


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 (GEMSI)

Before we start, a brief over view of IS & EW. IS&T doesn't usually deal with electronic warfare; however they do deal with information security; which is related to information warfare, and therefore EW.

One can argue that many EW systems are information systems; they comprise of hardware, software/firmware, and persware(operators), just like information systems. Intelligence gathering systems provide information to aid analysis and decisions; and to identify contacts/signals by their EM characteristics means there is some form of information storage.

Information systems can provide spectrum control – there can be databases for the restricted frequencies, or provide higher degrees of spectrum control, such as the Spectrum XXI system and the newer GEMSI, which can scan the EM spectrum in real-time, and allocate available frequencies.

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.

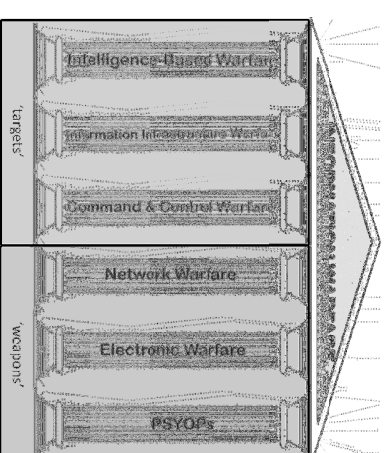
❖ Electronic Warfare

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

Information warfare can be defined to activities that attack or defend information, information-based processes and information systems in the physical, information and cognitive domains.

Electronic warfare is denying the enemy use of the EM spectrum and preserving it for one's own use. Traditionally based on RF electronic countermeasures and counter-counter measures.

IW Functional Areas



Intelligence Based Warfare (IBW) – maximise intel gathering, assessment & dissemination processes & degrade those of the adversary.

Information Infrastructure Warfare (IIW) – protect one's infrastructure while exploiting and attacking the enemy's.

Command & Control Warfare (C2W) – effectively command and control ones forces, whilst hindering the oppositions abilities.

Network Warfare (NW) – attacks the enemy's information networks whilst protecting one's own.

Electronic Warfare (EW) – already been discussed.

Psychological Operations (PSYOPS) – aims to alter perception and ultimately behaviour of an audience to favour one's objectives, and counter similar operations by the enemy.

[click] The grouping of NW, EW+PSYOPS can be seen as weapons, which are used to create 'effects' i.e. attack, the grouping of IBW, IIW, C2W. Will focus mainly on EW, NW, and IIW.

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.

Often there is confusion about the different terminologies – some think that Electronic Warfare and Information Warfare are the same thing, or that the combination of Network Warfare and Electronic Warfare is cyberwar;
[click] this is not the case.

[click] IW is a much broader discipline, and as it also covers the cognitive domain, it is not limited to operations based on electronic equipment; as such EW is only a subset of IW. EW mission area exists in the EM Spectrum, whereas NW exists in the information networks & cyberspace. There is an overlap between these domains, however it is small, so that cyberspace cannot incorporate the EW mission area and vice versa.

Relationships of Pillars

| Analogies Between EW and CNW | | | |
|----------------------------------|------------------------------------|---|--|
| Tactic | EW | | NW |
| Denial of Medium | Jamming | | Denial-of-Service (DOS) Attack |
| Decoys/Deception | Chaff / Flare Dispensers | | Honey Pots & Honey Nets |
| Identification | Identification Friend or Foe (IFF) | | Public Key Infrastructure & Firewalls |
| Constrainment | Low-Observable Platforms | | Virtual Private Network, Root-kits |
| Threat Warning | Radar Warning Receiver | | Firewalls & Intrusion Detection System |
| Intelligence Gathering | Electronic Intelligence (ELINT) | | Sniffers, Scanners & Backdoors |
| | Support | Radar, Electronic Support System, Spectrum Management | Intrusion Detection Systems, Firewalls, Bandwidth Management |
| — Cyberwar is neither EW, nor NW | | | |

There are also similarities in concepts between some pillars – the example here is the parallel tactics in EW and NW, and some of these tactics may apply to, or affect, Infrastructure Warfare, Command and Control Warfare or Intelligence-Based Warfare.

From top to bottom: deny that information gathering or disseminating medium by jamming/DOS attack – which will consequently affect the enemy's infrastructure and intelligence/command abilities.
Decoys and Deception, will provide false or conflicting information to hinder the decision cycle.
Provide identification methods, conceal your presence, warn of enemy threats, gather intelligence, and support provide support to these and other operations.

