

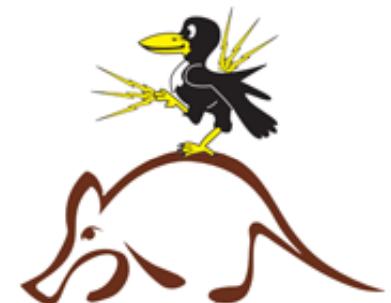


SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY



Future Roles of EW in IW

Brett van Niekerk
Prof. Manoj Maharaj



Information Systems and EW

- ❖ EW equipment = information systems.
 - ELINT/SIGINT/COMINT provide information for analysis & decision making.
 - Identify contacts by EM characteristics.

- ❖ Spectrum Control.
 - Restricted frequency list database
 - SPECTRUM XXI
 - Global EM Spectrum Information System (GEMSIS)

Agenda

- ❖ Information Warfare & EW
 - Definitions
 - Functional Areas
- ❖ Trends in Conflicts
- ❖ Future Roles of EW in the IW Spectrum
- ❖ Conclusion

Information Warfare & Electronic Warfare

Definitions

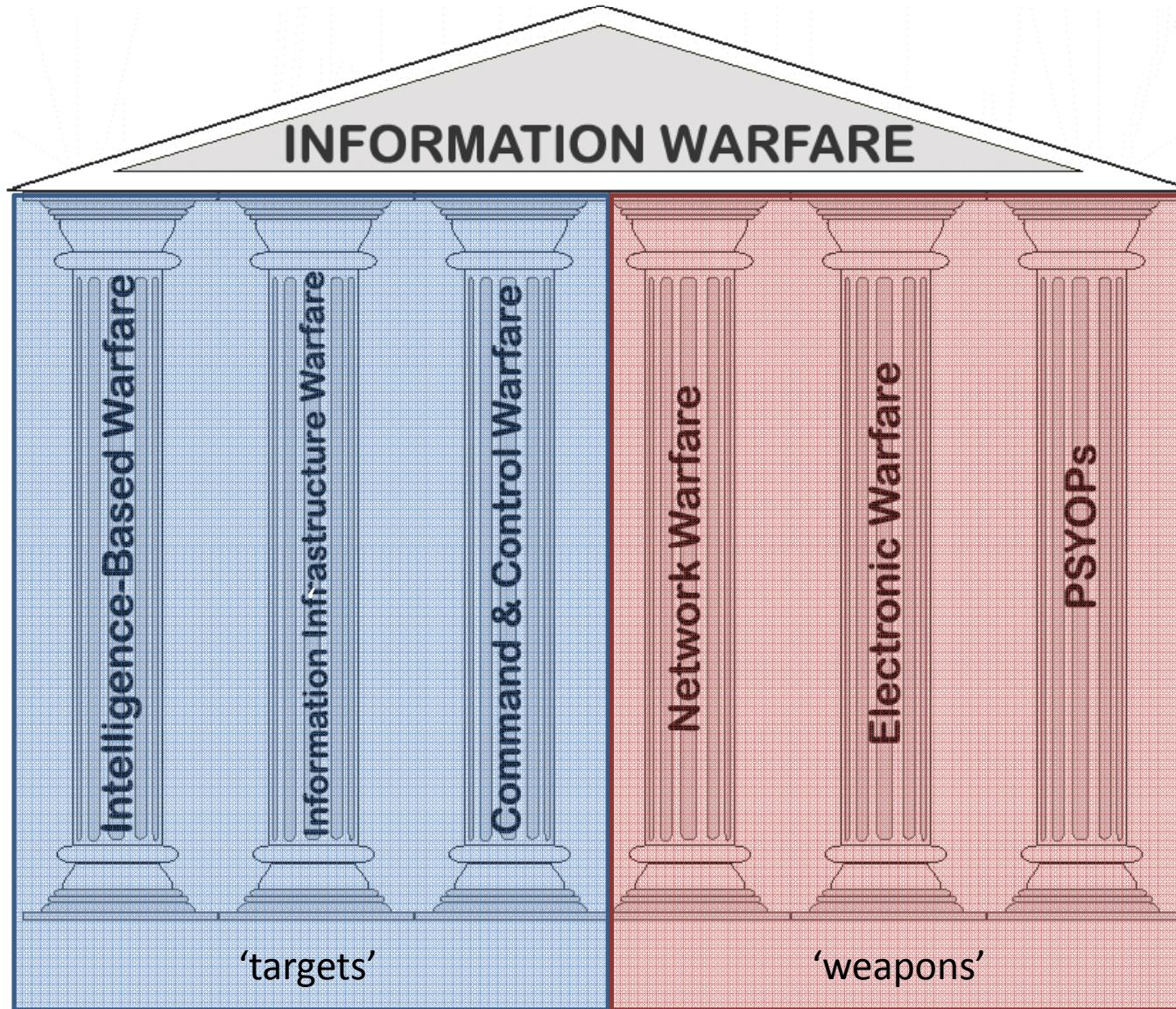
❖ Information Warfare

- Attack/defend information, information-based processes and systems.
- Physical, information & cognitive domains.

