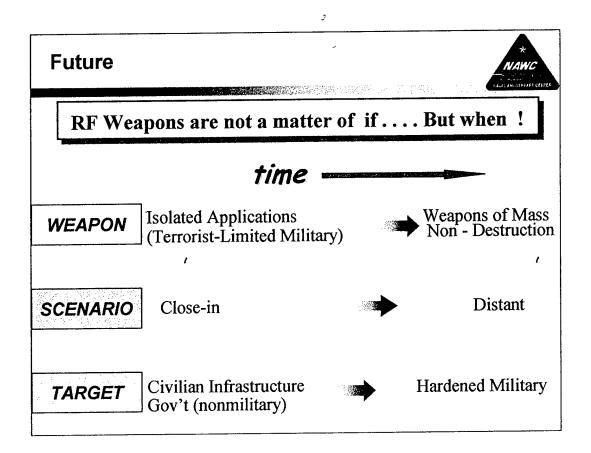
Golf War - CNN reported continuously

J

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

J

J



# Summary and Conclusions

J

1

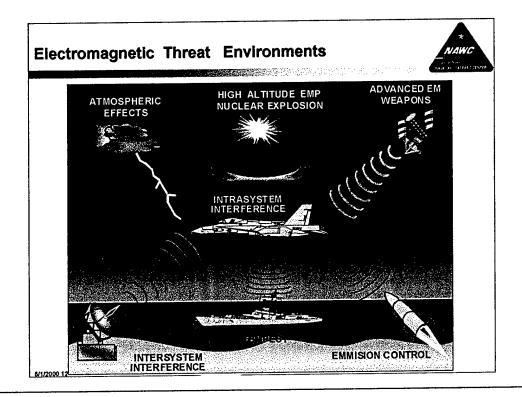
- RF Weapons are Coming !
  - Not if, ... But when
  - Will evolve from limited device (terrorism & extortion) into a weapon of mass non-destruction

