CYBERDEFENSE REPORT

A Digital Army: Synergies on the Battlefield and the Development of Cyber-Electromagnetic Activities (CEMA)

Stefan Soesanto

Zürich, August 2021

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zürich

ETH zürich

Available online at: css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Stefan Soesanto

ETH-CSS project management: Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Benjamin Scharte, Head of the Risk and Resilience Team; Andreas Wenger, Director of the CSS.

Editors: Jakob Bund, Kevin Kohler, and Benjamin Scharte
Layout and graphics: Miriam Dahinden-Ganzoni

DOI: 10.3929/ethz-b-000502731

Table of Contents

Executive Summary

Over the past decade, the US Army has embarked on a massive effort to harness the synergies between cyber and electronic warfare. The conceptual foundations to develop cyber-electromagnetic activities (CEMA) were outlined within the US Army sometime between 2007 and 2010. By 2011, the term CEMA was doctrinally incorporated into several Army Field Manuals, and by 2015 the first experimental CEMA pilot units were stood up. This includes: the CEMA Support for Corps and Below (CSCB), the 915th Cyber Warfare Battalion, the Starblazor pilot that seeks to put code developers into the field, the I2CEWS within the newly created multi-domain task force, and the Department of the Army Strategic Operations, which oversees system requirements, interoperability, and the Army's digital and cultural transformation toward CEMA.

Driving the US Army's desire to adopt CEMA was likely a unique mix of events, lessons, learned, and operations conducted elsewhere. This likely ranged from PLA Major General Dai Qingmin conceptually thinking about "Integrated Network Electronic Warfare" (2000) and the Israeli air strike against the Syrian nuclear facility at Dayr az-Zawr (2007), to Russian military inadequacies during the Russo-Georgian war (2008), the deployment of Stuxnet against the Iran uranium enrichment facility at Natanz (2009-10), and the role of social media during the Arab Spring (2010-12).

The UK Ministry of Defense (MoD) conceptually introduced CEMA in 2016 and created a doctrine around it in the years 2017-2020. To date, there are no known experimental CEMA units the UK has stood up, nor has the term CEMA garnered visible traction in other UK MoD publications. The UK is currently the only NATO member that recognizes cyber-electromagnetic as one warfighting domain.

To figure out what other NATO members and services were thinking about CEMA, this report conducted interviews with eight respondents. Five respondents were active-duty personnel in the area of cyber and three respondents were former personnel on electronic warfare. The report also conducted an unstructured review of open-source material available on CEMA to find additional information. Overall, it can be said that while the concept of CEMA is known to other nations, its adoption is seen as resource-intensive, organizationally complicated, and to a degree unnecessary due to the types of conflicts some countries are politically willing to engage in.

UK doctrinal documents and US military writings provide some insights into envisioned rudimental CEMA tactics, such as sequencing attacks (e.g., signal herding), combination of actions, and blended/layered attacks.

Introduction

Cyber electromagnetic activities – or CEMA for short – is a doctrinal concept that was introduced by the US Army sometime around 2009/2010 to connect both domains at the hip. Initially, CEMA was envisioned solely as an organizational change to plan, coordinate, and deconflict non-kinetic US Army operations. In this setup, a military commander in the field would receive information as to how a certain action taken on the battlefield would resonate in cyberspace and the electromagnetic spectrum, including to what degree offensive cyber operations and electronic attacks could be helpful in supporting kinetic operations on the battlefield. Given the US Army's dependence on cyberspace and the electromagnetic spectrum for communications, lethality, sensors, and self-protection, the overarching doctrinal goal was that commanders would fully integrate CEMA within every operation and planning process.

Throughout the years, the US Army added several other components to increase the CEMA profile by experimenting, exploring, and creating more and more synergies between the Army's cyber and electronic warfare missions. Among other items, this has resulted in the formation of dedicated Army CEMA units – meaning offensive cyber operators deploying alongside electronic warfare operators in the field – specialized training programs to raise awareness of CEMA functions and effects. These efforts have even led to the renaming of job titles and Army career paths toward enabling CEMA.

Among the six service branches of the US military, only the US Army currently uses CEMA as a doctrinal concept to distinctly merge its cyber- and electronic warfare missions.[1] By contrast, the US Navy and US Marine Corps think in terms of "operations in the information environment" – or OIE for short – which is based on joint doctrine and much broader than CEMA. OIE for example includes propaganda, disinformation, narrative warfare, civil-military operations, and the whole outreach section of public and civilian affairs. In the OIE context, cyber and electromagnetic activities are a subset of tools to wage "information warfare" – i.e., "operation[s] to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[2] The US Air Force also follows the "information warfare" concept through what Lt. Gen Timothy Haugh calls "convergence." Created back in October 2019, the 16th Air Force is the pillar of how the Air Force thinks about synchronizing "Cyberspace; Intelligence, Surveillance, and Reconnaissance (ISR); Electromagnetic Warfare (EW); Information Operations (IO) – across the continuum of cooperation, competition, and conflict, and support[ing] the joint force's ability to compete, deter, and win wars across multiple domains."[3]

As of this writing, the Army essentially follows a dual path by (a) further adopting and refining CEMA (i.e., Army doctrine), while also (b) "evaluating whether OIE, [information warfare], or some other concept should replace [information operations] to describe an expanded Army mission in the [information environment]", effectively moving it closer to joint doctrine.[4] Part of that effort also encompasses solving the question as to what having an advantage in the information environment actually looks like, what capabilities it necessitates, and how it can be sensibly codified within Army doctrine.[5]

Among the NATO member states, CEMA has only been doctrinally replicated by the UK Ministry of Defense (MoD) back in 2016, when the UK officially recognized "cyber and electromagnetic" as its own warfighting domain alongside land, sea, air, and space. Some initial discussions on CEMA have also been held to varying degrees in France, the Netherlands, and Australia, to name a few. Yet, so far, these talks have not resulted in doctrinal publications or the build-up of dedicated CEMA units and distinct organizational fire and coordination functions on the battlefield.

[1] Note: CEMA is supposedly also a technical concept that allows for the development and exchange of capabilities across the services and in collaboration with international partners. The precise nature and actual extent of such cooperation is difficult to assess based on publicly available documents.

[2] Joint Chiefs of Staff, "Joint Publication 3-13 - Information Operations," 20.10.2014, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf, p. ix

[3] Timothy D. Haugh et al., "16th Air Force and Convergence for the Information War," Cyber Defense Review, Summer 2020, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Haugh_Hall_Fan_CDR%20V5N2%20Summer%202020.pdf?ver=2020-07-27-053232-357, p. 29

[4] Stephen G. Fogarty & Bryan N. Sparling, "Enabling the Army in an Era of Information Warfare," Cyber Defense Review, Summer 2020, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fogarty_Sparling_CDR%20V5N2%20Summer%202020.pdf, p. 18; For a comprehensive discussion on "information advantage" see: Christopher Paul, "Understanding and Pursuing Information Advantage," Cyber Defense Review, Summer 2020, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Paul_CDR%20V5N2%20Summer%202020.pdf?ver=2020-07-27-053231-950

[5] Mark Pomerleau, "US Army emphasizes 'information advantage,'" C4ISR.net, 25.05.2021, https://www.c4isrnet.com/information-warfare/2021/05/25/us-army-emphasizes-information-advantage/; Mark Pomerleau, "Army to set in stone the importance of information advantage, with new capabilities on deck," C4ISR.net, 01.07.2021, https://www.c4isrnet.com/information-warfare/2021/07/01/army-to-set-in-stone-the-importance-of-information-advantage-with-new-capabilities-on-deck/

Today, CEMA remains a niche subject that US defense media outlets only sporadically cover and whose discussion is entirely absent from the wider cyber defense and information security debates. The limited coverage of CEMA and non-adoption by US allies in both Europe (except the UK) and Asia, has spurred the rationale for this report to (a) explain the logics of CEMA, (b) derive its conceptual origin, and (c) outline its evolutionary path within the US Army and the UK Ministry of Defense.

Section one of this report starts with a short primer for the reader to understand the electromagnetic spectrum and the electronic warfare mission. Section two dives into the origins of CEMA within the US Army by contextualizing geopolitical developments and Army doctrinal changes over time. Section three explains why and how the US Army and UK MoD adopted CEMA. Section four then goes on to highlight potential CEMA tactics in the field. And section five concludes with final thoughts on whether emulating CEMA is an option that ought to be adopted by other armed forces.

Please note that this study will not consider in depth Chinese and Russian cyber and information warfare doctrine.

1 Primer: EMS, EW, A2AD, MDO

CEMA operates across two separate yet increasingly interconnected domains: cyberspace and the electromagnetic spectrum (EMS). Numerous militaries around the world have recognized cyberspace as a distinct warfighting domain in line with land, sea, air, and space. The EMS by contrast is only classified by many militaries as an operational environment – i.e., "a maneuver space consisting of all frequencies of EM radiation."[6]

For the purpose of this report, and within the context of CEMA (i.e., multi-domain operations), the EMS is deemed an operational warfighting domain. As such, this report endorses the definition put forward by Jeffrey Reilly, co-founder of the journal *Over the Horizon* that focuses on multi-domain operations and strategy, which describes a domain as "a critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission."[7]

The historic foundation of cyberspace was built upon the telephone network. Those of us growing up in the 1980s and 90s will still remember connecting their modem to their computer, plugging it into the telephone wall socket, and hearing the all too familiar dial-up tones when the modem "shook hands" with the Internet to go online. If you do remember this, then you certainly also remember what would happen when someone in the house picked up the phone. The modem would disconnect, the Internet would "vanish", and only a healthy scream could rectify the mental breakdown.

But if you take a look around your home today, you will not encounter this problem anymore, partially because your router/modem is connected to a dedicated glass fiber line, the TV line (cable), or a telephone copper line (xDSL) that connects you to the Internet and the world wide web. However, there is also a second segment of infrastructure in your home that was not pervasive during the 1980s and propagates through the electromagnetic spectrum. This includes all of your wireless peripheral devices that connect to your PC/laptop via Bluetooth; the numerous Wi-Fi connections that your router/modem is managing – including to your PC/laptop, cell phone, and Internet-of-Things (IoT) devices – the signal your cell phone uses to communicate with the nearest cell tower so you can make a call, surf the web, or set up a mobile Wi-Fi hotspot for other devices to connect to the web via your phone. It even includes the global position and timing signals coming from satellites in medium-Earth orbit that provide your cell phone and apps with location and timing data.

All of these wireless communications taking place in "the space in-between" are radio waves travelling at different modulations and frequencies to transmit data and other signals through the EMS. Within this radio wave spectrum – which includes all frequencies below 300 GHz – we find varying levels of frequency bands.[8] Wi-Fi and Bluetooth use frequencies in the ultra-high frequency band (300 MHz - 3GHz) and military satellites such as the Advanced Extreme High-Frequency (AEHF) system – which consists of six military communication satellites in geostationary orbit that provide "secure, survivable and near-worldwide satellite communications" – utilize super high-frequency range

[6] See: Joint Chiefs of Staff, "Joint Publication 3-85 - Joint Electromagnetic Spectrum Operations," 22.05.2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf?ver=2020-04-09-140128-347, p. I-1; For a discussion on whether the EMS should be a domain see for example: Sydney J. Freedberg Jr, "Spectrum (EW) Should Be A Warfighting Domain: Rep. Bacon," 29.11.2017, https://breakingdefense.com/2017/11/spectrum-ew-should-be-a-warfighting-domain-rep-bacon/

[7] Jon Farley, "Reilly Multi Domain Final," 09.04.2018, https://www.youtube.com/watch?v=jcTicq1BagM, time: 9:41-10:00; For more see: Jared Donnelly & Jon Farley, "Defining the "Domain" in Multi-Domain," 17.09.2018. https://othjournal.com/2018/09/17/defining-the-domain-in-multi-domain/; Erik Heftye, "Multi-Domain Confusion: All Domains Are Not Created Equal," 26.05.2017, https://thestrategybridge.org/the-bridge/2017/5/26/multi-domain-confusion-all-domains-are-not-created-equal; Note: This report disagrees with Reilly's assertion that cyberspace is not a distinct domain.

[8] From 300 GHz to 3000 GHz the EMS includes infrared, visible light, ultraviolet, X-rays, and Gamma rays.

(3 GHz – 30 GHz) and extreme high-frequency range uplinks (30 GHz – 300 GHz).[9]

. On the other hand, if you are underground in a mine or are exploring a cave you will likely have special radios communicating in the very-low frequency band (1-30 kHz) that can penetrate through earth and rock. Similarly, if you are serving on a submarine, you will have communication equipment that can send and receive super low frequency radio waves (30-300 Hz) through water. The vast majority of wireless devices have their own dedicated frequency band. For example, garage door openers and alarm systems operate around 40 Hz, baby monitors around 49Hz, and wildlife tracking collars at 215-220 MHz.

The entire EMS spans all frequencies of electromagnetic radiation from zero to infinity. It includes radio waves, microwaves, infrared, visible light, ultraviolet, X-ray, and Gamma-rays. The US Armed Forces are highly dependent upon access to the EMS across every domain. Uses range from tactical radios in the field (radio waves) to radar to track and identify targets (microwaves), infrared- and night vision goggles (infrared), electro-optical scopes (visible light) and ultra-violet missile seekers (ultraviolet).

The US Army defines electronic warfare (EW) as all "military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[10] EW is sub-divided into three tasks:

(a) **Electronic attack** is the "use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires."[11] This includes anything from electromagnetic jamming; position, navigation, and timing denial; electromagnetic deception; directed energy; to antiradiation missiles.

A practical example during peace time: In 2017, the automatic identification system (AIS) of at least 20 vessels in the Black Sea was jammed and spoofed to show all their positions to be near Russia's Gelendzhik Airport – 32 km inland.[12] As David Last, former president of the UK's Royal Institute of Navigation, concisely explained: "Jamming just causes the receiver to die, spoofing causes the receiver to lie."[13]

A practical example during war time: In Iraq and Afghanistan, the US Army used vehicle mounted and man-portable counter radio-controlled improvised explosive device electronic warfare (CREW) systems, that would jam a segment of radio signals which insurgents used to detonate improvised explosive devices (IEDs).[14] This cat and mouse game evolved over time with defenders adjusting their electronic countermeasures as insurgents transitioned from garage door openers and car alarm fobs to two-way radios and ultimately the mobile phone to trigger IEDs.[15]

(b) **Electronic protection** "involve[s] actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability."[16] This includes tasks such as electromagnetic spectrum management (i.e., deconfliction of spectrum usages and the prevention of spectrum interferences), electromagnetic hardening (i.e., resistance against ionized radiation), and emission control (i.e., controlling and reducing electromagnetic emissions to facilitate concealment).

(c) **Electronic warfare support** is defined as activities to "search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations."[17] This can include anything from a surface-to-air missile locking onto an aircraft to gathering electronic signatures for targeted identification purposes (ELINT) and signals intelligence collection.

In sum, the EMS enables a broad range of military capabilities, from communications, signals intelligence, and command & control, to sensing, navigation, and targeting. Since the first recorded EW applications in 1904 during the Russo-Japanese war (i.e., signals interception and jamming), militaries have been operating in the EMS spectrum.[18] The major challenge that modern warfare is facing – both now and into the

[9] Air Force Technology, "Advanced Extremely High Frequency (AEHF) Satellite System," airforce-technology.com, n.d., https://www.airforce-technology.com/projects/advanced-extremely-high-frequency-aehf/

[10] Headquarters, Department of the Army, "ATP 3-12.3 - Electronic Warfare Techniques," July 2019, https://armypubs.army.mil/epubs/dr_pubs/dr_a/pdf/web/arn18105_atp%203-12x3%20final%20web.pdf, p.1-1

[11] Joint Chiefs of Staff, "Joint Publication 3-13.1 – Electronic Warfare," 08.02.2012, https://fas.org/irp/doddir/dod/jp3-13-1.pdf, p. I-5

[12] David Hambling, "Ships fooled in GPS spoofing attack suggest Russian cyberweapon," 10.08.2017, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

[13] *Ibid*.

