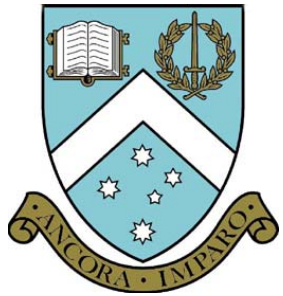


CSE468
Information Conflict

Lecturer: Dr Carlo Kopp, MIEEE, MAIAA, PEng

Lecture 09

Forms of Information Conflict, Analysis and Modelling of Information Conflict Attacks and Techniques

Reference Sources and Bibliography

- **Winn Schwartau, Information Warfare: Cyberterrorism : Protecting Your Personal Security in the Electronic Age, New York, NY: Thunder's Mouth Press, 1995, Second Edition.**
- **Carlo Kopp's publications at http://www.ausairpower.net/iw.html**

Why a Taxonomy?

- Given the diversity of possible ways in which information and its supporting infrastructure can be attacked, a taxonomical division is an important means of organising one's understanding of the problem.
- While specific forms of attack might all map back to the canonical four strategies, the severity and context of the attack may vary considerably.
- There are many arbitrary classifications applied to sorting modes, regimes and types of attack.
- Schwartau's class model is widely used and representative.

The ‘Class Model’ of Information Conflict

- **Class I IW** - Compromising Personal or Corporate Privacy is the lowest grade of IW, and occurs when for instance your personal account is compromised and confidential information accessed.
- **Class II IW** - Industrial and Economic Espionage is the next step up, in which instance government or corporate computers are hacked into and information covertly stolen.
- **Class III IW** - Info-Terrorism and Denial of Services. The intentional destrcution of another party's computer or network, or denial of service via other means is usually described as info-terrorism. The offending party may be a malicious hacker, a criminal extortionist, a genuine terrorist or a foreign government seeking to take down a system or systems.
- **Military IW** - The use of all of the above combined with other military techniques in order to disrupt an opponent's military operations, government activity and economy qualifies as military IW. Military IW is the most destructive as it involves both soft and hard kill techniques.