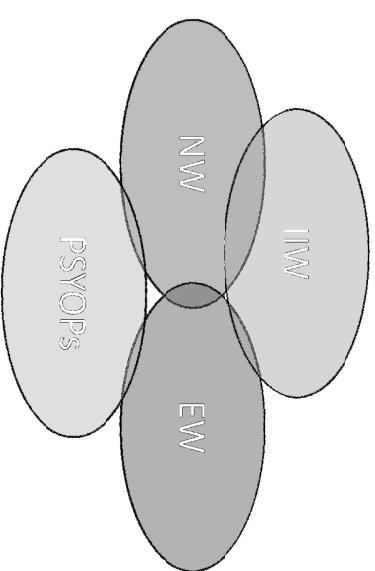
Relationships of Pillars

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

Other examples of a pillar creating an affect in another's domain can be:

[Read from slide]

Relationships of Pillars



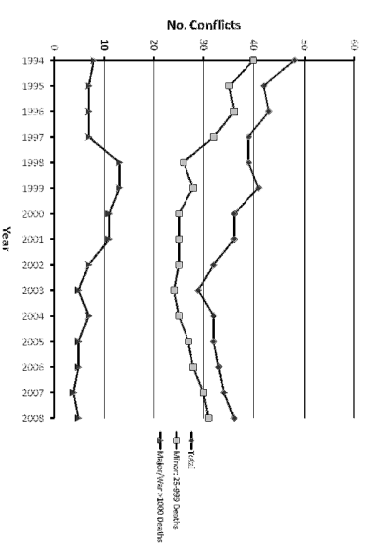
As there are parallels in tactics, and pillars can create affects in the domains of the other functional areas; therefore there are overlaps in the various mission areas. This may result in additional equipment design considerations, the need for equipment with new or extended capabilities (such as the IED jammers in Iraq and Afghanistan).

These overlaps may also alter the way conflicts are conducted; they may introduce new variables, or modify and expand existing ones. This will then in turn require more adaptations to changes in equipment to meet the new requirements.

Trends in Conflicts

To assess the possibilities for the future roles of EW, we first need to attempt to predict the changes in conflict that may occur. By looking at the use of technology in conflicts over the last 15 years, it may be possible to extrapolate trends to the future.

Number of Armed Conflicts



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

The graph shows the number of armed conflicts in the last 15 years; there was a general decrease until 2003, recently the trend has changed and has shown an increase. The number of wars (defined by the number of casualties exceeding 1000 in a calendar year) has remained stable, yet the number of minor conflict is increasing.

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.

There was a predominate (and effective) use of cell-phones and cheap 2-way radios that were used for intelligence and C2 purposes. This presented a problem to the US forces as their sophisticated equipment was not designed/capable of dealing with the 'low-tech' of the Somalis. There was also an effective use of the media; the bodies of US servicemen were dragged in front of the CNN cameras – these images sent shockwaves and effectively resulted in the US withdrawal from Somalia.

The genocides and related civil wars in Africa usually have a 'low-tech' implementation; again civilian media broadcasts were used, this time to instigate the violence and disseminate hate messages.

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.

When tensions escalated to conflict, Ethiopia and Eritrea surprisingly fielded advanced modern equipment, mainly Eastern-block equipment, in large scale force-on-force conflicts. This illustrates the unpredictability of conflicts – these are two of the poorer nations, yet they deployed some of the most advanced equipment on the continent.

Kosovo has been described as a virtual war; the majority of the conflict was aerial bombardment by the NATO forces, using modern targeting, communications and C2 systems. The media played a huge role; this was one of the first true 'media wars'. Low-scale cyberattacks (web defacements by supporters) also made their appearance. This was also an infrastructure war; bridges and transport routes were attacked, broadcasting infrastructure was attacked to limit propaganda, and the power infrastructure was attacked with specialised weapons to create 'temporary' outages.

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.

Both Afghanistan and Iraq campaigns started as high-tech conventional wars, with increased media involvement through embedded journalists, and the propaganda of the Taliban & Iraqi regimes. After the regimes were toppled, the conflict continued, where 'resistance' movements attack the occupying forces conducting stability operations, using asymmetric/terrorist-like tactics. The most effective weapon employed through the entire conflict in the region is the IED – many of which are detonated using radio-controlled devices, and in particular, cell phones.

The conflicts between Israel and the surrounding nations, has been generally asymmetric, with raids and terrorist tactics being used, and the occasional force-on-force conflict. More recently, the antagonism has moved to the internet, where hackers on both sides of the conflict use low scale web-defacements. This is reported to have been taken a step further, with the Israelis hacking into cell phones and media to broadcast PSYOPs messages. This further illustrates that civilian infrastructure may be utilised in conflicts.