[14] Robert K. Ackerman, "Iraq Hones Army Electronic Warfare," 06.2007, https://www.afcea.org/content/?q=iraq-hones-army-electronic-warfare

[15] Army Technology, "Big bang theory: IEDs and military countermeasures," 18.08.2011, https://www.army-technology.com/features/feature127559/

[16] Joint Chiefs of Staff, "Joint Publication 3-13.1 – Electronic Warfare," 08.02.2012, https://fas.org/irp/doddir/dod/jp3-13-1.pdf, p. I-5

[17] *Ibid*.

[18] In January 1904, the British ship HMS Diana was able to intercept Russian wireless signals that were sent out to mobilize the Russian fleet for the Russo-Japanese War. In April 1904, the Russian defenders

future – is how militaries survive, operate, and win in highly congested, contested, and complex EMS environments. For the US Armed Forces this is of particular importance, given their past experiences in expeditionary campaigns and global alliance commitments within the context of a rising great power and peer-adversarial ambitions within regional theatres. For more than a decade, elements of a highly-contested EMS environment were understood to fall under the umbrella of so-called Anti-Access/Area Denial (A2/AD). The term describes a collection of strategies, technologies, and systems with increased range and lethality, that are designed to prevent opposing forces from maneuvering to or within an operational area. In the context of defeating A2/AD, the US Navy and US Air Force went on to develop the concept of AirSea Battle (ASB) in 2009. ASB's vision essentially encompasses networked, integrated, and attack-in-depth operations across all the interdependent warfighting domains (air, maritime, land, space, and cyberspace), to disrupt, destroy, and defeat A2/AD capabilities.[19]

In recent years however, the term A2/AD has come under increased scrutiny due its lack of a precise definition. US Chief of Naval Operations Adm. John Richardson, for example, wrote back in 2016 that "[t]o some, A2AD is a code-word, suggesting an impenetrable 'keep-out zone' that forces can enter only at extreme peril to themselves. To others, A2AD refers to a family of technologies. To still others, a strategy. In sum, A2AD is a term bandied about freely, with no precise definition, that sends a variety of vague or conflicting signals, depending on the context in which it is either transmitted or received."[20] Richardson would go on to eventually ban the usage of the term A2AD within the US Navy.[21]

With no real alternative terminology replacing A2AD, the discussions surrounding improving EMS capabilities and consolidation EMS operations oversight were left lingering as the DOD churned out EMS strategy after EMS strategy in 2013, 2017, and 2020. The latest strategy was criticized by members of Congress and outside analysts for lacking the teeth to realize its ambitious goals. Speaking at the Hudson Institute on 11 May 2021, former one-star Air Force electronic warfare officer and current House Representative Don Bacon (R-NE) noted that "we have had to force this on the services and the Joint Staff … if it wasn't for Congress, none of this would be done."[22] On 5 August, the Department of Defense (DoD) finally released its still classified implementation plan for the EMS Strategy 2020.[23] Time will tell if the plan will reinvigorate EMS operations and EW in the joint force.

By contrast, CEMA as envisioned by the US Army moved from the initial ideas of jointness and combined arms operations to fully endorsing the concept of multi-domain operations (MDO) – which describes "how Army forces fight across all domains, the electromagnetic spectrum (EMS), and the information environment and at echelon."[24] As pamphlet 525-3-1 by the Army's Training and Doctrine Command (TRADOC) explains: "When necessary, Army forces penetrate and dis-integrate enemy anti-access and area denial systems and exploit the resultant freedom of maneuver to achieve strategic objectives. […] The Army solves the problems presented by Chinese and Russian operations in competition and conflict by applying three interrelated tenets: calibrated force posture, multi-domain formations, and convergence."[25] It is within these three tenets that CEMA units are currently being developed, organized, and experimented with, to eventually be deployed on the battlefield of tomorrow.

Although the US Army does not explicitly state the exact conflict scenarios it expects MDOs to engage with in the future, we can to a certain degree infer that those will be fought at the temporal edge (i.e., high speed maneuver and rapid decision-making), in a contested environment marked by degraded information, intelligence, logistics, and mobility. Depending on adversarial capabilities, operating in such an environment will necessitate that units can operate and decide somewhat independently to exploit adversarial weaknesses, wherever and whenever they occur. Sensing, understanding, deciding, and acting faster than the adversary will become crucial to advance Army objectives and wining adversarial engagements. Offensive cyber operations and EW are of particular importance in in this context, as cyber operations rise

at Port Arthur successfully jammed Japanese naval communications that were trying to correct the artillery fire directed against the city.

[19] Air-Sea Battle Office, "Air-Sea Battle – Service Collaboration to Address Anti-Access & Area Denial Challenge," May 2013, https://dod.defense.gov/Portals/1/Documents/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf, p. 4

[20] John Richardson, "Chief of Naval Operations Adm. John Richardson: Deconstructing A2AD," The National Interest, 03.10.2016, https://nationalinterest.org/feature/chief-naval-operations-adm-john-richardson-deconstructing-17918

[21] Christopher P. Cavas, "CNO bans 'A2AD' as Jargon," Defense News, 03.10.2016, https://www.defensenews.com/naval/2016/10/04/cno-bans-a2ad-as-jargon/

[22] Mark Pomerleau, "Congress can't 'take foot off the gas' on DoD electronic warfare," C4ISR.net, 12.05.2021, https://www.c4isrnet.com/electronic-warfare/2021/05/12/congress-cant-take-foot-off-the-gas-on-dod-electronic-warfare/

[23] Mark Pomerleau, "DoD pledges militarywide alignment on electromagnetic spectrum ops," C4ISR.net, 05.08.2021, https://www.c4isrnet.com/electronic-warfare/2021/08/05/new-plan-dod-pledges-militarywide-alignment-on-electromagnetic-spectrum-ops/

[24] TRADOC, "The U.S. Army in Multi-Domain Operations 2028," Army.mil, 06.12.2018, https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf, p. 5

[25] *Ibid*., p. vii

and fall depending on their access to the EMS in theater and tactical operations. So, for example, Army CEMA units will be looking at manipulating and degrading adversarial communication systems, sensors, information, etc. to confuse or even command adversarial assets.

Notably, civilian infrastructure – particularly in the context of urban warfare – will highly likely not escape physical destruction in such a conflict scenario, nor will it be spared from being targeted by electronic warfare measures and offensive cyber operations executed from the homeland (i.e., stand-off cyber operations). Accordingly, the envisioned conflicts of the future will highly likely not be exclusively fought on some distant battlefield but will also drag from house to house and street to street in tomorrow's megacities.[26] That being said, it is still unknown how military targeting procedures, and the laws of armed conflict will evolve as CEMA operations are used in these highly digitalized urban environments.

2 The Doctrinal Origins of CEMA

The specific term "cyber-electromagnetic activities" was conceptually developed by the US Army sometime between the first withdrawal of US military forces from Iraq in 2007 and the creation of US Army Cyber Command in early 2010. While there are no publicly available documents that pinpoint when exactly the Department of the Army came up with the idea of CEMA, we can to some extent retrace the Army's logic for marrying cyber and electromagnetic activities.

2.1 CEMA and the US Army

With the eruption of the insurgencies in both Iraq and Afghanistan back in 2003, the US Army had to significantly re-invent and rebuild its electronic warfare capabilities and systems. Defeating an adversary that soldiers could see and engage on a clearly defined battlefield was one thing. But hunting down insurgents and protecting military patrols in urban environments against remotely detonated IEDs was quite another. Not only did the need for mobile EW capabilities to protect lives and limbs by disrupting adversarial communications skyrocket, but also the training of Army soldiers in the basic understanding of EW and what EW can bring to the battlefield grew exponentially.[27]

As a result of this re-emerging need for mobile EW systems, EW knowledge, and EW professionals, the Army gained a renewed interest in the overall funding, growth, and appreciation of a variety of EW capability usages for future conflicts.

With the beginning of the withdrawal from Iraq and Afghanistan in 2007 and 2011, respectively, the DoD slowly shifted priorities from counter-insurgency operations back toward regional great power competition and defeating near-peer adversaries in unified land operations. In other words, the Army had to reposture itself while also trying to retain the EW knowledge and valuable EW lessons it had learned over the past decade. However, as Maj. Michael Senft, functional Area 24 program manager at the Office Chief of Signal, explained in the *Cyber Defense Review*, "with less than 1,000 officers, warrant officers and enlisted personnel, the EW career field has struggled with finding its role as combat deployments have significantly decreased. As a result, when not deployed, EW personnel are often assigned to other duties, resulting in EW is often derided [sic] as standing for 'extra worker'."[28]

With defense budget cuts looming and electronic warfare being viewed as the ugly and outdated cousin of the more attractive and glittering cyber field, the idea formed within the Army to attach EW and cyber at the hip.

On the cyber end of the equation, the Army was well-positioned to foresee the "increasing global scope of the cyberspace mission," given that then Army Lt. Gen. Keith Alexander began his stint as the longest-serving Director of the NSA in 2005 and also became Commander of the Joint Functional Component Command-Network Warfare (JFCC-NW) in 2008.[29] In February 2010, the Army Chief of Staff approved and directed the establishment of Army Force Cyber Command (ARFORCYBER) at Fort Meade and the Army Cyberspace Operation and Integration Center (ACOIC) at Fort Belvoir.[30] ARFORCYBER was subsequently created on 21 May 2010, and ACOIC declared initial operating capability on 30 June. On 1 October 2010, the Army

[26] See: Modern War Institute at West Point, "Urban Warfare Project," https://mwi.usma.edu/urban-warfare-project/

[27] Adrienne Moudy, "Untold Stories from Electronic Warfare Soldiers," Army.mil, 21.08.2013, https://www.army.mil/article/109304/Untold_Stories_from_Electronic_Warfare_Soldiers/

[28] Michael Senft, "Convergence of Cyberspace Operations and Electronic Warfare Effects," Cyber Defense Review, 04.01.2016, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136055/convergence-of-cyberspace-operations-and-electronic-warfare-effects/

[29] US Army Cyber Command, "History," June 2020, https://www.arcyber.army.mil/Organization/History/; For a study outlining the history and development of US defense strategy in cyberspace see: Stefan Soesanto, "Trend Analysis: The Evolution of US Defense Strategy in Cyberspace (1988-2019), CSS Cyber Defense Project, August 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-The-Evolution-of-US-defense-strategy-in-cyberspace.pdf

[30] US Army Cyber Command, "History," June 2020, https://www.arcyber.army.mil/Organization/History/

designated ARFORCYBER and ACOIC to become part of a three-star command known henceforth as Army Cyber Command (ARCYBER) – an operational-level Army force reporting directly to the Headquarters of the Department of the Army (HQDA). As one of the four military service cyber components to US Cyber Command (USCYBERCOM), ARCYBER's support role evolved both in lockstep with the conceptual plans developed by USCYBERCOM – such as the Army contributing 41 of the 133 Cyber Mission Teams that make up the nation's Cyber Mission Force – as well as the Army's own vision to create a digital Army that is capable of operating, fighting, and winning in multi-domain operations.[31]

It is highly likely that the popular uprising during the Arab Spring in December 2010 reinforced and refined the Army's views on the need for multi-domain operations in different environments. Apart from the information warfare concerns (i.e., disinformation and propaganda), this might have spurred Army thinking about how to maneuver and operate in various theatres depending on the existing wired and wireless infrastructure within a target battlespace.

For example, we can roughly discern between urban and rural settings (population density), developed and under-developed spaces (infrastructure density), and data rich and poor environments (signal density). On the modern battlefield, the volatility of each of these three density metrics can rapidly change depending on the in- and outflux of populations and devices, as well as infrastructure availability. These variables in turn constantly reshape and transform the CEMA battlefield. As such, there is a discernable difference between the signal density and operational maneuvering opportunities against an adversarial battalion that stops and moves throughout a desert run and the signal density and maneuvering opportunities against an adversarial battalion deployed in a mega city, whose infrastructure is being bombed and shelled.

The Army's thinking on multi-domain maneuver and tactics was highly likely also influenced by Stuxnet – i.e., the offensive cyber operation widely believed to have been conducted by the NSA, Israel's Unit 8200, and Dutch intelligence, against Iran's uranium enrichment facilities in Natanz in 2009/2010.[32] While it is unclear what exactly the Army learned from Stuxnet, we can somewhat confidently presume that Army strategists explored initial ideas and concepts on the potential usages of forward deployed offensive cyber operators – or intermediaries – in the field, and how to pair those operators with other parts of the Army – such as EW.

When the Army talks about translating these rudimental ideas, new skills, and lessons learned into doctrine, we have to distinguish between small d doctrine and capital d doctrine.[33] Small d doctrine describes all the knowledge that has been written down in the Army's doctrinal publications. Whereas capital d doctrine encapsulates all the accumulated professional knowledge currently residing within the Army.[34] The discrepancy between the two terms somewhat explains as to why the Army's knowledge and ideas on CEMA only gradually enter the Army's doctrinal publications and has evolved from a rudimental framework at its onset to more substance over time.

What we definitely do know is that the Army's doctrinal changes to marry cyber and electronic warfare officially commenced when TRADOC released the Cyberspace Operations Concept Capability Plan 2016-2028 on 22 February 2010. The Capability Plan recognized that "Army forces are increasingly dependent on electromagnetic, computer network, and space-based capabilities that are converging; therefore exerting technical influence will require forces that are prepared to fight and win on an emerging 'cyber-electromagnetic battleground.'"[35] According to TRADOC, prevailing in this "cyber-electromagnetic contest means making progress at the same time along three lines of effort:

[31] US Army Cyber Command, "The Facts: Cyber Mission Force," Fact Sheet, 07.02.2020, https://www.arcyber.army.mil/Portals/34/Fact%20Sheets/Cyber%20Mission%20Force/ARCYBER%20fact%20sheet%20-%20Cyber%20Mission%20Force%20(7Feb2020).pdf?ver=9hogFsBylRoHHLJ0oN2MAQ%3D%3D; Army.mil, "2019 Army Modernization Strategy: Investing in the Future," n.d., https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf

[32] Kim Zetter & Huib Modderkolk, "Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran," Yahoo News, 02.09.2019, https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html; Kim Zetter, "Countdown to Zero Day - Stuxnet and the Launch of the World's First Digital Weapon," Crown, September 2015.

[33] Note: The distinction between the two terms is informal and does not reflect the Army's grammatical usage of the term doctrine.

