MONASH University
Information Technology

E-Bombs vs. Pervasive Infrastructure Vulnerability

Pacific Theater Air, Sea, Land Battle Concept:
IO/EW/Cyber Operations International Conference
Information Operations Institute and the Association of Old Crows

Dr Carlo Kopp
Associate Fellow AIAA, Senior Member IEEE, PEng
Monash University / Air Power Australia
Carlo.Kopp@monash.edu
http://www.csse.monash.edu.au/~carlo/

Pervasive Digital Infrastructure == Vulnerability

Over the last two decades we have observed unprecedented global expansion of the digital infrastructure:

- Spanning the civil, military and “dual use” domains;
- Spanning industry, commerce, administration, education;
- Spanning fixed and wireless infrastructure domains;
- Personal devices like cellphones, pads, notebooks pervasive.

- **The digital infrastructure has become deeply embedded across all facets of our social, economic and military systems.**
- **Increasingly we observe integrated and distributed applications, where the system comprises a large number of globally distributed components, which are mutually dependent on fixed and mobile components, and networks.**
- ***The digital infrastructure is now a “single point of failure”.***

Types of Attack vs. Digital Infrastructure

- There are numerous ways in which the digital infrastructure can be subjected to attacks;
- Broadly attacks can be divided into “penetration attacks” where the attacker gains access to exploit the infrastructure, or do damage to transmitted or stored information, or “Denial of Service” attacks, where the infrastructure is temporarily or permanently damaged;
- While cyberwar DoS attacks can do permanent damage, mostly such DoS attacks are transient with non-persistent damage effects;
- Electromagnetic weapons are designed to produce either transient or permanent damage effects, or both;
- ***Pervasive digital infrastructure makes the development of electromagnetic weapons potentially very profitable.***

The “Cascade Failure” Problem

- Digital infrastructure is highly interconnected and thus interdependent;
- Common reliance on power grid, telecommunications cabled and wireless connections, local and remote servers, single and multiple site Clouds and Grids;
- A mass destruction effect in one geographical area can cause cascading failures as interdependent systems fail;
- Lusser’s Product Law:

$$P[S] = \prod_{i=1}^{N} P_i \ [S]$$

- ***Damage effects are thus no longer localised in extent, e.g. destroying a server or Cloud in Washington DC may crippled dependent systems globally.***

Types of Electromagnetic Weapons

- *There are many possible taxonomical divisions for electromagnetic weapons;*
- Directed Energy Weapons vs. “one shot” E-Bombs;
- Nuclear (HEMP) E-Bombs vs. Non-nuclear E-Bombs;
- Narrowband Weapons vs. Wideband or UWB Weapons;
- High Power Microwave vs. “Low Band” weapons;
- Pulsed weapons vs. Continuous Wave (CW) weapons;
- Persistent Area Denial (AD) weapons vs. Non-Persistent weapons;
- Explosively pumped vs. Electrically pumped weapons;
- There is enormous diversity in possible electromagnetic weapon designs, for both large scale and highly focussed attacks, both against civil and military targets.

The COTS "Military-Technological Revolution"

- Cold War era military equipment built to MilSpec design standards, very frequently hardened against nuclear EMP;
- Equipment mostly built using low density digital hardware and analogue hardware, usually well shielded and robust, with MilSpec interfaces and interconnections;
- Contemporary military equipment mostly heavily dependent on COTS processing hardware, COTS networking hardware, and often COTS packaging and EMC provisions;
- COTS hardware is mostly "electromagnetically soft" compared to typical Cold War era "electromagnetically hard" designs, where HEMP, EMC and HERO were planned for;
- COTS hardware uses very high density CMOS technology which requires much less energy to damage or wound;
- Wounded equipment fails intermittently, not immediately.

The Critical Coupling Problem

- **The effectiveness of all EM weapons is constrained by the physics of the coupling problem;**
- **Power generated by the weapon must be emitted, must propagate through the environment, and couple into the target, to access internal electrical components and do damage;**
- **Emitted weapon Power/EIRP determined by weapon design;**
- **Propagation determined by spectral content, propagation losses and distance – *Friis* inverse square law equation;**
- **Coupling at target determined by spectral content, incident power, and target design;**
- **Coupling modes: "front door" via antennas or other apertures; "back door" by power supplies and other cables;**
- ***As coupling behaviours vary strongly, prediction of EM weapons effects is difficult and always "statistical" in nature.***

Nuclear E-Bombs: Electro Magnetic Pulse Effect

- A nuclear weapon detonated at altitude ionises the upper atmosphere -> HEMP (High altitude Electro Magnetic Pulse);
- EMP produces high voltage transients on cables, which damage electronic equipment;
- Digital equipment mostly highly vulnerable due high content of high density CMOS devices;
- Effect similar to lightning strikes, but faster and more powerful;
- Nuclear MHD effect – ionospheric recovery generates slow long line DC transients;
- Nuclear MHD effects can produce similar delayed damage effects to electricity grids as geo-magnetic storms, but more intensive and localised.

Non-Nuclear or “Conventional” E-Bombs

- Many feasible design strategies, technology is still evolving;
- Broadly divided by pump mechanisms – explosive or electrical; and by spectral output – narrowband or wideband;
- Weapon footprint and coupling per available power depends strongly on weapon design, HPM weapons can exploit coupling opportunities other weapons cannot;
- *Explosively Pumped Flux Compression Generators* – used as power sources for HPM weapons, or used directly as low frequency weapons;
- HPM weapons used high power “one shot tubes” such as Virtual Cathode Oscillators (Vircators); tens of GigaWatts for 100s of nanoseconds; High Power Spark Gaps also feasible for wideband pulsed weapons;
- Small warheads – explosively pumped rare earth magnets.