Classes of IW

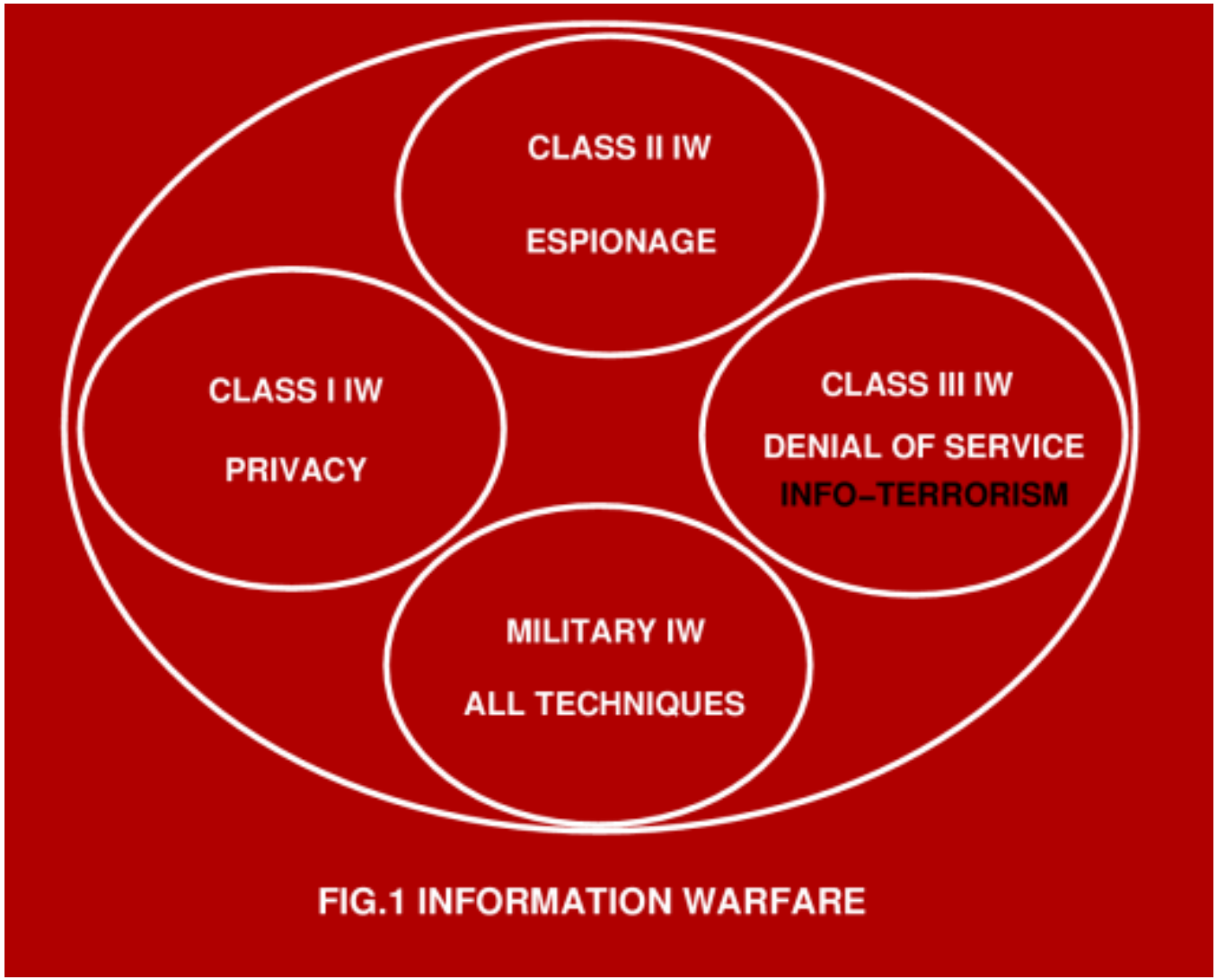


FIG.1 INFORMATION WARFARE

Class I Information Warfare

- Class I IW involves breaches of privacy and confidentiality targeting individuals, usually with the aim of stealing money or bandwidth.
- Example – a hacker steals a credit card number to deplete the available credit to his advantage.
- Example – a phracker steals account information to charge calls against an individual's account (*phracking*).
- Example – a whacker penetrates a wireless network to steal bandwidth (*whacking*).
- Example – a bogus website emulating a finance organisation or company website is constructed to steal passwords and credit card numbers (*phishing*).
- Example – spammers substituting email addresses.

Class II Information Warfare

- Industrial and Economic Espionage is a more severe form of attack, in which instance government or corporate computers are hacked into and information covertly stolen.
- While the methodology may be similar or the same to many Class I attacks, the amounts of money or the value of the information stolen are significantly higher.
- A key problem with Class II attacks is that victims may not be prepared to report an attack to avoid their clientele losing confidence and withdrawing funds.
- Class II attacks are performed typically by professional criminals or government agencies.
- Examples – widely reported past attacks on banks, NASA, US DoD, DOE and other computer systems.

Class III Information Warfare

- Info-Terrorism and Denial of Service attacks. The intentional destruction of another party's computer or network, or denial of service via other means is usually described as *info-terrorism*.
- The offending party may be a malicious hacker, a criminal extortionist, a genuine terrorist or a foreign government.
- Examples – ping of death attacks (historical), packet storm attacks, physical attacks on systems.
- Case Study – during the NATO bombing of Serbia, the NATO website was attacked using a range of techniques.
- Case Study – during the invasion of East Timor attacks on Australian systems increased in frequency.

Military (Class IV) Information Warfare

- Military IW covers the whole spectrum of possible attacks.
- *Soft Kill* attacks may fall into Class II and Class III categories.
- *Hard Kill* attacks have included the use of smart bombs and cruise missiles to cripple communications nodes such as civilian and military telephone switches and satellite terminals.
- Military IW includes techniques such as propaganda and psychological warfare (psywar).
- A recent development is the penetration of opposing military networks to generate false target information.