❖ Electronic Warfare

- Prevent enemy use of EM spectrum.
- Preserve EM spectrum for own use.
- Traditionally based on RF ECM & ECCM.

IW Functional Areas



Relationships of Pillars

- ❖ Is EW and IW the same thing?
- ❖ Does EW + NW = Cyberwar?
- ❖ Answer: **NO.** Why?
 - IW is much broader – EW is a ‘subset’.
 - EW exists in EM spectrum.
 - NW exists in networks/cyberspace.
 - Very small overlap.

Relationships of Pillars

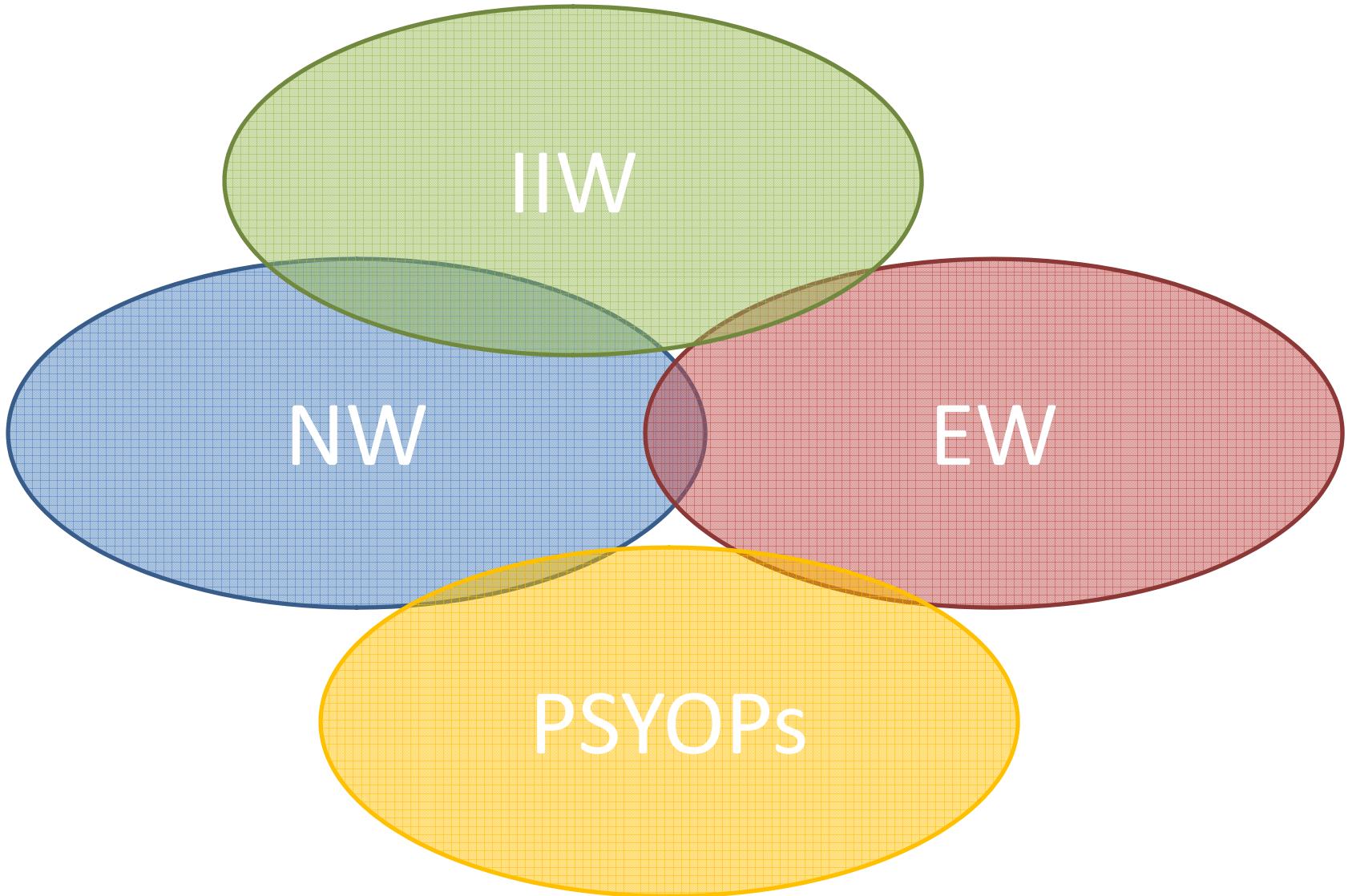
| Analogies Between EW and CNW | | |
|-------------------------------|---|--|
| Tactic | EW | NW |
| <i>Denial of Medium</i> | Jamming | Denial-of-Service (DOS) Attack |
| <i>Decoys/Deception</i> | Chaff / Flare Dispensers | Honey Pots & Honey Nets |
| <i>Identification</i> | Identification Friend or Foe (IFF) | Public Key Infrastructure & Firewalls |
| <i>Concealment</i> | Low-Observability Platforms | Virtual Private Network, Root-kits |
| <i>Threat Warning</i> | Radar Warning Receiver | Firewalls & Intrusion Detection System |
| <i>Intelligence Gathering</i> | Electronic Intelligence (ELINT) | Sniffers, Scanners & Backdoors |
| <i>Support</i> | Radar, Electronic Support System, Spectrum Management | Intrusion Detection Systems, Firewalls, Bandwidth Management |