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.

The Russian incursion into Georgia was conventional warfare, but this is the first time that in coincided with strong cyber-attacks that effectively hindered communication with the outside world, limiting the flow of information to Russian sources for the initial stages of the conflict.

In 2007 the Estonians faced continuous cyber attacks for weeks after angered the Russians by moving a war memorial. The primary targets were financial and government. In 2009, a series of cyber-attacks were directed at South Korean and US government websites, financial institutions and other commercial ventures. These were not of the scale as seen in Estonia, only lasting for a couple of days, yet the attacks seemed to originate from 16 countries.

A series of bombs rocked Cape Town from 1998, a number of these were remotely detonated, some using cell phones. These are the same concepts as the IEDs being currently used in Iraq & Afghanistan.

The post-election demonstrations in Iraq resulted in a media-blackout by the authorities, however information was still available through the internet where cell-phone images and videos were uploaded. Certain websites were eventually blocked to curb this, yet messages were still available through Twitter. This further illustrates the role that civilian infrastructure may play in providing and disseminating information in a conflict.

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. |

From these examples, there are two main technological routes conflicts take; The low-tech route exhibits asymmetric warfare, improvisation with available equipment, which is usually based on civilian infrastructure, and there is a possibility of low-key cyber warfare.

The High tech route exhibits more conventional warfare with modern/advanced equipment, where new technologies are introduced and deployed. Here there is a definite convergence of ICT technology – particularly with cell-phones and the internet, and massive cyber-attacks.

However both are exhibiting use of civilian media and infrastructure.

[Click] Conflicts may transition between the two routes; in Africa (and Kosovo) many conflicts were initially internal ethnic/political problems – some of these transition when international peace-keepers get involved. In Iraq & Afghanistan the conflict transitioned from force-on-force to asymmetric during the 'stability operations'. Conflicts may contain characteristics of both, yet one route tends to dominate.

Future Reasons for Conflict

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

Conflicts may arise for a number of reasons; the most recent tend to be ideological/political reasons, which can include ethnic clashes. These do not necessarily require physical hostilities, and may be limited to electronic/virtual methods.

They may also arise in an attempt to control natural resources, such as diamonds, gold, oil and other strategic materials; this would need an occupying force, and could therefore exhibit force-on-force clashes.

In the future, as information is becoming a strategic resource and the financial sector is based on information and 'virtual' money, conflict may arise over economic reasons – in the examples the some cyber attacks tended to focus on banking infrastructure.

Concentrated attacks on the banking infrastructure may result in further hostilities. Another possibility is environmental issues; environmental extremists may use cyber-attacks on corporations/nations they perceive are damaging the environment; or as a radio advert suggests, conflict may arise to control fresh water if pollution reaches high levels.

Future Role of EW in IW

Areas Affecting EW Mission

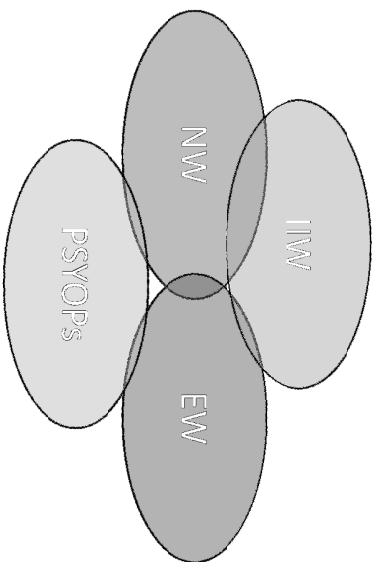
- ❖ Use of civilian wireless communications technologies and media broadcasters.
- ❖ Target & threat identification.
- ❖ Conflict may incorporate both/either 'low-tech' and 'high-tech' solutions.
- ❖ Convergence of ICT.

A major area affecting EW mission is the increasing use of civilian technology – specialised IED jammers have been designed and deployed to combat this threat. Civilian media infrastructure has been targeted due to propaganda – EW may also play a role here, jamming broadcasts instead of the physical destruction of the infrastructure.

The asymmetric style of warfare, and use of civilian ICT raises the problem of threat identification and targeting: which signal is actually a threat or just an innocent phone call? If conflicts incorporate both high-tech and low-tech solutions, EW may not be capable for handling both, such as in Somalia where the SIGINT/COMINT equipment could not intercept the signals from the cheap two-way radios.