General Arrangement – Helical FCG

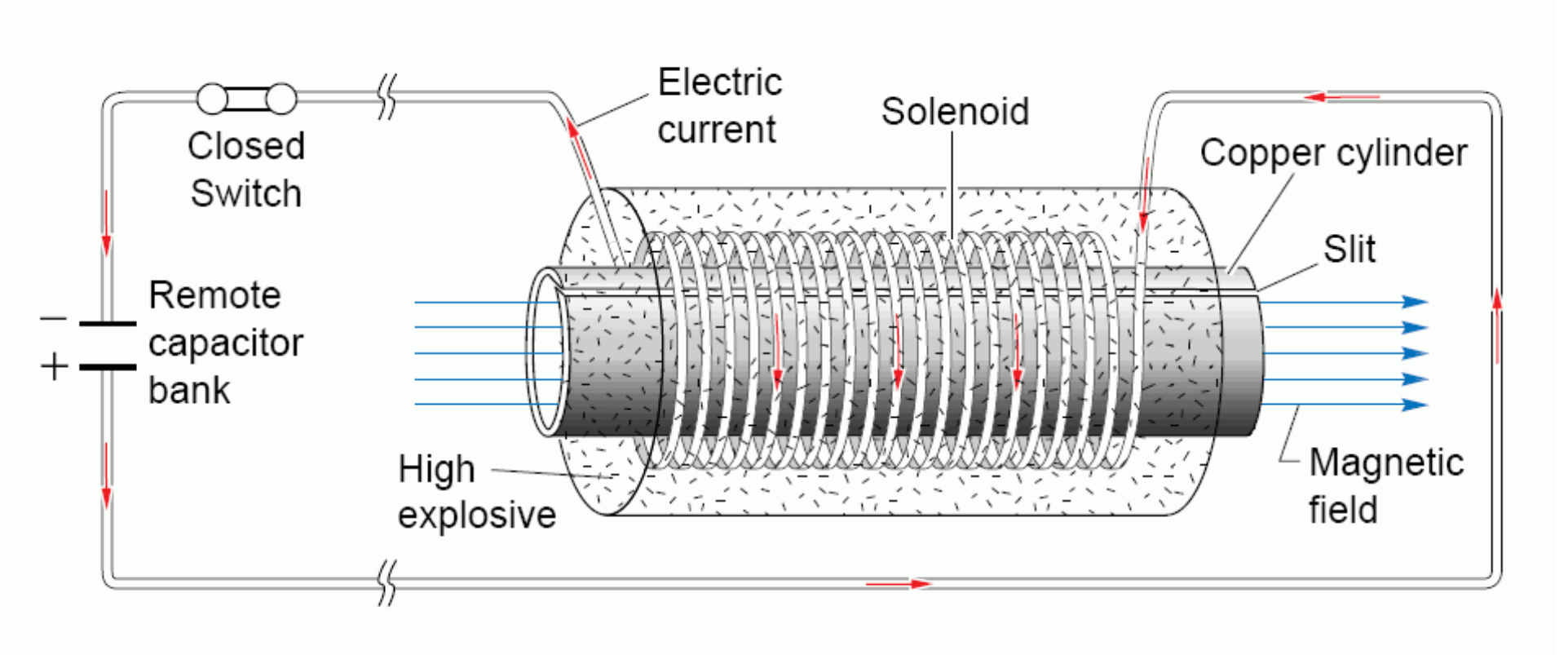


Image: Los Alamos National Laboratory

Helical FCG Operation

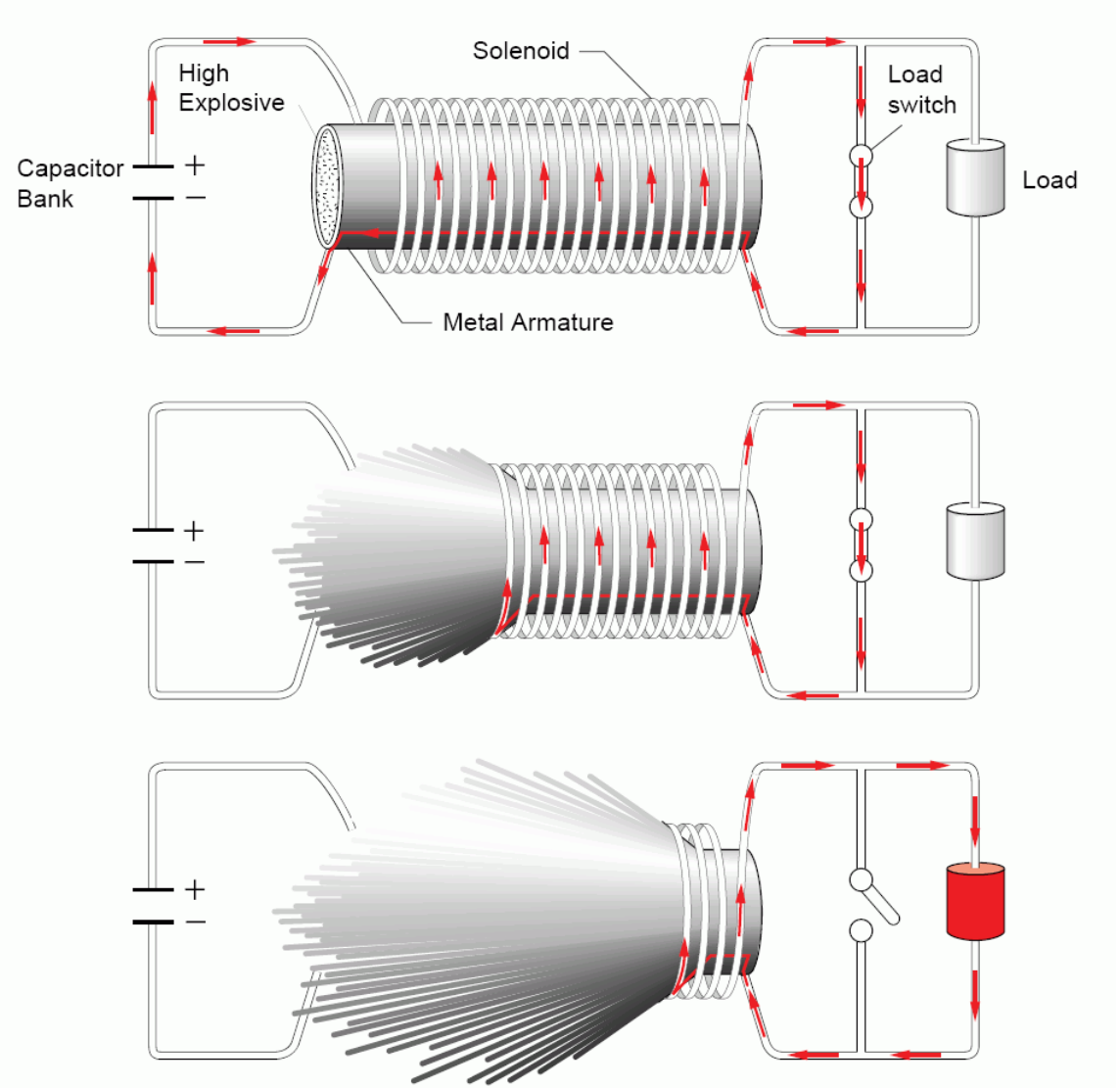
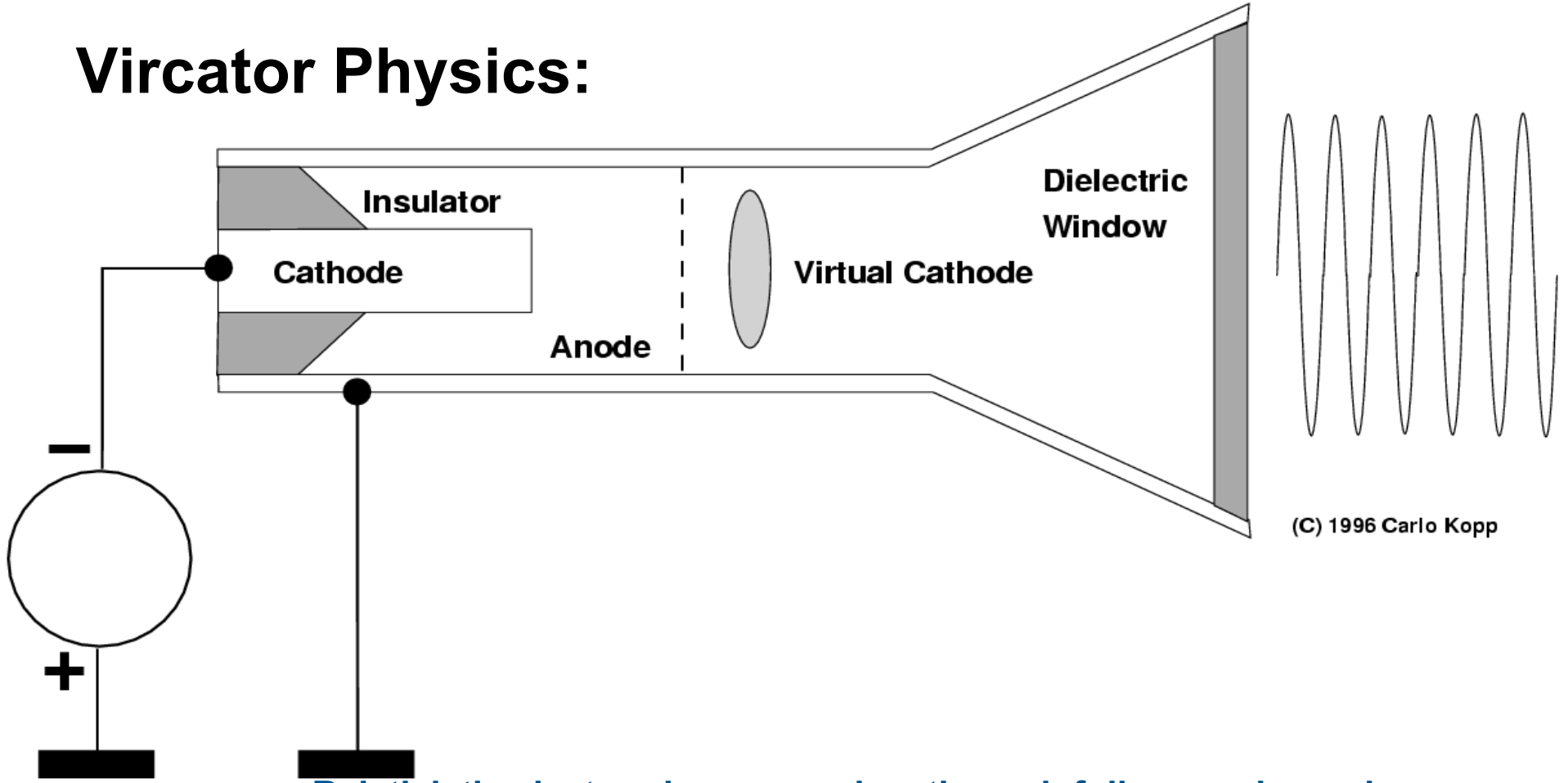