Denial of Service Attacks

- Denial of service attacks are an offensive technique intended to cripple an organisation by preventing it from using its digital systems.
- Denial of Service attacks are increasingly common especially involving attacks on websites, and large scale attacks on networked systems using viruses and worms.
- Where an organisation depends on its digital infrastructure such attacks can produce significant material losses.
- Recently documented Denial of Service attacks have been associated with nation state conflicts, and political, religious or ideological disputes.
- Many attacks are performed by malicious individuals for personal gratification. This is especially true of virus/worm attacks which are performed for no material gain but costs hundreds of millions in lost productivity and repair time.

Denial of Service Attacks

- Denial of Service (DoS) attacks may be categorised as hard kill or soft kill, depending on the means used.
- The aim is either temporary or permanent denial of service provided by a facility, be it a network, communications link, computer system, or other information gathering, transmission or processing asset.
- Broadly DoS attacks can be divided into *logical/electronic attacks* (eg hacking, virus, worm, radiofrequency jamming), *direct physical attacks* (eg cutting cables, smashing equipment, bombing sites), *radiofrequency* or *electromagnetic attacks* (eg E-bomb, HERF gun).
- The downtime of the victim asset is determined by the severity of the attack, be it hard kill or soft kill.

Denial of Service Attacks

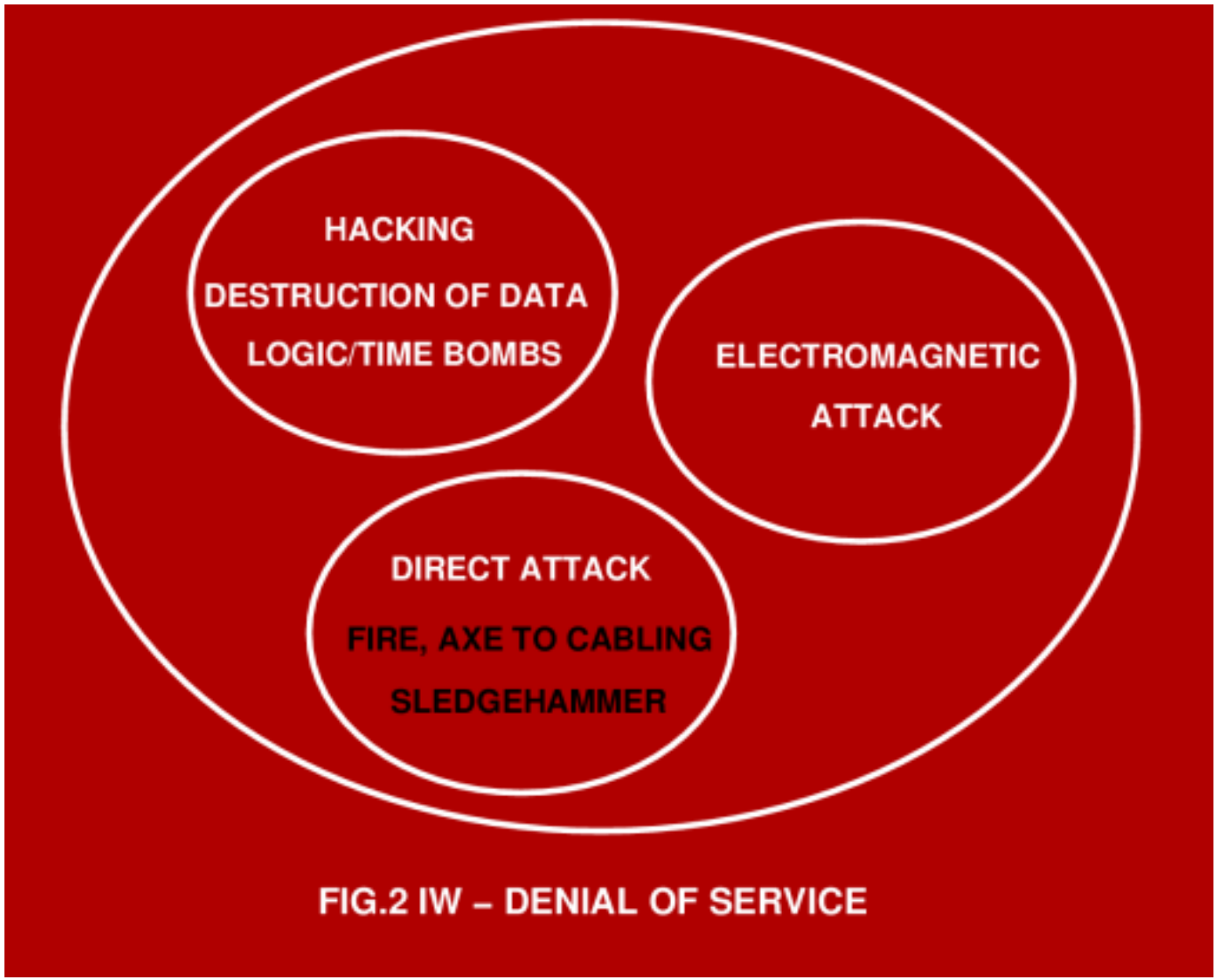


FIG.2 IW – DENIAL OF SERVICE

Logical/Electronic Attacks

- This category of attack is typically in the soft kill category, although some such attacks may require days to recover from.
- Viruses can be used to damage operating system installations and user files.
- Worms can be used to cripple systems, consuming memory, disk and bandwidth.
- Logic bombs and other destructive trojan horse programs can be used to damage operating system installations and user files.
- Radiofrequency jammers can be used to cripple voice, digital communications and networks.
- Such attacks can be launched globally due to the vast footprint of the Internet and communications network.

Direct Physical Attacks

- Such attacks are typically hard kill attacks, intended to destroy specific pieces of equipment or cables.
- Example – putting a fire axe, blowtorch or sledgehammers to bundles of cables – be they for data or mains power supply.
- Example – attacking a computer system with an axe or sledgehammer.
- Example – sending a suicide bomber or truck bomber against a telephone switch, computer centre or television studio.
- Example – dropping a smart bomb on a telephone switch or satellite uplink (Baghdad 2003).
- The attacker must be in direct contact with the victim system/target.

Radio Frequency Denial of Service Attacks