[34] John Spencer, "What Does Army Doctrine Say About Urban Warfare?" MWI Urban Warfare Project podcast, 20.03.2021, https://open.spotify.com/episode/2ipg9at2vpkWOHbw3VPssj, time stamp: 5:22- 6:08; The Army defines doctrine per ADP 1-02 as: "Fundamental principles, with supporting tactics, techniques, procedures, and terms and symbols, used for the conduct of operations and as a guide for actions of operating forces, and elements of the institutional force that directly support operations in support of national objectives." See: Headquarters, Department of the Army, "ADP 1-01 - Doctrine Primer," July 2019, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18138_ADP%201-01%20FINAL%20WEB.pdf, p. 1-2

[35] US Department of the Army, "Cyberspace Operations Concept Capability Plan 2016-2018," TRADOC Pamphlet 625-7-8, 22.02.2010, https://fas.org/irp/doddir/army/pam525-7-8.pdf, p. 7

gaining advantage, protecting that advantage, and placing adversaries at a disadvantage."[36]

TRADOC's notion of a cyber-electromagnetic contest/battleground did not come out of nowhere. In November 2009, the US-China Economic and Security Review Commission prominently highlighted that "analysis of writings from authoritative PLA [China's People's Liberation Army] publications […] revealed the existence of a guiding PLA operational concept titled 'Integrated Network Electronic Warfare.' Integrated Network Electronic Warfare [INEW] incorporates elements of computer network operations in tandem with elements of traditional electronic warfare. […] The goal is to create a multispectrum attack on enemy command, control, communications, computers, intelligence, surveillance, and reconnaissance systems in the early stages of conflict."[37] INEW was conceptually developed by PLA Major General Dai Qingmin in April 2000 writing in the China Military Science journal. Writing in 2001, retired US Army Lt. Col. Timothy Thomas aptly observed that, "Dai broke tradition and advocated pre-emptive attack to gain the initiative and seize information superiority. This offensive emphasis contradicts China's military strategy of active defense."[38]

Notably, Dai's theoretical writings and the current existence of the PLA's Fourth Department – which is officially tasked with conducting electronic warfare and computer network attacks (CNA) – does not necessarily mean that the Chinese have figured out how to tactically and operationally marry EW and CNA. But, the mere existence of INEW as an operational concept and the PLA's modernization efforts, highly likely underpinned the US Army's thinking and need to prepare for a cyber-electromagnetic contest with its near-peer competitor in the Indo-Pacific.[39] As of this writing, it is still unknown as to how advanced the PLA's INEW concept is. Pentagon officials have long lamented that "the US lost the electromagnetic spectrum," as Alan Shaffer did in late 2014 when he was the Pentagon's research and engineer chief.[40] Similar views were most recently expressed by former director of electronic warfare in the Office of the Secretary of Defense, William Conley, who noted before the House Armed Services Committee in March 2021 that "the part that China did with their Strategic Support Force […] is first off, the blending of electronic warfare, cyberspace, and space operations as peers. And secondarily, the strategic elevation to say that this is strategically important and we are going to use it to achieve a strategic outcome. It's the combination of both of those things that I think are really important for operationally what they have been able to do. […] But what they have achieved operationally I think is really darn impressive."[41]

Prior to the release of the Army's Capability Plan, none of the Army's doctrinal documents attempted to marry cyber operations with electronic warfare. For example, the Army's Field Manual (FM) 3-36, titled "Electronic Warfare Operations" and published in February 2009, includes no references whatsoever to the cyber domain, cyber operations, or the CEMA concept. In fact, the term "cyber" is not mentioned once in the entire document.[42] Similarly, FM 6-02.70 on the "Army Electromagnetic Spectrum Operations" of 20 May 2010 does not mention cyber at all.[43]

Fast forward to 2011 and CEMA can be found everywhere in the Army's doctrinal documents. Most importantly, the Army's Field Manual (FM) 3-0 Change 1 of 22 February 2011, titled "Operations," broadly incorporates and highlights the importance of "cyber/electromagnetic activities."[44] FM 3-0 uses the term 43 times, which is significant considering that FM 3-0 is one of only two Army capstone doctrinal publications – the other being FM 1 on literally "The Army".

In the foreword of FM 3-0, then TRADOC Commander Gen. Martin E. Dempsey laid out the decision to "'unburden' the term information

[36] US Department of the Army, "Cyberspace Operations Concept Capability Plan 2016-2018," TRADOC Pamphlet 625-7-8, 22.02.2010, https://fas.org/irp/doddir/army/pam525-7-8.pdf, p. iv

[37] US-China Economic and Security Review Commission, "2009 Report to Congress," November 2019, https://www.uscc.gov/sites/default/files/annual_reports/2009-Report-to-Congress.pdf, p. 171

[38] Timothy Thomas, "China's Electronic Strategies," Military Review, May-June 2001, https://www.armyupress.army.mil/Portals/7/Hot%20Spots/Documents/China/Thomas-China-1999.pdf, p. 47

[39] Note: The mission profile of the PLA's 4th Department (4PLA) is rather broad. Depending on the source and translation used it veers between electronic warfare and radar, to information warfare, and computer network attacks. Over the years, components of the 4PLA were incorporated into the Strategic Support Force's (SSF) Network Systems Department.

[40] Sydney J. Freedberg Jr., "US Has Lost 'Dominance In Electromagnetic Spectrum': Shaffer," Breaking Defense, 03.09.2014, https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/

[41] US House Armed Services Committee, "Virtual Hearing: DoD Electromagnetic Spectrum Operations: Challenges and Opportunities," YouTube, 19.03.2021, https://www.youtube.com/watch?v=L3VaZMCp_dE, time stamp: 32:50-33:02

[42] Headquarters, Department of the Army, "Electronic Warfare in Operations," FM 3-36, February 2009, http://www.bits.de/NRANEU/others/amd-us-archive/fm3-36(09).pdf

[43] Headquarters, Department of the Army, "Army Electromagnetic Spectrum Operations," FM 6-02.70, May 2010, https://fas.org/irp/doddir/army/fm6-02-70.pdf

[44] Headquarters, Department of the Army, "Operations," FM 3-0 Change 1, 22.02.2011, https://www.globalsecurity.org/military/library/policy/army/fm/3-0/fm3-0_c1_2011.pdf

operations and regroup tasks under two headings: inform and influence activities (IIA) and cyber/electromagnetic activities."[45]

The underlying explanation for this doctrinal move was based on the notion that "[t]he impact of modern electronic and information technologies on human society and military operations increases daily. The electromagnetic spectrum is essential for communication, lethality, sensors, and self-protection. Army forces increasingly depend on cyberspace. Within cyberspace, units use electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems. Given the Army's dependence on cyberspace as well as the electromagnetic spectrum, commanders fully integrate cyber/electromagnetic activities within the overall operation. These activities employ a combined arms approach to operations in a contested cyberspace domain and a congested electromagnetic spectrum. Cyber/electromagnetic activities seize, retain, and exploit advantages in cyberspace and the electromagnetic spectrum. The result enables Army forces to retain freedom of action while denying freedom of action to enemies and adversaries, thereby enabling the overall operation."[46]

According to FM 3-0, cyber/electromagnetic activities consist of seven components: (1) cyber situational awareness, (2) networks operations, (3) cyber warfare, (4) electronic attack, (5) electronic protection, (6) electronic support, and (7) electromagnetic spectrum operations.[47] As this shows FM 3-0 still separates between cyber and EW as distinct professional disciplines necessitating different skills and different personnel. Curiously, the Information Operations Primer released on November 2011 by the US Army War College's Department of Military Strategy, Planning, and Operations notes that cyber electromagnetic activities encompass only six sub-components, namely "cyber network operations, cyber warfare, electronic attack, electronic protection, and electronic warfare support, and electromagnetic spectrum operations."[48] It is unclear why the Primer discounted cyber situational awareness, but it beautifully highlights the new complexities that the shift toward cyber/electromagnetic activities suddenly introduced into the Army's doctrinal thinking and overall organization and tactical understanding.

The new concept of cyber/electromagnetic activities cascaded throughout Army doctrinal documents. Looking back at the Army publications at the time, it becomes obvious that bits and pieces were introduced with little coherence.

FM 3-93 on "Theater Army Operations", for example, published in October 2011, outlines the creation of a dedicated CEMA section that would operate alongside a G6 (assistant chief of staff, signals), G7 (assistant chief of staff, inform and influence), and G9 (assistant chief of staff, civil affairs operations) within the Theatre Army Mission Command Cell.[49] It even envisioned the staffing of the CEMA section to consist of "a chief, a cyber electromagnetic operations and plans officer, a signals intelligence and electronic warfare support warrant officer, a cyber electromagnetic defensive analyst, and a cyber electromagnetic offensive analyst."[50] However, given that the term cyber electromagnetic activities was only recently introduced, it is highly unlikely that many of the positions outlined even existed or could be filled at the time.

FM 3-93 also introduced the CEMA working group, which is nowhere mentioned in FM 3-0 nor does it appear in any other publicly available Army documents in 2011. As FM 3-93 explains, "[t]he CEMA section coordinates, integrates, and synchronizes army, joint, multinational, and interagency CEMA capabilities to support theater army plans. The primary vehicle for doing this is the CEMA working group. The working group coordinates with both internal and external entities, including the targeting cell, and nominates targets for attack and exploitation. It also develops, prioritizes, and recommends CEMA targets, target sets, and target objectives to support campaign and contingency planning. It predicts, integrates, and synchronizes the effects of friendly and enemy CEMA with the G-2 intelligence operations section, the G-6 operations section, and the fires cell."[51]

Essentially, FM 3-93 envisioned a whole new organizational decision-making pathway to integrate CEMA into theatre planning structures at the headquarter level. As such, it simply stipulates that "the fires cell headquarters element coordinates and

[45] Headquarters, Department of the Army, "Operations," FM 3-0 Change 1, 22.02.2011, https://www.globalsecurity.org/military/library/policy/army/fm/3-0/fm3-0_c1_2011.pdf, Foreword; Note: On 26 May 2011, Gen. Martin E. Dempsey was nominated by President Obama to become the next Chairman of the Joint Chiefs of Staff.

[46] Headquarters, Department of the Army, "Operations," FM 3-0 Change 1, 22.02.2011, https://www.globalsecurity.org/military/library/policy/army/fm/3-0/fm3-0_c1_2011.pdf, p. 6-20

[47] Headquarters, Department of the Army, "Operations," FM 3-0 Change 1, 22.02.2011, https://www.globalsecurity.org/military/library/policy/army/fm/3-0/fm3-0_c1_2011.pdf, p. 6-21

[48] US Army War College, "Information Operations Primer – Fundamentals of Information Operations," November 2011 – AY12 Edition, https://apps.dtic.mil/dtic/tr/fulltext/u2/a555809.pdf, p. 74

[49] Headquarters, Department of the Army, "Theater Army Operations," FM 3-93, October 2011, https://fas.org/irp/doddir/army/fm3-93.pdf, p. 14-1

[50] *Ibid*., p. 14-2

[51] *Ibid*., p. 14-2

manages theater army fire support. Through the targeting process it also integrates cyber electromagnetic activities (CEMA) targeting with the CEMA section in the mission command warfighting cell."[52] The detail that FM 3-93 introduced into the Army's doctrine is somewhat surprising, but it also shows the bold ambition – and probably also lessons learned – for the necessity to coordinate non-kinetic fires and integrate them into theatre planning processes. What is even more curious is that FM 3-93 seems to be the only Army doctrinal publication in 2011 that extensively uses the abbreviation CEMA for cyber electromagnetic activities.

FM 3-0 was eventually superseded by the Army through a concept known as Doctrine 2015. As Ancker and Scully explain, "in 2009, senior leaders in the Army expressed a concern that soldiers were not reading doctrine due to the length of the manuals. […] As a result, in 2009 the Combined Arms Center began an effort known as 'Doctrine Reengineering.' Doctrine Reengineering was intended to reduce the number of field manuals, as well as review the size of the manuals."[53] The end product was a series of Army Doctrine Publications (ADP) that highlighted key fundamentals and principles, and associated Army Doctrine Reference Publications (ADRP) that expanded on the ADP's major topics.

In October 2011, the Army published ADP 3-0 – an only 29-page long document – that superseded the 174-page long FM 3-0. True to the goal of Doctrine 2015, the term "cyber" appears only three times and "cyber electromagnetic activities" are only mentioned once in the context of listing primary staff functions within mission command.[54]

A look into ADRP 3.0 on "Unified Land Operations", published in May 2012, provides a bit more insight. For instance, it finally introduced the official term of and definition for "cyber electromagnetic activities" into the Army's terminology.[55] Strangely though, the abbreviation CEMA is never used within the 76-page document. According to ADRP 3-0, cyber electromagnetic activities are defined as "activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. Cyber electromagnetic activities consist of cyberspace operations, electronic warfare, and electromagnetic spectrum operations."[56] In essence, ADRP 3-0 significantly slimmed down the CEMA definition found in FM 3-0 and reduced the seven previous CEMA components into three overarching categories. As of this writing, the CEMA definition found in ADRP 3-0 is the working definition used by the Army today.

ADRP also explains that "modern information technology makes cyberspace and the electromagnetic spectrum indispensable for human interaction, including military operations and political competition. These two mediums inherently impact the influence of an operational environment and will be simultaneously congested and contested during operations. All actors—enemy, friendly, or neutral—remain potentially vulnerable to attack by physical means, cyberspace means, electronic means, or a combination thereof."[57]

The inclusion of the term "political competition" is rather curious as FM 3-0 seemed to go to extraordinary lengths to stipulate the apolitical notions of "inform and influence".

Within the Army's doctrinal narrative on CEMA, the EW branch was central to its implementation to the extent that it *de facto* owned the entire process. US Army Cyber Command, by contrast, is not mentioned in any of the CEMA documents at the time. Nowhere does this become clearer than in FM 3-36 on "Electronic Warfare", published in November 2012. While it prominently includes CEMA, it also portrays it as a subtask within electronic warfare. For example, it notes that "the EW element, usually through the EW working group, leads and facilitates the integration of cyber electromagnetic activities (CEMA)."[58] Consequently, the CEMA working group that FM 3-93 outlined a year earlier is nowhere to be found. In fact, FM 3-36 goes so far as to note that, "the EW working group integrates and synchronizes information related to CEMA to achieve desired conditions in cyberspace and the electromagnetic spectrum. The EW working group seeks to unify the offensive and defensive aspects of CEMA

[52] *Ibid*., p. 11-2

[53] Clinton J. Acker & Michael A. Scully, "Army Doctrine Publication 3-0 – An Opportunity to Meet the Challenges of the Future," Military Review, January-February 2013, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20130228_art009.pdf, p. 39

[54] Headquarters, Department of the Army, "ADP 3-0 - Unified Land Operations," October 2011, https://www.army.mil/e2/downloads/rv7/info/references/ADP_3-0_ULO_Oct_2011_APD.pdf, p. 13

[55] Headquarters, Department of the Army, "Unified Land Operations," ADRP 3-0, May 2012, https://www.lsu.edu/hss/milsci/resources/adrp3_0.pdf, p. vi; Note: For a concise overview as to the measures and tasks encompassing CEMA as envisioned in 2011 see: Department of the Army Headquarters, "The Army Universal Task List," FM 7-15 Change 9, December 2011, https://www.bits.de/NRANEU/others/amd-us-archive/fm7-15C10%2812%29.pdf, p. 5-85 – 5-91

[56] Headquarters, Department of the Army, "Unified Land Operations," ADRP 3-0, May 2012, https://www.lsu.edu/hss/milsci/resources/adrp3_0.pdf, p. 3-3

[57] *Ibid*., p. 1-1

[58] Headquarters, Department of the Army, "Electronic Warfare," FM 3-36, November 2012, https://fas.org/irp/doddir/army/fm3-36.pdf, p. 3-1

(including cyber warfare, network operations, electronic attack, electronic protection, and electronic warfare support)."[59] In essence, FM 3-36 stipulated that the EW working group was the *de-facto* CEMA working group.

