Ministry of Defence

Joint Doctrine Note 1/18

Cyber and Electromagnetic Activities

Development, Concepts and Doctrine Centre

Joint Doctrine Note 1/18

Cyber and Electromagnetic Activities

Joint Doctrine Note (JDN) 1/18, dated February 2018,
is promulgated as directed by the Chiefs of Staff

Assistant Head Doctrine

Conditions of release

Authorisation

The Development, Concepts and Doctrine Centre (DCDC) is responsible for publishing strategic trends, joint concepts and doctrine. If you wish to quote our publications as reference material in other work, you should confirm with our editors whether the particular publication and amendment state remains authoritative. We welcome your comments on factual accuracy or amendment proposals. Please send them to:

DCDC, Ministry of Defence Shrivenham, Swindon, Wiltshire, SN6 8RF

E-mail: DCDC-DocEds@mod.gov.uk   Telephone: 01793 31 4216/4217/4220

Copyright

Distribution

Distributing Joint Doctrine Note (JDN) 1/18 is managed by the Forms and Publications Section, LCSLS Headquarters and Operations Centre, C16 Site, Ploughley Road, Arncott, Bicester, OX25 1LP. All of our other publications, including a regularly updated DCDC Publications Disk, can also be demanded from the LCSLS Operations Centre.

LLCSLS Help Desk: 01869 256197   Military Network: 94240 2197

Our publications are available to view and download on the Defence Intranet (RLI) at: http://defenceintranet.diif.r.mil.uk/Organisations/Orgs/JFC/Organisations/Orgs/DCDC

This publication is also available on the Internet at: www.gov.uk/mod/dcdc

Preface

Purpose

1.   Joint Doctrine Note (JDN) 1/18, *Cyber and Electromagnetic Activities* attempts to capture the widest concept of cyber and electromagnetic activities (CEMA) and draws together elements of existing doctrine and best practice. However, the principles and concepts expressed are not yet wholly agreed. This JDN sets a baseline for CEMA within UK Defence, Government Communications Headquarters (GCHQ) and other partners across government (PAG). It provides a working description of the CEMA environment and will enable the single Services to develop a tailored CEMA concept whilst remaining aligned with Joint Forces Command (JFC) and GCHQ intent.

Context

2.   To succeed against complex and diverse threats that exploit the pervasive information environment we need to do things differently. At the heart of this concept is the enhancement of joint action and, therefore, our influence by contesting the information environment, being more integrated as a force and more adaptable to changing circumstances. Conventional and non-conventional adversaries may be state or non-state; and may employ mission-tailored, decentralised, asymmetric and agile actors. Therefore, it is important that we have doctrine that examines how we adapt operations to the changing environment rather than trying to control it. This is the context within which Defence must undertake CEMA.

3.   JDN 1/18, aims to clarify the nature of CEMA and offers guidance on how to enable, realise, employ and exploit it. It considers how CEMA supports understanding, offensive and defensive actions and how it enables commanders and staff to make effective decisions and create effects within the full spectrum approach.

Audience

4.   This publication is aimed at military commanders and staff (J1-J9) at Permanent Joint Headquarters and at higher tactical levels. It should also

inform staff and planners working with PAGs who may provide critical CEMA interdependencies. Finally, this JDN should further inform military and civilian staff developing related doctrine, conducting force generation and procuring future capability.

Structure

5.   JDN 1/18 is divided into four chapters.

      a.   Chapter 1 explains the need for CEMA.

      b.   Chapter 2 explores the scope of CEMA and defines the concept.

      c.   Chapter 3 describes CEMA development and functional relationships.

      d.   Chapter 4 explains how we plan and conduct CEMA.

Linkages

6.   This JDN should be read alongside:

- Allied Joint Publication (AJP)-3.6B, *Allied Joint Doctrine for Electronic Warfare*, Edition B;
- AJP-3.9, *Allied Joint Doctrine for Joint Targeting*;
- AJP-3.10, *Allied Joint Doctrine for Information Operations*;
- AJP-5, *Allied Joint Doctrine for Operational-level Planning* (with UK national elements);
- Defence Instructions and Notices (DIN) 2017DIN03-014: *Cyber and Electromagnetic Activities (CEMA) in Defence – Definition OS*;
- Joint Concept Note (JCN) 1/17, *Future Force Concept*;
- JSP 900, *UK Targeting Policy;*
- JDN 4/10, *Single SIGINT Battlespace*;
- JDP 0-50, *UK Cyber Doctrine*; and
- *Full Spectrum Approach Primer*.

Contents

The need for cyber and electromagnetic activities

Chapter 1 explains the background and need for cyber and electromagnetic activities (CEMA) to create operational effect. It goes on to describe how other countries are integrating CEMA to ensure decisive advantage.

Chapter 1

1

1

"

…to **understand, manage and control** the electromagnetic environment is a **vital role in warfare** at all levels of intensity. The **outcome of future operations** will be **decided by the protagonist** who does this to **decisive advantage**.

"

Chief of the Defence Staff
Air Chief Marshal Sir Stuart Peach

Chapter 1 – The need for cyber and electromagnetic activities

Section 1 – Introduction

1.1.   Cyber and electromagnetic activities (CEMA) are interdependent and within the electromagnetic environment (EME). The EME will be contested by actors using both cyber and electromagnetic activity to achieve operational advantage. Digitisation has led to the convergence of cyber and information activities to such an extent that CEMA coordination across the joint force will be imperative for operational success. Freedom to flexibly use or to deny, degrade or constrain adversary access to the EME and parts of cyberspace will offer significant operational advantage.

> The CEMA Vision is:
>
> 'The synchronisation and coordination of cyber and electromagnetic activities, delivering operational advantage thereby enabling freedom of movement, and effects, whilst simultaneously, denying and degrading adversaries' use of the electromagnetic environment and cyberspace.'[1]

1.2.   CEMA must address the longstanding challenges of acquiring, using and integrating information with physical actions to create the desired effect. In addition, information and the systems which create, collect, manage and exploit this information, are critical to successful conflict outcomes. The need for CEMA coordination, coherent with a full spectrum approach and mission assurance, has escalated in recent years because of the sheer volume of information, the ease of access to it and the increasing means by which it can be exploited.

....
1   The Cyber and Electromagnetic Activities (CEMA) Vision was devised by the CEMA Capability Integration Group (CIG).

1.3.   There is also the challenge of achieving interoperability and sustaining knowledge parity while conducting joint and coalition operations. While many of these challenges will also be faced by our adversaries, low entry costs and the rapid adoption of cutting edge technology means they may be equally, or better, placed to use information as a force multiplier. However, our challenge is to operate within the constraints of UK and Allied, policy, doctrine and law, whilst our adversaries have no need to and indeed gain an edge in not doing so.

1.4.   Russian operations in south-eastern and eastern Europe highlighted the effectiveness of synchronising CEMA with conventional operational activities to shape both the adversary's and international perception.[2] However, within the North Atlantic Treaty Organization (NATO) and specifically UK doctrine, force and capability development have not kept pace. Joint Concept Note (JCN) 1/17, *Future Force Concept* identified the need for CEMA while this joint doctrine note (JDN) provides clarification by exploring how the CEMA concept is implemented so it can be undertaken with decisive advantage.

1.5.   There are areas where cyber activities and electromagnetic activities overlap and these need to be defined. The nature of CEMA is such that it should be coordinated and may be synchronised across any, or all, activities. To deliver operational advantage, a deployable headquarters will need to synchronise as well as coordinate electronic warfare, spectrum management, signals intelligence[3] and cyber operational activities with CEMA-enabling activities and other non-CEMA operational activity. The list below indicates some of the areas to be considered by a CEMA synchronisation and coordinating authority. This list is not exhaustive and issues of mission assurance should be considered.