- Jamming of radio frequency communications channels has been practiced for almost a century, usually in wartime. During the Cold War the Soviets continuously jammed Western radio broadcasts.
- Jamming involves transmitting a signal which interferes with the modulation used by the signal, degrading intelligibility. A wide range of jamming techniques exist against all known modulation types.
- Designers of military communications equipment plan from the outset to deal with jamming. This is generally not true of commercial equipment which usually has very poor jam resistance.
- Jamming equipment to disrupt mobile phones (GSM, CDMA etc) is now widely available and is built to prevent terrorists from using mobile phones to set off bombs remotely.
- Wireless 802.11 networks are highly susceptible to jamming due to the use of short Barker code modulations.
- Denial of Service attacks against mobile phones or wireless networks can be effected quite cheaply using ‘throwaway’ expendable jammers and can be very difficult to prove.

Electrical Denial of Service Attacks

- The dependency of computer and digital communications equipment upon electrical power feeds and electrical data cables makes it vulnerable to electrical denial of service attacks.
- Such attacks aim to inject high voltage or radio frequency signals into mains power or data cables to cause electrical damage or computer crashes and loss of service.
- **Example A:** a Tazer device with a cable harness and connector allowing it to inject high voltage into a local area network via a wall socket can destroy network adaptors in dozens of computers.
- **Example B:** a shortwave radio transmitter connected to mains voltage power can destroy power supplies in computer or communications equipment.
- The best defence is to deny access to electrical power and data cables to ensure an attacker cannot connect his equipment.
- Proving such an attack can be difficult.

Radio Frequency Weapons – Denial of Service

- Denial of service can also be effected by radio frequency (RF) weapons which emit enough RF power to damage or disrupt the function of computing and communications equipment.
- RF radiation can couple into mains and data cabling, or cooling apertures on equipment, causing equipment to crash or fail permanently with electrical damage.
- *HERF guns* are portable devices which emits pulsed or continuous wave RF radiation.
- *Tesla coils* can be used to emit high voltage RF fields with similar effects to HERF guns. A hidden battery powered Tesla coil can cripple equipment inside buildings for as long as the battery lasts.
- Radio frequency weapons were claimed to have been used during the 1990s for criminal extortion against at least one bank. To date there are no confirmed reports of E-bombs being used in combat operations, despite ongoing speculation.
- The best defensive measure is electromagnetic hardening of computer and communications equipment – the electrical equivalent of armour plating.