In February 2014, the Department of the Army eventually published FM 3-38 on "Cyber Electromagnetic Activities".[60] FM 3-38 is the first and to date one of only two doctrinal documents published by the Army exclusively devoted to CEMA. As such, it introduces the concept of CEMA, describes how the elements of CEMA function separately and together, and defines the respective roles and responsibilities of commanders and soldiers within the CEMA context. Notably, while FM 3-38 quotes ADRP 3-0 for the definition of CEMA, it slightly renames the three overarching categories into: "cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO)."[61]

Two points are of imminent importance when reading FM 3-38. First, FM 3-38 emphasizes that while "CO, EW, and SMO differ in their employment and tactics; […] their functions and capabilities must be integrated and synchronized to ensure synergy with one another and other combined arms capabilities."[62] The epitome of this is the CEMA working group – which includes anything from the Judge Advocate General staff, intelligence staff, air liaison officers, civil affairs staff, and many more, who are solely focused on optimizing decision-making and maximizing effects on the non-kinetic battlefield. Central to pulling together the strings for the CEMA element are four key personnel staff: the electronic warfare staff (which encompasses the central role of the electronic warfare officer (EWO)), the spectrum manager, the G2 (intelligence), and the G6 (signal). Notably absent from the mix is staff exclusively devoted to cyber operations – which echoes the EW ownership of the CEMA working group as outlined in FM 3-36. As per FM 3-38, the G2 (intelligence) is seen as the primary facilitator for cyber operations, as they coordinate with the intelligence community and military intelligence units (think NSA, US Cyber Command, and US Army Cyber Command), and can request reach back support on cyber operations.[63] In subsequent years, this conundrum will lead to EW/CEMA staff having to undergo additional training to familiarize themselves with the policies, regulations, and restrictions pertaining to offensive cyber operations to fulfill their CEMA function. Open-source reporting is unclear as to why US Army Cyber Command was not specifically represented by its own liaison officer within the CEMA working group. It might be that this was simply the easiest way to deconflict and engage the intelligence community on offensive cyber operations.

Second, because the functions of the CEMA Working Group are focused on planning, synchronizing, deconflicting, and complying with legal authorities to approve lethal and non-lethal fires, its role is not out on the front lines. As per FM 3-38, the Working Group only exists at the theater/field army (90,000+ soldiers), corps (45,000), division (15,000), and brigade level (5,000).[64] Meaning, Army doctrine did not yet envision mobile CEMA teams and detachments that would provide EW/cyber support and accelerated decision-making at lower level on the front lines. In subsequent years, the Army would embark on experimenting with different setups and units to broaden the scope of CEMA toward building a truly digital army whose units could operate somewhat independently, without querying the field commander for legal authorities pertaining to every CEMA action taken.

In December 2014, the Army published Army Techniques Publication (ATP) 3-36, which replaced FM 3-36 on "Electronic Warfare Techniques". Notably, ATP 3-36 officially clarified that "the CEMA working group replaces and assumes the duties and functions formerly performed by the EW working group."[65]

In April 2017, FM 3-12 on "Cyberspace and Electronic Warfare Operations" was published.[66] It is the second Army doctrine publication exclusively devoted to CEMA and supersedes FM 3-38. In contrast to FM 3-38, FM 3-12 acknowledges in its foreword that "[o]ver the past decade of conflict, the U.S. Army has deployed the most capable communications systems in its history. U.S. forces dominated cyberspace and the electromagnetic spectrum (EMS) in Afghanistan and Iraq against enemies and adversaries lacking the technical capabilities to challenge our superiority in cyberspace. However, regional peers have since demonstrated impressive capabilities in a hybrid operational environment that threaten the Army's dominance in cyberspace and the

[59] *Ibid.*, p. E-1

[60] Headquarters, Department of the Army, "Cyber Electromagnetic Activities," FM 3-38, February 2014, https://fas.org/irp/doddir/army/fm3-38.pdf

[61] *Ibid.*, p. 1-1

[62] *Ibid.*, p. 2-2

[63] *Ibid.*, p. 2-4

[64] US Department of Defense, "Military Units – Army," https://www.defense.gov/Experience/Military-Units/Army/; Headquarters, Department of the Army, "Cyber Electromagnetic Activities," FM 3-38, February 2014, https://fas.org/irp/doddir/army/fm3-38.pdf, p. 2-6

[65] Headquarters, Department of the Army, "Electronic Warfare Techniques," ATP 3-36 (FM 3-36), December 2014, https://www.bits.de/NRANEU/others/amd-us-archive/atp3_36%2814%29.pdf, p. 1-9

[66] Headquarters, Department of the Army, Cyberspace and Electronic Warfare Operations," FM 3-12, April 2017, https://fas.org/irp/doddir/army/fm3-12.pdf, p. vi

EMS."[67] Also, in contrast to FM 3-38 – which was prepared by the Army Combined Arms Center at Fort Leavenworth – FM 3-12 was put together by the Army Cyber Center of Excellence (CCoE) at Fort Gordon. This implies that sometime between 2014 and 2017, the CCoE took ownership over the process of developing CEMA doctrine.

In July 2019, the Army Cyber Center of Excellence published ATP 3-12.3 on "Electronic Warfare Techniques", which supersedes ATP 3-36.[68] One of the obvious changes the document introduced was the role of the cyber electronic warfare officer (CEWO). The CEWO replaced the position of the electronic warfare officer (EWO) within the CEMA working group. The name change led to a bit of confusion between the roles of the cyber electronic warfare officer (17B) and the cyber warfare officer (17A).[69] The latter being responsible for actually conducting offensive and defensive cyber operations, while the former is responsible for coordinating and planning CEMA activities. Eventually the title of cyber warfare officer was changed to cyber operations officer to likely clarify the distinction.[70] The Army CCoE currently maintains a special role within the CEMA context as it is responsible for "driving innovative concepts, doctrine, force structure, and capabilities for the Army and Joint forces," while also being responsible for education and training to establish "the essential foundations enabling execution of cyberspace operations and EW responsibilities as the Army's proponent."[71]

While ADP 3-0 of July 2019 did not introduce any major changes relevant to CEMA, it might be interesting to highlight three non-Army documents for contextual purposes. Joint Publication (JP) 3-12 on "Cyberspace Operations", published by the US Joint Chiefs of Staff in June 2018, does not include any reference to CEMA. On the other hand, JP 3-85 of May 2020, titled "Joint Electromagnetic Spectrum Operations" (JEMSO), mentions CEMA four times in the context of service support. It explains that "each Service has a different approach to organizing [electromagnetic spectrum operations]: Army commanders and their staffs conduct cyberspace electromagnetic activities (CEMA) to plan, integrate, and synchronize cyberspace and EW operations as a unified effort to project power in and through cyberspace and the EMS."[72] By contrast, "Electromagnetic maneuver warfare is the Navy's warfighting approach to gain decisive military advantage in the EMS and is the foundational concept that supports JEMSO."[73] And the "Air Force organizes to conduct EMSO primarily through the non-kinetic operations coordination cell (NKOCC) located in the air operations center."[74] As these differentiated approaches further underscore, the Army's CEMA doctrine and organizational effort to combine cyber and EW at the hip is unique to the Army and its land operations, even within the US Armed Forces.

However, this does not mean that CEMA is legally viewed by the Army as a unified arms approach in line with information-related capabilities (IRC) – i.e. "tools, techniques, or activities that are inherently information-based or primarily focused on affecting the information environment."[75] The Operational Law Handbook 2020, published by the Army's Judge Advocate General's Legal Center & School, specifically highlights that "Judge advocates should also be aware of the term cyberspace electromagnetic activities (CEMA). CEMA 'is the process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations.' CEMA is 'not an IRC in and of itself; cyberspace operations and EW operations are IRCs. Through CEMA, the Army plans, integrates, and synchronizes these missions, supports and enables the mission command system, and provides an interrelated capability for information and intelligence operations.'"[76]

Doctrine-wise, the story of CEMA as written down in US Army's doctrinal documents (capitalized D) ends here. But in the context of the small D doctrine, the story of CEMA is still being written as the Army is currently experimenting with units and organizational processes to figure out how to exactly leverage CEMA on the

[67] *Ibid*., Foreword

[68] Headquarters, Department of the Army, "ATP 3-12.3 - Electronic Warfare Techniques," July 2019, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18105_ATP%203-12x3%20FINAL%20WEB.pdf

[69] GoArmy, "17B Cyber and Electronic Warfare Officer," https://www.goarmy.com/careers-and-josbs/career-match/signal-intelligence/languages-code/17b-cyber-electronic-warfare-officer.html

[70] GoArmy, "Cyber Operations Officer," https://www.goarmy.com/careers-and-jobs/career-match/signal-intelligence/locations-stats-frequencies/17a-cyber-operations-officer.html

[71] US Army Cyber Center of Excellence, "Strategic Plan 2019," November 2018, https://cybercoe.army.mil/images/CyberCoE%20Documents/strategicplan2019_Final_08NOV18_2.pdf, p. 7, 10

[72] Joint Chiefs of Staff, "Joint Publication 3-85 - Joint Electromagnetic Spectrum Operations," 22.05.2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf?ver=2020-04-09-140128-347, p. viii

[73] *Ibid*., p. viii

[74] *Ibid*., p. viii-ix

[75] The Judge Advocate General's Legal Center & School, "Operational Law Handbook," National Security Law Department, 2020, https://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2020.pdf, p. 223

[76] *Ibid*.

battlefield. Section 3.1 of this report will outline the Army's approaches on this front.

To develop additional context, let us however first take a look at how the UK adopted CEMA doctrine and how a handful of other countries have been discussing CEMA.

2.2 CEMA and the UK MoD

In July 2016, the Development, Concepts and Doctrine Centre (DCDC) within the UK Ministry of Defense published the second edition of its Cyber Primer publication.[77] The Primer plays an important part in the MoD's Defence Cyber Programme and is formally tied to all future editions of UK cyber doctrine. The second edition is the first UK doctrinal document that introduces the term CEMA. Among the mere eight times the 100-page strong document uses the term CEMA, it explains that: (a) "the relationship between cyber and [electromagnetic activities] should be seen as one of resilience and complementary in nature rather than as one of competition," and that (b) CEMA "needs to be delivered in an increasingly coordinated manner within Defence."[78] As examples of potential CEMA synergy, the Primer mentions: (1) an "electronic attack [that] could be used to herd an adversary's communications onto a network already under surveillance;" and (2) a blended attack comprising cyber and electronic warfare means against an adversarial air defense system to create safer passage for attacking aircraft and destroying the enemy's situational awareness.[79]

In September 2017, the DCDC published Joint Concept Note (JCN) 1/17 titled "Future Force Concept". According to the UK's Joint Chief of Defense Staff the document "provides the principle Defence-level guidance and coherence for all future force development in the strategic headquarters and in all commands."[80] It is the first publicly available doctrinal document that in detail outlines the various aspects encompassing cyber and electromagnetic activities.[81] In fact, the entire section on the cyber domain is exclusively devoted to (a) introducing the CEMA approach, (b) explaining CEMA situational awareness, (c) CEMA integration and control, (d) CEMA specialists, (e) CEMA education, training and experimentation, and (f) CEMA resilience.[82]

Similar to US Army CEMA doctrine, JCN 1/17 envisions "standardize[d] interfaces, protocols and approaches to cyber and electromagnetic battlespace management that allow information exchange across joint forces" and allies.[83] At one point it even mentions "CEMA teams," which "will need to be multi-disciplined, highly trained (not just technically adept) and closely coordinated and deconflicted with other activity across all operational levels."[84] These CEMA teams likely include what JCN 1/17 calls CEMA specialists – ranging from "cyber specialists, electronic warfare, communications and EME management specialists, plus intelligence analysts."[85] This constellation sounds very similar to the US Army's CEMA working group. The document also highlights that "operations and planning teams must have sufficient expertise to ensure that CEMA is fully integrated into all joint action activities across all domains."[86]

In February 2018, the DCDC published Joint Doctrine Note (JDN) 1/18 titled "Cyber and Electromagnetic Activities."[87] While the document aims to "capture the widest concept of cyber and electromagnetic activities (CEMA) and draws together elements of existing doctrine and best practice," it also states that "the principles and concepts expressed are not yet wholly agreed."[88] As such, JDN 1/18 merely 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."[89]

[77] UK Ministry of Defence, "Cyber Primer – Second Edition," Development, Concepts and Doctrine Centre, July 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf

[78] *Ibid*. p. 61

[79] *Ibid*. p. 61, 77

[80] UK Ministry of Defence, "Concept Note 1/17 - Future Force Concept," Development, Concepts and Doctrine Centre, July 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf, Foreword

[81] Note: In 2017 the UK Ministry of Defence published Defence Instructions and Notices (DIN) 2017Din03-014 titled "Cyber and Electromagnetic Activities (CEMA) in Defence – Definition OS". As of this writing, the publication is not publicly available.

[82] UK Ministry of Defence, "Concept Note 1/17 - Future Force Concept," Development, Concepts and Doctrine Centre, July 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf, p. 20-24

[83] *Ibid*., p. 21

[84] *Ibid*., p. 20

[85] *Ibid*., p. 22

[86] *Ibid*., p. 22

[87] UK Ministry of Defence, "Joint Doctrine Note 1/18 – Cyber and Electromagnetic Activities," Development, Concepts and Doctrine Centre, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf

[88] *Ibid*., Preface

[89] *Ibid*.

Curiously, JDN 1/18 explains that the UK's "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 optimize the application of cyber and electromagnetic activities. The approach to this implementation should be driven by the CEMA Vision and Strategy."[90] In a corresponding footnote JDN 1/18 clarifies that "the strategy sets out a three phase, eight year programme," and that "at the time of publishing this joint doctrine note the strategy is awaiting endorsement."[91] As of this writing the UK MoD has not publicly released any documents titled CEMA Vision and Strategy.

JDN 1/18 provides the UK's CEMA definition as endorsed by the CEMA Capability Integration Group (CIG) as: "The synchronisation and coordination of offensive, defensive, inform and enabling activities, across the electromagnetic environment and cyberspace."[92] Although using different terminologies, the UK's CEMA definition is essentially the same as how the US Army defines and delineates CEMA. The only caveat that might be interesting to note is that in the UK's case "there are no approved definitions for either cyber activities or [electromagnetic activities]."[93]

Chapter four on planning and conducting for the first time envisions specific CEMA units and organizations within the chain of command. The document outlines a CEMA Synchronization and Coordination Group – including a CEMA planning team and a CEMA effect assessment cell – and a Multinational CEMA Coordination Cell that will conduct collaborative planning and targeting with already existing cells.[94]

Overall, however, it needs to be stressed that all CEMA elements mentioned in the document have not yet been endorsed nor functionally figured out. In fact, chapter three devotes a whole section to explain a development maturity progression framework for CEMA along four steps.

Actions under step 1 are rather unclear as it is only described as 'initial step' that takes place in the context of austerity under which resources and funding are already allocated across the current force. As such, "the ability to point to early realization of benefit will engender confidence in the [CEMA] concept."[95] Step 2 – the evolving step – "provides a substantial degree of synchronisation and coordination without re-designing cyber and electromagnetic force structures, funding lines and legal frameworks."[96] Step 3 – the integrated step – examines options in the context of the future force concept which "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."[97] And finally step 4 – the ubiquitous step – "recognises that there may be elements of cyber and electromagnetic activities (EMA) [that are] never fully integrated into CEMA."[98]

Sometime in 2018, the DCDC released an updated edition of its Joint Doctrine Publication 0-01.1 titled "UK Terminology Supplement to NATOTerm," which recognizes that "operational domains are maritime, land, air, space, and cyber and electromagnetic."[99] The Allied Joint Doctrine for the Planning of Operations (UK joint doctrine), released under the auspices of the NATO Standardization Office in May 2019, aligns with the UK's doctrinal decision to include the cyber and electromagnetic domain as its fifth operational warfighting domain.