Adapted from Smith & Knight (2005)

Relationships of Pillars

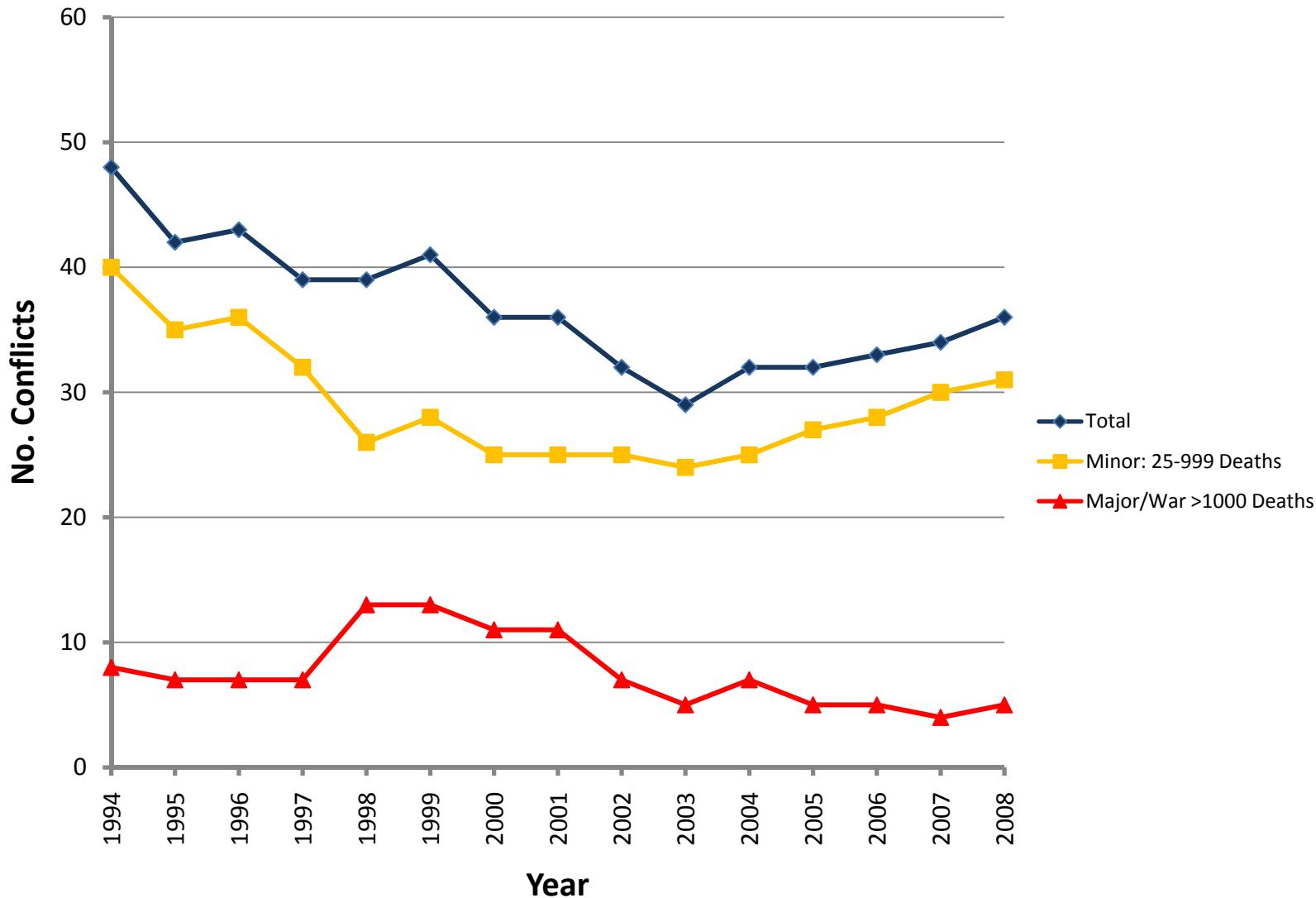
- ❖ EW jams PSYOPs broadcast.
- ❖ NW ‘hacks’ into air-defence system.
- ❖ EW jams wireless network.
- ❖ NW disrupts power grid.
- ❖ NW distributes PSYOP messages on WWW.