Electromagnetic Weapons

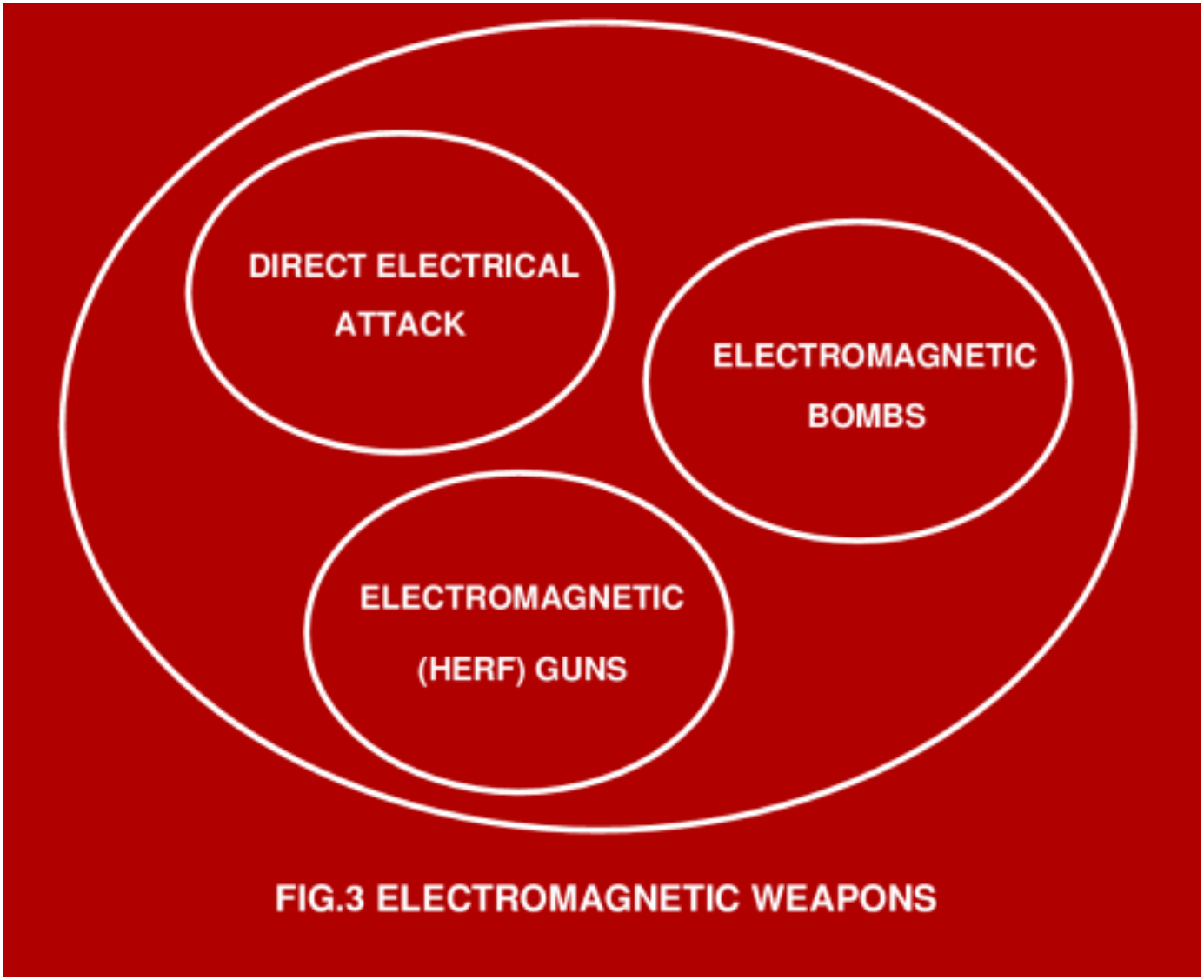


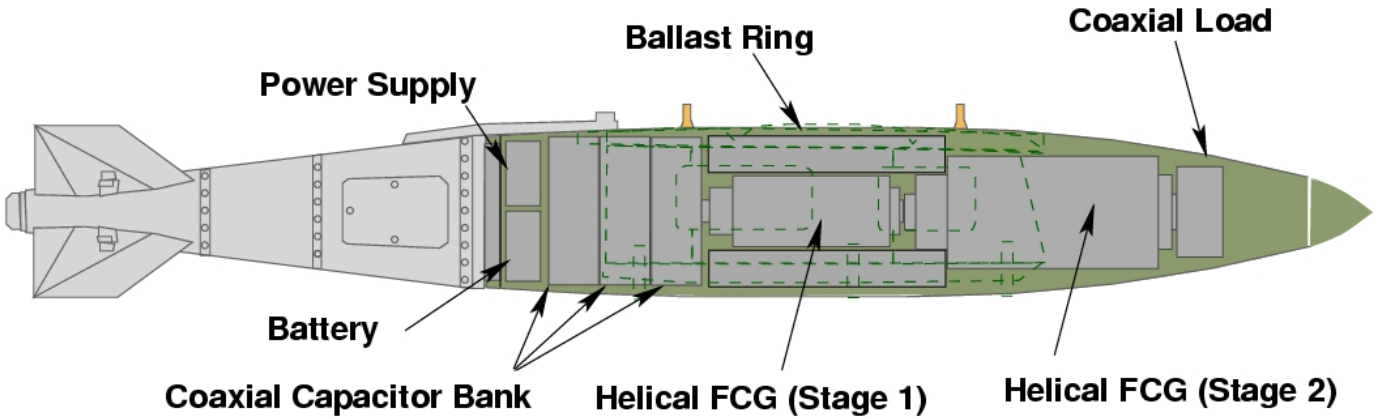
FIG.3 ELECTROMAGNETIC WEAPONS

Electromagnetic Bombs

- Nuclear EMP weapons – nuclear bombs initiated at very high altitude can blanket footprints of almost continental size.
- *Electromagnetic bombs* (E-bombs) can produce damage over areas the