Finally, in November 2020, the DCDC published JCN 1/20 – an experimental and ambitious concept - on "Multi-Domain Integration". The JCN explains that "the domains of space, and cyber, and electromagnetic, although mostly unseen, are already part of the competitive battlespace; more of the contest is virtual and involves information. Well-connected, and continually evolving, systems and networks will therefore be the key enablers in delivering precision, timing and especially targeted audience effect."[100] It also highlights that "the cyber and electromagnetic domain is ubiquitous and pervades all other domains; in all cases some degree of freedom of action in the cyber and electromagnetic domain is indispensable. The space and the cyber and electromagnetic domains underpin [multi-domain integration] with its emphasis on systems and networks and links to information activities; they are critical enablers and effecters, yet they are the least understood domains in UK Defence."[101] To overcome this lack of understanding, JCN 1/20 envisages a cultural

[90] *Ibid.*, p. 13

[91] *Ibid.*, p. 13, footnote 11

[92] *Ibid.*, p. 15

[93] *Ibid.*, p. 13

[94] *Ibid.*, p. 41

[95] *Ibid.*, p. 24

[96] *Ibid.*, p. 24

[97] *Ibid.*, p. 25

[98] *Ibid.*, p. 25

[99] UK Ministry of Defence, "Allied Joint Publication-5 – Allied Joint Doctrine for the Planning of Operations," NATO Standardization Office, Edition A Version 2 with UK national elements, May 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/837082/dcdc_doctrine_nato_planning_of_ops_ajp_5.pdf, p. Lex-13

[100] UK Ministry of Defence, "Joint Concept Note 1/20 – Multi-Domain Integration," Development, Concepts and Doctrine Centre, November 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950789/20201112-JCN_1_20_MDI.PDF, p. 6

[101] *Ibid.*, p. 18

change toward "much deeper multi-domain competence than is currently present across Defence."[102] In particular, it points out that "there needs to be an early and substantial improvement in understanding of the cyber and electromagnetic and space domains and how to integrate them. The educational foundation for this must be developed. This presents a much-increased demand on professional military education and is at least as important as any other capability requirement described."[103]

Most importantly, JCN 1/20 emphasizes that "while allies and adversaries generally recognise maritime, land, air and space, only the UK combines cyber and electromagnetic into one."[104]

Confusingly though, the UK MoD's 2021 paper titled "Defence in a Competitive Age" – which is the ministry's contribution to the UK's Integrated Review of Security, Defence, Development and Foreign Policy – states that "the electromagnetic environment, of which cyber is a part, is a fundamental aspect of the modern battlespace."[105] It is unclear to this author as to why that distinction was made, and why nowhere in the 76-page document CEMA is actually mentioned.

2.3 CEMA and Other States

This section provides a non-exhaustive overview of a handful of militaries that at one point or another publicly touched upon CEMA. It also summarizes interviews conducted with current and former military officers on the topic of CEMA non-adoption.

As of this writing, CEMA has not been emulated nor has it been widely adopted among NATO member states or many of the great powers of today. While China is embarking on its distinct vision of INEW, and Russia is refining what it calls "information confrontation" (*informatsionnoye protivoborstvo* or IPb), CEMA remains a concept that is specifically designed for the future trajectory of the US Army.

It should thus not come as a surprise that in several interviews with military officers from various nations, the reasons for CEMA non-adoption stretched from a wait-and-see approach – to appraise the tangible outcomes of CEMA – to viewing CEMA as purely offensive and expeditionary in character. Notably, most stakeholders were unfamiliar with the CEMA concept, nor could they pinpoint its exact purpose and function on the modern battlefield. Some even argued that they actually implemented CEMA-like concepts, but when pressed on specifics they pointed to disparate EW and cyber stovepipes that were not synchronized nor coordinated organizationally within combined arms operations. It certainly did not help that many respondents further explained that offensive cyber operations were a topic they could not freely talk about, and that generally electronic warfare took a backseat in their nation's doctrinal framework and capability development, limiting views of its importance in future conflicts. One respondent even argued that while cyber military exercises were geared toward building up offensive skills and coordination of defensive efforts among allies, the electronic warfare component was largely ignored – if not entirely neglected – in the playthrough scenarios. As such, the respondent explained that offensive cyber operations were largely envisioned as stand-off capabilities leveraged from the homeland rather than expeditionary ones that could be deployed at scale in the field alongside infantrymen and special forces operators. Another respondent explained that offensive cyber operations against mobile military units in the field were not a political priority nor a desired capability, because the cost-benefit calculation and Army's envisioned participation in future conflicts did not merit the development of CEMA solutions. In his view, kinetic options were far cheaper and easier to leverage, and their effects could be immediately determined and evaluated. Overall, it has to be said that many respondents felt uncomfortable to even talk about offensive cyber and electromagnetic activities, as well as their theoretical operational sequencing to take out an adversarial military target. Discussing CEMA operations that might be leveraged against civilian infrastructure was seen as a no-go during the interviews. Curiously, most respondents pointed to US doctrinal CEMA documents and were unaware that the UK MoD adopted CEMA for its future joint force.[106]

An unstructured open-source review confirms some of the interviewees' hesitation of endorsing CEMA doctrine.

In France, for example, the concept of cyber electronic warfare was briefly discussed back in November 2011 at a conference hosted by Le Centre de Recherche des écoles de Coëtquidan and Alliance GéoStratégique.[107] However, the idea of CEMA was not

[102] *Ibid*., p. 56

[103] *Ibid*., p. 56-57

[104] *Ibid*., p. 17

[105] UK Ministry of Defence, "Defence in a competitive age," Presented to Parliament by the Secretary of State for Defence by Command of Her Majesty, March 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971859/_CP_411__-_Defence_in_a_competitive_age.pdf, p. 45

[106] Interviews were held with eight respondents.

[107] Nicolas Caproni, "[Livre] Attention: Cyber! De la cyberguerre au combat cyber-électronique," Cyber-security.fr, 29.01.2014,https://www.cyber-securite.fr/2014/01/29/livre-attention-cyber-de-la-cyberguerre-au-combat-cyber-electronique/; Francois Chauvancy, "Cyberstratégie et colloque à l'Ecole militaire

further pursued in subsequent years for publicly unspecified reasons. Aymeric Bonnemaison and Stéphane Dossé – both former chef de corps of the 54th signal regiment – are two of the most prominent proponents for CEMA adoption in France. Both wrote a book together in 2014 titled "Attention: Cyber! Vers le combat cyber-électronique". More recently, Dossé wrote a chapter in 2019 for the French think tank Institut français des relations internationales (IFRI) titled "L'avènement du combat cyber-électronique." In the chapter, Dossé talks about the US Army's CEMA adoption but mentions in no part any steps the French Army has taken to adopt CEMA itself.[108] Thus, even though French doctrinal documents are sparse – both on cyber operations and electronic warfare – we can safely assume that the French armed forces have not adopted CEMA as of this writing.

In Australia, Jennifer McArdle, Assistant Professor of Cyber Defense at Salve Regina University, highlighted CEMA most prominently at the 2018 Royal Australian Air Force's (RAAF) Air Power Conference. McArdle talked about the need for Australian "military forces to train to fight in – and through – a contested environment saturated by adversary cyber and electronic operations."[109] She also made the point that training for cyber and electronic operations can serve as force multipliers on the modern battlefield. As examples McArdle mentioned (a) the 2007 Israeli airstrikes against Syria's nuclear facility at Dayr az-Zawr – in which "the Israeli's may have penetrated Syria's air defense network – for instance, transmitting malicious packets through the air defense system's radio-frequency (RF) signal via a stealthy unmanned aerial vehicle (UAV," and (b) Russian malware between 2014-2016 that was "covertly implanted on a legitimate Android application developed for the Ukraine artillery. […] the deployment of the malware likely facilitated Russian reconnaissance and superior targeting of Ukrainian artillery units."[110] Please note that the latter example is still highly disputed, with Crowdstrike standing by its malware analysis, while multiple information security researchers and Ukrainian sources question Crowdstrike's research findings.[111]

A deeper dive into deliberations in Australia on cyber and electronic warfare might be necessary to gain a full grasp, but apart from McArdle's presentation, no Australian publications stick out or are in part devoted to – what essentially amounts to – CEMA.

The Netherlands is probably the most interesting case. In January 2021, the Hague Center for Strategic Studies published a study titled "Naar een Cybercapaciteitenportfolio voor de Koninklijke Landmacht," (Engl.: "Toward a Cyber Capabilities Portfolio for the Royal Land Force"), which was commissioned by the Royal Netherlands Army to investigate (a) what the (possible) role of the Army can or should be in the cyber domain, and (b) what capabilities the Army should develop in order to achieve the appropriate effects for this role.[112]

To a large degree, the study tries to transpose CEMA into the context of the Dutch Army. As such, its CEMA-related recommendations are: (1) "Cyberspace and electromagnetic capabilities (together CEMA) should be integrated into land action doctrine as an essential element of coordinated and impact-based action, taking into account not only physical impact, but also the information dominance of the Army."[113] (2) "Expeditionary Cyber / CEMA Mission Teams that produce operational and tactical effects must have sufficient defensive and offensive freedom of action, also in the legal and political sense (mandate); have the right expertise and reachback capacity at the same time. These teams should be part of a broader Concept of Operations to be set up by [Dutch Cyber Command] and Operational Commands."[114] (3) "Cyber security and cyber operations must be approached as a specialism, but at the same time as part of the broader training set-up within the Army. This creates support and prevents cyber from being treated as an isolated or niche function."[115]

The study concludes by stating that "the [Dutch] Army is at the start of an equally urgent and long-term development process of clout in cyberspace and the

(Paris),"Theatrum Belli, 05.12.2011, https://theatrum-belli.com/cyberstrategie-et-colloque-a-lecole-militaire-paris/; Aymeric Bonnemaison & Stephane Dossé, "Attention, cyber - vers le combat cyber-électronique," Economica, 02.01.2014.

[108] Olivier Letertre et al., "Regards Croisés sur la Guerre Electronique," Etudes de l'Ifri – Focus Stratégique 90, July 2019, https://www.ifri.org/sites/default/files/atoms/files/letertre_justel_lechable_dosse_guerre_electronique_2019.pdf, p. 45-51

[109] Jennifer McArdle, "The Disruptive World and the Integrated Force: Achieving Readiness through LVC," in: Australian Department of Defence, Air Power Development Centre, "Air Power in a Disruptive World – Proceedings of the 2018 RAAF Air Power Conference," https://airpower.airforce.gov.au/sites/default/files/2021-03/CONF37-RAAF-Air-Power-Conference-2018-Air-Power-in-a-Disruptive-World.pdf, p. 118

[110] *Ibid*., p. 120

[111] Eduard Kovacs, "Experts Doubt Russia Used Malware to Track Ukrainian Troops," Security Week, 03.01.2017, https://www.securityweek.com/experts-doubt-russia-used-malware-track-ukrainian-troops; Oleksiy Kuzmenko, "Skeptics Doubt Ukraine Hack, Its Link to DNC Cyberattack," VOA, 23.12.2016, https://www.voanews.com/usa/skeptics-doubt-ukraine-hack-its-link-dnc-cyberattack

[112] Louk Faesen et al. "Naar een Cybercapaciteitenportfolio voor de Koninklijke Landmacht," The Hague Center for Strategic Studies, January 2021,https://mk0hcssnlsb22xc4fhr7.kinstacdn.com/wp-content/uploads/2021/01/Cybercapaciteit-Koninklijke-Landmacht-Final.pdf, p. 4

[113] *Ibid*., p. 21

[114] *Ibid*., p. 22

[115] *Ibid*., p. 23

EMS. An integrated CEMA approach is essential in this respect. In this way, overlap, deconflicting and coordination are anchored within an effect-oriented approach that efficiently uses scarce cyber expertise and capabilities. It is high time to draw up a vision, CONOPs and roadmaps, for which the considerations and recommendations outlined here can serve as input."[116]

As of this writing it is unclear whether the Royal Netherlands Army will implement any of the CEMA recommendations outlined in the study.

3 CEMA Adoption

The question as to why CEMA was adopted in the first place is an important one to clarify. Many militaries around the globe are recognizing cyberspace as a domain of operations. The NATO allies, for example, have done so as recently as 2016 at the Warsaw Summit.[117] Most NATO member states have established a dedicated cyber command and some even publicly published summaries of their cyber operation doctrines and strategies – including the US, Denmark, and France.[118] By contrast, the electromagnetic spectrum - and with it electronic warfare – has not been recognized as an operational warfare domain by NATO and many others around the globe. Very few states have in fact formulated and publicly released dedicated EW strategies and doctrinal documents.

3.1 Motivations Driving Adoption

In 2013, the US Department of Defense released its first Electromagnetic Spectrum Strategy, subtitled "A Call to Action," which notes that "adversaries are aggressively fielding electronic attack and cyber technologies that significantly erode DoD's ability to use the spectrum to conduct military operations."[119] Only as recently as October 2020 did the DoD release a dedicated 28-page long Electromagnetic Spectrum Superiority Strategy, which explains that "the Nation has entered an age of warfighting wherein U.S. dominance in air, land, sea, space, cyberspace, and the electromagnetic spectrum (EMS) is challenged by peer and near peer adversaries."[120] Even though the DoD does not talk in CEMA terms – due to CEMA being a unique concept to the Army – it does note that EMS dependent systems "must be resilient against RF-enabled cyberspace attack". The strategy further speaks of "integrated cyber and EMS operations," and highlights the development of robust electromagnetic battle management capabilities to enhance "the ability to plan, coordinate, and synchronize electronic warfare, spectrum management, and cyber operations."[121]

The UK MoD published its 19-page long Electromagnetic Spectrum Blueprint in August 2019. Even though CEMA is only mentioned five times, the document prominently notes that "through embracing [digital and information technologies] and CEMA, we can make better use of the specialist skills we have within the MOD, working towards common, co-ordinated and, where appropriate, synchronised outputs."[122]

The UK's Joint Doctrine Note 1/18 on "Cyber and Electromagnetic Activities" answers the question as to why the UK adopted CEMA. On the one hand, it assumes that "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."[123] Interestingly, the document also highlights the results of failure if CEMA is not adopted,

[116] *Ibid*., p. 29

[117] NATO, "Cyber defence," https://www.nato.int/cps/en/natohq/topics_78170.htm

[118] Joint Chiefs of Staff, "Joint Publication 3-12 - Cyberspace Operations," 08.06.2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150; US Cyber Command, "Achieve and Maintain Cyberspace Superiority – Command Vision for US Cyber Command," April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf; Danish Defence, "Joint Doctrine for Military Cyberspace Operations," Royal Danish Defence College, September 2019, https://fak.dk/globalassets/fak/dokumenter/publikationer/-fakpub-150-1-eng-.pdf; Comcyber, "Éléments publics de doctrine militaire de lutte informatique offensive," Ministère des Armées, 2019, https://www.defense.gouv.fr/content/download/551555/9394645/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdfs

[119] Department of Defense, "Electromagnetic Spectrum Strategy 2013 – A Call to Action," 11.09.2013, https://www.airforcemag.com/PDF/DocumentFile/Documents/2014/DOD_EM_Spectrum%20Strategy_2013.pdf, p. letter by the deputy secretary of defense

[120] Department of Defense, "Electromagnetic Spectrum Superiority Strategy," October 2020, https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF, p. foreword

[121] *Ibid*., p. 7, 12, 9

[122] UK Ministry of Defense, "Electromagnetic Spectrum Blueprint – Version 1," 09.08.2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/833094/Electromagnetic_Spectrum_Blueprint_V1-O.pdf, Foreword

[123] UK Ministry of Defense, "Joint Doctrine Note 1/18 – Cyber and Electromagnetic Activities," Development, Concepts and Doctrine Centres, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, p. 6

by analyzing Russian military weaknesses during the Russo-Georgian war in 2008.

