Conceptual Basis of Future EW

AOC EW Conference
Kuala Lumpur
11 March 2014
Topics

• A very brief history of EW – start of the problem!

• What is EW today and why it really matters tomorrow.

• Transformational concepts:
  – NATO
  – China: Integrated Network EW – New Info War Concept
  – UK Electromagnetic Environment (EME) Review
  – US Army Cyber EM Activity

• I will include several operational vignettes

• Some thoughts on the EME, EW and Cyber

• Regional Opportunities
Afterglow Light Pattern 400,000 yrs.

Dark Ages

Development of Galaxies, Planets, etc.

Dark Energy Accelerated Expansion

Inflation

Quantum Fluctuations

1st Stars about 400 million yrs.

Big Bang Expansion 13.7 billion years
The Evolution of Warfighting Domains

All these domains represent operational use of a particular environment. They are:

- Unique
- Have military application, value & ROE
- Have strengths and weaknesses
- Interdependent
  - Work better together
- Require investment
  - Of intellect and capital
- Subject to law
- Often surprising
- Slow to gain recognition
- May upset vested interests

1200 BC

~3000 BC

Land  Land

Sea  Sea

Air  Air

Land  Land

1910’s

EM  EM  EM

Air  Air  Air

Land  Land  Land

1940’s

EM  EM  EM

Air  Air  Air

Land  Land  Land

1970’s

Space  Space

EM  EM

Air  Air

Land  Land

1990’s

Cyber

Space

EM

Air

Sea

Land

Today
The Evolution of Warfighting Domains

All these domains represent operational use of a particular environment. They are:

- Unique
- Have military application, value & ROE
- Have strengths and weaknesses
- Interdependent
  - Work better together
- Require investment
  - Of intellect and capital
- Subject to law
- Often surprising
- Slow to gain recognition
- May upset vested interests

<table>
<thead>
<tr>
<th>Time</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1200 BC</td>
<td>Land</td>
</tr>
<tr>
<td>~3000 BC</td>
<td>Sea</td>
</tr>
<tr>
<td></td>
<td>Land</td>
</tr>
<tr>
<td>1910's</td>
<td>Air</td>
</tr>
<tr>
<td></td>
<td>EM</td>
</tr>
<tr>
<td>1940's</td>
<td>EM</td>
</tr>
<tr>
<td>1970's</td>
<td>Space</td>
</tr>
<tr>
<td>1990's</td>
<td>Cyber</td>
</tr>
<tr>
<td>Today</td>
<td>Cyber</td>
</tr>
</tbody>
</table>

Op Environment

time
Congested
Contested
Connected
Complex
Constrained
Chaotic?
Electronic Warfare exam question.

Q. How many Lethal EM-based weapons are there? Give examples.
EM Domain – Lethal Weapons (UNCLAS)

Type of weapon or system:
• RF guided eg SA-11, 20,
• IR guided eg SAM 7,14,16,20,
• RF triggered – eg IEDs
• Laser guided
• Laser dazzle
• Directed energy
• Counter comms/command\(^1\)
• Counter navigation\(^1\)
• Counter sensor\(^1\)
• Counter BFT/IFF\(^1\)

• Many 20+ types, 1,000s deployed worldwide
• Very many 20+ types, 100,000s deployed
• Very many 12+ types, incalculable
• Many
• Many freely available, COTS,
• Developing
• Many
• Increasing
• Increasing
• Increasing

\(^1\) A soldier without C2, navigation, blue force tracking or sensors is a very vulnerable soldier
What is Operational EW today?

- Single-service, Joint, Allied, Coalition, deep, near, strategic, tactical, has ROE, lawful, multidimensional, effects-based, etc. – just like all other military activity.
- Electronic Surveillance eg - ESM  ISTAR  SIGINT
- Electronic Defence eg – Force & Platform Protection, C-IED
- Electronic Attack eg – SEAD, Comms & Sensor jamming
- EM Management eg – SM, EWOS, EWCC, SEWOC
  - EM Battlestaff (EMB)
- EW Manoeuvre units – ALL of the Above!
- Highly classified, secretive, difficult, not understood, misunderstood, costly – it doesn’t have to be ANY of these!
View of the EM Battlespace – 1990’s

Civil Comsat/GBS

Military Comsat

Surveillance Satellite

Air Support

Attack Helicopters

Battlefield Radar

UAV

JTDS

Air Defence

Tactical HQ

MLRS

Infantry

Surface Fleet

Submarines

VLF

LF

HF

JFHQ

AFLOAT
“Linking sensors, decision-makers and weapon systems so that information can be translated into synchronized and overwhelming military effect at optimum tempo”
Requirement: Train EW Professionals to plan, coordinate, synchronize and deconflict EW support to Full Spectrum Operations

