EW … the future beyond CEMA?

Ideas and further thoughts

Alan Blackwell

ABAL Insight Ltd

EW ... the future beyond CEMA?

- Until 2000, EW relatively well bounded.
- Since 2000, our understanding and practices have been disruptively shaped by:
  - rapid pace of technological change;
  - new – very different – threats;
  - changing nature of warfare (‘attrition’ to ‘cognition’) and the Information Age.
- This presentation will:
  - reflect on the journey we have taken since 2000;
  - consider the emerging technologies, threats and practices that will shape the future;
  - propose an approach to handling the (near) future;
  - offer further thoughts on issues raised so far.

The 21st century so far ...

- First decade:
  - Iraq experience changed mindset;
  - Distinction between ‘tactical’ and ‘strategic’ blurred;
  - Convergence of ‘EW’ and ‘SIGINT’.

The 21st century so far ...

- First decade:
  - Iraq experience changed mindset;
  - Distinction between ‘tactical’ and ‘strategic’ blurred;
  - Convergence of ‘EW’ and ‘SIGINT’.

The 21st century so far ...

- First decade:
  - Iraq experience changed mindset;
  - Distinction between ‘tactical’ and ‘strategic’ blurred;
  - Convergence of ‘EW’ and ‘SIGINT’.

- Second decade:
  - Lessons from Afghanistan;
  - Democratisation of technology and the rise of cyber;
  - Resurgent peer adversaries.

The 21st century so far ...

First decade:

- Iraq experience changed mindset;
- Distinction between ‘tactical’ and ‘strategic’ blurred;
- Convergence of ‘EW’ and ‘SIGINT’.

SSB

Second decade:

- Lessons from Afghanistan;
- Democratisation of technology and the rise of cyber;
- Resurgent peer adversaries.

CEMA

CEWO

The 21st century so far ...

- First decade:
  - Iraq experience changed mindset;
  - Distinction between ‘tactical’ and ‘strategic’ blurred;
  - Convergence of ‘EW’ and ‘SIGINT’.

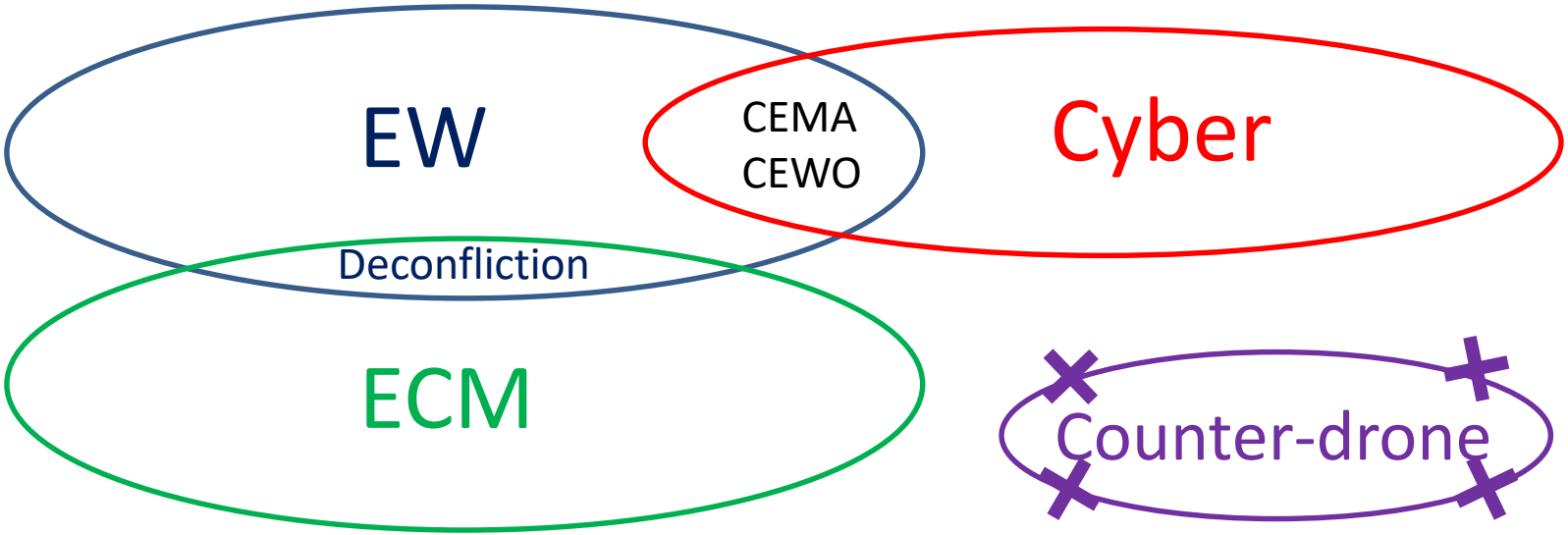
- Second decade:
  - Lessons from Afghanistan;
  - Democratisation of technology and the rise of cyber;
  - Resurgent peer adversaries.