- 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



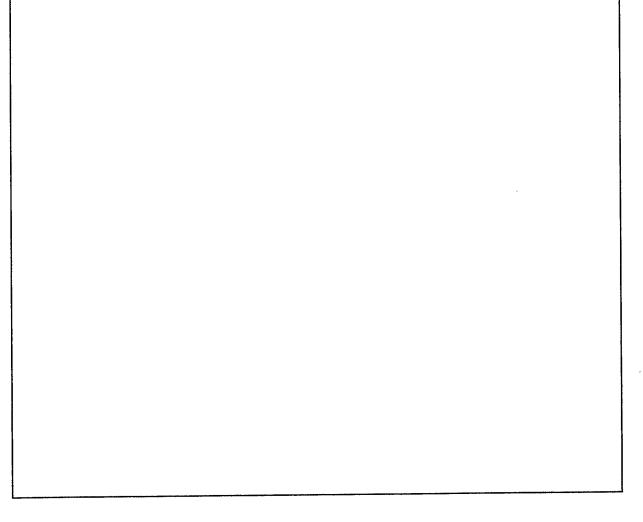
# RFW RDT&E

5/1/2000 12:41:47 PM



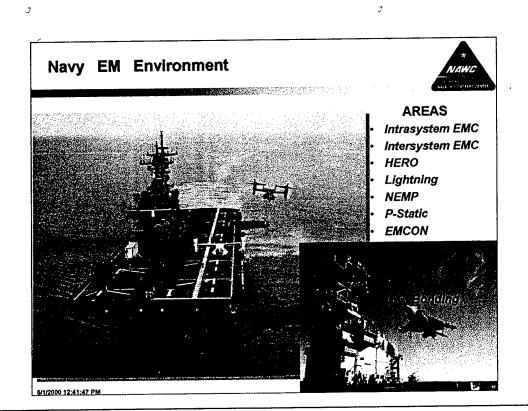
Э

.7



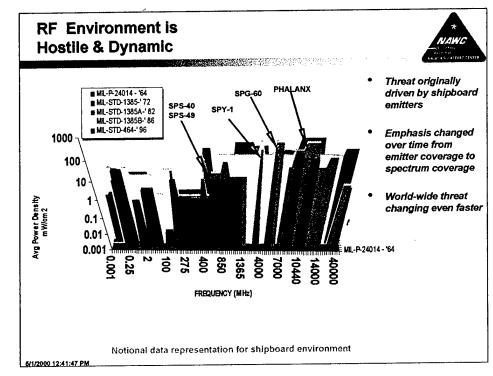
25

t



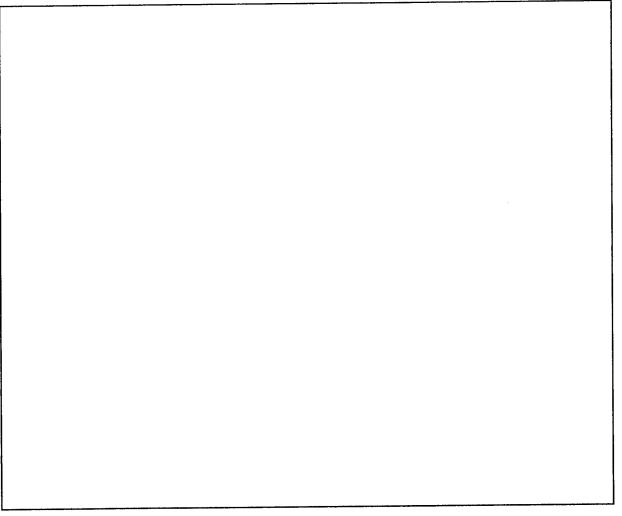
t

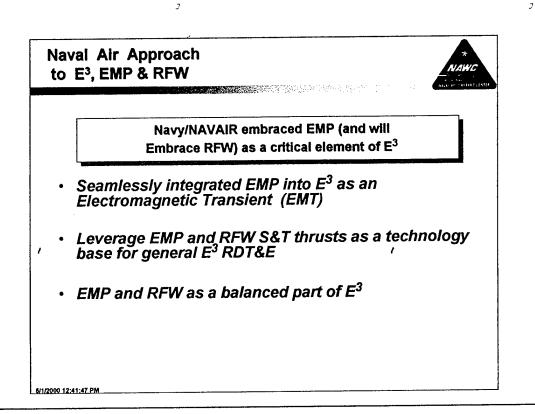
ł

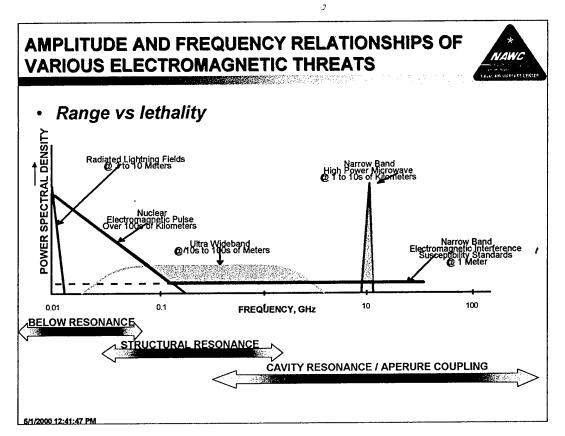


З

ł



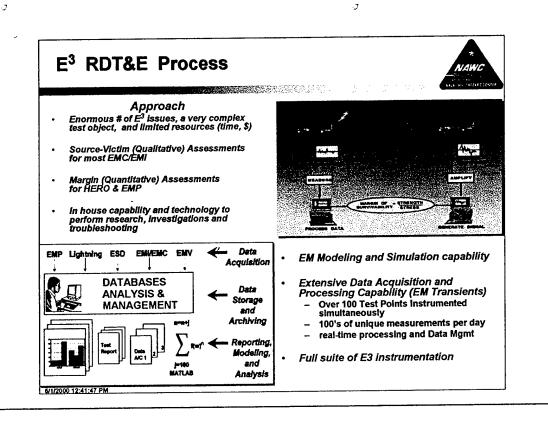




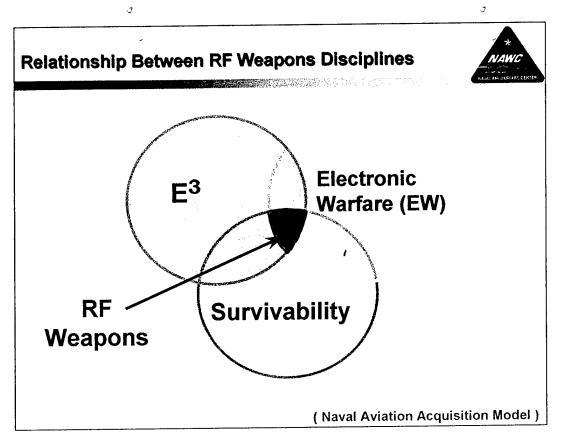