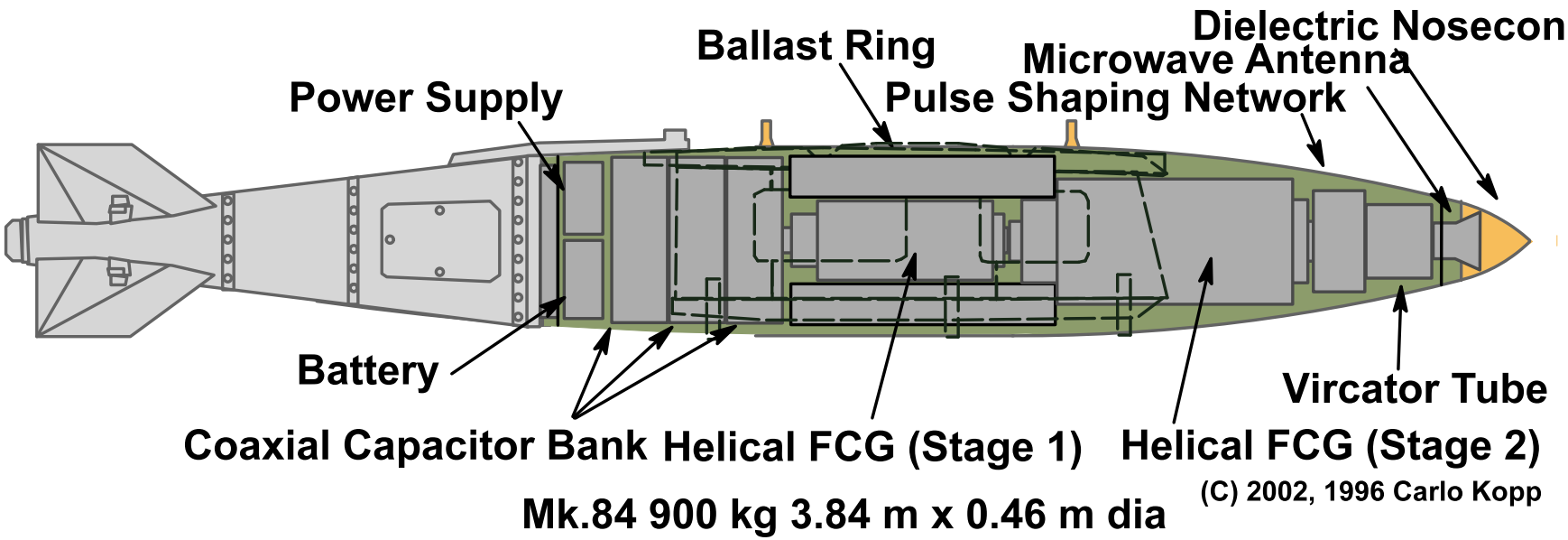
Image: Los Alamos National Laboratory

Vircator Physics:



- Relativistic electron beam punches through foil or mesh anode.
- "Virtual" cathode formed by space charge bubble behind anode.
- Peak power of up to tens of GigaWatts for 100s of nanoseconds.
- Anode typically melts in about 1 μsec; Cheap and simple to manufacture; Wide bandwidth allows chirping of oscillation – multiple mode cavity resonances facilitate mode coupling.

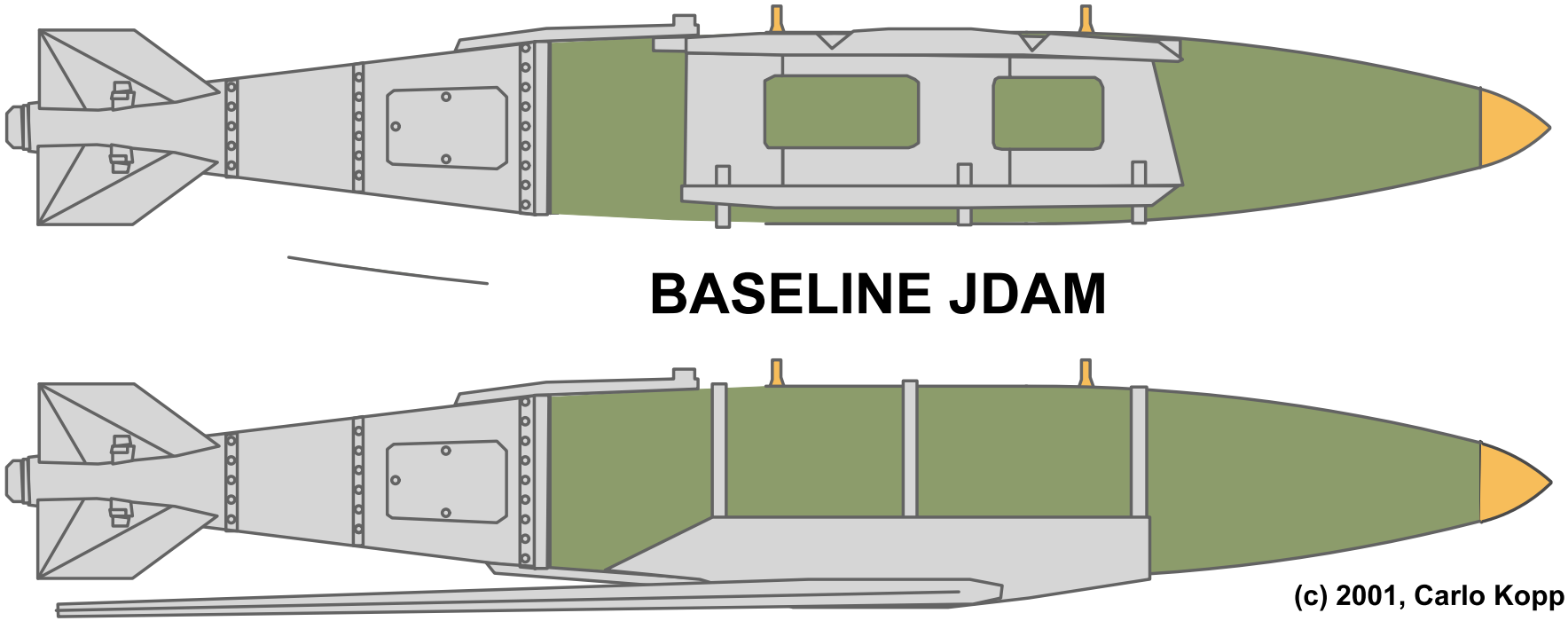
HPM (Microwave) E-Bomb Layout



HIGH POWER MICROWAVE E-BOMB - GENERAL ARRANGMENT MK.84 PACKAGING WARHEAD USING VIRCATOR AND 2 STAGE FLUX COMPRESSION GENERATOR

HPM E-BOMB WARHEAD (GBU-31/Mk.84 FORM FACTOR)

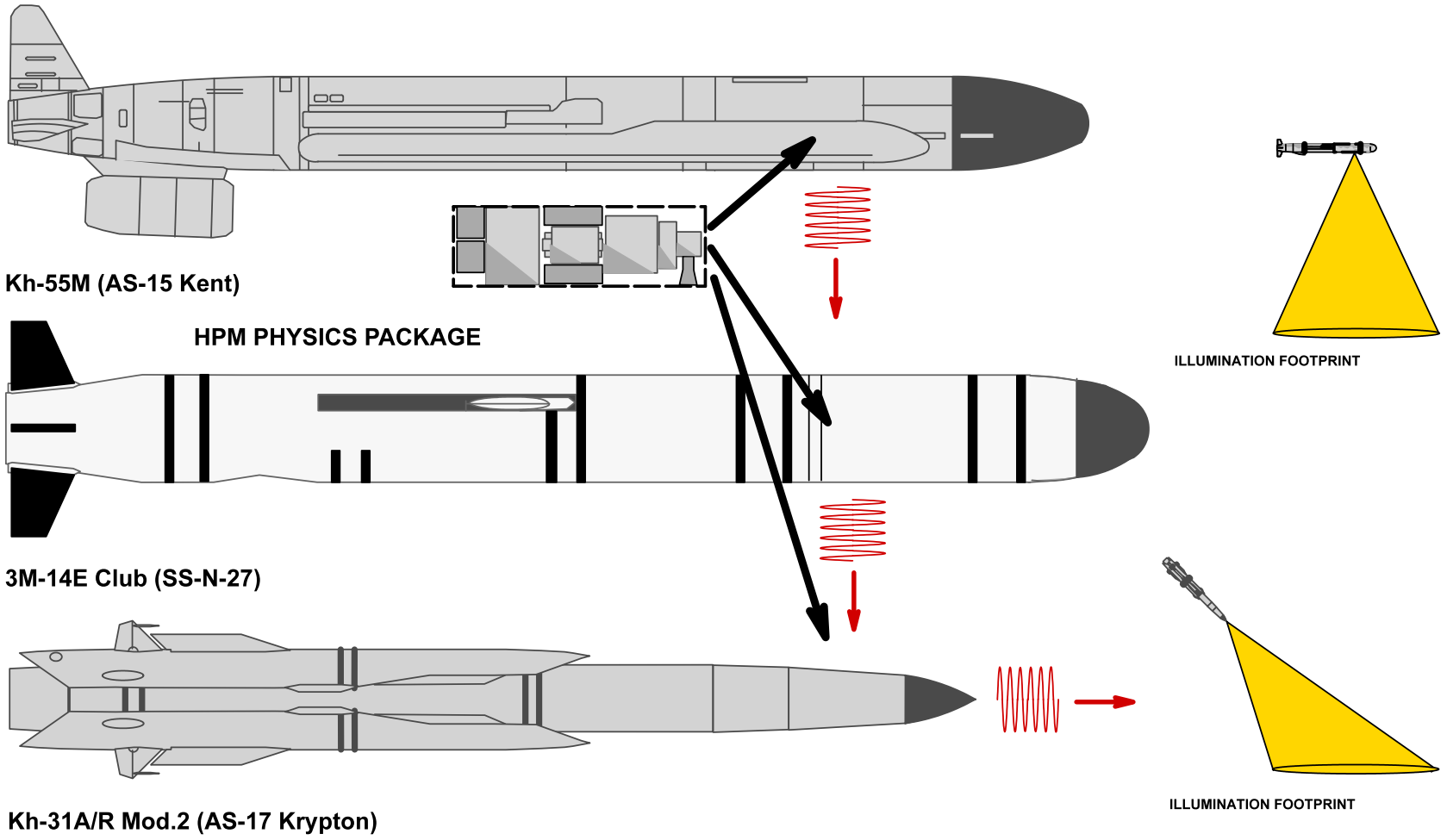
Deployment Options: GPS Aided Guided Bombs