An issue that will need to be addressed is the convergence of ICT – switch phone networks use computers, and carry internet traffic. Cellphones are connected to both the internet and PSTN, and have associated mobile data services. WLAN and Bluetooth also provide data transfer over wireless channels. Media services can use both traditional broadcasting, but also online-streaming, and again are reliant on computers, networks and wireless communications.

Convergence of Pillars



Due to the convergence of technology, the previous distinctions of media, telecommunications and computer networks are becoming blurred. This results in a blurring of the distinctions between the pillars of IW; [click] as a result there is increasing overlaps and opportunities to create effects in each other's domain; resulting in increased overlaps.

Fibre optics can be used to illustrate this blurring; in utilises light, which is in the EM spectrum, and consequently any actions against fibre optics could be considered as EW – yet it is generally not catered for in the EW mission area. However fibre is primarily used for networking and communications, and forms the backbone of infrastructure – so this also falls into NW and IIRW.

Future Role of EW in IW

- ❖ Target civilian systems
 - Cell phones (C2W, IBW & IEDs)
 - Media broadcasters (PSYOPS)
 - Wireless networks (NW, IIRW, C2W, IBW)
 - 'Low-tech' radios (C2W, IBW & IEDs)
- ❖ Target military systems
 - Radar & EW (C2W, IIRW, IBW)
 - Communications (C2W, IIRW, IBW)
 - Threat warning, countermeasures.

The future roles of EW may include targeting civilian systems, such as cell phones used for command&control/IED detonators, media outlets broadcasting PSYOPS/propaganda, wireless data networks and low-tech radios that may be used for improvised command and control.

This will be in addition to the traditional military targets such as radar, communications, other EW systems and threat warning and 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'

Due to the changing nature of conflict there are a number of considerations that should be taken into account when designing new systems or planning missions.

If civilian systems are being employed – this raises a number of ethical issues: when is it ok to target civilian systems? Using EW may be preferable as the effects are temporary – physical destruction as used in Kosovo is far more lasting. If these systems are to be targeted, how broadly is this going to be done? An entire area could be subjected to jamming, or broadcasts could be monitored and only certain content could be jammed.

Technically, the EM spectrum is becoming crowded with the increase in wireless technology and the number of users. This crowding can result in electronic fratricide, where jamming and communications frequencies interfere with each other. This may call for 'precision' EW, where the jamming power is more efficiently used in smaller bandwidths.

Due to the simpler radios being employed, EW systems may require broader technical capabilities to deal with both the 'low-tech' and 'high-tech' systems.

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.

As the pillars and technology are converging, EW may be called to support, or be supported by, the other EW pillars. However, EW may have a negative effect on interoperability, due to fratricide, where incompatibilities or poor co-ordination may further hinder communications or command and control.

EW may also need to support security services; cell phones have been used to 'hack' into bank accounts, and this makes them difficult to track as they are mobile. EW techniques and equipment may be used by security services to triangulate and trace the cell phone that is being used in order to make the arrest.

EW may also aid deception operations or operational security; mobile threat simulators could be used to mimic air defence networks, giving the enemy false locations, or EW emissions can be directed to mask communications and movements, providing operations security. Both of these areas are considered part of IW.

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

According to an article in issue 45 of Joint Forces Quarterly in 2007, \$3 billion spent on funding IED jammer programs in 2006, and over \$300 million spent on procurement 2003-2006. The EC-130 Compass Call EW aircraft also upgraded, allows them to target cell phones and IEDs.

There are unconfirmed reports that the Israeli's are using UAVs to jam communications; however the Fury platform carrying the Thunderstorm communications electronic attack system was successfully tested in US.

Systems such as the Active Denial System (ADS) which uses millimetre energy waves to create burning sensations, or directed microwave pulses to burn circuitry, Airborne Laser and related systems utilise the EM spectrum; however some argue that such systems are not traditional EW as it targets intentional receivers & transmitters (Hoad & Jones, 2004).

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.

EW is not an isolated pillar that is independent of the other functional areas – there are overlaps and parallels in tactics with the others.

There is an increasing use of civilian infrastructures, and the various ICT technologies are converging. This results in the IW pillars converging, and new threats/targets for the EW mission area.

EW technologies may need to adapt/evolve to cater for the new threats, and may need to become more involved in other areas of IW.

Thank You. Questions?

Brett van Niekerk

+27 (0)31 260 8521

bvniekm@ukzn.ac.za

Prof. Manoj Maharaj

+27 (0)31 260 8023

maharajm@ukzn.ac.za