size of city blocks, or greater. E-bombs remain in development for military applications. Two categories exist:

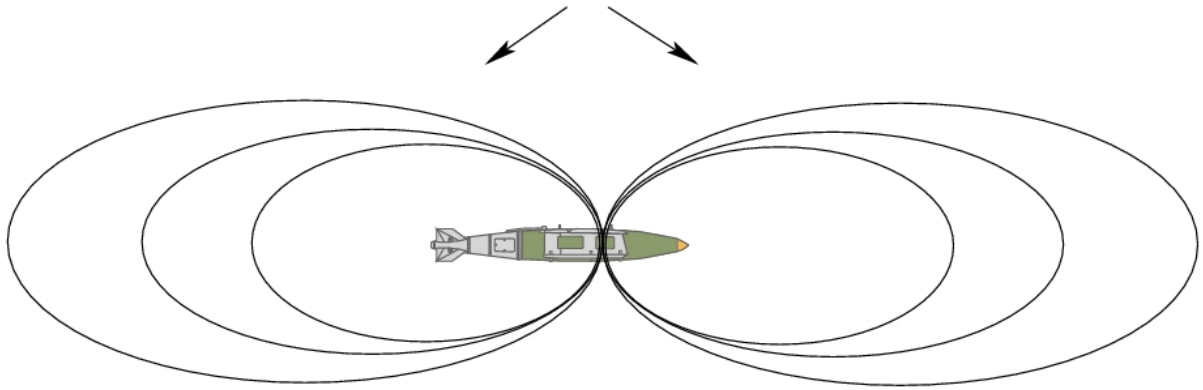
1. Flux generator bombs – produce localised fields similar to lightning strikes.
2. Microwave bombs – produce microwave radiation fields of high intensity over footprints of hundreds of metres diameter.