This slide reminds us that since most notional RF weapons could have higher frequency content. we may become concerned about different coupling modes.

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.



ŧ



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

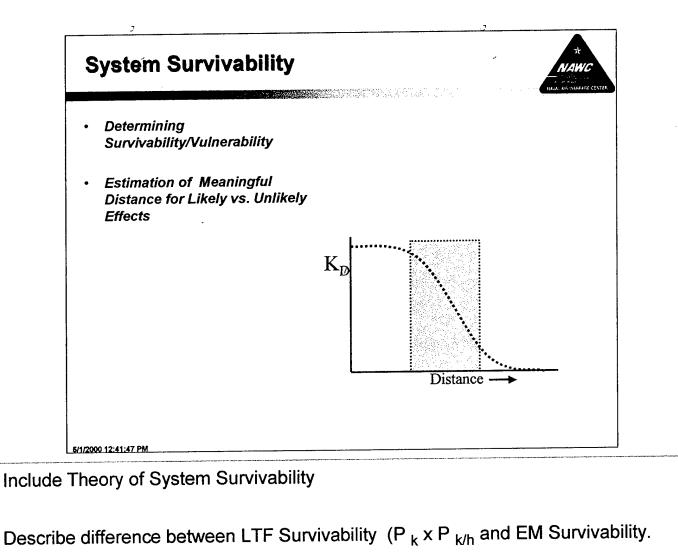
EW effects stop when EW emitter is turned off RF weapons effects remain

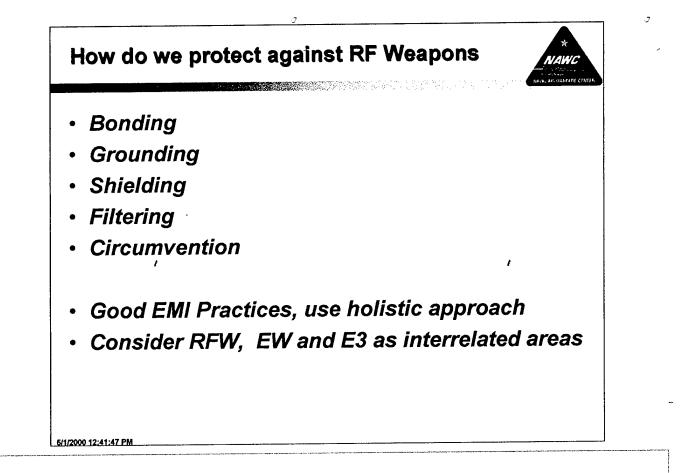
Other services or agencies may use another model for example the army may have a large ordnance area for RF munitions