- Third decade:

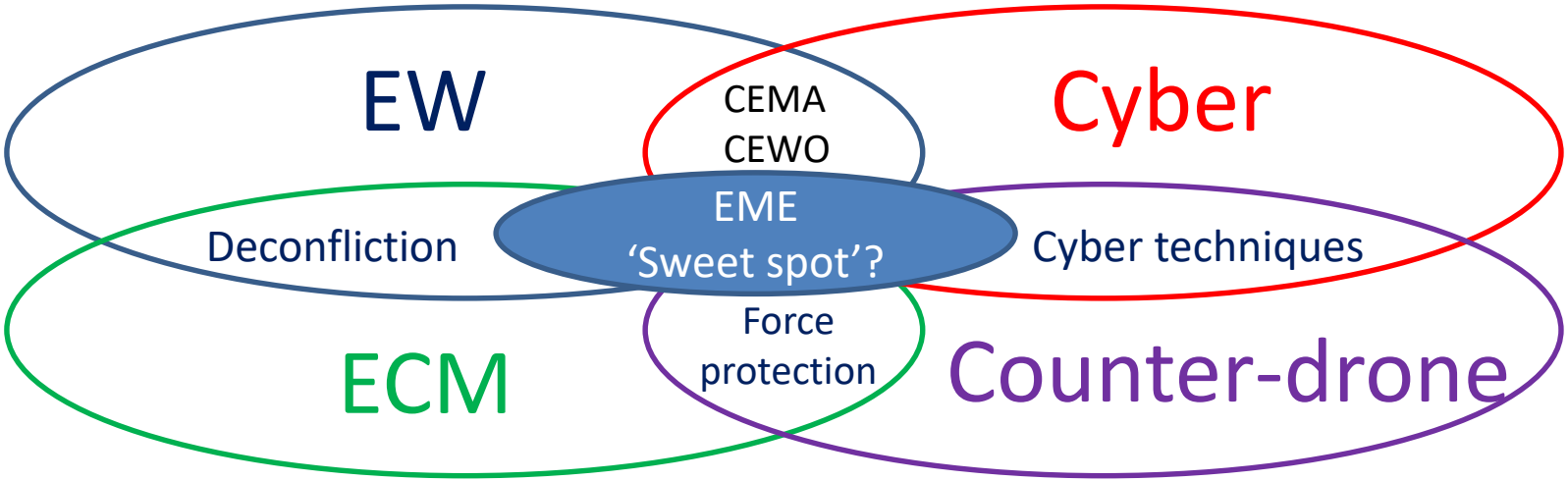
Current challenges

- **Fragmented approach:**
  - to sponsoring, specifying, buying, fielding and supporting equipment: increases complexity of training, doctrine, support, data fusion.
- **Range of threats:**
  - Relatively bounded during Iraq and Afghanistan;
  - Now more wide ranging and more difficult to predict;
  - and more (technically) complex ... but (commercially) simpler
- **Pace of technological change:**
  - Allows adversaries to adapt and hide better ... *but* ...
  - Also allows us to respond more flexibly.

