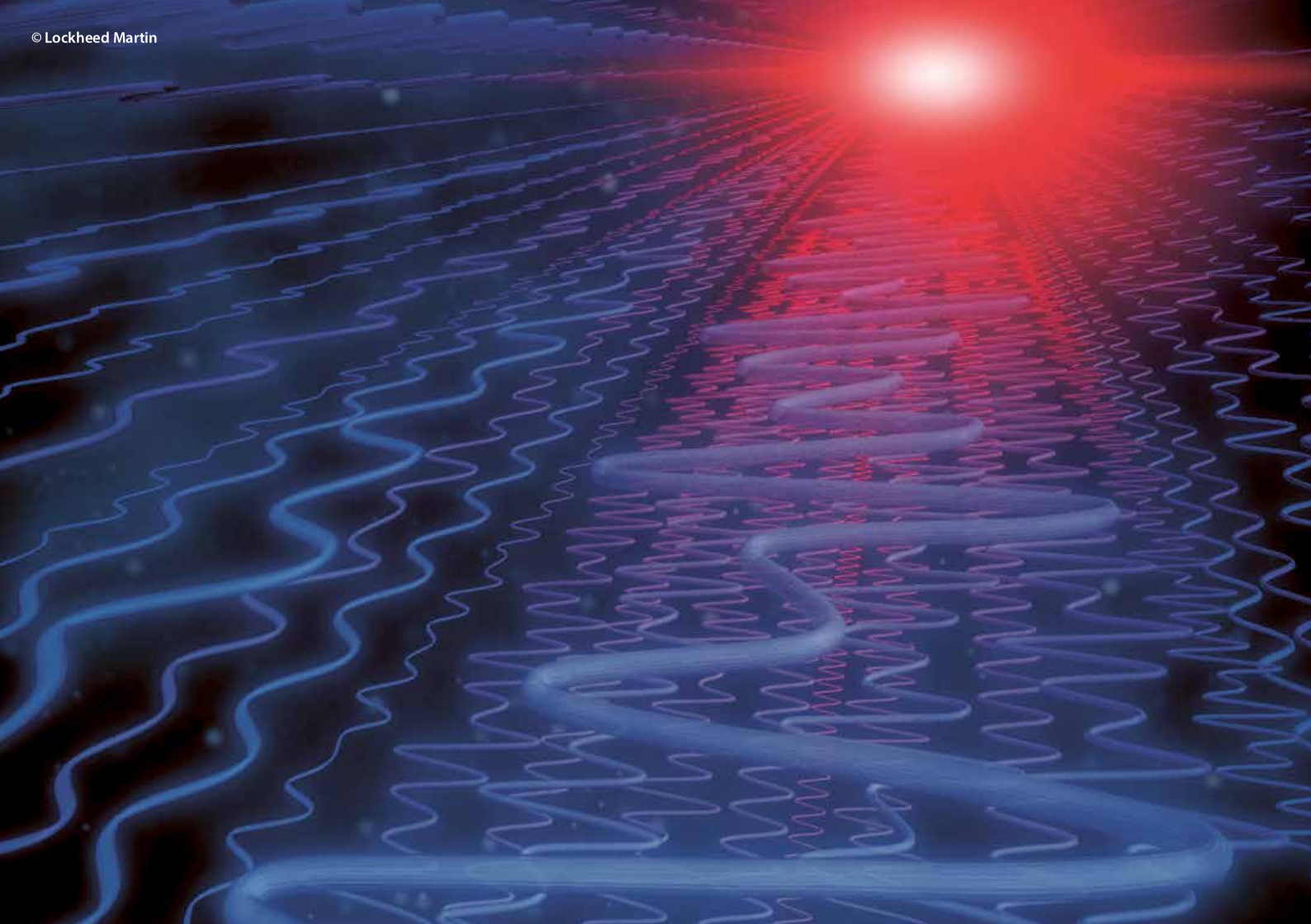
© Lockheed Martin

Superiority in the Electromagnetic Spectrum – Panel Introduction

XIV

With an Emphasis on Electronic Warfare

By Maj Andreas Wurster, GE Army
Joint Air Power Competence Centre

'The EMS is the cross-domain and fundamental glue which binds the other operating domains of Air, Land, Maritime, Cyber, and Space.'[1]

Introduction

The Joint Air & Space Power Conference 2021 will offer a platform to reflect upon various aspects of delivering NATO Air & Space Power at the Speed of Relevance. One of these aspects is the challenge for the Alliance to achieve operational superiority in the Electromagnetic Spectrum (EMS) using different means. One important pillar in this effort is the support of all divisions of Electronic Warfare (EW): Electronic Countermeasures, Electronic Protective Measures and Electronic Warfare Support.[2]