BASELINE JDAM

JDAM-ER EXTENDED RANGE WITH GLIDE WING

Deployment Options: Missiles (Regional)



Proliferation

- **The technology used in conventional E-Bombs is within the reach of any nation capable of designing nuclear weapons and high power radars – e.g. China, Iran, DPRK, Russia;**
- **OSINT source material very scarce on E-Bomb technology and designs, effort is usually well hidden from scrutiny;**
- **Potentially large area footprints of many square miles for GigaWatt class weapons, with the usual lethality prediction caveats – targets not tested may be unexpectedly resistant or susceptible at specific weapon frequencies / polarisations;**
- **Terrorist attacks predicated on the availability of proven designs or inventory E-Bomb munitions – emerging risk;**
- ***The high payoff in using E-Bombs as disruptive or area suppression weapons points to common use in future nation state conflicts involving developed nations.***

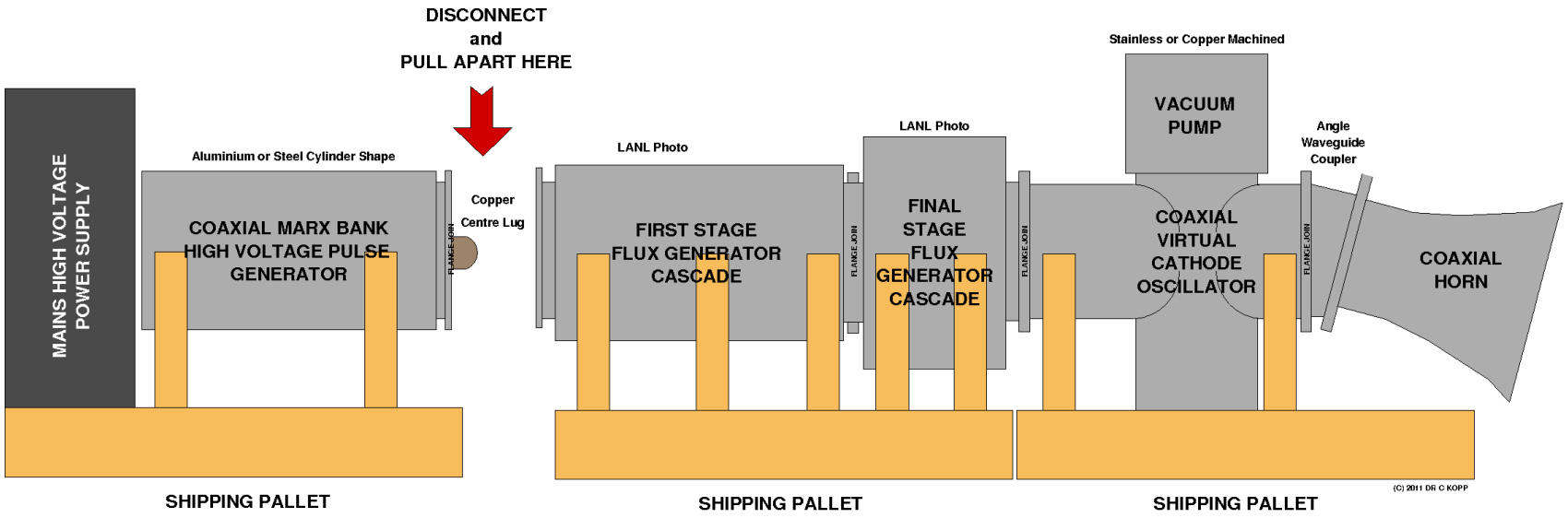
Risks / Conclusions

- **Since the term E-Bomb was coined in 1992, the scale of vulnerable infrastructure and systems has multiplied many times over, yet there has been no systematic effort to harden the infrastructure or military systems using COTS hardware;**
- **GRID Act (H.R. 5026) intended to introduce critical infrastructure hardening passed by HR but killed by Senate;**
- **Widespread scepticism and disbelief concerning weapon feasibility and infrastructure vulnerability, wholly a result of *technical illiteracy in electromagnetism*;**
- **The notion that a technology which is available and profitable to use in combat would not be used is wishful thinking;**
- ***Legislation for electromagnetic hardening of infrastructure and systems for military, dual use and critical civil applications should be introduced urgently.***

BACKUP SLIDES

NCIS-LA Ep 3.11 “Higher Power” – E-Bomb Prop

NCIS-LA E-Bomb Prop



- Original sketch used for prop fabrication in October, 2011;
- Based 1995 paper and LANL Flux Compression Generator;
- Intent to popularise risk issues to public and legislature;
- NCIS LA audience is > 35 million globally;
- Script by Joe Sachs (E.R. series) and Shane Brennan;
- Scientific advisor Dr Carlo Kopp, Monash University

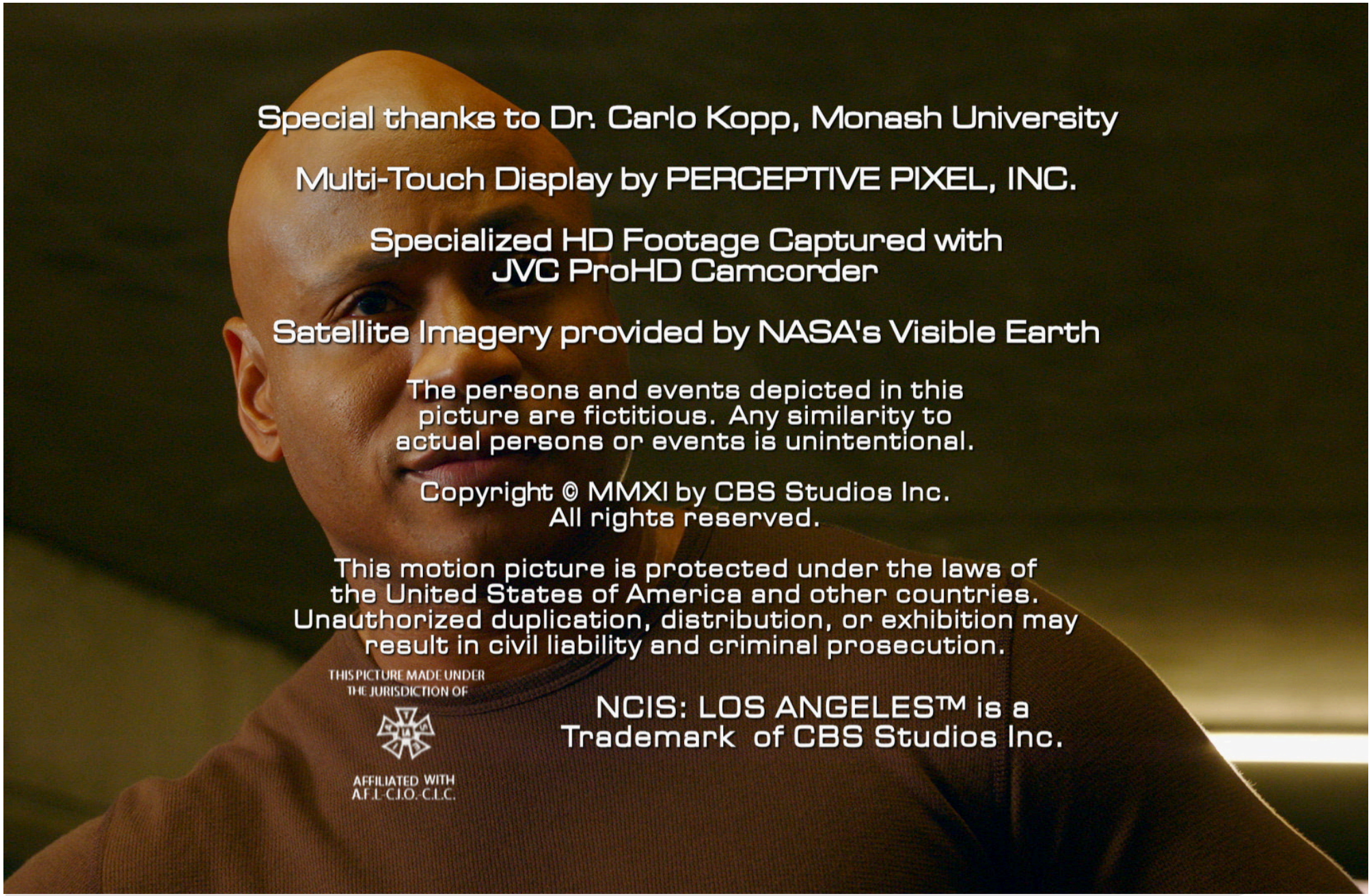
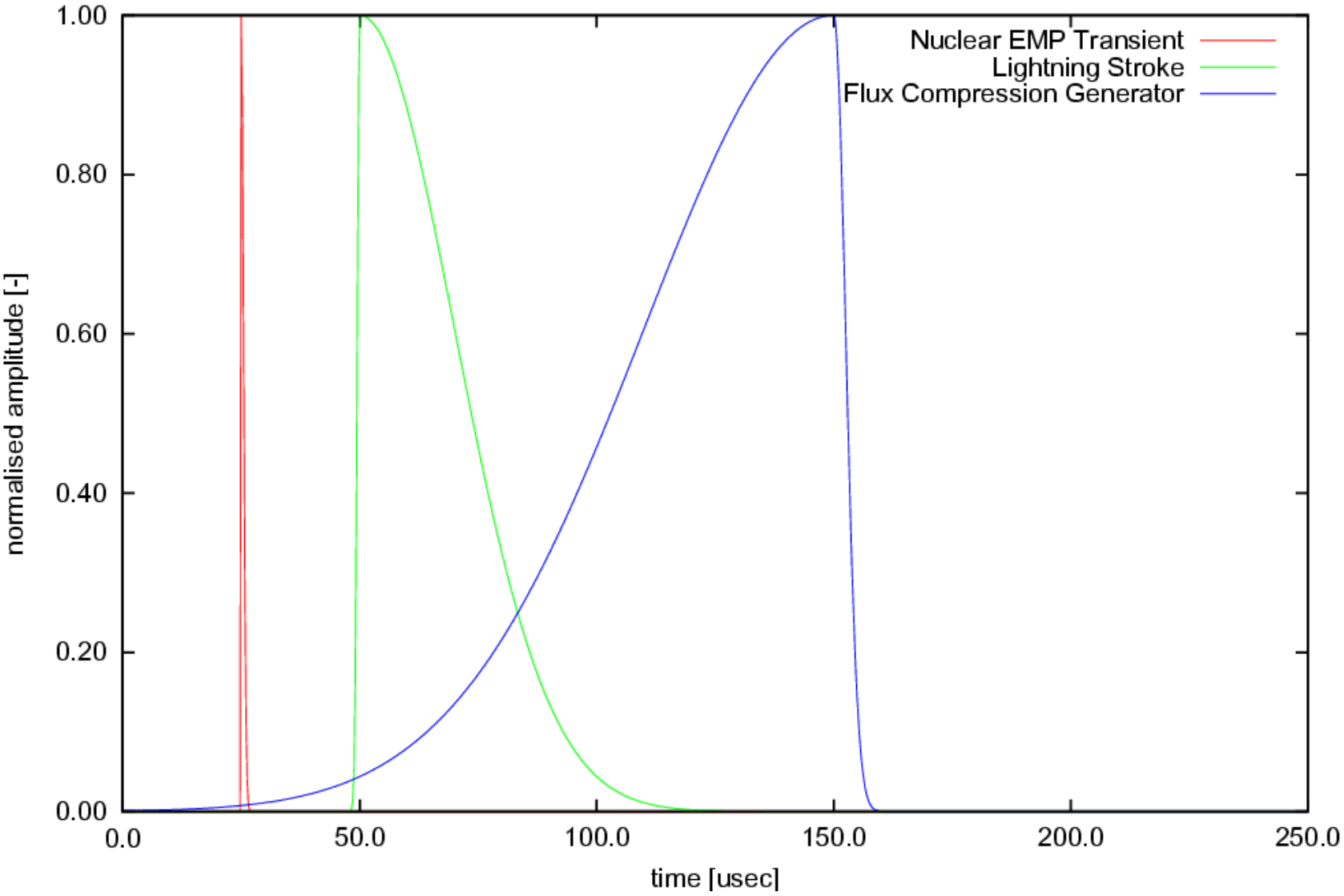