---

2   This joint doctrine note (JDN) will look at Russian use of both cyber activities and electromagnetic activities and how they have developed, drawing parallels with UK CEMA aspirations and developments. Chapter 1 looks at the problems Russia encountered during operations in Georgia. Chapter 3 points to the successes on operations in Ukraine, while Chapter 4 looks at how the Russian military has evolved and focused on coordinated and synchronised actions to achieve the commander's intent.
3   Signals intelligence incorporates electronic intelligence and communications intelligence.

a.   Assure CEMA capability coherence across Defence and the Government Communications Headquarters (GCHQ) for both new and existing capabilities.

b.   Inform and shape CEMA capability across Defence lines of development ensuring coherence across Service Commands, Defence Equipment and Support, Information Systems and Services and Defence Science and Technology Laboratory.

c.   Influence the production of CEMA policy and doctrine.

d.   Ensure key CEMA component and Service Command personnel receive core training at tactical, operational and strategic levels.

e.   Enable electromagnetic activities (EMA) and cyber activities to be developed coherently under the CEMA strategy.[4]

f.   Establish relationships with Defence industrial partners for supply chain issues and vulnerabilities.

1.6.   As cyber and EMA functions mature, CEMA will change. However, consideration must be given to how cyber and EMA capabilities under development can be synchronised and coordinated into the full spectrum approach. A CEMA policy, planned for 2018, will develop the links between cyber and EMA.

....

4   The Joint Force Cyber Group and British Army, as well as the United States of America Cyber Command, work to the National Institute of Standards and Technology Cyber Security Framework which provides a useful common language and description of functions (identify, protect, detect, respond, recover and their sub-categories). The CEMA strategy covers the period from 2017 to 2025 through three phases: phase 1 – definition and refinement (2017-2020); phase 2 – implementation (2020-2025); and phase 3 – business as usual (2025 onwards).

Section 2 – Background

1.7.   Technology will remain an essential element of future conflict and a driver of military change over the next 20 years. Maintaining a technological advantage across key capability areas has, for many years, enabled us to succeed with relatively small, professional Armed Forces. But these key capability areas were never integrated, leading to 'stove-piped' capability/force development where interoperability was coincidental rather than planned. However, with the convergence of computing and telecommunications and the pace of technology, the military is now trying to rebalance its understanding of the environments to encompass electromagnetic, cyber and information aspects.

1.8.   The rapid growth in non-kinetic activity challenges traditional notions of hostile action and accountability within international law. Cyber operations synchronised with electronic warfare in the context of a full spectrum approach may overmatch conventional forces that are not prepared for conflicts in the electromagnetic environment and cyberspace simultaneously. The situation now exists whereby technological advantage is being eroded by non-conventional warfare using electromagnetic and cyber activities. This has led to the United States of America (US) creating their 3rd Offset Strategy, introduced in Chapter 3.

Non-conventional warfare using electromagnetic and cyberspace
may overmatch unprepared conventional forces

Weaknesses identified in the Georgian Operation (from a Russian perspective)

In August and September 2008, Russia conducted a multi-pronged operation against Georgia in support of the Russian-backed, self-proclaimed republics of South Ossetia and Abkhazia.[5] While this operation was successful, it did highlight several weaknesses in Russian surveillance and communications capability between single Services, weaknesses that Russia has sought to address.

While the use of superior numbers of conventional ground forces and artillery was successful, other softer activities requiring modern equipment operated by agile joint forces proved less so.

  a.   The inability to counter the Georgian air defence capabilities led to limited fixed-wing air operations and almost no rotary wing air operations. Air superiority was only achieved once ground forces had neutralised Georgian air defences.

  b.   Russian military communications had little integration between different radio systems.

  c.   Russia had, until this time, limited their use of unmanned aircraft systems; this combined with electronic warfare weaknesses left a gap in intelligence provision.

Few Russian sources directly acknowledged these weaknesses, but following the Georgian operation, the Russian military took steps to address both cyber and electronic warfare capability development.[6]

1

---

5   More infromation is available at http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20091231_art009.pdf
6   More information is available at http://ssi.armywarcollege.edu/pdffiles/pub1069.pdf

Section 3 – Parity and pacing

1.9.   Following Russian operations in eastern Europe and the Middle East; and China's military activities worldwide, much has been discussed about regaining the initiative. Although NATO has been confident of its superiority there are areas where other nations have actually become peers, for example, where Russia and China have achieved this in relation to EMA, cyber and information activities. As a minimum they need only keep pace with NATO to maintain parity but could well be overmatching our capability.[7] With the rapid acceleration of CEMA technology and capability, NATO's lack of priority to produce up-to-date joint doctrine and policy has exacerbated the situation.[8]

1.10.   Russia's Chief of Electronic Warfare Troops, General-Major Yuriy Lastochkin provides an example of how Russia is maintaining parity and moving towards overmatching our capabilities in an interview in April 2017. He said:

"The entire system of measures of organizational development of Electronic Warfare Troops will substantially increase their contribution to winning superiority in command and control, and in employing weapons. The volume of effectively fulfilled missions in various strategic directions will grow by two to two and a half times and by 2020 will reach 85 percent. This in turn will become the basis of an effective air-ground electronic warfare system, capable of neutralizing the enemy's technological advantage in the aerospace sphere and the information-telecommunications space."[9]

....

7   For example, the impact of the WannaCry ransomware attack on the NHS in May 2017, or the December 2015 Ukraine power grid cyberattack.

8   Whilst no US joint doctrine exists, the US Army discussed CEMA in Army Field Manual (FM) 3-38, *Cyber Electromagnetic Activities*, however, that publication was not updated rather it was retired and replaced with FM 3-12, *Cyberspace and Electronic Warfare Operations* which describes CEMA as 'the planning, integrating and synchronising activity for echelon corps and below'.

9   More information is available at https://russiandefpolicy.blog/2017/05/30/electronic-warfare-chief-interviewed-2/

1.11.   As the world becomes ever more connected this leads to resource contention across electromagnetic spectrum frequency bands. Government and military activities in the electromagnetic environment and cyberspace must consider non-combatant use and ensure, where possible, that operations do not adversely affect access to this global common.**10**

Key points

- Low entry costs and the rapid adoption of cutting edge technology means our adversaries may be equally, or better placed to use information as a force multiplier.

- Challenges exist between using and integrating information while conducting joint and coalition operations.

- Cyber and electromagnetic activities (CEMA) is not the change or development agent for electromagnetic activities (EMA), nor cyber maturation; it is based on synchronising and coordinating these activities.

- CEMA needs policy and doctrine to ensure it is coherently undertaken across Defence, the Government Communications Headquarters and partners across government.

- It is important to learn lessons from past operations, such as events in Georgia, about the need to synchronise and coordinate cyber and electromagnetic activities.

- The electromagnetic environment and cyberspace are a congested resource and operations need to consider other users, both friendly and adversarial.

---

10   *Future Operating Environment 2035*, page 21.

Scope and definition

Chapter 2 offers a definition of cyber and electromagnetic activities (CEMA) as well as scoping its application. It explains that CEMA provides a synchronisation and coordination function for these activities.

2

Chapter 2

2

"

Sometimes it is the people **no one can imagine anything of** who **do the things no one can imagine**.

"

Alan Turing

Chapter 2 – Scope and definition

Section 1 – The Defence approach

2.1.   The *Joint Forces Command Command Plan 2016/17* sought to establish a Joint Cyber and Electromagnetic Activities (CEMA) Group to coordinate the tasking, planning and execution of Defence CEMA and produce a strategy to optimise the application of cyber and electromagnetic capabilities. The approach to its implementation should be driven by the CEMA Vision and Strategy.[11] The CEMA vision will be delivered by the Ministry of Defence and partners across government. This will ensure a coherent approach for military and CEMA partners, limiting the adversary and enhancing UK Armed Forces' freedom of manoeuvre, freedom of action, information advantage, decision superiority, and delivering operational advantage.[12] These, in, turn need adequate resources, including manpower empowered to make decisions and implement change across the necessary elements of Defence.

2.2.   CEMA is not the only available function to create the commander's desired effect and must be considered as part of full spectrum effects and full spectrum targeting.[13] Where CEMA is identified as appropriate then the discussions that follow inform the synchronisation and coordination of these activities and their contribution to the desired effect.

2.3.   CEMA is defined as: the synchronisation and coordination of offensive, defensive, inform and enabling activities, across the electromagnetic environment and cyberspace.[14] The definition broadly identifies four activities, which are conducted in the electromagnetic environment (EME), cyberspace, or a combination of both. Figure 2.1 expands on the definition with examples of these activities.

....

11   The strategy was devised by the Cyber and Electromagnetic Activities (CEMA) Capability Integration Group (CIG) to determine the approach for implementing CEMA. The strategy sets out a three phase, eight year programme. At the time of publishing this joint doctrine note the strategy is awaiting endorsement.