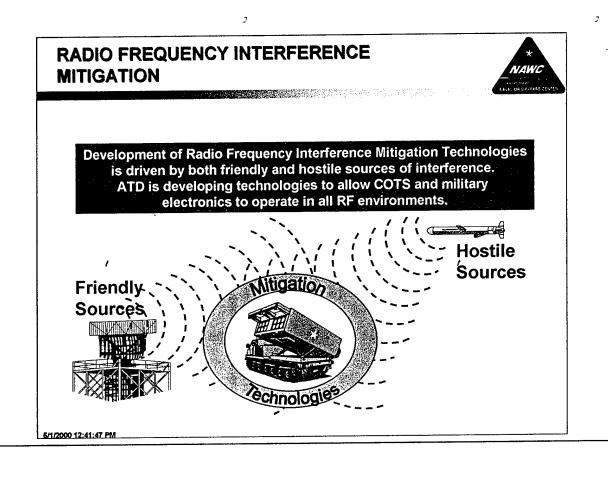
Both Offensive and Defensive

ł

E3 is concerned with Protection, lethality, fratricide







# **Categorization of Effects**



#### Test System Effects

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

J

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

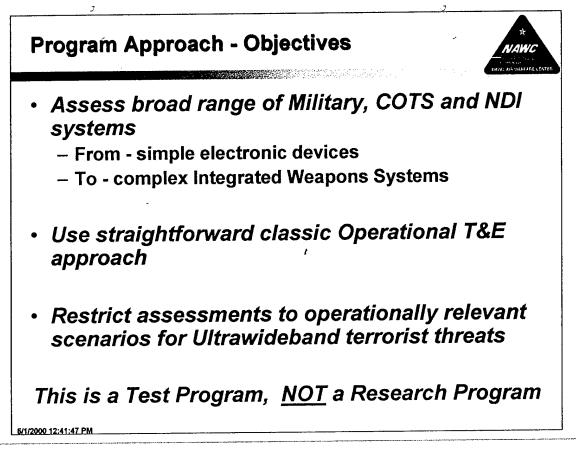
#### Operational Impact

How will the aggregate individual	Mission Category	Operational Impact of Effects
ayyregate murruuar	IV	None
effects from the various		Nuisance – Does Not Degrade Impact Mission Performance
systems/subsystems	11	Degraded – Requires Operator/Maintenance Intervention resulting in reduced effectiveness (Improved performance desireable)
impact/ affect the	1	Abort / Disabled - Serious Safety or mission Impact (Improved Performance required).

1

mission.

5/1/2000 12:41:47 PM



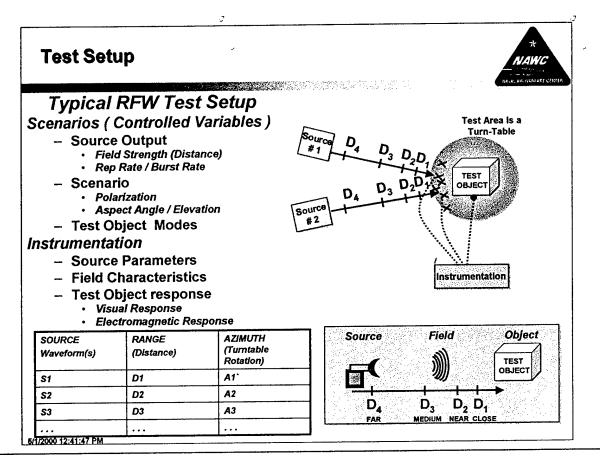
**Program Approach** 

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.