EW Effects
- Control
- Protect
- Deny
- Deceive
- Disrupt
- Degrade
- Destroy
\[
\frac{\partial}{\partial x} \mathcal{L} = \bar{\psi}(i \gamma^\mu D_\mu - m) \psi - \frac{1}{4} F_{\mu\nu} F^{\mu\nu} = \frac{4\pi}{c} J_k
\]

\[
-\nabla^2 A_k + \frac{1}{c^2} \frac{\partial^2 A_k}{\partial t^2} + \frac{1}{c} \frac{\partial}{\partial x} \left( \frac{\gamma^\mu}{c} F_{\mu\nu} \right)
\]

\[
R = K \alpha \left[ \frac{P_S \cdot G^2 \cdot \lambda^2 \cdot A_z \cdot t_i}{\mathbf{K} \cdot \mathbf{T} \cdot n_R \cdot (4\pi)^3} \sin \left( \frac{2\pi \cdot h_m \cdot \sin \gamma}{\lambda} \right) e^{-0.115 \delta R \cdot R_e} \right]
\]
NATO EW Transformation

- The Electromagnetic Environment (EME) is a real physical war-fighting environment

- It is an operational environment where military operations take place and effects are achieved

- Manoeuvre warfare operations - shaping, managing, exploiting, attack and defence – can take place in all environments, including the EME

- The EME connects within and bridges between the maritime, land, air, space and information environments

- Success in the EME in 21st Century warfare is generally a precursor to success in every environment

- Success in the EME may itself be sufficient to achieve a desired effect or end state but successful use of the EME requires the same investment, leadership and effort as does success in any operational environment, if not more

- Unthinking reliance on the EME or assumed superiority introduces vulnerabilities that will be exposed and exploited in future warfare.
MCM-0142 Military Committee Transformation Concept for Future NATO Electronic Warfare 23 Nov 2007

References
A. IH/OPEN/07/06 –10639, Concepts for Alliance Future Joint Operations (CAFO), 20 Feb 06
B. MC 0064/9 (Final), NATO Electronic Warfare Policy, 26 Apr 04
C. MC 0101/11 (Final), NATO Signals Intelligence Policy and Directive, 13 Dec 05
D. AJP-3E(A), Allied Joint Electronic Warfare Doctrine, Dec 03
E. SHIPLANS/2920-308/507/202484, Development of NATO's Effects-Based Approach to Operations (EBAO) - B-Strategic Command Discussion Paper, 2 Jul 07
F. NSAV/003-C3/4621, STANAG 4621 C3 (Edition 1) - Navigation Warfare Definition, 2 Nov 04
G. AAP-8 (2007), NATO Glossary of Terms and Definitions, 16 Apr 07

PREAMBLE
1. This concept document has been produced by NATO Nations to prepare the transition from traditional EW thought and processes towards NATO's transformation/evolution to Effects-Based Approach to Operations (EBAO). The concept serves as a starting point for definition and development of NATO policy and doctrine for operations in the Electro Magnetic Environment.

INTRODUCTION
2. NATO Transformation and Electronic Warfare (EW). The imperative for NATO to transform was articulated at the Prague Summit Declaration of 2002 and is recognized by the North Atlantic Council (NAC) and Military Committee (MC) as an Alliance priority. It was again endorsed at the Riga Summit in 2006. The B-SC Concepts for Alliance Future Joint Operations (CAFO) was issued on behalf of Supreme Allied Commander Europe (SACEUR) and Supreme Allied Command Transformation (SACT) to Director International Military Staff (DIMS) on 20 Feb 06 (Reference A). CAFO defines the conceptual framework that will inform and shape future development of concepts.
Operational Environments and their domains - Diagram from MCM 0142

Physical Domains:
- Electromagnetic
- Air/Space
- Land
- Maritime

Information*

*Cognitive Domain

*includes Cyberspace

Influence

Activity or Information
NATO EMO/EW Before 2007

- AGS
- C-Sensor
- DEW
- ESM
- ECM
- EPM
- EOD
- SEAD
- CIS
- SM
- SIGINT
- NAVWAR
- Accs
- Timing
- Platform Protection
- Navigation
- Data
- Voice
- Network
- Positioning
- Timing
- Area Protection
- Navigation
- Timing
- Area Protection
- Navigation
- Timing
Purpose:

Friendly EMO:
- Attack adversaries
- Recognize adversaries
- Defend own

Adversary EMO:
- Recognize friendly
- Attack friendly
- Defend own

NATO ELECTROMAGNETIC OPERATIONS (EMO)
ELECTROMAGNETIC OPERATIONS (EMO)

Purpose:

EA - Electronic Attack
ES - Electronic Surveillance
ED - Electronic Defence
NATO EW effects based definitions:

• Electronic Warfare (EW) - military action that exploits EM energy to provide situational awareness and achieve offensive and defensive effects.