Relationships of Pillars



Trends in Conflicts

Number of Armed Conflicts



Source: UCDP/PRIO Armed Conflict Dataset Version 4-2009; Gleditsch et al. (2002)

Example Conflicts

- ❖ Somalia (1993)
 - Use of cell phones & cheap two-way radios for C2 & intelligence; still used by pirates.
 - Use of civilian media (PSYOPs).

- ❖ Rwanda (1994), DRC (1997) & Sudan (2003)
 - Use of radio broadcasts to incite genocide.
 - ‘Low-tech’ implementation (machetes, AK-47s).
 - Peace-keeping missions.

Example Conflicts

❖ Ethiopia-Eritrea (1998-2000)

- Use of advanced & modern equipment.
- Large scale force-on-force.

❖ Kosovo (1999)

- ‘Virtual War’.
- Use of media & targeting of broadcast stations.
- Infrastructure war.

Example Conflicts

- ❖ Afghanistan & Iraq (2001-present)
 - Initial conventional war & ‘media war’.
 - Moved to asymmetric ‘low-tech’.
 - IEDs using cell phones / radio detonation.
- ❖ Israel
 - Asymmetric, continuous low-key cyber attacks.
 - Reports of Israel ‘hacking’ into cell phones & media stations for PSYOPs broadcasts.

Example Conflicts

- ❖ Georgia (2008)
 - Advanced equipment, force-on-force.
 - Cyber-attacks.
- ❖ Estonia (2007) & Korea (2009)
 - Cyber-attacks.
- ❖ South African Urban Terrorism (1998-2000)
 - IEDs using cell phones / radio detonation.
- ❖ Iran (2009)
 - Use of cell phones, internet and media.

Trends in Recent Conflicts

| 'Low-tech' Route | 'High-tech' Route |
|--|--|
| Asymmetric | Force-on-force |
| Make use of available (civilian) equipment. | Deploy modern technology & introduce new technologies. |
| Improvisation with available equipment e.g. IEDs | Convergence of communication technology. |
| Use of civilian media. | Use of civilian media. |
| Possibility of cyber-war & hacking. | Cyber-war & hacking. |