Tes	t Metho	odology	and the second s	ومنعقب والمعرور		THE ALL ALL WALFE
• Sc	ope of 1	Testing (by 1				
Larga		PLANNING 120 DAYS			DAYS	LYSIS AND REP 30 DAYS
Large		PRE-TEST PREDICTIONS 12	0 DAYS	<b>&gt;</b>		
	V	PRE-TEST PREDICTIONS 20 DAYS	5			
Small			OUCT AYS ANALYSIS AN 10 DA		However, Ma Resource A Proportional <sub>i</sub>	llocation al
Small	MANPOWER and	PLANNING 30 DAYS 2 DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION	AVS ANALYSIS AN	YS Test Object	Resource A Proportional	llocation al to Test Sco Man
Small	MANPOWER and Test management	PLANNING 30 DAYS 2 DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pre-Test Predictions	DUCT AYS ANALYSIS AN 10 DA	YS 1 Test Object Support	Resource A Proportional <sub>/</sub>	llocation ai to Test Sco
Small	MANPOWER and	PLANNING 30 DAYS 2 DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pre-Test Predictl Test Object Survey Deterrine Critical Systems	AVS ANALYSIS AN	YS Test Object Support Ferrying On Site Logistics	Resource A Proportional/ Man Peolity hrs Resources Fulser Operation Instrumentation	llocation al to Test Sco Man
Small	MANPOWER and Test management Hanning	PLANNING 30 DAYS 2DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pre-Test Predicti Test Object Survey Determine Othel Systems Determine Othel Paths	ANALYSIS ANA	YS Test Object Support Ferrying	Resource A Proportional, Man Paolity hrs Resources Pareources	llocation al to Test Sco Man
Small	MANPOWER and Test management Aanning Safety Security	PLANNING 30 DAYS 2 DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pre-Test Predictl Test Object Survey Deterrine Critical Systems	ANALYSIS ANA	YS Test Object Support Ferrying On Site Logistics Safety	Resource A Proportional, Man Pacility Inter Operation Instatumentation Support Maintenance Repair	llocation al to Test Sco Man
Small	MANPOWER and Test management Hanning Safety	PLANNING 30 DAYS 2 DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pre-Test Predicti Test Object Survey Deterrine Citical Systems Deterrine Citical Systems Deterrine Citical Systems Deterrine Citical Pattes Circut Analysis Seect Points Load Parameters	ANALYSIS ANA	YS Test Object Support Gerying On-Sie Logistice Secury Secury SystemOperation Hocedures	Resource A Proportional/ Man Feolity hrs Resources Resources Support Watterance Repair Safety	llocation al to Test Sco Man
Small	MANPOWER and Test management Asning Safety Security Operating Pocedures Pre - Test Production	PLANNING 30 DAYS PLANNING 30 DAYS PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pre-Test Predictly Determine Otkial Systems Determine Otkial Patta Ofcut Analysis Select Pohts	ANALYSIS ANA	YS Test Object Bupport Ferrying On-Ske Logistics Security Security System Operation	Resource A Proportional, Man Pacility Inter Operation Instatumentation Support Maintenance Repair	llocation al to Test Sco Man