• Electronic Surveillance (ES) - use of EM energy to provide situational awareness and intelligence.

• Electronic Defence (ED) - use of EM energy to provide protection and to ensure effective friendly use of the EM spectrum.

• Electronic Attack (EA) - use of EM energy for offensive purposes.

• Source MCM 0142 “Military Committee Concept for Transformation of NATO Electronic Warfare”
Figure 2.2 – EW Operations Relationships

**Electromagnetic Environment**

- Desired Effects
  - Protection
  - Denial
  - Deception
  - Disruption
  - Neutralization
  - Destruction
  - Degradation
  - SSA

- EMO / Capabilities
  - Protection / Platform Protection / CIED / C-RAM Radar / NAVWAR Direct Energy / Etc.

- Action
  - ED
  - EA
  - ES

- Measure
  - ESM
  - ECM
  - EPM

- Task
  - Search
  - Intercept
  - Identify
  - Locate
  - Jamming
  - Deception
  - Neutralize
  - Protect: Active Passive
This concept document has been produced to trigger the transition from *traditional* EW thought and processes towards NATO’s transformation.

The concept serves as a starting point for definition and development of NATO *policy and doctrine* for Electromagnetic Operations (EMO) in the Electromagnetic Environment (EME).
## NATO EW Pubs Summary

<table>
<thead>
<tr>
<th>Publication</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCM 0142-2007</td>
<td>Approved 2007 EW Transformation Concept</td>
</tr>
<tr>
<td>MC 0064/10</td>
<td>Approved 2008 NATO EW Policy</td>
</tr>
<tr>
<td>MC 515/1</td>
<td>Approved 2011 NATO SEWOC Concept</td>
</tr>
<tr>
<td>AJP-3.6(B)</td>
<td>Allied Joint EW Doctrine ratified 2012</td>
</tr>
<tr>
<td>ATP-3.6.2</td>
<td>EW in the Land Battle ratified Nov 13</td>
</tr>
<tr>
<td>ATP-3.6.3</td>
<td>EW in Air Operations ratified Nov 13</td>
</tr>
<tr>
<td>MC-0485/1</td>
<td>SEAD Policy sent to MC Nov 13</td>
</tr>
</tbody>
</table>
The People's Liberation Army (PLA) considers active offence to be the most important requirement for information warfare to destroy or disrupt an adversary's capability to receive and process data. Launched mainly by remote combat and covert methods, the PLA could employ information warfare pre-emptively to gain the initiative in a crisis. Specified information warfare objectives include the targeting and destruction of an enemy's command system, shortening the duration of war, minimizing casualties on both sides, enhancing operational efficiency, reducing effects on domestic populations and gaining support from the international community. The PLA's Information Warfare (IW) practices also reflect investment in electronic countermeasures and defences against electronic attack. The Chinese have adopted a formal IW strategy called “Integrated Network Electronic Warfare” (INEW) that consolidates the offensive mission for both Computer Network Attack (CNA) and Electronic Warfare (EW). China's Computer Network Operations (CNO) include computer network attack, computer network defence, and computer network exploitation. The PLA sees CNO as critical to seize the initiative and achieve “electromagnetic dominance” early in a conflict, and as a force multiplier. Although there is no evidence of a formal Chinese CNO doctrine, PLA theorists have coined the term “Integrated Network Electronic Warfare” to outline the integrated use of electronic warfare, CNO, and limited kinetic strikes against key command and control, communication and computers nodes to disrupt the enemy's battlefield network information systems.

EXECUTIVE SUMMARY
This chapter examines the implications of China’s advances in space, cyber, and electronic warfare technologies.

Main Argument
China’s rapid progress in space, cyber, and electronic warfare technologies holds important implications for Asian security. Chinese military observers and scholars argue that in order to guarantee victory in a modern war, the People’s Liberation Army (PLA) must first achieve superiority in the information domain, preferably by striking first. The PLA thus intends for its space, cyber, and electronic warfare operations both to gain an asymmetric advantage over the U.S. military and to fulfil its mandate under the “new historic missions” rubric in order to protect China’s interests in space and the electromagnetic sphere.