Special thanks to Dr. Carlo Kopp, Monash University
Multi-Touch Display by PERCEPTIVE PIXEL, INC.
Specialized HD Footage Captured with
JVC ProHD Camcorder
Satellite Imagery provided by NASA's Visible Earth
The persons and events depicted in this
picture are fictitious. Any similarity to
actual persons or events is unintentional.
Copyright © MMXI by CBS Studios Inc.
All rights reserved.
This motion picture is protected under the laws of
the United States of America and other countries.
Unauthorized duplication, distribution, or exhibition may
result in civil liability and criminal prosecution.
THIS PICTURE MADE UNDER
THE JURISDICTION OF
AFFILIATED WITH
A.F.L.-C.I.O.-C.L.C.
NCIS: LOS ANGELES™ is a
Trademark of CBS Studios Inc.

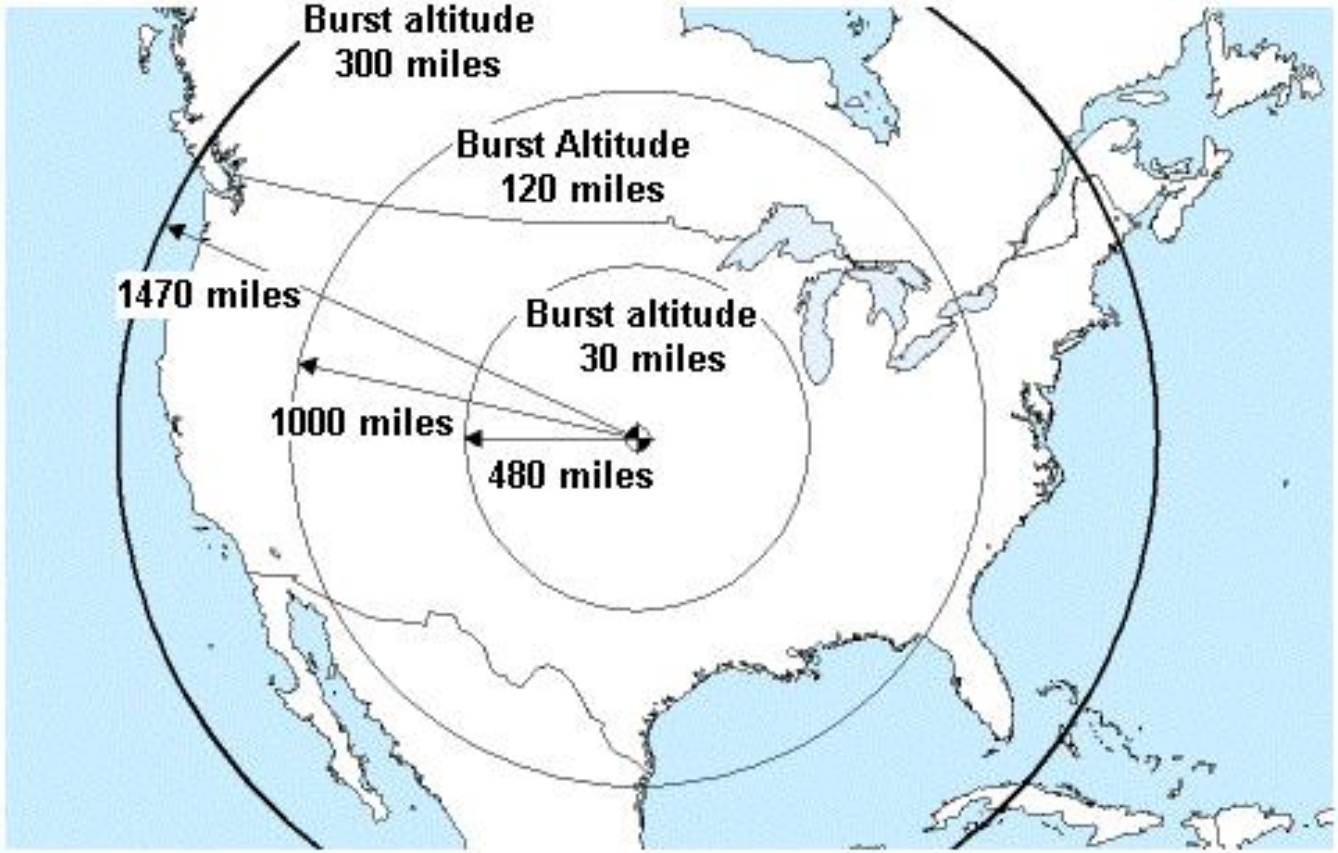
Fig.1 Typical Electromagnetic Pulse Shapes



HEMP Components

- **Three components to any HEMP event;**
- **IEC 61000-2-9 designates these as E1, E2 and E3 components;**
- ***E1 is a fast and short high field strength pulse from gamma photons ionising gas molecules; ~50 kiloVolts/metre for conventional boosted fission or fusion warheads.***
- ***E2 is produced by the neutron flux generated by the warhead;***
- ***E3 duration of up to hundreds of seconds, MHD-EMP (Magneto-Hydro Dynamic EMP);***
- **E3 is similar to solar Geomagnetically Induced Current (GIC) effects; The E3 component can often penetrate soils and reach buried cables; mitigated by highly electrically conductive soils, exacerbated by dry or highly resistive soils.**