Small	MANPOWER and Test management Panning Safety Security Operating Procedures	PLANNING 30 DAYS 2DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pre-Test Prediction Test Object Survey Determine Orbial Systems Determine Orbial Paths Circuit Analysis Select Parts Load Parameters Run Models	AYS ANALYSIS AN IO DA	YS Test Object Support Ferrying On-Ske Logistics Security System Operation Procedures - check fasts	Resource A Proportional/ Man Psolity hrs Resources Fuller Oppartion Instrumentation Support Maintenance Ropair Safety Sacurky Physical Outa	llocation al to Test Sco Man
Small	MANPOWER and Test management Aanning Sacurky Operating Procedures Fre - Test Prodictions Analysis	PLANNING 30 DAYS 2 DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pre-Test Predicti Test Object Survey Deterrine Citical Systems Deterrine Citical Systems Deterrine Citical Systems Deterrine Citical Pattes Circut Analysis Seect Points Load Parameters	AYS ANALYSIS AN 10 DA 10 DA 10 DA	YS Test Object Support Ferrying On-Site Logistice Safety Security System Operation Procedures - phack lata - inecting	Resource A Proportional/ Man Peolity hrs Resources Hele Operation Support Maintenance Repair Sacurity Security Physical	Nocation ai to Test Sco Men hre
Small	MANPOWER and Test management Assning Safety Security Operating Procedures Fre - Test Productions Analysis Reporting	PLANNING 30 DAYS PLANNING 30 DAYS PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pre-Test Predict Test Object Survey Determine Citical Systems Determine Citical Systems Determine Citical Parts Citical Analysis Citical Citical Analysis Citical Citical Analysis Citical Citical Analysis Citical	AYS ANALYSIS AN 10 DA 10 DA 10 DA	YS Test Object Support Ferrying On-Site Logistice Safety Security System Operation Procedures - phack lata - inecting	Resource A Proportional/ Man Paolity hrs Resources Public Operation Nationance Repair Saport Maintenance Repair Security Security Physical Deta User Spaces	Nocation ai to Test Sco Men hre
Small	MANPOWER and Test management Aanning Sacurky Operating Procedures Fre - Test Prodictions Analysis	PLANNING 30 DAYS 2 DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man hrs Pre-Test Predictly Deterrine Ofbial Systems Deterrine Ofbial Systems Deterrine Ofbial Parts Circue Analysis Select Points Load Parameters Run Models TEST OBJECT RESOURCE ALLU Ferrying tofromWEEKS	AYS ANALYSIS AN 10 DA 10 DA 10 DA	YS Test Object Support Ferrying On-Site Logistice Safety Security System Operation Procedures - phack lata - inecting	Resource A Proportional/ hrs Resources Pulser Operation Instrumentation Support Maintenance Repair Safety Security Physical Otac User Spaces Shielded Erobsure	Nocation ai to Test Sco Men hre
Small	MANPOWER and Test management Anning Safety Security Operating Procedures Pre - Test Predictions Analysis Reporting Test Object Support	PLANNING 30 DAYS 2 DA PRE-TEST PREDICTIONS 20 DAYS RESOURCE ALLOCATION Man Pro-Test Predictly hrs Test Object Survey Determine Of Big Systems Determine Of Big Systems	AYS ANALYSIS AN 10 DA	YS Test Object Support Ferrying On-Site Logistice Safety Security System Operation Procedures - phack lata - inecting	Resource A Proportional/ hrs Resources Pulser Operation Instrumentation Support Maintenance Repair Safety Security Physical Otac User Spaces Shielded Erobsure	Men hrs