Policy Implications
• Advances in these technologies will improve China’s capabilities to protect its national interests and to project power, not just in Asia but also globally.
• Chinese emphasis on information warfare strikes at the heart of a U.S. military whose superiority is based in large part on networked forces. China’s progress in these areas raises the possibility that U.S. military forces could be delayed or disrupted while the PLA achieves rapid information dominance over a smaller, less advanced military.
• PLA analysts’ tendency to accentuate the positive offensive outcomes of information warfare while ignoring its limitations and unintended consequences may lead Chinese leaders to use the full spectrum of space, cyber, and electronic warfare capabilities.
China next month will stage military exercises using computer-equipped units that combine traditional firepower and electronic warfare capabilities, state media reported Wednesday. The upcoming drills will demonstrate the strides Beijing has made in adopting U.S.-style technological warfare, stoking concerns among the U.S. and its allies about China’s cyber capabilities.

The exercises will be held in late June at the People’s Liberation Army (PLA) Zhurihe training base in north China’s Inner Mongolia Autonomous Region, Beijing's largest military training facility, China’s official Xinhua News Agency reported. They will involve “digitalized units, special operations forces, army aviation and electronic counter forces,” Xinhua said.
Operational Demands

The full spectrum of U.S. military capabilities on land, sea, and air now depend on access, control and awareness of the electromagnetic spectrum.

Chuck Hagel
Secretary of Defense

What we have found in many of the cases to be our competitive advantage on the battlefield is getting as much knowledge to the edge as possible.

Admiral Sandy Winnifeld
Vice Chairman, Joint Chiefs of Staff

We aggressively seek bandwidth capacity to improve the reliability and diversity of our C4 networks. STRATCOM currently utilizes all the available bandwidth to full capacity, but theater and fiber networks are vulnerable to single point failures in the global information grid.

General Bob Kehler
Commander STRATCOM
Acquisition Demands

EW has been used effectively as a critical element of warfare by the US and other nations for the past 50 years. Looking ahead to the future, the unprecedented global spread of highly sophisticated electronics technology will impact EW in many ways. In the coming decades the Department must better understand how it can use advanced EW techniques to its advantage; how potential adversaries might use such techniques against us; and, in both cases, what effectiveness we might expect and what counter-measures might be used to limit such effectiveness.

To ensure spectrum dominance, we must understand the value of EW techniques/capabilities in combination with cyber and kinetic effects at a higher warfighting level, how combinations of techniques may be utilized to advantage or what unintended disadvantageous consequences may occur in a complex multi-system environment that may not be obvious in “one-on-one” examinations.

Control of the air is critical to how the US fights. We need to examine the role of manned and unmanned platforms and integrated concepts that combines various mixes of capabilities networked together. We should also examine the cost effectiveness of alternative systems that provide ISR, EW and weapon functions.

Frank Kendall
OSD/AT&L
10 Oct 2012
Global Technology Demands

Global Forces
- Demographics
- Climate
- Resources (Natural, Talent, Treasure, Time)
- Globalization/Proliferation
- Conflict

Space:
- Congested
- Competitive
- Contested

Cyberspace: threatened by malicious insiders, supply chain attacks, and advanced persistent threats to deceive, degrade, disrupt, destroy

Global Sectors
- Manufacturing and Materials
- Transport and Logistics
- Energy and Utilities
- Health and Pharma
- Communications and IT
- Financial Services
- Education and Training

Command and Control (C2) & Intelligence Surveillance and Reconnaissance (ISR) targeted as a center of gravity threatening integrated and resilient global operations

Air:
- Anti-Access
- Area Denial (A2/AD)

Global Vigilance, Reach and Power dependent upon contested Global Domains and Globalized Industrial Sectors
Operational Domains

Physical – maritime, land, air/space and electromagnetic

Cognitive

Information including Cyberspace
Operational Domains

Physical – maritime, land, air/space and electromagnetic

Particles

Photons

Thoughts

Cognitive

Bits

Information including Cyberspace
Operational experience of Electronic Warfare

Maj Jonny Hill RM
Y Squadron
3 Commando Brigade
Royal Marines
Operational experience of Electronic Warfare