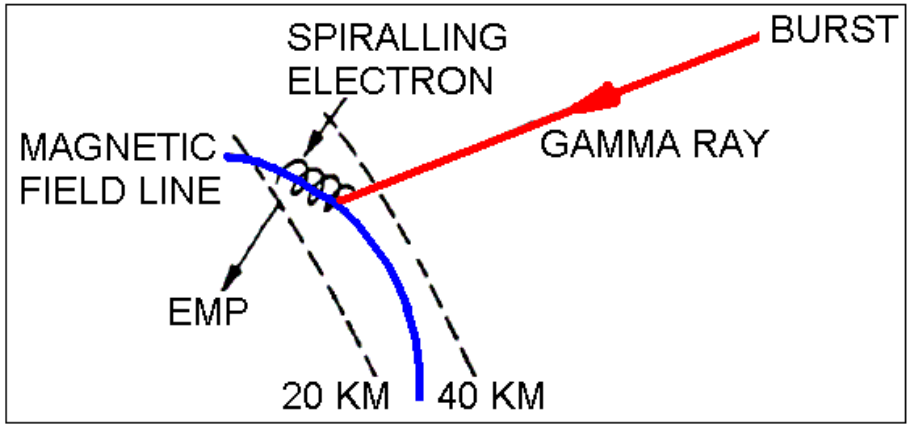
HEMP Footprint (A)

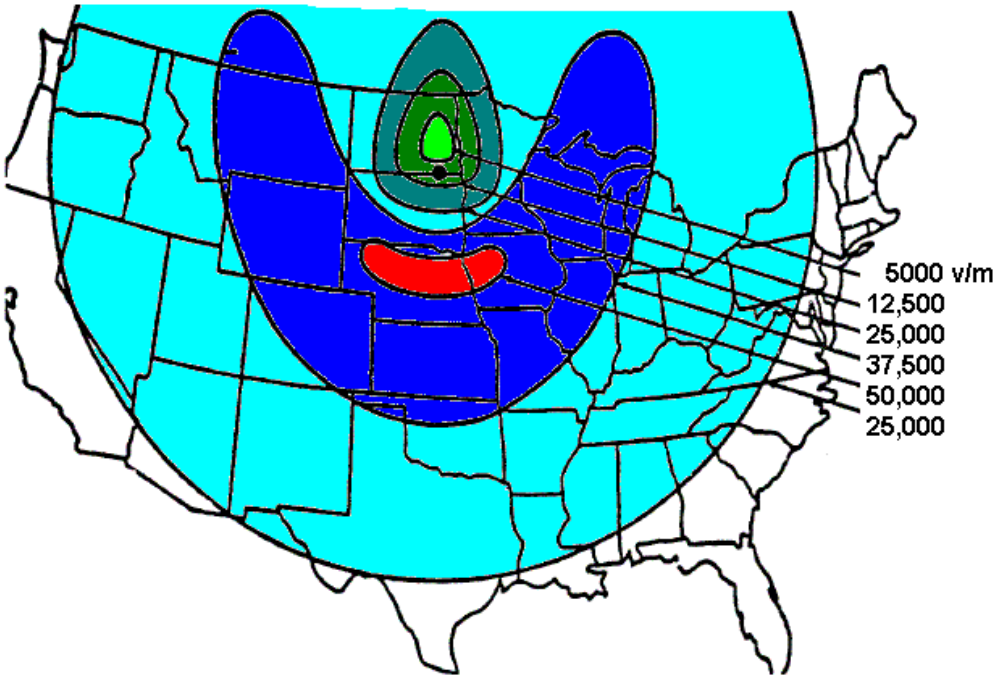


EMP AREA BY BURSTS AT 30, 120 and 300 MILES

Gary Smith, "Electromagnetic Pulse Threats", testimony to House National Security Committee on July 16, 1997

HEMP Footprint (B)



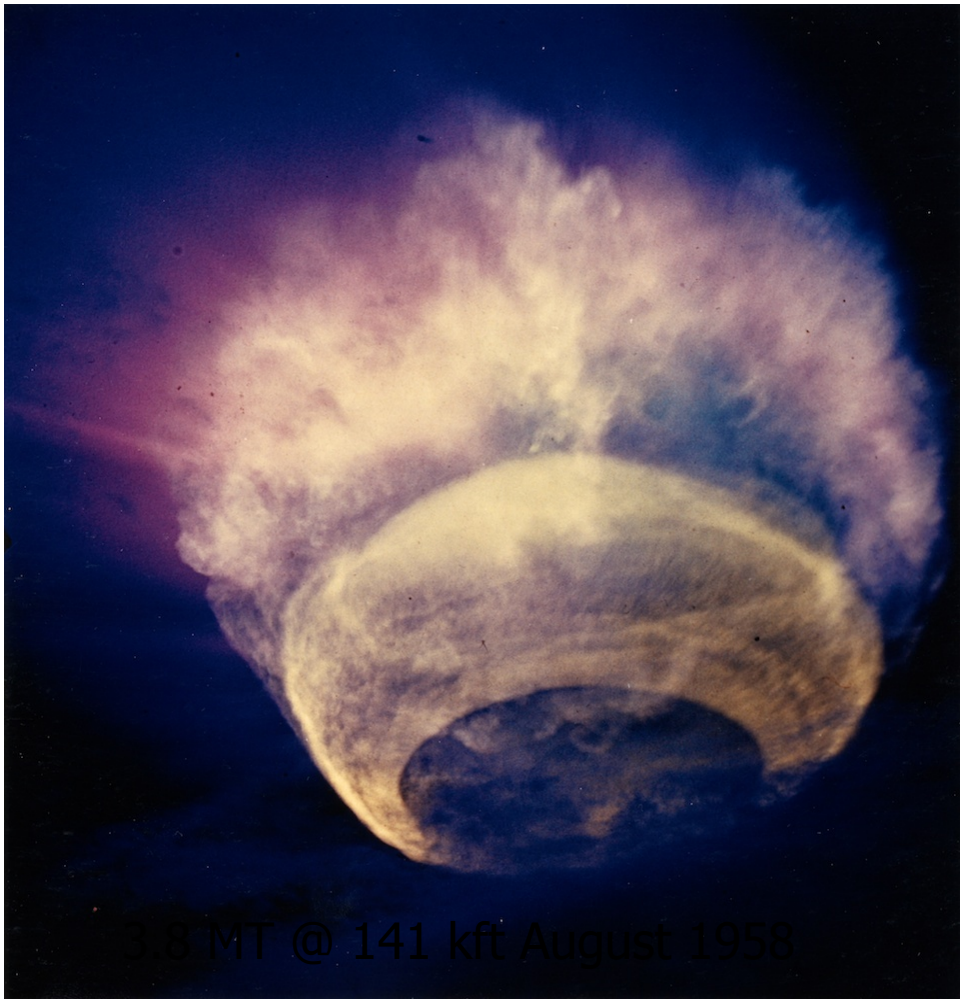


Source: Nuclear Environment Survivability,
U. S. Army, report AD-A278230 (1994)