12   The CEMA Vision is at Chapter 1, paragraph 1.1. It was endorsed by the CEMA CIG in March 2017.

13   Joint Service Publication (JSP) 900, *UK Targeting Policy.*

14   This is a CEMA CIG working group endorsed definition.
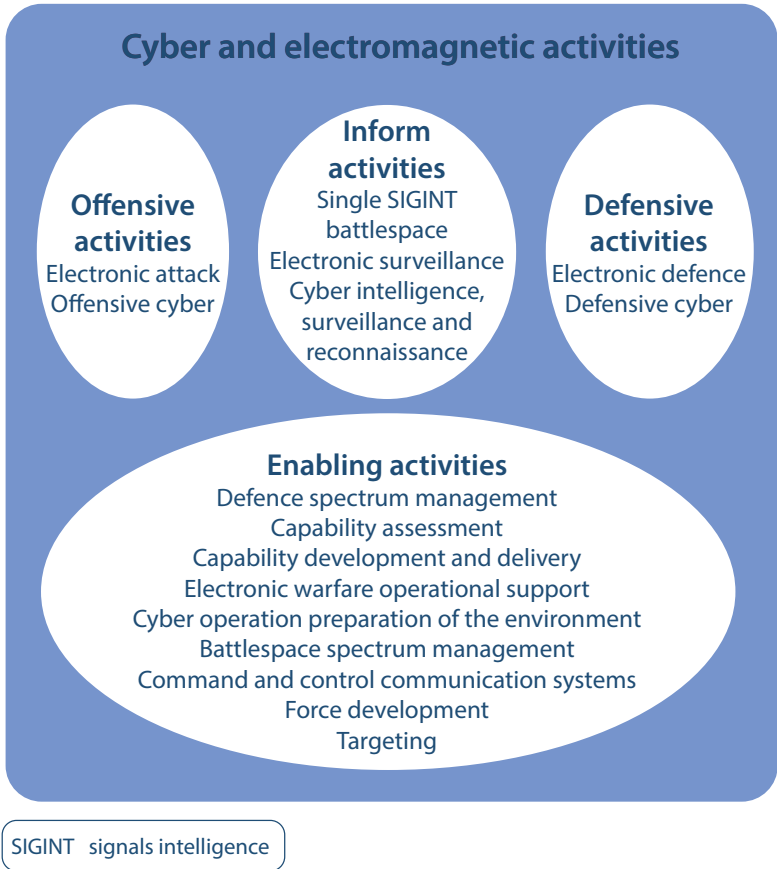
Figure 2.1 – A visual definition of cyber and electromagnetic activities

2.4.   Defensive, offensive and inform activities are underpinned by enabling activities which provide the necessary operational analysis, resources and infrastructure. While many enabling activities do not contribute directly to the military operation, a failure to conduct them will lead to less effective offensive, defensive and inform activities and ultimately pose a risk to operational success.

Section 2 – Functional scope

2.5.   CEMA should be coordinated and may be synchronised across any, or all, activities. Although the intent within CEMA is to synchronise offensive, defensive and inform activities, that may not be practical against the whole range of joint force activities.

2.6.   CEMA comprises cyber activities and electromagnetic activities (EMA) however, there are no approved definitions for either cyber activities or EMA. Identifying these two groups of activities would help in the understanding of the CEMA scope. The proposed definition of electromagnetic activities is: all offensive, defensive and inform activities that shape or exploit the electromagnetic environment and the enabling activities that support them.[15]

2.7.   Cyber activities have not been defined. However, equivalents can be found in the four cyber operations' roles:[16]

- offensive cyber operations (OCO);

- defensive cyber operations (DCO) (including active defence);

- cyber intelligence, surveillance and reconnaissance (cyber ISR); and

- cyber operational preparation of the environment (cyber OPE).

2.8.   CEMA will also coordinate with organisations and actors conducting non-CEMA activities where required. For example, CEMA is an enabler for psychological operations that are considered to be part of information operations. Figure 2.2 illustrates this relationship with some examples (not all) of non-CEMA activities.[17]

....

15   This definition was proposed and endorsed by the CEMA CIG on behalf of the Head Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance and Cyber joint user.
16   *Cyber Primer,* 2nd Edition, page 51.
17   Joint Tactics, Techniques and Procedures (JTTP) 3-70;1, *Joint Tactics, Techniques and Procedures for Battlespace Management*, Version 2, paragraph 23.

2

Cyber and electromagnetic activities

Offensive activities
Electronic attack
Offensive cyber

Inform activities
Single SIGINT
Battlespace
Electronic surveillance
Cyber intelligence
surveillance and
reconnaissance

Defensive activities
Electronic defence
Defence cyber

Enabling activities
Defence spectrum management
Capability assessment
Capability development and delivery
Electronic warfare operational support
Cyber operation preparation of the environment
Battlespace spectrum management
Command and control communication systems
Force development
Targeting

Non-cyber electromagnetic activities

Example of activities
Kinetic effects
Media operations
Psychological operations
Intelligence (generic)

Activities to be synchronised
where possible

SIGINT

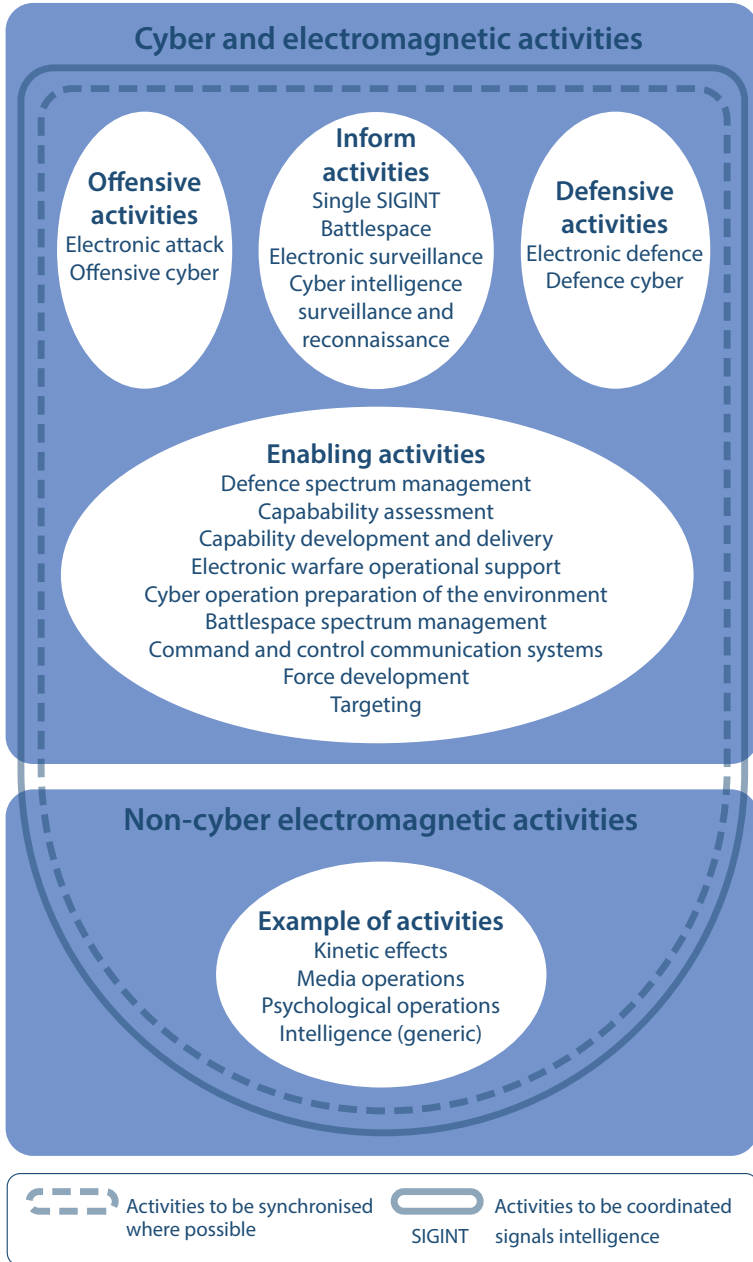Activities to be coordinated
signals intelligence

Figure 2.2 – The synchronisation and coordination of CEMA and non-CEMA

2.9.   The North Atlantic Treaty Organization (NATO) states that operational EMA should comprise of electromagnetic operations (EMO), which are defined as: all operations that shape or exploit the electromagnetic environment, or use it for attack or defence including the use of the electromagnetic environment to support operations in all other operational environments.[18] This definition does not include all enabling activities and therefore EMO must not be considered interchangeable with EMA.