- BACKHAND 71 (USMC PROWLER).
- HERDING EF off VHF repeaters.
- EF forced onto 2 local freqs.
- Deployed RRTs exploit and produce cut.
- UAV FMV leads to GMLRS STRIKE.
Operation Eagle’s Summit

- Deliver $64M Turbine to Kajaki Dam in N Helmand Province—Aug 2008
- British Led Operation (16 Air Assault Bd—TF Helmund)
  - 7 sections of turbine, each weighing 20-30 tons
  - 100 vehicles in convoy, stretching for 4km
  - 50 armored vehicles
  - 3,000 British forces involved
  - 1,000 other Coalition troops
  - 1,000 Afghan soldiers
  - **Expected coalition KIA: 30-40**
  - CFACC sent 1 x EC-130 from OIF to OEF
Planning

• Conventional planning starts 4 months prior
  • Determining route and assessing viability
  • Force structure needed
  • Convoy security
• What about EW/IO?
  • IO shaping started 5 days prior (broadcasts, tribal negotiations)
  • EW—both ES and EA used
    • Counter-comms was a key element
Develop America's Airmen Today... for Tomorrow

ROUTE HARRIET

Gorak Pass

Route 611 (deception route)
End Result

- Turbine successfully delivered

Control of the Electromagnetic Environment is a consistent and vital factor to mission success regardless of theater or threat.

- 0 Friendly KIA on delivery operation
Background

EME Framework

CAP Capability Stocktake

Organisation

Governance

Tasking

Manpower & Training

Future of the EME
EME Review

Outcomes

- **92 Key Points**
  - Pan DLOD, risks, weaknesses, capability gaps & incoherency across ES, EA and ED components of EW

- **49 Recommendations**
  - Some easily rectified
  - Some longer term
  - 2 x quick wins – Tx of DEWC and WHSS under JFC

- **Summary**
  - Lacked EW champion for years
  - No Jt oversight of pan-DLOD issues; ES, EA, ED activities
  - Equip often UOR derived, sS specific and not sustained
  - EW “effects” not considered in the round – lack of whole spectrum planning & operational Comd
  - Various Governance, Tasking, Project lines
EME Review
Next Steps

- Defence Authority for EW – CDI for Comd JFC
- EW Policy set & issued under CDI leadership, consistent with NATO
- EW Joint User established under DCI3 orbat
- C4ISR Functional Model to delegate specific EW responsibilities for
  Develop, Plan, Manage, Deliver, Generate and Operate functions
- Pan-DLOD EW Delivery Programme established – ES, EA, ED
- Jt EW operational planning team established under Comd FJC
- Review of Defence ELINT requirement
- EW Cap audit undertaken in advance of SDSR 15
Regional Opportunities

- If you don’t have one, develop a joint concept for EW and the EM environment/domain as a physical warfighting manoeuvre space.
- Review and Plan across all the lines of development.
- Think across the levels – from state to individual.
- Work with others, consider partnerships.
- Knowledge is the key.
- Do it now.
Outcomes – Choose Again?

- EM/EW Concept fit for 21st century
- Language and doctrine fit for purpose
- Awareness of the character of future conflicts – the C words
- Capability development that works
- Coalition partners
- Evolution
- Advocacy
Churchill Quotes

• “In Critical and baffling situations, it is always best to return to first principle and simple action.”

• “Gentlemen, we’ve run out of money – now we have to think!”
What Happens in an Internet Minute?

- 639,800 GB of global IP data transferred
- 210 million emails sent
- 70 million messages sent
- 20 new victims of identity theft
- 204 million app downloads
- 47,000 in sales
- 40 million photo views
- 20 million photo uploads
- 320 new Twitter accounts
- 100,000 new tweets
- 61,141 hours of music
- 277,000 logins
- 6 million Facebook views
- 2+ million search queries
- 1.3 million video views
- 30 hours of video uploaded
- 6 new Wikipedia articles published
- 135 new mobile users
- 100+ new LinkedIn accounts
- 1,300 new Facebook users
- 6 new botnet infections

And Future Growth is Staggering

- Today, the number of networked devices = the global population
- By 2015, the number of networked devices = 2x the global population
- In 2015, it would take you 5 years to view all video crossing IP networks each second
Many International Local Chapters

Join Us! At www.crows.org
Evolving EW in The ASEAN and Pacific Regions

Conceptual Basis of Future EW

Wing Commander John Clifford OBE
MSc, MBCS, CEng, CITP, RAF (Retd),
President, UK Chapter AOC
Director JMC Defence Ltd
jonclif@aol.com

clifford@crows.org
AOC Director Global Operations
QUESTIONS