JDN 1/18 stresses that: (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."[124] And (d) following the Georgian operations, "the Russian military took steps to address both cyber and electronic warfare capability development."[125]

In the US Army's CEMA doctrinal context, the Russo-Georgian war is never explicitly highlighted nor emphasized, which is most likely the result of slimming down Army doctrine.[126] Yet, writing for the Strategic Studies Institute at the US Army War College, Cohen and Hamilton noted in their analysis on the Russo-Georgian war that, "one of the areas in which Russian deficiencies were most starkly demonstrated was that of command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), which has been bluntly described as unsatisfactory by military analysts. The aforementioned lack of interoperability between the radio systems of different services and the vulnerability of Russian radios to electronic warfare led Russian commanders to rely on mobile phones for a considerable portion of their command and control requirements during the war. Although this in itself is bad enough, the fact that these calls went over Georgian mobile phone networks, which are the primary networks serving South Ossetia, makes the problem even more significant from a communications security standpoint."[127] Cohen and Hamilton go on to note that "the criticality of satellite imagery, navigation, and guidance was also amply demonstrated during the war. The fact that GLONASS [Russia's GPS equivalent] was not fielded and that GPS data were disrupted—presumably at the request of the United States—led to massive problems in selecting targets for the air campaign and in delivering precision strikes on Georgian targets."[128] The lack of "satellite navigation capability also presumably led to operational security breaches as units used radios or—more likely—mobile phones to report their positions to their higher headquarters, rather than higher headquarters simply following the positions of all of its units on a digital map."[129]

JDN 1/18 also criticizes NATO doctrine and its policy pace as a reason for the UK's push toward CEMA. As the document explains: "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. 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."[130] In US Army CEMA doctrine, there is no similar critique of NATO.

On the practical side, the UK's Cyber Primer mentions Israel's air strike against the Syrian nuclear facility at Dayr az-Zawr in September 2007 (also known as Operation Orchard/Operation Outside the Box). While unconfirmed, several media outlets reported that Israeli intelligence agencies were successful in deploying a piece of malware within the Syrian integrated air defense system. According to these accounts, prior to the air strike, the Israeli forces ran a blended attack comprising cyber and electronic warfare to destroy Syrian situational awareness and create a safe passage for the attacking aircraft. As the Cyber Primer concludes: "This alleged use of cyber as a mainstream military component may well be an indicator to a future integrated force structure."[131]

The US Army's CEMA drive primarily draws its lessons from the experience in Iraq and Afghanistan. As Col. Jeffrey Church, formerly the head of the Army's Electronic Warfare Division, explained in reference to his time in Iraq: "there weren't a lot of wires attached to me – it was wireless. So there you start getting into the electromagnetic spectrum…I see electronic warfare and cyberspace operations working together and to put it

[124] *Ibid*., p. 7

[125] *Ibid*., p. 7

[126] John Spencer, "What Does Army Doctrine Say About Urban Warfare?" MWI Urban Warfare Project podcast, 20.03.2021, https://open.spotify.com/episode/2ipg9at2vpkWOHbw3VPssj, time stamp: 55:21-58:22

[127] Ariel Cohen & Robert E. Hamilton, "The Russian Military and the Georgia War: Lessons and Implications," Strategic Studies Institute, June 2011, https://ia802802.us.archive.org/29/items/TheRussianMilitaryAndTheGeorgiaWarLessonsAndImplications/12-RussianMil.pdf, p. 51-52

[128] *Ibid*., p. 52

[129] *Ibid*., p. 52

[130] UK Ministry of Defense, "Joint Doctrine Note 1/18 – Cyber and Electromagnetic Activities," Development, Concepts and Doctrine Centre, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, p. 8

[131] UK Ministry of Defense, Cyber Primer – Second Edition," Development, Concepts and Doctrine Centre, July 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf, p. 77

into the infantry general-type of terms, that's a combined arms operation."[132]

As previously explained, the creation of US Army Cyber Command, the successful deployment of Stuxnet, as well as the Army's shift toward preparing for great power and near-peer adversarial conflict, has spurred the Army's desire to connect EW and cyber at the hip. The realization that "today electronic hardware and software are increasingly embedded in everything from vehicles to guided missiles, and are often integrated into systems which are difficult and costly to update or upgrade," certainly also helped to move CEMA higher and higher up the Army's priority list.[133]

In addition to these broader developments, the Army has also drawn valuable operational lesson from the anti-ISIS coalition fight to liberate the Iraqi city of Mosul. As TRADOC's Mosul Study Group states in its 2017 report on "what the Battle for Mosul Teaches the Force,": "[t]he ability to navigate the electromagnetic spectrum environment is critical to combat effectiveness. The electromagnetic spectrum is constantly changing and requires coordination and synchronization to operate successfully within it. All phases of operations can be impacted by the retention, degradation, and/or denial of the electromagnetic spectrum. On an increasingly digitized battlefield, the electromagnetic spectrum is key terrain. However, it is difficult to achieve electromagnetic spectrum dominance. There are no easy solutions; completely blocking the spectrum restricts U.S. and anti-ISIS coalition capabilities. Conversely, leaving unblocked gaps in the spectrum comes with the risk that the spectrum may be utilized by the adversary. The U.S. Army must be able to operate within a congested and contested electromagnetic spectrum environment for both offensive and defensive purposes."[134]

Transposing the Battle of Mosul onto a near-peer adversarial battlefield (think major urban centers, harbors, airports etc.) provides a more accurate perspective as to what kind of combined arms operation the Army will have to prepare for in future conflicts. CEMA serves as the interconnecting tissue that synchronizes offensive and defensive activities in the non-kinetic realm to allow the US Army to move faster, with greater lethality, and punch through adversarial stand-off A2/AD environments.

3.2 Dedicated CEMA Units

Apart from the development of CEMA doctrine, the US Army has been evolving over the past decade to spread and integrate CEMA across all echelons and started to experiment with dedicated CEMA organizations and units. This section will cover some of the most important developments and experiments. Other capabilities, such as the Terrestrial Layer System Brigade Combat Team (TLS-BCT), the TLS-Echelons Above Brigade (TLS-EAB), and the envisioned Offensive Cyber Operations Signal Battalion (OCOSB) are not included in this section nor covered by this study, because it is currently unclear what exactly their technical capabilities are in regard to CEMA operations.[135]

DAMO-CY/DAMO-SO

In July 2016, the Army formed a new directorate within the Deputy Chief of Staff G-3/5/7 headquarters, known as DAMO-CY, short for Department of the Army's Management Office – Cyber, which was primarily focusing on CEMA.[136] Headed at the time by Maj. Gen. Patricia Frost, DAMO-CY was responsible for kicking of the cultural changes within the Army to transition toward cyber and electromagnetic activity integration. As Maj. Gen. Frost explained it in 2017, "if we look at future electronic warfare capabilities that we might want to field—well, there's a dependency. There's a dependency on the network. There's a dependency on data feeds. There's a dependency on the intelligence that's going to give you the threat information. You don't want to just deploy a capability without thinking about the second- and third-order effects and the mission workload that you just put on another staff entity."[137]

On CEMA's defensive end, DAMO-CY created the Army's Task Force Cyber Strong in May 2017. As Maj. Gen Frost explained, DAMO-CY efforts were "getting the commands to ask themselves: How do you see yourself? What do you need to defend? How do you prioritize

[132] Amber Corrin & Mark Pomerleau, "Army merging electronic warfare into new cyber directorate," C4ISR.net, 12.07.2016, https://www.c4isrnet.com/c2-comms/2016/07/12/army-merging-electronic-warfare-into-new-cyber-directorate/

[133] Statement by Lieutenant General Edward C. Cardon, Commanding General U.S. Army Cyber Command and Second Army before the Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, Operationalizing Cyberspace for the Services, United States Senate, First Session, 114th Congress, 14.04.2015, https://www.armed-services.senate.gov/imo/media/doc/Cardon_04-14-15.pdf, p. 8

[134] Mosul Study Group, "What the Battle for Mosul teaches the Force," TRADOC & US Army, No. 17-24 U, September 2017, https://www.armyupress.army.mil/Portals/7/Primer-on-Urban-Operation/Documents/Mosul%20(Public%20Release).pdf, p. 65

[135] See: Mark Pomerleau, "Army shares details on new electronic warfare units," C4ISR.net, 31.12.2020, https://www.c4isrnet.com/electronic-warfare/2021/01/01/army-shares-details-on-new-electronic-warfare-units/; Sydney J. Freedberg Jr., "Army Electronic Warfare: Big Tests In '21," Breaking Defense, 12.08.2020, https://breakingdefense.com/2020/08/army-electronic-warfare-big-tests-in-21/

[136] The G-3/5/7 denotes the Army's general staff on 'Operations, Plans, and Training.' It is responsible for developing, integrating, and managing training operations and requirements, concepts, policies, and plans.

[137] Sandra Jontz, "Army Accelerates Cyber, EW Integration," AFCEA, 29.06.2017, https://www.afcea.org/content/army-accelerates-cyber-ew-integration

what needs to be defended? What do you look at hardening first? Where do you need to be resilient? Where do you need to have contingency operations?"[138] Task Force Cyber Strong set out to strategically help major Army commands to (a) increase operational understanding of CEMA across the force and all echelons, (b) identify what methods work and eliminate redundancies, (c) develop an overarching resourcing strategy, and (d) home in on control systems, including the weapons systems and industrial control systems used in and by the Army.[139]

In January 2020, DAMO-CY was reorganized as DAMO-SO (short for Department of the Army Strategic Operations), which now encompasses not only CEMA but is also pulling the strings together on "information operations, space, enterprise IT networks, tactical communications networks, data architectures and artificial intelligence."[140] As Brig. Gen Martin Klein, director of DAMO-SO explained to C4ISRNET, the office is "also bringing into the directorate the capabilities of really underwriting the Army's ability to digitally transform into this new era … Part of what [DAMO-SO has] been asked to do is underwrite multidomain operations and then to digitally enable our warfighting systems."[141] Practically, DAMO-SO serves as a policy integrator, whose task is to figure out how to better organize, restructure, and resource the Army in the non-kinetic realm. In cooperation with Army Futures Command, it also looks at emerging capabilities and examines what capabilities the Army will need now and in the future. Organizationally, DAMO-SO "puts one general officer in charge of the full range of joint all-domain operations to help synergize solutions," as Col. Chapman, division chief of Mission Command in the Army CIO/G-6 office explained in February 2020.[142] Col. Elizabeth Casely, who served as chief of staff in the Network Cross Functional Team within the Army Futures Command, further explained that "instead of each of the services building solutions and then trying to make them interoperable, leaders from the various services are starting to discuss system requirements and interoperability much earlier."[143]

CSCB

In 2014, then US Army Cyber Commander Lt. Gen. Edward Cardon envisioned that "small cyber teams could be attached to brigades or lower-level units. These teams could be 'tethered' back to national-level agencies for the sake of obtaining authorization to act."[144] In May 2014, Gen. Odierno, then Army Chief of Staff, ordered US Army Cyber Command to develop a 'Cyber Support to Corps and Below' (CSCB) pilot to demonstrate cyber effects at corps level and echelons below.[145]

The initial plan for CSCB was to deploy a team of four cyber specialists to a brigade conducting war games at Combat Training Centers. In one of the first rotational exercises that was specifically aimed at figuring out how to better meld cyber and electronic warfare at the brigade and company levels, the National Training Center at Fort Irwin invited the 1st Armored Brigade Combat Team of the 1st Infantry Division in August 2016 for a two-week simulated fight protecting a fictional ally from an aggressive neighbor. The plan was that a team of 40-45 US Army Cyber Command personnel would join the brigade – with two to three Army Cyber personnel attached to each company – and the brigade command would work closely with other parts of the CEMA teams.[146] However, according to Breaking Defense, it "quickly became clear that a much larger contingent was required to set up the necessary infrastructure for training, let alone conduct effective operations."[147] According to the Army, "the cyber team conducted reconnaissance of the training scenario's operational information environment to gain an understanding of the adversary's activities and then sent the information to an analytical cell, where a team developed insights and actionable intelligence. […] All of these operations occur as the brigade move[d] quickly through the battlespace […] so the cyber team is constantly busy and must always be on their toes."[148] Similarly, the Army

[138] Sandra Jontz, "New Army Cyber Task Force Does Deep-Dive Review," AFCEA, 05.05.2017, https://www.afcea.org/content/?q=new-army-cyber-task-force-does-deep-dive-review

[139] *Ibid*.

[140] Mark Pomerleau, "The Army's new directorate eyes multidomain integration," C4ISR.net, 21.07.2020, https://www.c4isrnet.com/smr/information-warfare/2020/07/21/the-armys-new-directorate-eyes-multidomain-integration/

[141] *Ibid*.

[142] George I. Seffers, "Army Expands Mission of Cyber Directorate," AFCEA, 14.02.2020, https://www.afcea.org/content/army-expands-mission-cyber-directorate

[143] *Ibid*.

[144] Joe Gould, "Ground commanders with cyber skills," Army Times, 16.07.2014, https://www.armytimes.com/news/your-army/2014/07/16/ground-commanders-with-cyber-skills/

[145] Army.mil, "The Cyber Support to Corps and Below," 16.07.2015, https://www.army.mil/standto/archive/2015/07/16/

[146] Kyle Jahner, "Army to keep tinkering with company-level cyber integration at NTC next month," Army Times, 17.06.2016, https://www.armytimes.com/news/your-army/2016/06/16/army-to-keep-tinkering-with-company-level-cyber-integration-at-ntc-next-month/

[147] Sydney J. Freedberg Jr., "Army Boosts Electronic Warfare Numbers, Training, Role," Breaking Defense, 07.08.2018, https://breakingdefense.com/2018/08/army-boosts-electronic-warfare-numbers-training-role/

[148] David Vergun, "Army explores using cyber teams to aid maneuver commanders," Army.mil, 30.08.2016,

stressed that while the rotation only lasted two weeks, "cyber personnel were involved in the 180 days of planning and exercises leading up to this NTC [National Training Center] event. In that time, cyber operators participated in training exercises with 24 of the 25 companies that make up the 4,000-person brigade. That time spent with them gave the cyber team cohesion with every element of the brigade."[149]

The Army also realized that a cyber team needed a healthy mix of other skills and expertise in diverse areas, including military intelligence, electronic warfare, signals intelligence, and sometimes even space.[150] Sometime between 2014 and 2017, CSCB was renamed into "CEMA Support to Corps and Below". Testifying before the Senate Subcommittee on Cybersecurity in 2017, Lt. Gen. Nakasone – then commanding general of US Army Cyber Command – explained that "in 2015 the Army initiated a Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) pilot program. The CSCB effort serves four primary purposes: Define what offensive and defensive cyber effects to integrate at the echelon Corps and below; Determine expeditionary Defensive Cyberspace Operations, Offensive Cyberspace Operations, Electronic Warfare, and Information Operations capability for deployed tactical forces; Leverage Combat Training Centers (CTCs) and operational deployments to inform CEMA Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities development (DOTMLPF); and Determine the enduring CEMA environment at CTCs."[151]

On the defensive end, CSCB also helped brigades during their home station training to get a sense as to what electromagnetic signals the brigade was producing. Some brigades "lit up like a Christmas tree", and the CSCB team showed brigade commanders how to effectively reduce their signal emission.[152] It is unclear whether this type of show-and-tell was newly introduced by CSCB, was practiced prior in a different context, or was not made widely available to corps and formations below.