Section 3 – Command considerations

2.10.   There are several command considerations applicable across the entirety of CEMA. **Coordination** is the activity CEMA actors undertake, whereas **operational imperative**, **agility**, **execution**, **redundancy** and **resilience** are the ethos which guide them.

a.   **Operational imperative.** This is the key principle upon which all others depend. As CEMA activities are not yet sufficiently established, all actors must be informed of, understand and be focused on delivering the commander's intent.

b.   **Agility.** Both cyberspace and the EME are being contested by the adversary. Therefore the ability to flex resource, effort and processes as required is critical.

c.   **Coordination.** This must be conducted at the highest level and filter down to all force elements and coalition partners.

d.   **Execution.** CEMA will be integrated with the wider military under the full spectrum approach. This means CEMA battlespace execution is likely to require a command and control approach emphasising centralised control but decentralised execution, where execution authority is delegated to the point of best understanding for decision-making.

2

....
18   NATO*Term.*

e.   **Redundancy.** As cyberspace and the EME are being contested by the adversary, planning for redundancy and reversionary practices should be undertaken and exercised.

f.   **Resilience.** Resilience is the ability of the community, services or infrastructure to withstand the consequences of an incident.[19] This is related to both execution and redundancy.

Key points

- Cyber and electromagnetic activities (CEMA) is defined as: the synchronisation and coordination of offensive, defensive, inform and enabling activities, across the electromagnetic environment and cyberspace.

- Enabling activities provide the necessary operational analysis, resources and infrastructure.

- Synchronisation and coordination of CEMA contributes to the commander's intent.

- CEMA will also coordinate with organisations and actors conducting non-CEMA activities where required.

- Electromagnetic operations are not the same as electromagnetic activities.

- A commander should consider the application of operational imperative, agility, coordination, execution, redundancy and resilience across CEMA.

2

....

19   Joint Doctrine Publication (JDP) 02, *Operations in the UK: The Defence Contribution to Resilience*, 2nd Edition.

Notes

2

Development and functional relationships

Chapter 3 describes the development of cyber and electromagnetic activities and offers a framework to guide its progression, roles and responsibilities. It highlights that technological exploitation of the electromagnetic spectrum has increased demands for this resource.

3

3

"

Digitisation has led to the **convergence of cyber and information activities**, heralding an age where **CEMA coordination** across the joint force will be an **imperative for operational success**.

"

Joint Concept Note 1/17,
Future Force Concept

Chapter 3 – Development and functional relationships

Section 1 – Development approach

3.1.   The relationships between cyber activities and electromagnetic activities are still maturing making a single approach to cyber and electromagnetic activities (CEMA) challenging. Therefore our adoption and implementation of the CEMA concept and its integration into the full spectrum approach will benefit from an incremental development approach. Individual needs, for the single Services, may need to be tailored.

> At the tactical level, a planned operation requires phone use to be blocked in the operations area. This is achieved by an electronic warfare operation jamming the broadcast tower. Due to insufficient synchronisation and coordination, it was not appreciated that jamming the tower also stopped an ongoing strategic cyber operation being conducted by partners across government.

3.2.   A development maturity progression framework that outlines levels of synchronicity is shown in this chapter. Progression towards each of these representative maturity levels is implemented in various ways. However, all maturity levels will need to consider Defence lines of development for each step and how these levels align with the future force concept.

   a.   **Level 1: initial step.** The initial step is the most difficult to address as funding and resources will already be allocated across the current force.[20] This step, demonstrated in Figure 3.1, will be set in the context of austerity and have to overcome extant doctrine, policy and

....
20   The current force is identified in Joint Concept Note (JCN) 1/17, *Future Force Concept*.

entrenched ways of working. The ability to point to early realisation of benefit will engender confidence in the concept.
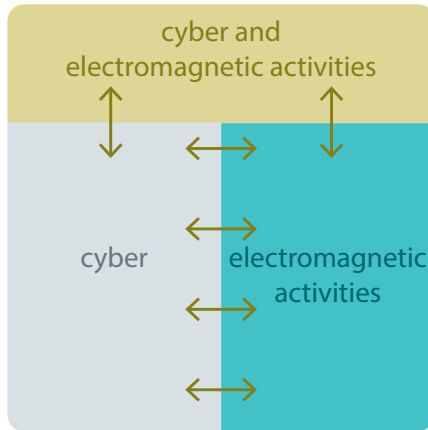

Figure 3.1 – Level 1: initial step

b.   **Level 2: evolving step.** This step provides a substantial degree of synchronisation and coordination without re-designing cyber and electromagnetic force structures, funding lines and legal frameworks. Figure 3.2 may be achievable in a funded force.[21]
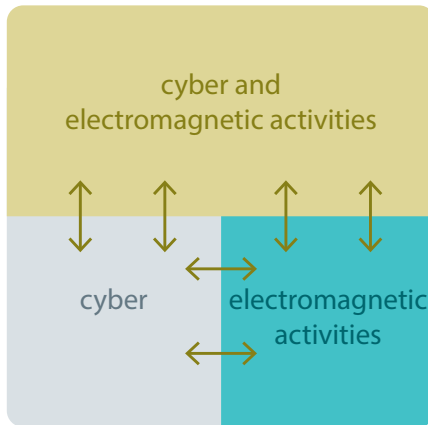

Figure 3.2 – Level 2: evolving step

21   Joint Concept Note (JCN) 1/17, *Future Force Concept*.

c.   **Level 3: integrated step**. Options will be examined in future concept studies such as Joint Concept Note (JCN) 1/17, *Future Force Concept*. Figure 3.3 and Figure 3.4 will involve looking ten or more years into the future and this may require a reactive and agile approach due to rapid developments in technology.
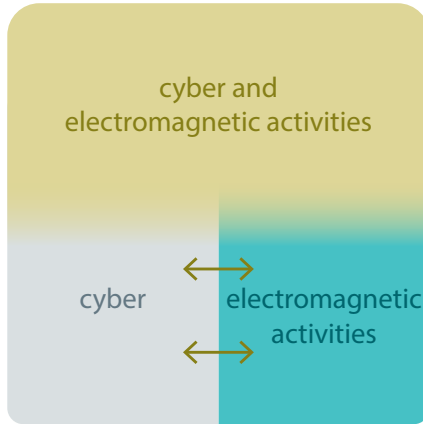

Figure 3.3 – Level 3: integrated cyber
electromagnetic activities

d.   **Level 4: ubiquitious step**. Figure 3.4 recognises that there may be elements of cyber and electromagnetic activities (EMA) never fully integrated into CEMA. An example of this may be down to security issues, but these boundaries will become less defined over time.
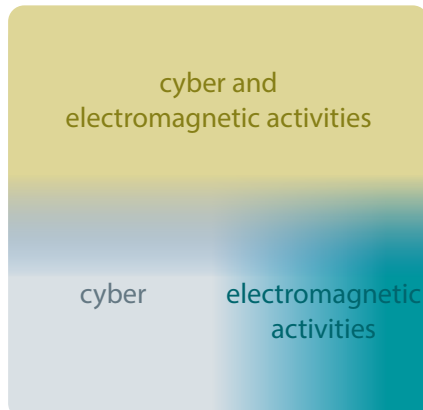

Figure 3.4 – Level 4: ubiquitous cyber
electromagnetic activities

3

The United States 3rd Offset Strategy[22] and Russian non-linear war[23]

With the resurgence in Russian military effectiveness, the United States of America (US) has had to once again examine how it might 'offset' the asymmetrical aspects of adversaries' development.

For the 3rd Offset Strategy the Department of Defense took a more holistic approach asking 'who are our pacing competitors, what are they doing, how can they affect the US and how can we counter the effects?' Once understood, force development and capability development can focus on the problem.

Currently, the US Department of Defense's five key technology areas for exploitation are:

- autonomous learning systems;
- human-machine collaboration;
- assisted human operations through technology;
- advanced human-machine combat teaming; and
- network-enabled autonomous weapons and high-speed weapons.