Future Reasons for Conflict

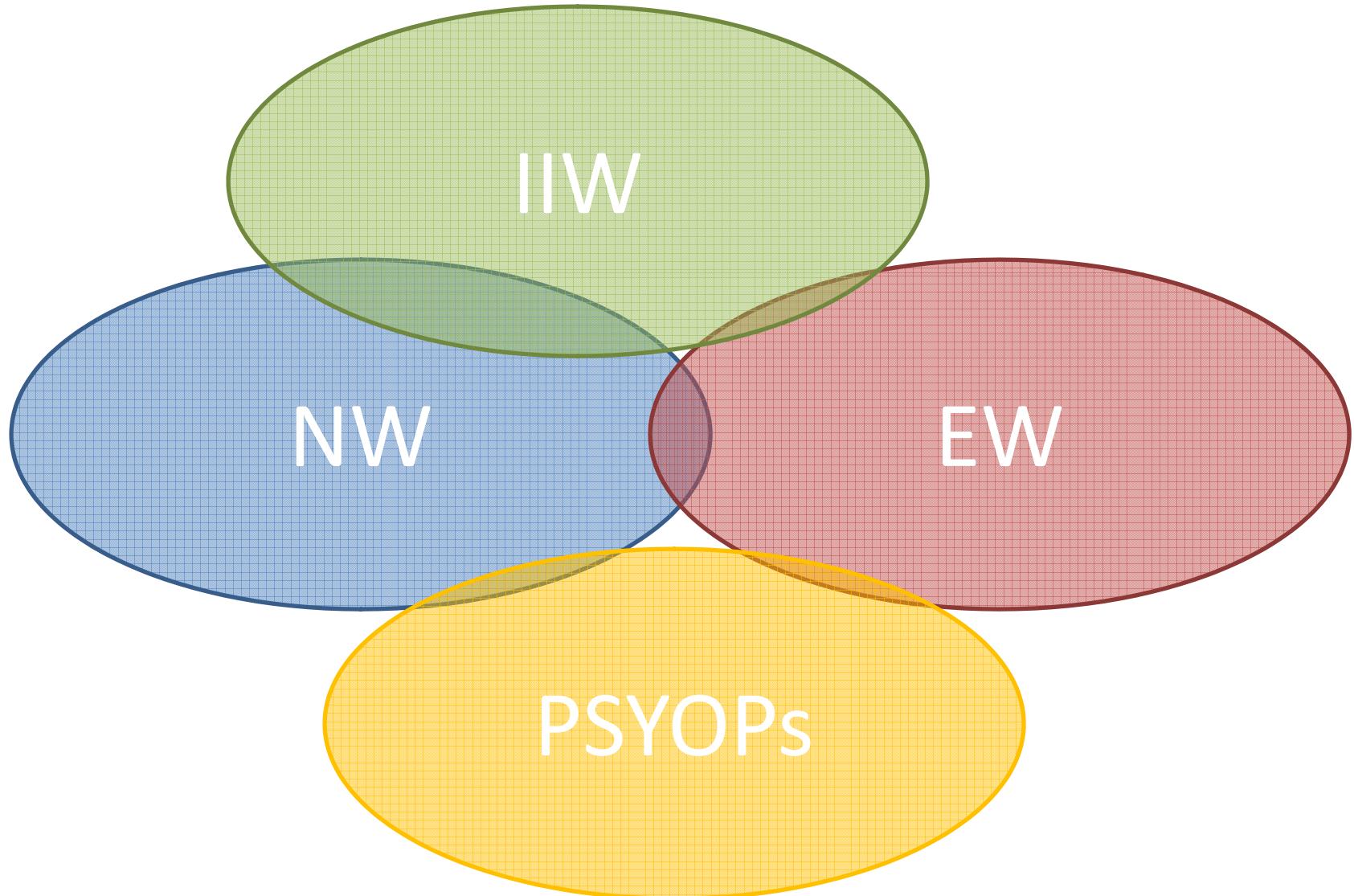
- ❖ Ideological & Political.
- ❖ Resources.
- ❖ Economic?
- ❖ Environmental?

Future Role of EW in IW

Areas Affecting EW Mission

- ❖ Use of civilian wireless communications technologies and media broadcasters.
- ❖ Target & threat identification.
- ❖ Conflict may incorporate both/either ‘low-tech’ and ‘high-tech’ solutions.
- ❖ Convergence of ICT.

Convergence of Pillars



Future Role of EW in IW

❖ Target civilian systems

- Cell phones (C2W, IBW & IEDs)
- Media broadcasters (PSYOPs)
- Wireless networks (NW, IIW, C2W, IBW)
- ‘Low-tech’ radios (C2W, IBW & IEDs)

❖ Target military systems

- Radar & EW (C2W, IIW, IBW)
- Communications (C2W, IIW, IBW)
- Threat warning, countermeasures.

Considerations

❖ Ethical:

- When is it OK to target civilian systems?
- How broadly should systems be targeted?

❖ Technical:

- Crowded EM spectrum → electronic fratricide
- Precision EW
- Capability for both ‘low-tech’ and ‘high-tech’

Considerations

❖ Interoperability:

- Mutual support of IW Pillars
- Fratricide → effective management & C2
- Support security services

❖ Deception Operations & OPSEC?

- Use mobile threat simulators as decoy air defence system.
- Direct EW emissions to mask communications.

New and Future EW Technology

❖ IED jammers

- \$3 Billion funding (2006)
- Upgraded EC-130

❖ UAV EW systems

- Fury / Thunderstorm EA system.
- Israeli drone platforms?

❖ Directed Energy Weapons

Conclusion

Conclusion

- ❖ EW is not independent of other IW areas.
- ❖ Increasing use of civilian infrastructures and convergence of ICTs.
- ❖ EW technologies may need to adapt or evolve to incorporate the new threats.
- ❖ EW may need to become more involved in other areas of IW.

Thank You. Questions?

Brett van Niekerk

+27 (0)31 260 8521

991160530@ukzn.ac.za

brettvn@gmail.com

Prof. Manoj Maharaj

+27 (0)31 260 8023

maharajms@ukzn.ac.za