In 2018, Lt. Gen. Stephen Fogarty, current commander of US Army Cyber Command, testified before the Senate Subcommittees on Cybersecurity and Personnel that, "Army Cyber Command has built real-time reach-back links between [CEMA Support to] Corps and Below level forces at the National Training Center and cyber operators at Fort Meade, Maryland and Fort Gordon, Georgia, that further enhance training capabilities for the Army's Brigade Combat Teams as well as our cyber forces. Based on lessons learned from the CSCB initiative, the Army will start building a Cyber Warfare Support Battalion (CWSB) in FY2019, dedicated to integrating tactical operations with strategic cyber capabilities, and supporting Electronic Warfare and cyber planning and integration." [153]

915th CWB

As a result of the 2015 CEMA Support to Corps and Below pilot program, the Secretary of the Army ordered ARCYBER to build the 915th Cyberspace Warfare Battalion (CWB) to "help meet the Army's current and projected tactical Cyberspace Electromagnetic Activities (CEMA) requirements."[154] In 2019, US Army Cyber Command officially created the 915th CWB, encompassing 12 expeditionary CEMA Teams (ECTs) – i.e., "fly away" teams – which are solely meant to support brigade combat teams or other tactical formations with cyber and EW capabilities in a scalable way.[155] According to the Army, "the 915th CWB, through its Expeditionary CEMA Teams (ECTs), provides a scalable capability to deploy Expeditionary Cyberspace Operators to conduct operations to deny, degrade, disrupt, destroy and influence cyberspace effects for Army maneuver commanders."[156]

The whole reason for building ECTs is grounded in the fact that back in 2018/19 planners had to submit

https://www.army.mil/article/173344/army_explores_using_cyber_teams_to_aid_maneuver_commanders

[149] *Ibid*.

[150] David Vergun, "Integrated Army cyber activities teams playing pivotal role in warfare," Army.mil, 09.01.2018, https://www.army.mil/article/198871/integrated_army_cyber_activities_teams_playing_pivotal_role_in_warfare

[151] Statement by LTG Paul M. Nakasone, Commanding General U.S. Army Cyber Command, before the Subcommittee on Cybersecurity, Committee on Armed Services, United States Senate, First Session, 115th Congress, on U.S. Army Cyber Posture, 23.05.2017, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_05-23-17.pdf

[152] David Vergun, "Integrated Army cyber activities teams playing pivotal role in warfare," Army.mil, 09.01.2018, https://www.army.mil/article/198871/integrated_army_cyber_activities_teams_playing_pivotal_role_in_warfare

[153] Statement by Lieutenant General Stephen G. Fogarty, Commander United States Army Cyber Command, before the Subcommittees on Cybersecurity and Personnel, Committee on Armed Services, United States Senate, Second Session, 115th Congress, on Cyber Operational Readiness, 26.09.2018, https://www.armed-services.senate.gov/imo/media/doc/Fogarty_09-26-18.pdf, p. 4

[154] Steven Stover, "Battalion helping shape Army tactical capabilities in the information environment," Army.mil, 30.01.2020, https://www.army.mil/article/231091/battalion_helping_shape_army_tactical_capabilities_in_the_information_environment

[155] Mark Pomerleau, "US Army conducts first-of-its-kind exercise for tactical information warfare unit," C4ISR.net, 12.10.2020, https://www.c4isrnet.com/show-reporter/ausa/2020/10/12/us-army-conducts-first-of-its-kind-exercise-for-tactical-information-warfare-unit/

[156] Steven Stover, "Battalion helping shape Army tactical capabilities in the information environment," Army.mil, 30.01.2020, https://www.army.mil/article/231091/battalion_helping_shape_army_tactical_capabilities_in_the_information_environment

their request up the chain to higher echelons to get permission to leverage particularly offensive cyber effects in the field. This not only slowed down operations, but also made brigade commanders hesitant to leverage offensive cyber capabilities in the first place. ECTs were a way to solve that problem. As CSCB exercise planner Matt Funk explained to Fifth Domain, the pilot had two functions: "the first is to inform Army doctrine for tactical cyber to include recommendations on force structure and necessary infrastructure changes at training centers to better represent cyber capabilities. The second is to improve how these experimental teams operate within a brigade."[157] At its core, an ECT consists of an expeditionary element, i.e., offensive cyber operators that generate effects in the field – and CEMA planners at the brigade staff – i.e., the CEMA working group.

According to Col. Brian Vile, commander of the 780th Military Intelligence Brigade, "the 915th is assembling the most technically gifted Soldiers, putting them into the most challenging environments, and asking them to figure out new ways to employ technology and information to deliver effects in the physical, virtual, and cognitive domains. […] We won't tell them how to operate; instead, we'll tell them what needs to be done and ensure they have the tools and authorities to do it."[158]

In September 2019, the CWB deployed one of its 45-person strong ECTs to Germany to participate in the large-scale Saber Junction 2019 exercise.[159] Its participation presented the ECT with the opportunity to "plan and organize the integration of cyber warfare strategies and tactics, assigning CEMA technologies to battlefield operations."[160] According to the ECT commander Capt. Adam Schindler, the team "was able to dominate the information environment across the entire [Joint Multinational Readiness Center] network, enabling remote cyber operators at Fort Gordon to exploit and dominate the network, and effectively integrate cyberspace and information operations."[161]

In early October 2020, Expeditionary CEMA Team 1 – or ECT-01 – underwent its first field training exercise (FTX) at the Muscatatuck Urban Training Center (MUTC) in Indiana.[162] As Lt. Col. Matthew Davis, commander of the 915th, explained the purpose of the FTX, "[p]riority one is the ECT's training proficiency and having a scenario constructed around them as a training audience. The second purpose is to develop a training plan for how we are going to train ECTs as we build them. This is our first ECT and there are 11 more to come – so how are we going to train them. We have a draft, a beta, and this is a pilot run of the beta to figure out have we established the right task, condition, and standards, training objectives, and is this the right training plan."[163]

The MUTC provided the ECT with a realistic battleground across four square kilometers, including 953 structures ranging from "a multi-story hospital, fresh-water and waste-water treatment facilities, a coal-fired steam plant, an embassy, high school, and even a prison."[164] Nicholas Marchuk, special ops training and development lead at MUTC notes that, "over 50% of the buildings are connected via [a] tunnel system […]. We are able to run all kinds of fiber – that support some of our cyber efforts – through those tunnels. And then all our power [i.e., steam heat created by the power plant] goes through those […]. The other thing we have is SMEIR. It is the social media environment Internet replication system. So, we can do IO campaigns, open-source scraping, instead of Facebook it has like Bookface, instead of Twitter it has something very close to Twitter. So instead of having a thousand people typing and putting stuff in, we just turn this on and it populates all that, and we can tailor the messages and triggers. So, a unit can exploit that […]. The other really unique thing we have is the Onyx system, which is a 3G/4G wireless network the government owns. It is closed loop so we can use it for testing and training without upsetting Mr. Spring and Mr. T-Mobile."[165]

One specific example highlighted by Amanda Lockwood, solutions architect at IDS international – which provides the social media environment and Internet replication product at the MUTC – was that in one drill "the ECT identified a house with a virtual machine inside as significant to the team's objective. As part of the robust environment at Muscatatuck, this house was equipped with devices on the Internet of

[157] Mark Pomerleau, "How the Army will infuse cyber operations on the battlefield," Fifth Domain, 05.07.2018, https://www.fifthdomain.com/dod/army/2018/07/05/how-the-army-will-infuse-cyber-operations-on-the-battlefield/

[158] Steven Stover, "Battalion helping shape Army tactical capabilities in the information environment," Army.mil, 30.01.2020, https://www.army.mil/article/231091/battalion_helping_shape_army_tactical_capabilities_in_the_information_environment; Note: While ARCYBER maintains operational control over CWB, the command authority and administrative control over CWB falls to the 780th Military Intelligence Brigade.

[159] *Ibid*.

[160] *Ibid*.

[161] *Ibid*.

[162] Army.mil, "The Army's Only Cyber Warfare Battalion Confirms Training Program," 13.10.2020, https://www.army.mil/article/239869/the_armys_only_cyber_warfare_battalion_confirms_training_program; For more on the history, development, and training of the MUTC, listen to the Urban Warfare Project's podcast episode on 'Multi-domain Operations at Muscatatuck Urban Training Center," at https://open.spotify.com/episode/4hOvTnLHnSuqUiF8wZ4aAd

[163] *Ibid*.

[164] *Ibid*.

[165] John Spencer, "Multi-Domain Operations at Muscatatuck Urban Training Center" MWI Urban Warfare Project podcast, 08.2020, https://open.spotify.com/episode/4hOvTnLHnSuqUiF8wZ4aAd, time: 9:37-11:00

Things, with physical and virtual machines run wirelessly or connected directly to a network. Using publicly available open-source tools, the team was able to target the identified system in the house and gain information to enable more physical operations."[166]

As Staff Sgt. Robert Vickery, ECT-01 fire support specialist, put it: "We're building SOPs (standard operating procedures) and identifying how we execute things efficiently because that hasn't been done before. That's one big takeaway. Another thing MUTC provides is a realistic urban environment where you can actually see effects. When you go to NTC [National Training Center] or JRTC (Joint Readiness Training Center), most of the time effects are white-carded, these guys are actually getting to see the results."[167]

On 29 January 2021, the 915th formally activated its Bravo Company. According to Capt. James Conway, the newly appointed commanding officer of Bravo Company, "[i]t's a huge leap forward, and a good steppingstone for expeditionary cyber and expeditionary CEMA […] to provide units at different echelons with capabilities that they may not have had before; to bring a different perspective to help them engage and win against the enemy."[168] Lt. Col. Matthew David added to this that, "once you have the blueprint, the blueprint lets you build capacity […]. So Bravo Company's most important job for the foreseeable future is to develop and train their first team so they can get that one off the ground."[169]

In March 2021, the Army conducted Cyber Quest 2021, which was co-organized by Army Futures Command and the Army Maneuver Center of Excellence – to bring together 14 vendors and their technologies to be field-tested by, among others, the 915th CWB. One tool developed by Accenture that was tested was designed "to obfuscate cyber operations. In the event the software code used for offensive operations is intercepted or reverse engineered, the tool is designed to limit attribution or identification of its origin."[170] Other items included anti-jamming radios, and tools "to detect enemies, send data back up the chain of command, have it analyzed and then sent back — something that often takes longer than they can afford. Soldiers were even able to link a small drone to their network to inform movements."[171] Army leaders also learned how units responded to threats of adversarial jamming and adapted maneuvers. For example, "units altered their paths or used other experimental assets, such as drones, for better forward reconnaissance based upon what the adversary was doing in the electromagnetic spectrum. This flipped the script, providing the friendly forces an advantage."[172]

Starblazor

Back in late 2019, the Army discovered that one of the keys to success in cyber operations was to embed tool developers and coders alongside operators. Speaking at the Billington cybersecurity conference in September 2019, Lt. Gen. Fogarty explained that "when we built the mission force initially, it was this idea that we would pool the developers at a very central location. If you're on a team, you conduct an operation, you would send a problem up, they would work it and they would send it down […]. In practice, that just doesn't work."[173] As Fogarty went on to note, "[f]orces may need a certain exploit or adjust to a change the enemy made to its network immediately and can't wait to send it out for development."[174]

As a result, the Army started to develop a new programmer specialization role, which has led to a new pilot program called "Starblazor" that would place coders and software developers at the tactical edge. Talking to C4ISRNET, Eric Colon, a CEMA technician at Army Cyber Command noted that, "Starblazor will help the Army learn what is needed to train the cyber and electronic warfare operators with existing equipment and what these personnel will need for a future fight."[175] C4ISRNET's Mark Pomerleau further explains that, "Starblazor is aimed toward the Army's new 915th Cyber

[166] Mark Pomerleau, "US Army conducts first-of-its-kind exercise for tactical information warfare unit," C4ISR.net, 12.10.2020, https://www.c4isrnet.com/show-reporter/ausa/2020/10/12/us-army-conducts-first-of-its-kind-exercise-for-tactical-information-warfare-unit/

[167] Army.mil, "The Army's Only Cyber Warfare Battalion Confirms Training Program," 13.10.2020, https://www.army.mil/article/239869/the_armys_only_cyber_warfare_battalion_confirms_training_program

[168] John Portela, " Cyberspace battalion continues growth with activation of new company," Dvids, 02.02.2021, https://www.dvidshub.net/news/388197/cyberspace-battalion-continues-growth-with-activation-new-company

[169] *Ibid*.

[170] Mark Pomerleau, "Army participates in first-of-its-kind cyber exercise," C4ISR.net, 16.03.2016, https://www.c4isrnet.com/cyber/2021/03/16/army-participates-in-first-of-its-kind-cyber-exercise/

[171] Jackson Barnett, "Army working on new cyber, electromagnetic weapons after large-scale test event," Fedscoop, 15.03.2021, https://www.fedscoop.com/army-cyber-quest-2021-cyber-command-test-new-tools/

[172] Mark Pomerleau, "Army participates in first-of-its-kind cyber exercise," C4ISR.net, 16.03.2016, https://www.c4isrnet.com/cyber/2021/03/16/army-participates-in-first-of-its-kind-cyber-exercise/

[173] Mark Pomerleau, "The Army wants more coders alongside operators," C4ISR.net, 05.09.2019, https://www.c4isrnet.com/dod/army/2019/09/05/the-army-wants-more-coders-alongside-operators//

[174] *Ibid*.

[175] Mark Pomerleau, "US Army to test electronic warfare coders at the edge during upcoming exercise," C4ISR.net, 07.07.2021, https://www.c4isrnet.com/electronic-warfare/2021/07/07/us-army-to-test-electronic-warfare-coders-at-the-edge-during-upcoming-exercise/

Warfare Battalion […]. One intent of the group is to be able to go anywhere, utilize brigade-organic equipment and exploit hard targets by capturing a signal of interest, reverse engineering it and delivering an effect in months rather than years."[176] Starblazor was notably first deployed during Defender Pacific 2021.

I2CEWS

Back in 2016, then US Army Chief of Staff Gen. Mark Milley introduced a new Army concept – then known as multi-domain battle, and now known as multi-domain operations (MDO) – to confront regional peer-competitors on the battlefield of tomorrow. MDO essentially envisions the Army to conduct cross-domain fires. Meaning, it will attack enemy ships at sea, establish air superiority with land-based capabilities, and fight and win in denied environments across all operational warfare domains (i.e., counter A2/AD).