MONASH University
Information Technology

Hardtack I Teak

Hardtack I Orange

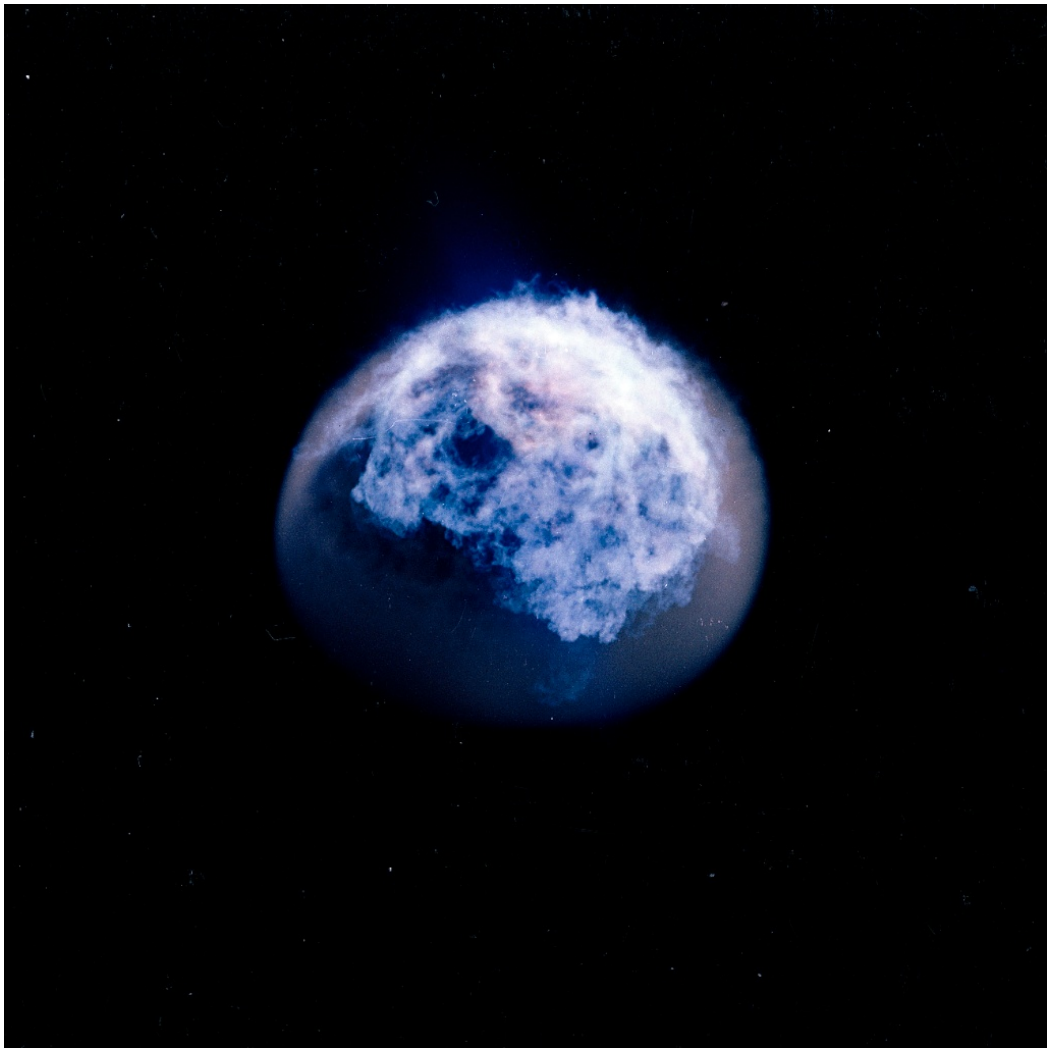


Fishbowl Starfish Prime

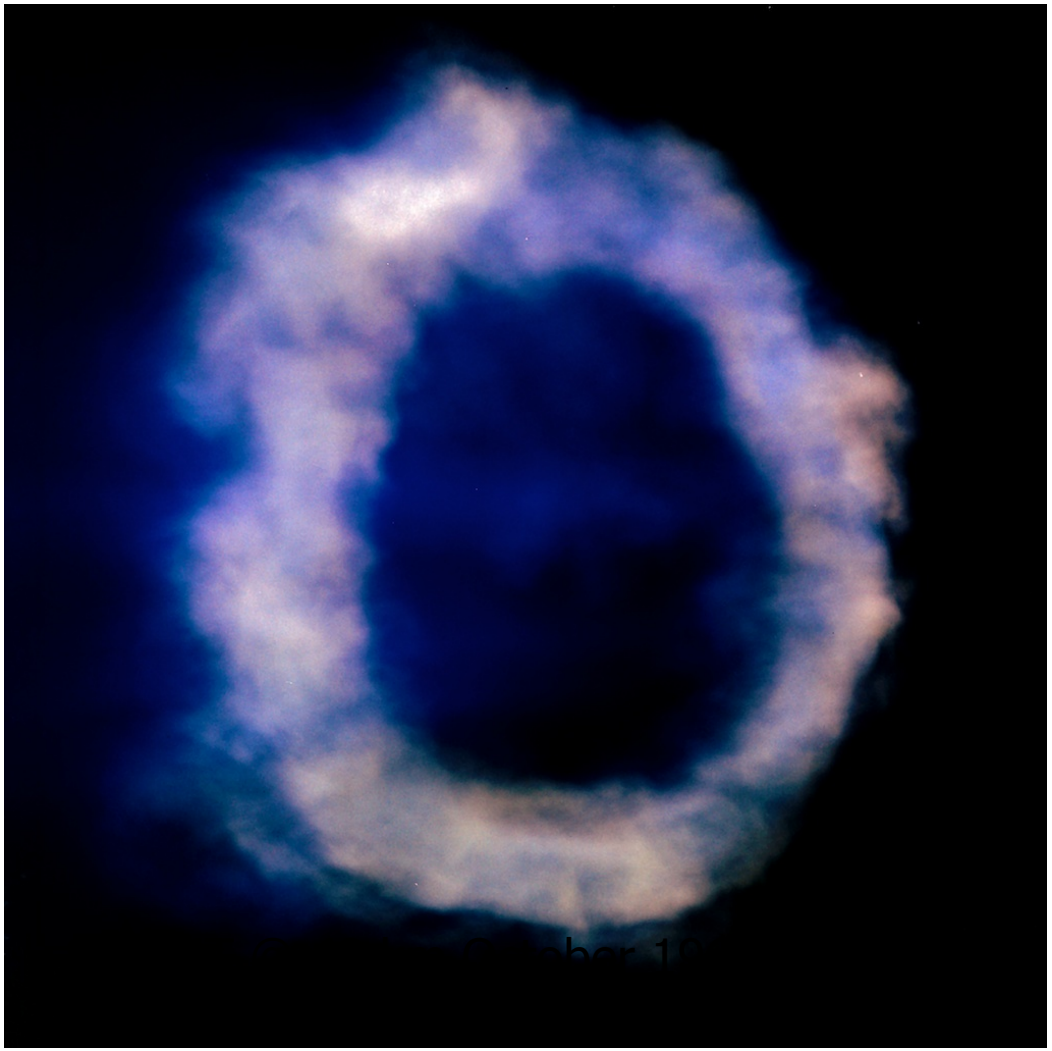
Fishbowl Starfish Prime

Fishbowl Starfish Prime

Fishbowl Bluegill Triple Prime



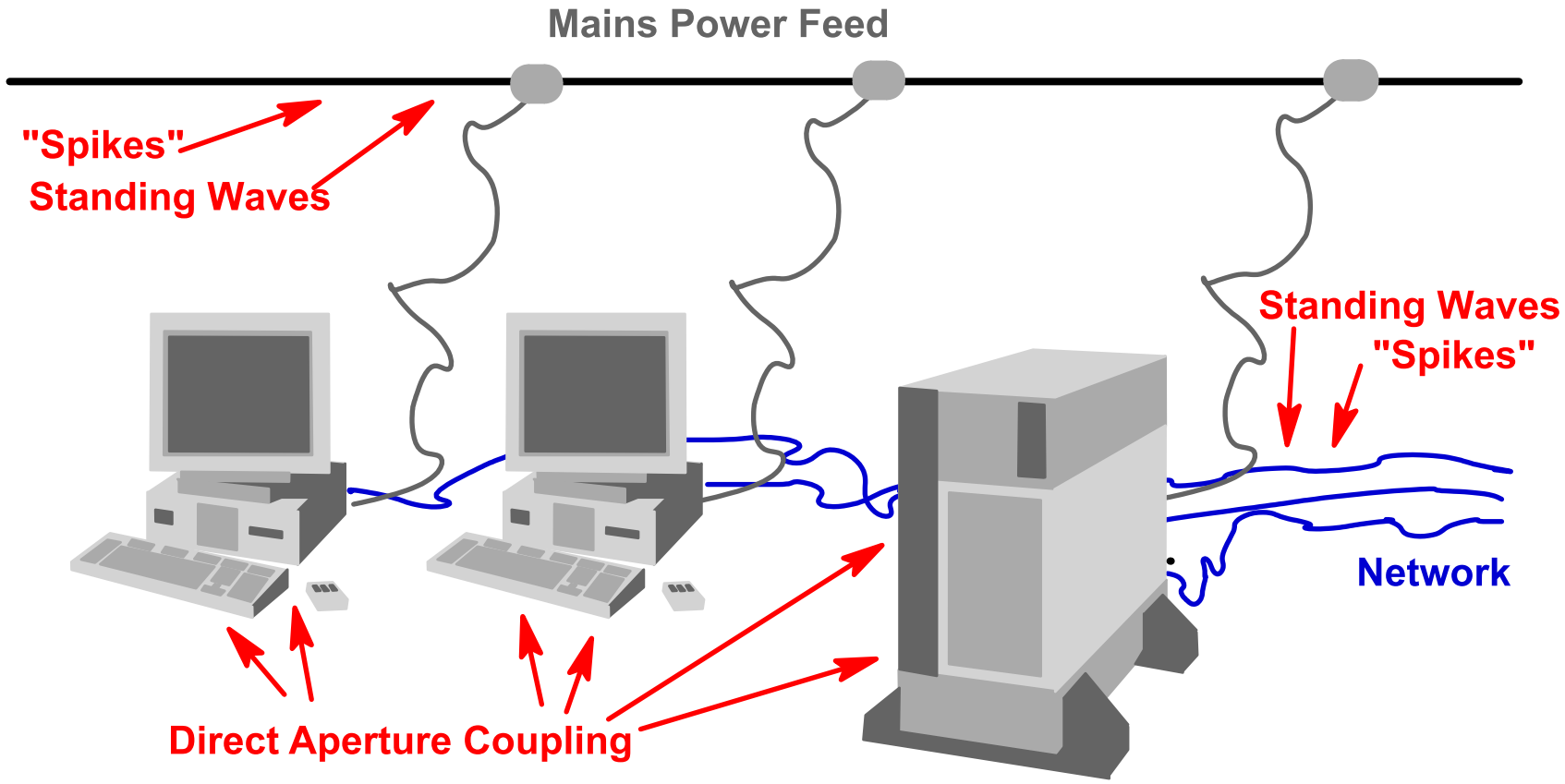
Fishbowl Bluegill Triple Prime



Vulnerability Reduction (Hardening):