2

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.



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

Intensity

Waveform

Rep rate

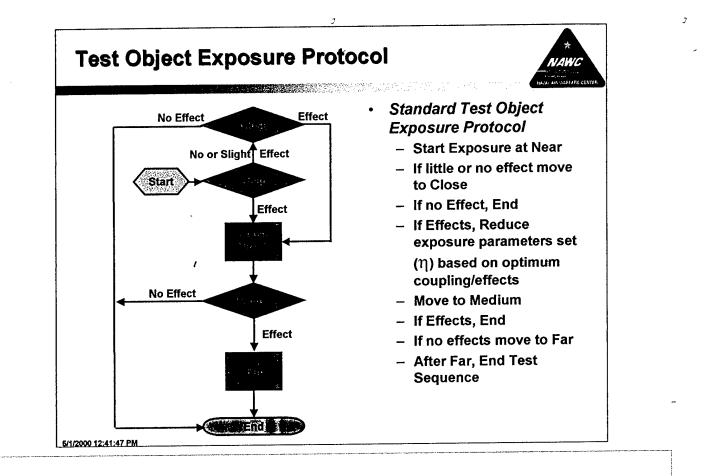
#### **Test Object**

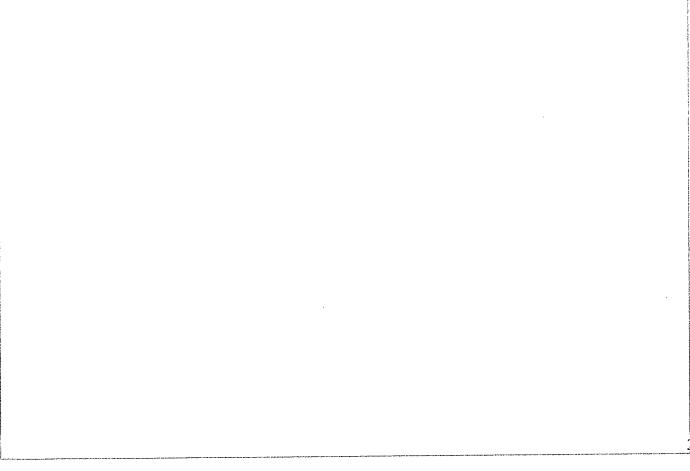
Modes

#### Scenario

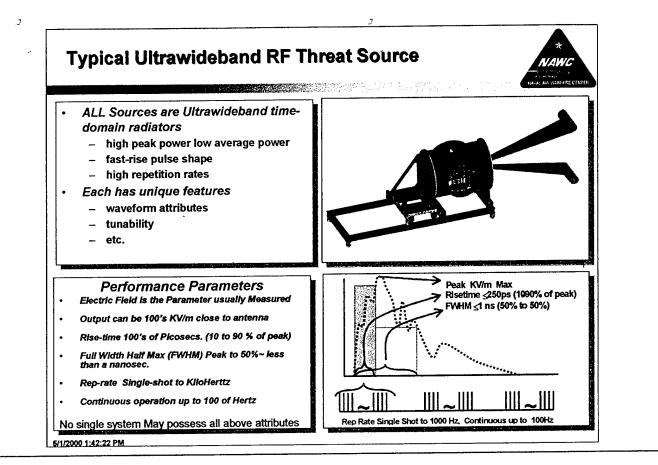
Polarization

Angle of Incidence





<u>3</u>9



### **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

6/1/2000 1:49:21 PM

				1					
REPO	<b>RT DOCU</b>	MENTAT	ION PAGE	Form Approved					
				<u> </u>	OMB No. 0704-0188				
and maintaining th information, include	e data needed, and comp ing suggestions for reduc	pleting and reviewing thi ing this burden, to Depar	s collection of information. Se Iment of Defense, Washington	nd comments regarding Headquarters Services, I	eviewing instructions, searching existing data sources, gathering this burden estimate or any other aspect of this collection of Directorate for Information Operations and Reports (0704-0188), g any other provision of law, no person shall be subject to any				
	to comply with a collection	on of information if it doe	s not display a currently valid C	MB control number. PI	EASE DO NOT RETURN YOUR FORM TO THE ABOVE				
ADDRESS.	ATE	2. REPORT T	VPF ,	3. DATES COV	TRED				
I. KEFORT D	AIL	Viewgraphs	II E	J. DAILS COV					
4. TITLE ANI	O SUBTITLE			5a. CONTRACT NUMBER					
Radio Frequer	ncy Weapons			5b. GRANT NUMBER					
				5c. PROGRAM ELEMENT NUMBER					
6. AUTHOR(S	5)			5d. PROJECT NUMBER					
Sam Frazier				5e. TASK NUMBER					
				5f. WORK UNIT NUMBER					
7. PERFORM	7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)				8. PERFORMING ORGANIZATION REPORT NUMBER				
Naval Air Wa	fare Center Aircra	ft Division							
	Point Road, Unit #6								
	r, Maryland 20670								
ADDRESS(ES		G AGENCY NAMI	E(S) AND	10. SPONSOR/MONITOR'S ACRONYM(S)					
Nousl Air Sug	tems Command			11. SPONSOR/MONITOR'S REPORT NUMBER(S)					
47123 Buse R									
	r, Maryland 20670	-1547							
	12. DISTRIBUTION/AVAILABILITY STATEMENT								
	ENTARY NOTES	ribution is unlimite	d.						
13. SUPPLEM	IENTART NOTES	1							
14. ABSTRAG	CT				4/4 ·····				
15. SUBJECT	15. SUBJECT TERMS								
			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Sam Frazier				
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (include area code)				
Unclassified	Unclassified	Unclassified	Unclassified	41	(301) 342-3582				

DTHO QUALITY INSPECTED 4

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