Notably, all of these use the electromagnetic spectrum and cyberspace and therefore open up novel attack vectors and present novel vulnerabilities. Interestingly, the Russian non-linear war seeks to exploit and protect similar attack vectors and vulnerabilities, leaving the West to determine whether it is once again in an arms race.

....

22   More information is available at http://csbaonline.org/research/publications/toward-a-new-offset-strategy-exploiting-u-s-long-term-advantages-to-restore

23   Non-linear war or hybrid war is a military strategy that blends conventional warfare, irregular warfare and cyber warfare. By combining kinetic operations with subversive efforts, the aggressor intends to avoid attribution or retribution. More information is available at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Section 2 – Roles and responsibilities

3.3.   The roles and responsibilities addressed in this joint doctrine note (JDN) already exist with none disappearing or being created. This JDN aims to identify the CEMA-related synchronisation and coordination activities that need developing within each role and/or function with these roles evolving over time. Understanding these changes, how that role performs its CEMA duties, or when and where, is not within this JDN. A joint doctrine publication (JDP) will be developed to address these issues.

3.4.   CEMA development must be driven and supported by Defence and partners across government, based on the vision and strategy.[24] Implementation should be within the joint user community. Force development and generation functions are listed below.

3

a.   **Force development.** CEMA is not a 'Genesis Option', as described by Finance and Military Capability – there is no extra funded manpower to support it.[25] CEMA should be considered by the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) branch of Joint Forces Command (JFC) Capability Directorate during force testing, exploration and design rather than separately as cyber and EMA activities to identify efficiency gains that enable CEMA's introduction.

b.   **Force generation.** Development should be driven by a Defence-wide need rather than by the single Services. Developing doctrine and policy needs to be underpinned by a corporate programme from which all other specialist training should evolve. Examples of this generation are listed below.

....

24   The Cyber and Electromagnetic Activities (CEMA) vision is at Chapter 1, paragraph 1.1. The strategy was endorsed by the CEMA Capability Integration Group (CIG) to determine the approach to implement CEMA. It sets out a three phase, eight year programme. It is expected to be endorsed in 2018.

25   The Finance and Military Capability Operating Model explains force development and force generation in more detail and outlines capability development. This document is only available on the UK Ministry of Defence's Intranet at: http://aof.uwh.diif.r.mil.uk/ aofcontent/cm/downloads/24601-FMC_Operating_Model_Version_1_Published.pdf

i.   **Whole Force management.** Whole Force by Design[26] refreshes the Whole Force concept and must guide Whole Force management. The Whole Force must comprise generalists and specialists and take into consideration their development and collaboration requirements. These specialists may come from partners across government. Stove-piping branch and trades should be avoided to allow the successful implementation of the CEMA concept.

ii.   **General education.** Education must focus on how our operations leverage CEMA and essential operations security practices.[27] We must provide continuous and developing education opportunities for all personnel to ensure that CEMA is understood and in line with techological advances.

iii.   **CEMA training.** Where possible training should be developed and delivered across the Whole Force rather than single Services or branches. Specialist training should be balanced against current needs and needs identified during force development. Aspects of CEMA training will be mandated by partners across government.[28]

iv.   **Exercises.** CEMA serials must be woven into the normal training programme and not seen as an add on. Exercises must be realistic and robustly test our Armed Forces' defensive and offensive capabilities. We must capably deal with degraded and denied cyberspace and electromagnetic environment (EME) operations, adapting quickly to reversionary war modes. Realistic training must include security against third parties collecting cyber or EME data on our forces and the challenges of electronic warfare or offensive cyber systems degrading civil systems. This will act as a driver for synthetic cyber and EME training systems.[29]

....

26   Whole Force by Design was conceived with National Security Council Review outcomes in mind, particularly Joint Force 2025 in accordance with the principle of achieving the most cost effective balance between regular and reserve forces, Ministry of Defence civilians and contractors.
27   JCN 1/17, page 22.
28   *Ibid.*
29   *Ibid.*

CEMA serials need to become a part of regular training programmes

v. **Expeditionary forces.** Expeditionary force design should take account of CEMA from inception.[30] The practice of retro-fitting CEMA force elements into a conventional force may lead to under-resourcing, unclear or complex chains of command and poor integration into a full spectrum approach.

vi. **Lead user.** While the role of lead user for tactical CEMA capabilities can be placed within a single Service, the default for the lead user role is the C4ISR joint user in JFC. This may be the case even if the capability is operated by a single Service.

vii. **Joint user.** This role should always stay with the C4ISR joint user in JFC. As CEMA is focused on synchronisation, coordination and the contribution to the full spectrum approach, the C4ISR joint user will have the remit to look across Defence.

viii. **Lead delivery agent.** This may sit with either Defence Equipment and Support (DE&S) or Information Systems and

....
30   This is to include planning staff.

Services and will depend on the balance of equipment or service to be provided.

Section 3 – Evolving functions

3.5.   The single Services have historically conducted EMA independently, even when operating as part of a joint force. Recent UK operations have focused EMA on tactical electronic defence, particularly on counterinsurgency and stabilisation operations.[31] However, our adversaries have also been developing wide-ranging EMA capabilities and employing them operationally.

3.6.   Recent efforts have concentrated on developing cyber forces and capability, and while significant progress has been made, development is often conducted along single-Service lines, with the exception of offensive cyber. This is not a problem confined solely to the UK. Few North Atlantic Treaty Organization (NATO) members have developed a coherent and comprehensive cyber approach and NATO has yet to incorporate 'cyber' into its definitions and terms. While achieving consensus on the concept of CEMA is difficult, a debate may start with the examination of the sub functions of core CEMA and how their scope interacts with each other; these being EMA and cyber activities, and their collective management.

3.7.   **Electromagnetic activities.** Operationally there are four EMA that are key elements: electronic warfare; signals intelligence; spectrum management; and communications. These functions are integral parts and interlinked in our operations.

a.   **Electronic warfare.** This is defined as: military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects.[32] It is made up of four elements.

....
31   Tactical operational activities in Iraq and Afghanistan have been supported by a wide variety of electronic countermeasures (ECM). A key function has been the jamming, deception and neutralisation of remote-controlled improvised explosive devices. ECM is a form of active electronic defence.
32   NATO*Term*.

i. **Electronic surveillance.** This is defined as the: use of electromagnetic energy to provide situational awareness and intelligence.[33] When developing CEMA, regard must be paid to the overlap between electronic surveillance and cyber intelligence, surveillance and reconnaissance (cyber ISR).

ii. **Electronic defence.** This is defined as the: use of electromagnetic energy to provide protection and ensure effective friendly use of the electromagnetic spectrum.[34]

iii. **Electronic attack.** This is defined as the: use of electromagnetic energy for offensive purposes.[35] This is employed to diminish an adversary's ability to understand, shape or exploit the operational environment and its use should be integrated into the full spectrum affect under CEMA.

iv. **Electronic warfare management.** This is the capability to coordinate and deconflict electronic warfare activities and, as such, is fundamental to coordinating CEMA.

b. **Signals intelligence.** This is defined as: intelligence derived from electromagnetic signals or emissions.[36] In some instances this intelligence may be collected by either electronic surveillance or cyber ISR, coordination is required to optimise activities.

c. **Spectrum management.** This is defined as: planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures with the objective of enabling military electronic systems to perform their functions within intended environments without causing or suffering harmful interference.[37] Spectrum management is a crucial CEMA-enabling activity that persists from capability development, acquisition and use, through to disposal. During military operations,

3

....

33 *Ibid.*
34 *Ibid.*
35 *Ibid.*
36 *Ibid.*
37 Spectrum management is defined in Allied Communications Publication (ACP) 190(C), *Guide to Spectrum Management in Military Operations.*

CEMA provides a coordinating function through battlespace spectrum management (BSM) to enable effective use of the electromagnetic spectrum (EMS). The end-state is to enable the commander freedom of movement in the EME.

d. **Communications.** Increasingly, military communications (both human and machine) face external demands for EMS to be released for commercial use. Technological advances have led to an increase in spectrum-dependent systems for gathering and transferring information with force elements increasingly reliant on detailed, immersive graphics and videos, all of which need high-bandwidth communication channels. Communications needs to be coordinated with other EMS users, through CEMA, to gain spectrum understanding and to meet operational needs while ensuring that users in the UK or host nation are not adversely affected.