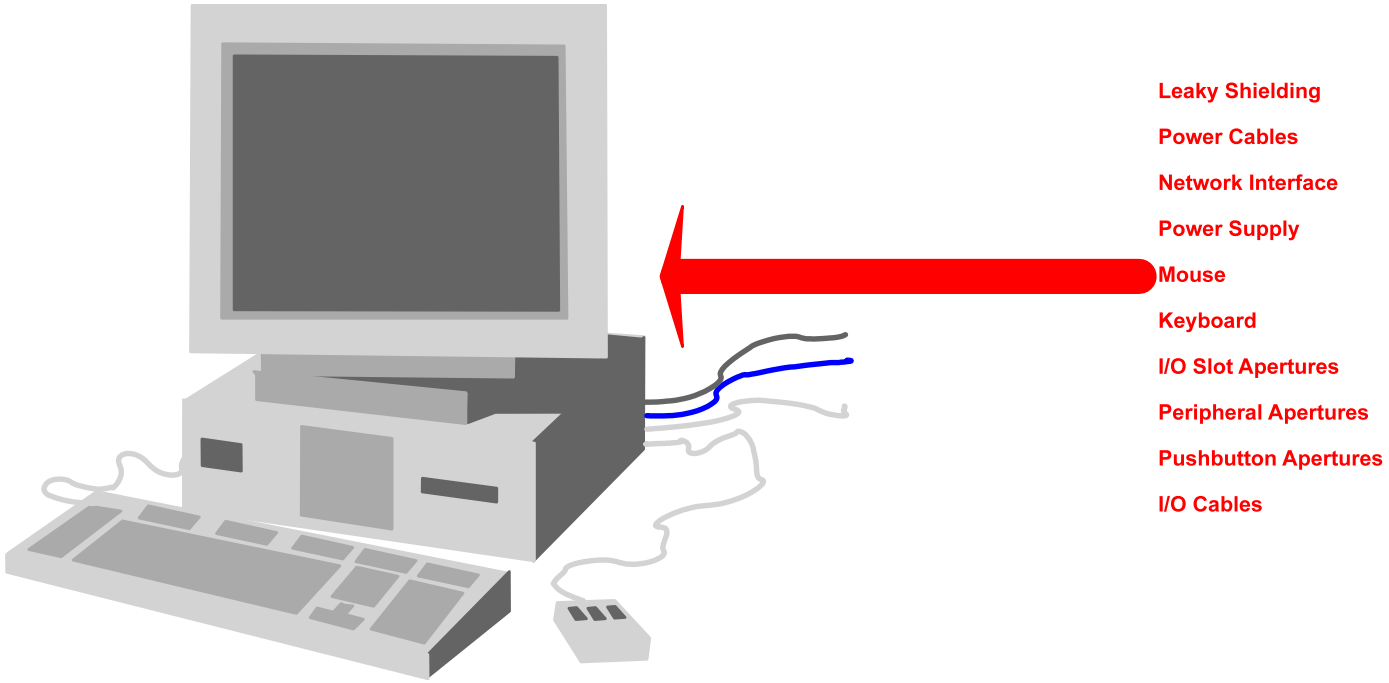
- convert computer rooms into Faraday cages.
- use optical fibres for data.
- isolate power feeds with transient arrestors.
- use non-electrical power feed schemes.
- use electromagnetic “air lock”.
- shielding must be comprehensive.

System Level Susceptibility



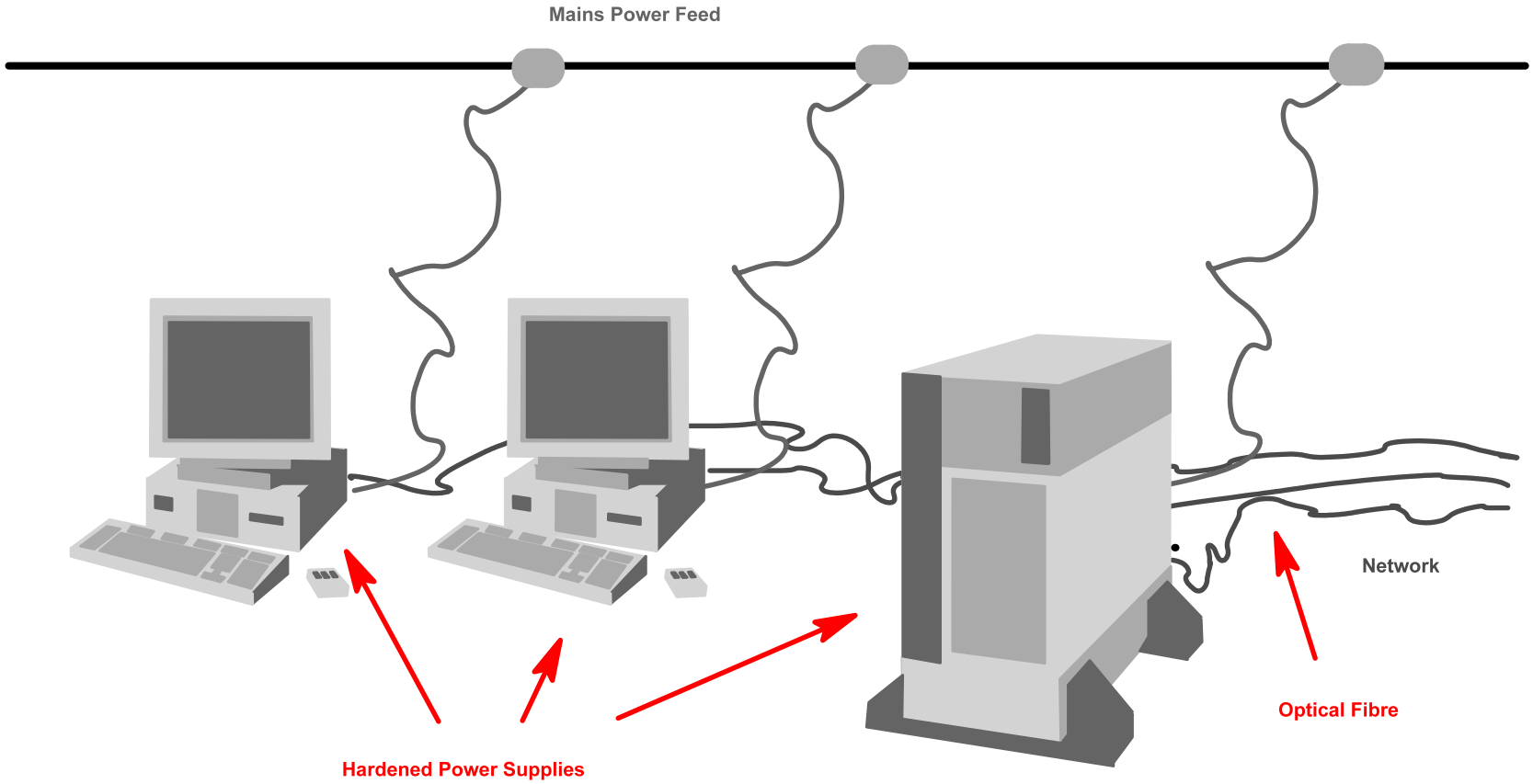
System Level Susceptibility

Host Level Susceptibility



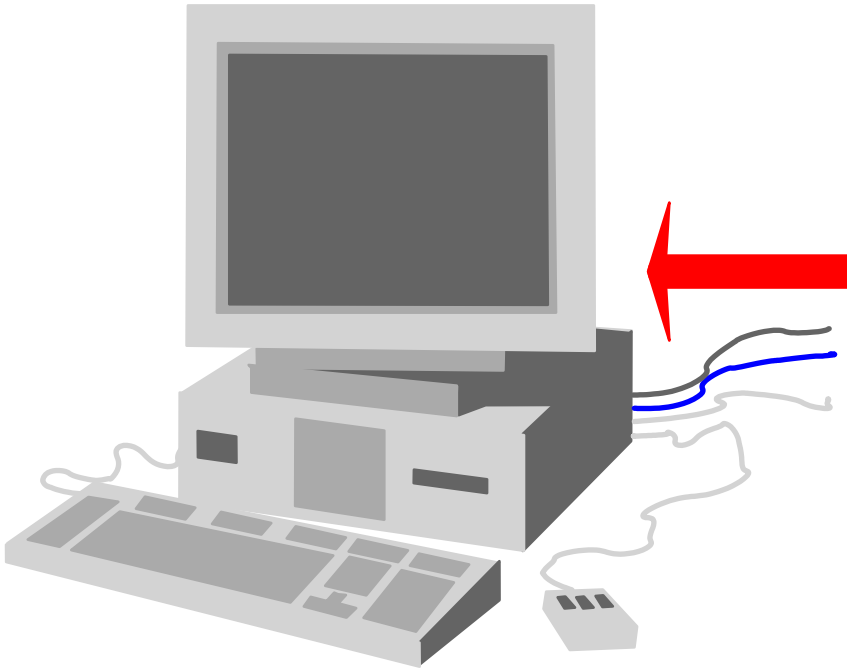
Host Level Susceptibility

I/O and Power Hardening



I/O and Power Interface Hardening

Comprehensive Hardening



- Comprehensive Shielding
- Ferrite Beads on Power Cables
- Optical Fibre Network Interface
- Non-Electrically Coupled Power
- Optical Mouse
- Optically Coupled Keyboard
- No I/O Slot Apertures
- No Peripheral Apertures
- No Pushbutton Apertures
- I/O Cables

Comprehensive Host Hardening

Computer Room Hardening