Due to NATO support for missions in the fight against terrorists and non-state groups since the beginning of the century, the subject matter has been pushed out of the focus of the Alliance. Opponents like the Taliban

in Afghanistan or Islamic State of Iraq and Syria (ISIS) are only rudimentarily able to operate in the EMS. This situation changed in 2014, due to the illegal and illegitimate annexing of Crimea by Russia and the ongoing wide-ranging military build-up in the Black Sea Region. These events showed that Russia has become an increasingly capable adversary of NATO. Russia has focused on developing and deploying a vast array of EW systems in this area. The ongoing Conflicts in Ukraine and Syria have also confirmed the already presumed importance of EW in Russian military operations and the necessity for NATO to enter this competition.[3] China, the other rising power in the world,[4] has been focused on developing EW capabilities and training to operate in a complex Electromagnetic Environment (EME) since the early 2000s. In the past few years, the Chinese People's Liberation Army (PLA) deployed EW and Signal Intelligence (SIGINT) capabilities, which is the Intelligence derived from electromagnetic signals or emissions,[5] on the seven island-reef outposts in the South China Sea.[6] This has demonstrated the requirement for NATO to keep pace with the developments in this sector. All of these developments have been recognized by NATO and have triggered an alignment of the Alliance's mindset and strategy in this sector.

The Intangible EMS

The EMS, as the range of frequencies of electromagnetic radiation, is a fundamental component of the natural environment. The EMS includes radio waves, microwaves, heat radiation, visible light, ultraviolet radiation, x-rays, electromagnetic cosmic rays and gamma rays.[7] The EMS is the foundational medium of the EME, which is the totality of electromagnetic phenomena existing at a given location.[8] The military term for this is the Electromagnetic Operational Environment (EMOE), which is the space in which military functions are performed.[9] In modern warfare, EMS superiority is a leading indicator and fundamental component of achieving superiority in

Air, Land, Sea, Space or Cyberspace. The EMS not only provides the critical connective tissue that enables all-domain operations but represents a natural seam and critical vulnerability across joint force operations.[10]

VISION: Freedom of Action in the Electromagnetic Spectrum and How to Manage That

When dealing with the battlefield of the future, most agree that such a battlefield extends over all domains: Air, Land, Sea, Space and Cyberspace, which must be connected to enable effective and resilient C2. This connection between the domains can be achieved exclusively through the EMS. For NATO, the EMS is an essential part of military operations, so much so that many Allied leaders now see the EME as an operational environment and a part of the battlespace where friendly forces manoeuvre in time, location, and spectrum to create electromagnetic effects in support of the commander's objectives.[11] NATO EMS Strategy aims to exploit, access, and control the EMS where and when needed to achieve NATO Military Strategic objectives and ensure that it will remain the superior military force, postured to take advantage of the EMS with the ability to exploit, mask, and manoeuvre within a congested and contested EME. The strategy's overarching goals are: (1) institutional awareness and advocacy, (2) effective joint EMO, and (3) robust EMO capabilities. EMO includes any type of activity which deliberately transmits and receives electromagnetic energy in the EME for military operations.[12]

The EW Contribution

EW, which is the military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects, has been the traditional warfighting element within the EMS since the

beginning of the 20th century. Today, a tremendous technological revolution has led to the emergence of new advanced capabilities and functions in the EME such as Directed Energy Weapons (DEW) and low emission radars.[13] In the context of Alliance defence, potential adversaries have significantly more capabilities in the field of EW than terrorist groups and possess the ability to impact not only the Alliance military forces, but also the civilian populations upon whose will Alliance cohesion depends. Therefore, NATO recognizes EW capability as an essential tool for the full spectrum of operations and other tasks undertaken by the Alliance.[14] Within NATO, this effort is led by the NATO Electronic Warfare Advisory Committee (NEWAC) which is responsible for overseeing the development of NATO's EW policy, doctrine, and command and control concepts as well as monitoring EW support to NATO operations.[15]

The 'Cyber' Part of the EMS

Cyberspace has become an attractive domain of operations for power projection. It is the only domain which has been created by humans and is exclusively accessible over the EMS (e.g. copper wires, fibre optic cables, and microwave and satellite relays).[16] NATO, in 2016, declared Cyberspace an operational domain giving the Alliance significant opportunities and also confronting the Alliance with serious challenges. In the context of collective defence, it is essential to ensure resilience against enemy bot and algorithm-attacks in the grey zone, where the line between war and peace is more blurred. Competition short of open conflict is increasingly becoming the norm, and NATO must maintain the ability to command and control operations during a conflict or crisis. The challenges for NATO and individual member states can be summarized in how they preserve freedom of action and achieve strategic and operational advantage in and through EMS, taking into consideration legal implications, technical feasibility, and especially human factors. NATO can best address these

challenges if they are tackled by the Alliance and the member states in cooperation with industry and academic partners.