3.8. **Cyber activities.** Cyber operations are described as the planning and synchronisation of activities in, and through, cyberspace to enable freedom of manoeuvre and to achieve military objectives.[38] With the growth of mobile and wireless connectivity it is increasingly important to consider EMA when conducting these operations. Cyber operations are categorised into four distinct roles.[39]

a. **Offensive cyber operations.** These are defined as: activities that project power to achieve military objectives in, or through, cyberspace.

b. **Defensive cyber operations.** These are defined as: active and passive measures to preserve the ability to use cyberspace.

c. **Cyber intelligence, surveillance and reconnaissance.** This is defined as: intelligence, surveillance and reconnaissance activities in, and through, friendly, neutral and adversary cyberspace to build understanding.

....

38 *Cyber Primer,* 2nd Edition.
39 *Ibid.*

d.   **Cyber operational preparation of the environment.** This is defined as: all activities conducted to prepare, and enable, cyber intelligence, surveillance and reconnaissance, defensive and offensive operations.

Cyber operations enable freedom of manoeuvre and
the achievement of military objectives

Section 4 – Development summary

3.9.   Organisations and structures that define information operations, cyber operations and electronic warfare have evolved to fit a changing technological world. These actions and operations use cyberspace and the EME to operate across the five domains and co-exist in CEMA littoral areas.[40]

3.10.   The mainstay of CEMA is the synchronisation and coordination of, and with, activities both internal and external to CEMA.[41] CEMA depends on technical and procedural interoperability using standardised interfaces, protocols and approaches. This ensures information exchange across joint forces, coalition, government and industry partners, which in turn improves integration and fosters adaptability.

3.11.   **Cyber and signals intelligence.** Cyber operations and signals intelligence (SIGINT) are predominately reliant on the same infrastructure, organisations, access to personnel training and skill-sets. However, they must also be seen as complementary, and not competing capabilities. The key difference between cyber and SIGINT is the intent and effect of the two.

3.12.   **Information bearer.** The EMS can be used indirectly as a bearer of information, or directly as a means of creating an effect. As a bearer of information, be that voice communications or digital-based information systems, this is an example of where EMA and cyber share a littoral. Responsibilities within this function include security and resilience and this is where the overlap with cyber is greatest. Defensive cyber operations are an integral and non-discretionary component of network operations and security resilience.

3.13.   **Coordination and synchronisation of activities external to CEMA.** Information operations and activities are not included within CEMA but elements are closely associated with the CEMA cyber capability. There is a large amount of overlap with the key distinguishing feature between the

....

40   JCN 1/17, *Future Force Concept*, paragraph 3.1 lists the domains as air, land, maritime, space and cyber.
41   This is illustrated in Figures 2.1 and 2.2 in Chapter 2.

two areas being the scope of the operating environment. Whilst cyber operations take place in, and through, cyberspace, information operations can also use other means.

3.14.   **Centralised control, decentralised execution.** CEMA battlespace execution will require a command and control approach that emphasises centralised control but decentralised execution. As well as integrating our own offensive actions, we must be able to mitigate the threat from adversaries' cyber or electromagnetic weapons while preventing negative impact to, and from, friendly or neutral systems.

3.15.   **Development challenges for Defence.** The CEMA evolution required by Defence roles and responsibilities presents a change which needs support through all Defence lines of development. It also requires each of us to change, cognitively and behaviourly, so that CEMA becomes routine. This cannot be achieved wholly through training but comes from embracing change. It should be noted that human factors present the biggest impact to CEMA in terms of enabling or threatening its success.

3.16.   **Training and education.** To prevent CEMA remaining the preserve of technically capable and interested individuals a programme of training and education is key to the successful integration of CEMA if it is to be ingrained in routine.[42]

Training and education are key to ingraining CEMA

....
42   The 1* CEMA Training Group is co-chaired by the Head Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance and Cyber Joint User and the Commander Joint CEMA Group.

Addressing the weaknesses[43]

During the 2008 Georgian operation the Russian military identified several capability and organisational weaknesses and sought to address the causes. Although their response was not the same as this doctrine note discusses, it reflects their investment in the same operational arena. In a similar vein, the Russian military has supported a drive for a more 'joint' approach across the formerly stovepiped single Services. In addition, they have invested in specialist units notably across cyber, electronic warfare and strategic military communications. All of this is underpinned by a series of strategic and operational command and control programmes such as the National Defence Control Center. This, combined with a plan to replace 70% of old equipment by 2020, means that Russian electronic warfare capabilities will approach, or exceed, those of many North Atlantic Treaty Organization (NATO) members well before that date. In many ways, this, like the changes in capability development and acquisition, parallel those changes undertaken by NATO members, most notably the United States of America.

....

43   Based on Internet research pieced together for this joint doctrine note, an example of which is available at http://ssi.armywarcollege.edu/pdffiles/pub1069.pdf

Key points

- Both the cyber and the electromagnetic activities concepts are still maturing; so the adoption and implementation of the cyber and electromagnetic activities (CEMA) concept will benefit from an incremental development approach.

- A four level CEMA development approach is proposed.

- CEMA roles and responsibilities will evolve, driven by Defence, based on the CEMA vision and strategy.

- Realistic training must include security against third parties collecting cyber or electromagnetic environment data on our forces and the challenges of electronic warfare or offensive cyber systems degrading civil systems.

- CEMA battlespace execution will require a command and control approach emphasising centralised control, but decentralised execution.

- Human factors present the biggest impact to CEMA in terms of enabling or threatening the success of its use. Therefore implementing CEMA successfully relies on embracing cognitive and behavioural change to make CEMA an automatic action, not an additional task.

3

Planning and conducting

Chapter 4 explores the planning and conducting of cyber and electromagnetic activities to create strategic effect.

Chapter 4

4

4

"
The **whole** is **greater** than the
sum of its **parts.**
"

Aristotle

Chapter 4 – Planning and conducting

Section 1 – The chain of command

4.1.   A cyber and electromagnetic activities (CEMA) synchronisation and coordination group is needed to implement the national direction. This group will ensure all strategic and operational effect is mapped against higher intent. Figure 4.1 outlines a suggested functional organisation. The structure that the CEMA synchronisation and coordination group sits within is illustrative and will need to be endorsed. Once the CEMA intent is understood, sub-units or departments can plan and direct operations and activities across, and in collaboration with, other departments.
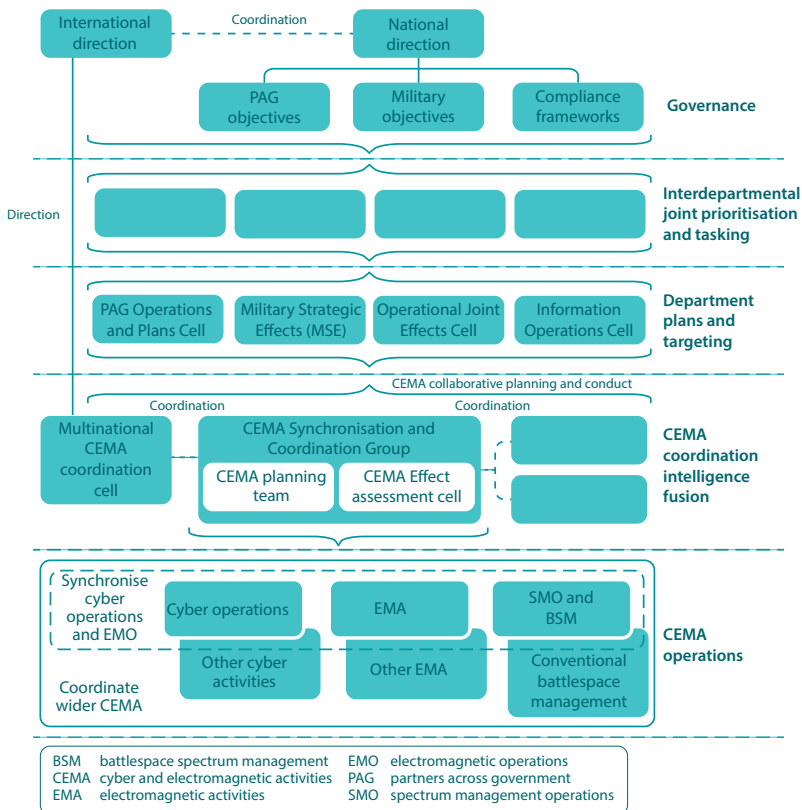

Figure 4.1 – CEMA functional organisation

4.2.   The planning and conduct of CEMA needs to be considered within strategic- and operational-level planning frameworks at a joint level. During the options development process, liaison and coordination between planning staff responsible for CEMA is paramount. This coordination will assess how these capabilities can be best used against the developing options or courses of action within legal boundaries or other restrictions. Force generation activities involving CEMA planning staffs are used to advise the commander on the CEMA component of the Whole Force, especially where deployed personnel numbers are fixed and where CEMA may be conducted with reachback to non-deployed CEMA specialists.