E-bombs – Low Frequency



LOW FREQUENCY E–BOMB – GENERAL ARRANGMENT MK.84 PACKAGING

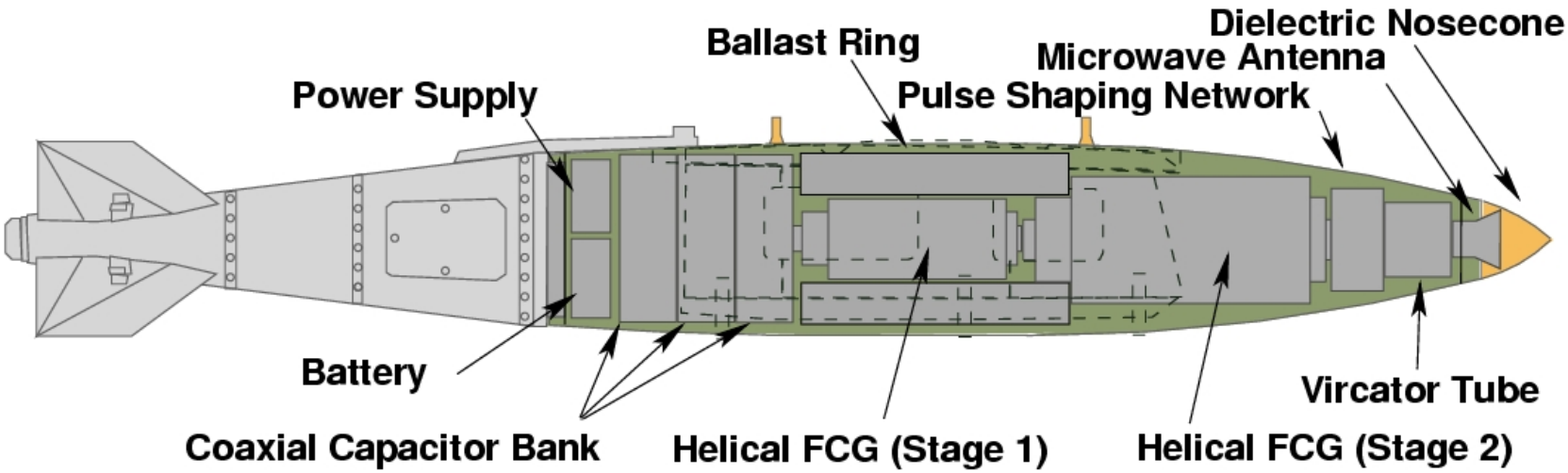
FCG Winding Near Field Pattern Lobes



(C) 1996 Carlo Kopp

LOW FREQUENCY E–BOMB WARHEAD (MK.84 FORM FACTOR)

E-bombs - Microwave



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)

Modelling Information Conflict

Systematic Modelling

- The best strategy is to follow a systematic approach.
- The first step is always the gathering of data to provide as complete a picture of the situation as is possible.
- The second step is to identify specific strategies, usually at the canonical level, since these are more readily identified.
- The second step is to identify players – attackers and victims.
- The third step is to identify the structure of compound strategies.
- Determining the aim of a complex compound strategy can often be quite difficult.

Validation Of Models

- Two basic scenarios for validating a model:
  1. **Validating a model of a strategy *in progress*.**
  2. **Validating *a posteriori* a past strategy.**
- The first case is usually much more difficult due to incompleteness of data and intentional efforts to conceal the nature of the strategy by the attacker.
- If intelligence information is available to penetrate defences, then analysis of strategies *in progress* is much simplified.
- Strategies in which information is hidden completely will always present analytical difficulties both *a priori* or *in progress*. This is the essence of *strategic surprise*, as defined in the hypergame framework.
- Without evidence to prove that a deception strategy is underway, it is not feasible to perform analysis.

Validation vs Uncertainty

- With poor data, the evolving strategy under analysis is uncertain.
- Effectively, analysis will require the definition of several alternative models for the compound strategy, all sharing those features which existing data can logically support.
- As the strategy evolves further, alternatives will collapse as actions by the player contradict the respective alternative models.
- The analyst therefore produces a tree structured graph identifying possibilities, and the graph is progressively pruned as incoming data causes specific branches of the tree to collapse.

Tutorial

- Q & A
- E-bomb Paper