Conclusion

As the theme of the 2021 conference suggests, 'delivering NATO Air and Space Power at the Speed of Relevance' must be ensured. To achieve this goal, it is incontestable that the speed and reliability of data transmission within the EMS for all Alliance's issues across all domains is the key to success.

The following articles will introduce the reader to some important aspects of these challenges which will be the focus of a panel discussion during the JAPCC Conference:

- ACM Sir Stuart Peach (UK Air Force) provides a Senior Leader's Perspective regarding the EMS, EW and Cyberspace. In his article, ***NATO Electronic Warfare and Cyberspace Resilience***, he derives the necessity for NATO to achieve its vision of Cyberspace and EMS exploitation, access, and control when and where needed to achieve Alliance objectives.

- The next article, ***Speeding Up the OODA Loop with AI***, is written by Mr Owen Daniels. In the piece the author examines both conceptual and technological challenges to the Observe, Orient, Decide, and Act Framework, as well as potential implications for Alliance militaries.

- Lieutenant Colonel Paul J. MacKenzie (CA Air Force) outlines the relevance of ***Cyberspace in Cyberspace and Joint Air and Space Power***. The author presents the importance of cybersecurity in particular, from the early and slow-moving stages of Air and Space systems Research

and Development (R&D) to how activities in these phases can eventually influence the Air and Space power capability gaps with potential adversaries.

- In ***Electronic Protective Measures*** Mr Dirk A. D. Smith and Mr Steve Tourangeau examine the importance of terms within the subject area of EW. The article addresses the confusion with the terms Electromagnetic Protection (EP) and Defensive Electromagnetic Attack (DEA). The authors clears-up the definitions through examples of each and makes the obvious suggestion of what needs to be done.

- Then, Mrs Melinda Tourangeau describes in her article, ***Managing the Electromagnetic Spectrum***, NATO's dependence on the EMS. She describes the access to the EMS on its way to becoming a global public goods resource like clean water, safe food sources, and responsible industrial waste management. The confluence of disparate issues across a singular public good presents what is classically called a Large-Scale Collective Action Problem (L-SCAP), which the author discusses in more detail in her article.

- The final article, ***Security Convergence for Air and Space Power***, comes from Colonel Eric D. Trias and Colonel Martin L. Rothrock (US Air Force). The authors address the concept of security convergence of the three protection disciplines, namely physical, cyber, and Continuity of Operations (COOP).

Major Andreas Wurster (GE Army) is the Subject Matter Expert for Intelligence in the JAPCC. He graduated a two-year study in economic computer science at the Bundeswehr College for business and computer science. He has an Intel-SOF and airborne background and was deployed three times on NATO missions in Afghanistan.

Endnotes

1. Willis, Matthew and Stathopoulos, Panagiotis, 'The Necessity of Integrating the Electromagnetic Spectrum's Disciplines Under a Single Domain of Operations', JAPCC Journal, no. 30 (2020): p. 72–77.
2. NATO AAP-06, 'NATO Glossary of Terms and Definitions', Edition 2020, p. 47.
3. Smith, Patrick, 'Russian Electronic Warfare, A Growing Threat to U.S. Battlefield Supremacy', American Security Project (ASP), https://www.americansecurityproject.org/wp-content/uploads/2020/04/Ref-0236-Russian-Electronic-Warfare.pdf, accessed 26 Mar. 2021.
4. Stoltenberg, Jens, 'NATO Secretary General's Press Conference following the meeting of the NACinLondon, 3–4 Dec. 2019', https://www.nato.int/cps/en/natohq/opinions_171554.htm, accessed 25 Feb. 2021.
5. Ibid. 2., p. 118.
6. Dahm, J. Michael, 'A survey of Technologies and Capabilities on China's Military Outposts in the South China Sea', Johns Hopkins University, https://www.jhuapl.edu/Content/documents/EWandSIGINT.pdf, accessed 26 Mar. 2021.
7. Ibid. 2.
8. Ibid. 2., p. 46.
9. Ibid.
10. US Department of Defense, 'Electromagnetic Spectrum Superiority Strategy' Oct. 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2397850/electromagnetic-spectrum-superiority-strategy-released/, accessed 26 Mar. 2021.
11. von Spreckelsen, Malte, 'Electronic Warfare – The Forgotten Discipline', JAPCC Journal, no. 27 (2018): p. 41–45.
12. Ibid.
13. Stathopoulos, Panagiotis, 'The Dimension of the Electromagnetic Spectrum', Joint Air & Space Power Conference 2020 Read Ahead: p. 111–117.
14. NATO Topics, Electronic Warfare (last updated Nov. 2016) https://www.nato.int/cps/en/natohq/topics_80906.htm, accessed 23 Feb. 2021.
15. NATO Topics, The 107th NEWAC convenes in Brussels (last updated Nov. 2019) https://www.nato.int/cps/en/natolive/news_171280.htm?selectedLocale=en, accessed 23 Feb. 2021.
16. Ibid. 1.