Section 2 – Synchronising and coordinating

4.3.   The synchronisation and coordination of CEMA within a joint force headquarters (JFHQ) can be conducted by the electromagnetic battlestaff (EMB) with cyber representation. The EMB structure uses and builds on the existing Electronic Warfare Coordination Cell (EWCC).[44] It is the role of the EMB to coordinate and monitor all aspects of electromagnetic activities within the electromagnetic environment on behalf of the Joint Forces Command (JFC) directorate staff.[45]

4.4.   Joint Concept Note (JCN) 1/17, *Future Force Concept*, states that 'Influence will only be achieved with a clear focus on audiences and effects, and by integrating and synchronising kinetic and non-kinetic activities conducted across the physical and virtual domains to try to achieve those

....

44   The Electronic Warfare Coordination Cell (EWCC) may comprise a liaison officer with reachback to supporting national bodies, or a staff of between three to as many as 12 or more, as necessary for a specific operation. Training is an essential element to EWCC where there is a need for highly skilled staff to carry out its activities. It is fundamental that in undertaking CEMA, extant functions such as EWCC are included. See Allied Joint Publication (AJP)-3.6, *Allied Joint Doctrine for Electronic Warfare,* Edition B, paragraphs 0205 and 0207 for more details.

45   Allied Joint Publication (AJP)-3.6 explains that electromagnetic battlestaff (EMB) would include members from the Joint Forces Headquarters (JFHQ) J3 (Operations), J5 (Planning), J2 (Knowledge) and J6 (Communications and information support) staff. The director of the EMB will be designated by J3. Note AJP-3.6, Edition C, was being drafted at the time of publishing.

effects.'[46] CEMA must be considered an integral part of joint action[47] and fully integrated alongside non-CEMA, sequencing and combining actions through the full spectrum approach to achieve the desired influence. Figure 4.2 provides an example of how CEMA may contribute to joint actions.
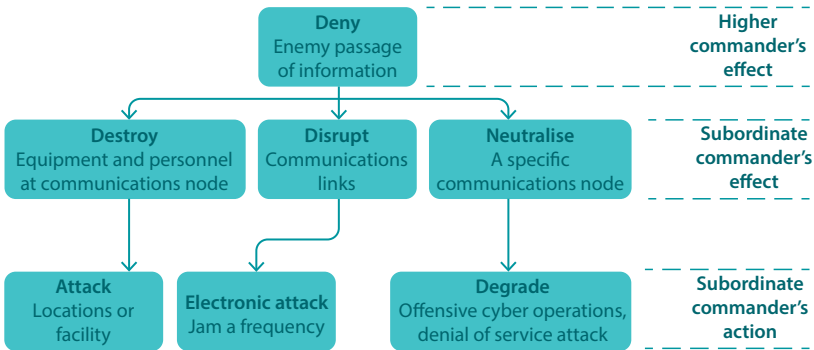

Figure 4.2 – An example of CEMA contribution to joint actions

4.5.   Under the full spectrum approach, and enabled by interoperable command and control systems, CEMA actions may be planned and conducted collaboratively. This can be carried out in a number of ways.

a.   **Action options against a single effect.** Rather than simply considering a kinetic action to create a desired effect, commanders should consider other effects, with CEMA providing these options. For example, if the target was in a non-combatant urban area an electronic attack or offensive cyber operations (OCO) may be more appropriate, according to the targeting policy.

b.   **Sequence of actions.** Where a commander may put into operation a series of interconnected actions to create effect. For example, OCO against several adversarial networks to shift communication onto a specific communications system, followed by the destruction of a

46   Influence is defined as: the capacity to have an effect on the character, or behaviour of someone or something or the effect itself. *Concise Oxford English Dictionary*, 12th Edition, 2011.
47   AJP-3(B), *Allied Joint Doctrine for the Conduct of Operations*.

number of soft-target nodes on that system, which further drives all communications onto a single, fortified node. Then at an appointed time, an electronic attack of that communication node leads to the adversaries' denial of communications or to the exploitation of their cyber intelligence.

c.   **Combination of actions.** For a large or complex target, the creation of a single action may not achieve the commander's intent. For example, a kinetic attack against a communications node will destroy a limited amount of equipment, but software-based system diagnostics may aid speedy recovery. However, when a kinetic attack is combined with an electronic attack that renders diagnostic software useless, repair may be impossible.

Section 3 – The recognised cyber and electromagnetic picture

4.6.   A common operational picture (COP) is a command and control tool that provides situational awareness as a graphical display, facilitating collaborative planning based on current or planned activities. A COP is defined as: an operational picture tailored to the user's requirements, based on common data and information shared by more than one command.[48] A COP is blended by Joint Task Force Headquarters on the basis of correlated, assessed and validated data from a variety of common tactical pictures with the graphic displayed dependent on the commander's requirement.[49]

4.7.   The requirement for a recognised electromagnetic picture (REMP) within a COP has been recognised and defined as: a complete and seamless depiction of the electromagnetic environment aiming at positively identifying and continuously tracking all the emitters and associated platforms and weapons in the area of responsibility.[50]

....

48   NATO*Term*.
49   Joint Doctrine Publication (JDP) 3-70, *Battlespace Management*, paragraph 118.
50   NATO*Term*.

UK and Afghan personnel plan operations in Afghanistan

4.8.   To support the planning and conduct of CEMA and to contribute to the COP, the REMP would need to include details of cyberspace activity, creating a recognised cyber and electromagnetic picture (RCEMP). The need for the RCEMP as a key enabler is identified and discussed in Joint Doctrine Publication (JDP) 0-50, *UK Cyber Doctrine*.

4.9.   The RCEMP, within a COP, will provide situational awareness and improved understanding of activities and entities[51] in cyberspace and the electromagnetic environment, enabling decision support and the selection of the correct CEMA effect. This enhanced situational awareness also provides for effective battlespace management and combat identification.[52]

4.10.   It would be preferable to create a RCEMP real time in an integrated system. However, the reality of dealing with multiple data sources across multiple classifications means that the best case for generating a RCEMP can only be near-real time (slightly slower than real time).

....

51   These entities are considered friendly, adversarial or neutral.
52   JDP 3-00, *Campaign Execution*, 3rd Edition (Change 1).

4.11.   Adding the RCEMP as a common tactical picture into the COP allows the joint force commander, subordinate staff, partners across government and non-governmental organisations tailored views based on a single data set. The arrangement is demonstrated in Figure 4.3.
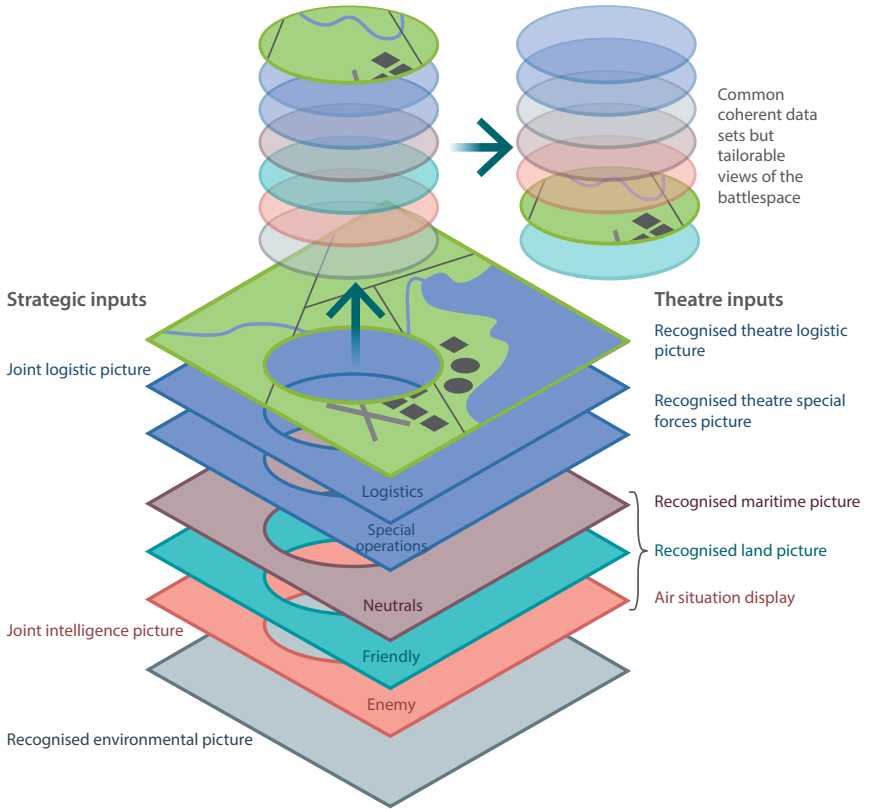