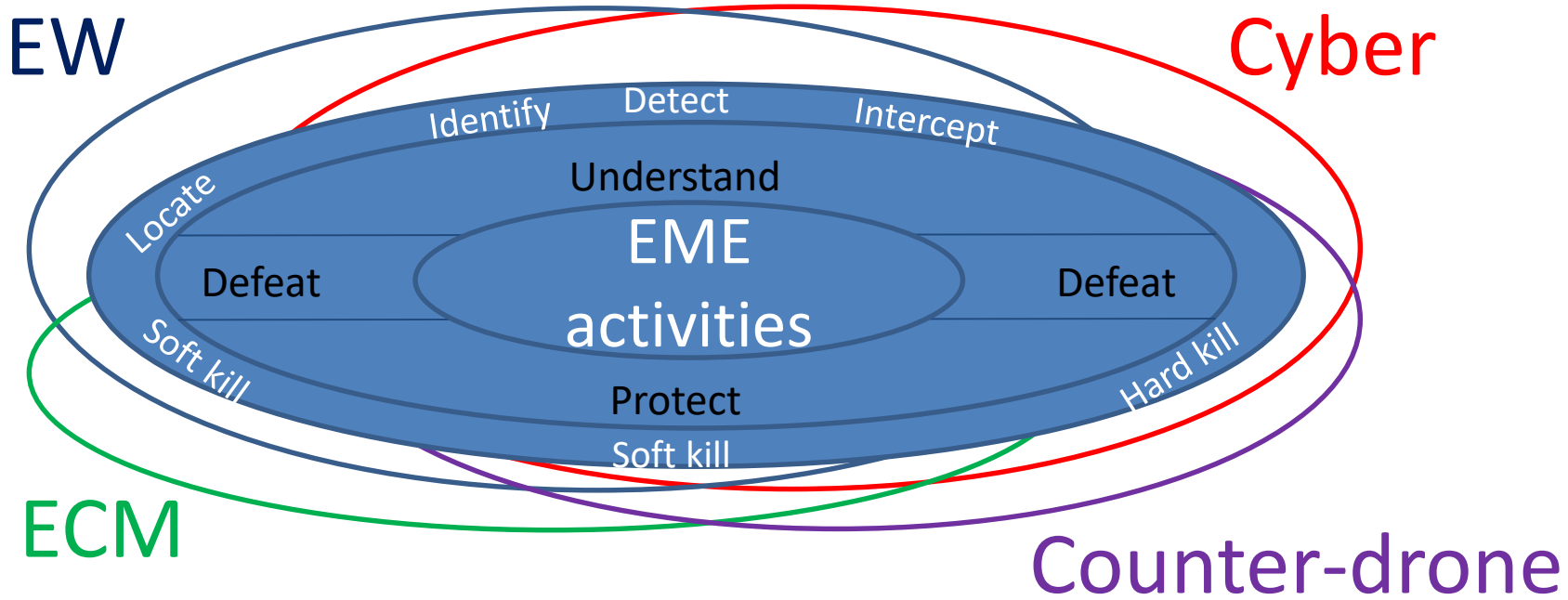
Current Approach



Converging the Approach



Coherent Approach



Coherent approach: how?

Single view of system

Management system

Tac EW | ECM | C-drone | Intelligence

EME Core

Cyber

Common architectural 'chassis' (open standards)

Industry & academia (research)

Test rig & innovation

. . . . . *sensors and effectors* . . . . . .

Notes:
- ⟷ are product-agnostic open standards
- ⟷ are data/information flows

Issues

- **Skills:**
  - Wider range of skills needed: is it realistic?
  - Skill fade?
  - Do sufficient, and sufficiently capable, people exist?
- **Management/governance:**
  - Will it be too complex to manage?
  - Where do you draw the system/capability boundary?
- **Data overload:**
  - Can AI/machine learning advance faster than our ability to collect data?
  - How to protect/classify information between different groups?
- **Collective risk:** does aggregation increase our own vulnerability too much?
- **Equipment/systems:** can we overcome our protective instincts?

Closing thoughts

What could EW look like beyond CEMA, and what are key issues?

- Wider remit: include FP ECM and counter-drone, and use such sources for EMS survey/defining ‘normal’
- Greater re-use of assets in support of EME activity
- ‘Gather once, use many times’ approach to information
- Shift emphasis from ‘collect’ to ‘data exploitation’?
- Exploit AI and machine learning to support decision making
- Span from tactical information to strategic influence
- **Capabilities focussed on EME as a warfighting environment**