Figure 4.3 – The common operating picture without a recognised cyber electromagnetic picture

Assessing success

As discussed in earlier chapters, following Russia's efforts to reorganise its military structure and address capability shortfalls, it supported pro-separatist forces in Ukraine and deployed its own forces in Syria.[53] On these two operations, electronic warfare and cyber capabilities operated alongside conventional forces under what has been labelled the 'Gerasimov Doctrine' or non-linear war.[54] Non-linear war, upon examination, is not new; it bears many similarities to joint action and has at its heart a focus on coordinated and synchronised actions to achieve the commander's intent.

Inherent in the Gerasimov Doctrine is the exploitation of cyber to create effects that are consistent with Russia's reflexive control techniques. These are: constructive reflexive control in which "the enemy is influenced to voluntarily make a decision favourable to the controlling party"; and destructive reflexive control in which means are employed "to destroy, paralyse, or neutralise the enemy's decision making processes".[55]

Cyber and electronic warfare forces along with robust end-to-end military communications support are key to non-linear warfare. Pro-Russian forces made extensive use of unmanned aerial vehicles in both surveillance and coordination functions. Pro-Russian cyber operations were coordinated with electronic warfare and conventional activities, in contrast to the limited use in Georgia.[56]

Russia has continued development along lines where they appear to be overmatching the West and specifically the United States of America with electronic warfare and cyber coming to prominence.

4

53   More information is available at http://posse.gatech.edu/node/8732
54   More information is available at https://www.chathamhouse.org/publication/russias-new-tools-confronting-west
55   More information is available at http://cco.ndu.edu/Portals/96/Documents/Articles/russia%27s%20renewed%20Military%20Thinking.pdf
56   More information is available at http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

Key points

- A cyber and electromagnetic activities (CEMA) synchronisation and coordination group is needed to implement the national direction.

- CEMA must be considered an integral part of joint action and fully integrated alongside non-CEMA, sequencing and combining actions through the full spectrum approach.

- The planning and conduct of CEMA needs to be considered within strategic- and operational-level planning frameworks and appropriately resourced.

- A recognised cyber and electromagnetic picture (RCEMP) will provide a combined depiction of the cyber and electromagnetic environment.

- A RCEMP needs to be added to the common operating picture to define the totality of intelligence available.

4

Lexicon
Part 1 – Acronyms and abbreviations

AAP	Allied administrative publication
AJP	Allied joint publication
BSM	battlespace spectrum management
C4ISR	command and control, computers, communication, intelligence, surveillance and reconnaissance
CEMA	cyber and electromagnetic activities
CEMA CIG	Cyber and Electromagnetic Activities Capability Integration Group
COP	common operational picture
Cyber ISR	cyber intelligence, surveillance and reconnaissance
DCO	defensive cyber operations
DE&S	Defence Equipment and Support
DIN	Defence instructions and notice
Dstl	Defence Science and Technology Laboratory
EMA	electromagnetic activities
EMB	electromagnetic battlestaff
EME	electromagnetic environment
EMO	electromagnetic operations
EMS	electromagnetic spectrum
EWCC	Electronic Warfare Coordination Cell
FSA	full spectrum approach
GCHQ	Government Communications Headquarters
ISR	intelligence, surveillance and reconnaissance
JCN	joint concept note
JDN	joint doctrine note

JDP	joint doctrine publication
JFC	Joint Forces Command
JFHQ	joint forces headquarters
NATO	North Atlantic Treaty Organization
NDCC	National Defence Control Center
NSS/SDSR 15	National Security Strategy and Strategic Defence and Security Review 2015
OCO	offensive cyber operations
PAG	partners across government
PJHQ	Permanent Joint Headquarters
REMP	recognised electromagnetic picture
RCEMP	recognised cyber and electromagnetic picture
SIGINT	signals intelligence

Part 2 – Terms and definitions

This section is divided into two parts. First, we list new definitions introduced in this publication, as this is a joint doctrine note these definitions have not been ratified. Secondly, we list endorsed terms and their definitions which may be helpful to the reader.

New definitions proposed by this publication

cyber and electromagnetic activities
The synchronisation and coordination of offensive, defensive, inform and enabling activities, across the electromagnetic environment and cyberspace. (Cyber and Electromagnetic Activities Capability Integration Group (CEMA CIG) endorsed definition)

electromagnetic activities
All offensive, defensive and inform activities that shape or exploit the electromagnetic environment and the enabling activities that support them. (CEMA CIG)

Endorsed definitions

command and control communication system
A communication system which conveys information between military authorities for command and control purposes. (NATO*Term*)

communications intelligence
Intelligence derived from electromagnetic communications and communication systems. (NATO*Term*)

coordination
The organisation of different elements of a complex body or activity so as to enable them to work together effectively. (A working definition for this publication derived from the *Concise Oxford English Dictionary*, 12th Edition)

coordinating authority
The authority granted to a commander, or other individual with assigned responsibility, to coordinate specific functions or activities involving two or more forces, commands, services or organizations.
Note: The commander or individual has the authority to require consultation between the organizations involved or their representatives, but does not have the authority to compel agreement. (NATO*Term*)

cyber
To operate and project power in and from cyberspace to influence the behaviour of people or the course of events. (*Cyber Primer*, 2nd Edition)

cyber operations
The planning and synchronisation of activities in and through cyberspace to enable freedom of manoeuvre and to achieve military objectives.
(*Cyber Primer*, 2nd Edition)

Cyber operational preparation of the environment
All activities conducted to prepare, and enable, cyber intelligence, surveillance and reconnaissance, defensive and offensive operations.
(*Cyber Primer,* 2nd Edition)

cyberspace
An operating environment consisting of the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the physical, virtual and cognitive domains. (*Cyber Primer*, 2nd Edition)

defensive cyber operations
Active and passive measures to preserve the ability to use cyberspace.
(*Cyber Primer,* 2nd Edition)

electromagnetic environment
The totality of electromagnetic phenomena existing at a given location.
(NATO*Term*)

electromagnetic spectrum
The entire and orderly distribution of electromagnetic waves according to their frequency or wavelength. (NATO*Term*)

electronic attack
Use of electromagnetic energy for offensive purposes. (NATO*Term*)

electronic defence
Use of electromagnetic energy to provide protection and to ensure effective friendly use of the electromagnetic spectrum. (NATO*Term*)

electronic intelligence
Intelligence derived from electromagnetic, non-communications transmissions. (NATO*Term*)

electronic surveillance
Use of electromagnetic energy to provide situational awareness and intelligence. (NATO*Term*)

electronic warfare
Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects. (NATO*Term*)

intelligence
The directed and coordinated acquisition and analysis of information to assess capabilities, intent and opportunities for exploitation by leaders at all levels. (JDP 2-00, 3rd Edition)

offensive cyber operations
Activities that project power to achieve military objectives in, or through, cyberspace. (*Cyber Primer*, 2nd Edition)

signals intelligence
Intelligence derived from electromagnetic signals or emissions.
Notes: The main subcategories of signals intelligence are communications intelligence and electronic intelligence. (NATO*Term)*

synchronisation
Cause to occur or operate at the same time or rate. (*Concise Oxford English Dictionary,* 12th Edition)