To figure out the doctrinal concepts necessary to make the concept of MDO workable in practice, the Army stood up an experimental multi-domain task force (MDTF) in 2017 that has been participating in multiple theater exercises in the Indo-Pacific. The MDTF's lessons learned – think translating joint targeting into tactical maneuver and action – then go straight into the Army's doctrine building. As Gen. Robert Brown explained to Defense News in 2018, "we are spinning it right off, and some of it is going into our doctrine that is being developed by the Army right away and some of it can be used — God forbid — if we had to fight tonight, we'd put it in right away."[177]

The CEMA element is located within the MDTF's I2CEWS, short for Intelligence, Information, Cyber, Electronic Warfare and Space. I2CEWS is an experimental battalion-sized unit stood up in January 2019 under the auspices of America's First Corps – the only Army corps aligned with US Indo-Pacific Command. Within the I2CEWS battalion, the CEMA team is confusingly also regularly referred to in multiple publications as the "I2CEWS detachment."[178] However, some articles, such as the one written by Maj. Kyle Borne in 2019 – who is currently serving as the CEMA company commander for the I2CEWS battalion – refer to the CEMA team by name.[179]

To hone its skills in practice, the I2CEWS's CEMA team participated in Cyber Blitz 2018 and 2019.[180] Cyber Blitz 2018 was exclusive focused on the CEMA team to examine "how the integration of I2CEWS could help a BCT gain and maintain the advantage against a regional peer in multi-domain operations."[181] Cyber Blitz 2019 helped answer questions about how the Army could conduct I2CEWS operations by providing a realistic first look at how the I2CEWS could fight and win as part of the MDTF. It was the first time since their activation that the entire I2CEWS operated together as a unit, exercising all functions in distributed operations.[182]

Speaking at the AFCEA TechNet Augusta Web seminar on 20 October 2020, General Paul Craft – chief of cyber and commandant of the US Army Cyber School at Fort Gordon – noted that in the future the I2CEWS "will be commanded by either a Signal Corps officer or a military intelligence officer or a cyber electronic warfare officer."[183] Craft also summarized that I2CEWS is currently working on three big areas: "One is the synchronization of all those capabilities at that echelon of operation. Two, is the integration of those capabilities, and how does electronic warfare work with signals intelligence or how does signals and space work together? How do our cyber forces fit within that?"[184]

CEMA Cells

In 2018, the Army decided to significantly increase the size of the CEMA personnel attached to the brigade, division, corps, and component command level. At the brigade level, the CEMA cell doubled from five to ten, and for the first time included a non-EW cyber operations officer. At the division level the cell grew from five to nine, and at the corps level from six to eight. The Army Service Component Commands did previously not have a standardized CEMA cell attached, so the Army decided upon a cell the size of seven.[185]

[176] *Ibid*.

[177] Jen Judson, "Multidomain Operations Task Force cuts teeth in Pacific," Defense News, 28.08.2018, https://www.defensenews.com/land/2018/08/28/multidomain-operations-task-force-cuts-teeth-in-pacific/

[178] Mark Pomerleau, "How the Army is taking cyber units to the battlefield," Fifth Domain, 13.03.2019, https://www.fifthdomain.com/dod/army/2019/03/13/how-the-army-is-taking-cyber-units-to-the-battlefield/

[179] Kyle David Borne, "Targeting in Multi-Domain Operations," Military Review, May-June 2019, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Borne-Targeting-Multi-domain/

[180] Several of the Army's exercise series were streamlined to bring together cyber and EW. Cyber Quest started to do so in August 2016; and Cyber Blitz started in April 2016. See: https://defensesystems.com/articles/2016/08/23/army-cyber-quest-cyber-ew.aspx; Mark Pomerleau, "Army's Cyber Blitz takes aim at cyber/EW convergence," Defense Systems, 04.05.2016, https://defensesystems.com/articles/2016/05/04/army-cyber-blitz-ew-cyber-integration.aspx

[181] US Army Cyber Center of Excellence, "Cyber Blitz 2019," https://www.dvidshub.net/publication/issues/50376

[182] US Army Cyber Center of Excellence, "Cyber Blitz 2019," https://www.dvidshub.net/publication/issues/50379

[183] Kimberly Underwood, " The Army Evolves Its Formations for Cyber and Electronic Warfare," AFCEA, 21.10.2020, https://www.afcea.org/content/army-evolves-its-formations-cyber-and-electronic-warfare

[184] *Ibid*.

[185] Sydney J. Freedberg Jr., "Army Boosts Electronic Warfare Numbers, Training, Role," Breaking Defense, 07.08.2018, https://breakingdefense.com/2018/08/army-boosts-electronic-warfare-numbers-training-role/

So far, the UK MoD has not publicly released any information in regard to the creation of dedicated CEMA units deployed in the field. What we do know, however, is that the MoD has established a "Joint Cyber and Electromagnetic Activities Group (JCG) to coordinate activities in cyberspace and the electromagnetic environment to gain freedom of movement, operational advantage and create effect, whilst simultaneously exploiting, denying and degrading our adversary's use of the same." The UK's Joint Force Cyber Group, which includes the UK's Joint Cyber Reserve and delivers the MoD's cyber capability, is subordinated to the JCG.[186] As of this writing it is unclear whether the UK is going to create dedicated CEMA teams.

While unclear as to the exact capabilities at play, and its relation to the MoD's CEMA push, the announcement of Britain's new National Cyber Force (NCF) in November 2020 might include some hints as to its participation in CEMA related activities. According to the MoD, cyber operations will include "interfering with a mobile phone to prevent a terrorist from being able to communicate with their contacts;" and "keeping UK military aircraft safe from targeting by hostile weapons systems."[187] The former might also be applicable to counter-IED operations and interfering with adversarial military communications in the field (think the Russo-Georgian war). And the latter could refer to CEMA operations such as the 2007 Israeli airstrike against the Syrian nuclear facility at Dayr az-Zawr.

Curiously, the UK MoD's 2021 "Defence in a Competitive Age" publication might have also hinted at a CEMA role for the 6th (UK) Division. As the paper notes, "the 6th (UK) Division will deliver cyber, electronic warfare, information operations and unconventional capabilities designed for warfighting and for operations conducted below the threshold of war."[188] As of this writing is unclear whether CEMA plays a role in this or whether those are independent capabilities leveraged without a CEMA mindset.

3.3 Initial Challenges and Best Practices

In 2017, the US Army Cyber Command's G-35 Office asked RAND to "develop and document an Army strategy for providing cyber support to corps and below (CSCB) units that describes how the Army should use its available resources to achieve mission objectives."[189] Looking at three case studies, the RAND team identified several best practices for implementing a strategy for operationalizing tactical cyber operations.

Best practices derived from the Joint Interagency Task Force South – which is a multiservice, multiagency task force that specializes in operations countering illicit trafficking and cooperates with partner nation agencies – included (a) the "sending of a liaison officer to a potential partner even before the organization has agreed to reciprocate;" (b) that "relations are forged and tested in the crucible of operations" and that there have to be plenty of opportunities to demonstrate success; (c) "understand[ing] and respect[ing] the equities of each organization," including "involving them in decision-making and priority setting and protecting their needs for privacy;" (d) that "collocation increase mutual understanding among participating organizations;" and that (e) "information-sharing procedures and rules of participating organizations must be accommodated."[190]

The case study on the US Marine Corps Tactical SIGINT – which in 2002 became the first service to receive access to the NSA's SIGINT database while in theater – highlighted that the US Marine Corps (USMC) was successful in incrementally building and sustaining trust with the NSA by demonstrating the value of the access it was requesting. Similarly, the strict adherence by the USMC to initial constraints set up by the NSA, "reminded the NSA that its trust in the USMC was not misplaced." In other words, "accepting conditions unconditionally makes it hard for a partner to say 'no'."[191]

The last case study covering the use of armed drones during Operation Enduring Freedom, tackled the issue of authorities. The RAND team took the view that "if you build [tactical offensive cyber operations] the authorities will come." In essence, they put forward a learning by doing approach.

Some of the lessons learned, the Army had to learn the hard way. Speaking at the Association of the Army in August 2018, Brig. Gen. Hartman – deputy commanding general at US Army Cyber Command – explained that "in order to execute CEMA operations at the BCT [brigade combat teams] level, the BCTs had to be enabled by

[186] UK Ministry of Defence, "Cyber Primer – Second Edition," Development, Concepts and Doctrine Centre, July 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf, p. 69-70

[187] UK Ministry of Defense, "National Cyber Force Transforms country's cyber capabilities to protect UK," Gov.uk, 19.11.2020, https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk

[188] UK Ministry of Defense, "Defence in a competitive age," Presented to Parliament by the Secretary of State for Defence by Command of Her Majesty, March 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971859/_CP_411__-_Defence_in_a_competitive_age.pdf, p. 53

[189] Isaac R. Porche III et al., "Tactical Cyber – Building a Strategy for Cyber Support to Corps and Below," RAND Corporation, 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf, p. iii

[190] *Ibid*., p. xiv

[191] *Ibid*., p. xv - xvi

proper intelligence. [But that] quite honestly, what the brigades had organically wasn't all that robust." [192] As such, "providing the infrastructure to deliver so-called reach-back support for information from an offensive and defensive cyber standpoint, as well as from an intelligence standpoint, made a difference." [193]

Similarly, Hartman pointed out that "the CEMA-related equipment that they brought to the Joint Readiness Training Center (JRTC) was outdated, built to fight the last war. […] and what I mean by that is it was large. It wasn't mobile. It was built to sit on a FOB [forward operating base] in a fixed location. It wasn't built to maneuver with a BCT."[194] This in turn necessitated the procurement of commercial-off-the-shelf solutions and modifications to the existing equipment. "That really allowed us to start innovating at a really, really quick pace," Hartman explained. The results were telling: "[E]quipment used for the first rotation provided the capability to survey and target at about 900 meters, while solutions after the first several rotations reached five kilometers. Now the BCTs have the equipment to mesh different sensors together and provide a common operating picture."[195]

4 CEMA Tactics

The publicly available US Army doctrinal documents do not reveal how exactly military planners envision CEMA tactics and actions to work in combination with kinetic operations. UK doctrinal documents, however, outline three CEMA actions:

Sequence actions: "Where a commander may put into operation a series of interconnected actions to create effect. For example, OCO [offensive cyber operations] against several adversarial networks to shift communication onto a 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."[196]

This tactic is also known as SIGINT herding. The Snowden Leaks contain one document from 2003 that explains that "during Operation Iraqi Freedom, the ability to collect, geolocate, and process HF communications was most clearly demonstrated. As part of the planning for this war, CENTCOM developed a SIGINT herding strategy. Communications hubs known to be used by Iraqi military were identified and prioritized. The elimination of these hubs forced the Iraqis to establish alternate means of communicating. The alternate means of communicating very often became HF communications […]."[197]

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."[198]

Blended/layered attacks: The idea of a layered CEMA attack was highlighted by Israel's Operation Orchard. While the details are unconfirmed, rumors have been circling that the Israelis used a system called 'Suter' to take out Syrian Air Defenses. From open source it is unclear what Suter actually is – other than having been developed by the US Air Force at one point. Some describe it as a highly clandestine computer program created by BAE Systems, others make it seem like a pod manufactured by L-3 Communications that can be installed on drones and manned aircraft. According to the story told, Suter was specifically designed to interfere with integrated air defense systems. Writing for Airforce-technology.com in March 2008, Richard Gasparre explains that "[a]fter pinpointing the target antennas, Suter then performs its real magic – beaming electronic pulses into the antennas that effectively corrupt, if not hijack, the processing systems that present the enemy operators with their physical picture of the battlefield. Unlike classic jamming or EMP attacks, these data streams do not flood enemy electronics with excess 'noise' or power, but instead insert customised signals, including specialised algorithms and malware, into the vulnerable processing nodes."[199] The end result

[192] Kimberly Underwood, "Army CEMA Teams Advance Information, Electronic and Cyber Warfare," AFCEA, 06.08.2018, https://www.afcea.org/content/army-cema-teams-advance-information-electronic-and-cyber-warfare

[193] *Ibid*.

[194] *Ibid*.

[195] *Ibid*.

[196] UK Ministry of Defense, "Joint Doctrine Note 1/18 – Cyber and Electromagnetic Activities," Development, Concepts and Doctrine Centre, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, p. 43-44

[197] SID Today, "The Evolution of HF," 17.07.2003, https://assets.documentcloud.org/documents/3008286/The-Evolution-of-HF.pdf; Note: HF is short for High Frequency, i.e. tactical military radios operating in the frequency band between 3 to 30 MHz

[198] UK Ministry of Defense, "Joint Doctrine Note 1/18 – Cyber and Electromagnetic Activities," Development, Concepts and Doctrine Centre, February 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, p. 44

[199] Richard B. Gasparre, "The Israeli 'E-tack' on Syria – Part II," Airforce Technology, 10.03.2008, https://www.airforce-technology.com/features/feature1669/

according to Gasparre is that "Suter operators can then act as replacement managers to control enemy radars," such as pointing it away from incoming aircraft.[200]

A similar claim was made by David Fulghum over at Aviation Week & Space Technology in 2010, as quoted by a RAND study in 2013. According to Fulghum, "the basic components of airborne electronic or cyber-attack are a sensor that can map an enemy network, the precise location of an antenna that feeds the network, and an electronic scanned antenna that can generate a data stream packed with inquisitive algorithms. That data stream can be beamed into the proper antenna; the target network can be entered and exploited."[201]

If such a capability exists in this form, it will have to combine offensive cyber operations (i.e., network intrusion and infection) with electronic warfare (i.e., specifically identifying the radar RF-receivers and jumping the air gap from several kilometers away). As of this writing it is still unclear how and whether this is technically possible or whether the Suter story is entirely made up.

What we definitely do know is that air defense systems have long been a thorn in an attacker's eye. The first unverified computer network operation against an air defense system occurred during the Kosovo war in 1999. Fred Kaplan explained in his book "Dark Territory" that a clandestine US intelligence unit called IOC "installed a device at the Serbian phone company's central station. The other bit of luck was that," [T]he Serbs had recently given their phone system a software upgrade. The Swiss company that sold them the software gave U.S. intelligence the security codes."[202] The end result: US intelligence could "roam through the entire [phone] network – including the air-defense lines and telecommunications for the entire Serbian military."[203] On the few occasions when US aircrafts needed additional protection, US intelligence would hack into the Serbian air defense system and feed it false information, "making the radar screen monitors think the planes were coming from the west, when in fact they were coming from the northwest."[204]

Recently, the big hit Israeli TV series "Tehran" depicted a similar scenario executed by the Mossad and the Israeli Air Force. It included trying to cripple the Iranian power grid prior to an Israeli air strike, breaching into the Iranian telephone network to gain access to Iranian air defense systems, as well as feeding Iranian radars false data to cloak the incoming Israeli strike package.

Overall, it needs to be highlighted that it is tremendously difficult for researchers, academics, and journalists to grasp and confirm what CEMA capabilities militaries around the world are working toward and able to leverage on the battlefield. The public-facing information security community is unable to open up this space, as they are generally unable to discover vulnerabilities and develop and test exploits against military systems. Looking at off-the-shelf solutions that militaries have procured could be of some help to gain a rudimental understanding as to the vulnerabilities of mobile troops in the field. But the picture is entirely different when we are talking about vulnerabilities in radar stations, missile systems, armed drones, or entire military aircrafts, ships, and tanks.

A partially unclassified 2021 audit by the DoD's Inspector General on "Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle," does however provide some relevant insights. The report looks at five weapon systems, including the MIDS Joint Tactical Radio System, the Advanced Anti-Radiation Guided Missile (AARGM), the B-2 Spirit Bomber and the AC-130J gunship. For the AARGM, for example, the report explains that, "the AARGM program officials used cyber risk and threat assessments provided by the Naval Criminal Investigative Service to assess risks and update requirements to mitigate cybersecurity risk."[205] The B-2 Spirit Division "updated cybersecurity requirements based on intelligence-based threat assessments and cyber resiliency penetration testing results."[206] And the AC-130J PSP officials "performed a series of assessments, which were used to develop Risk Assessment Reports, to identify and mitigate cybersecurity threats to the aircraft and subsystems that were designed to destroy specific targets. For example, a 2019 cyber risk assessment identified a cybersecurity threat [redacted]."[207]

If we take the standard information security viewpoint that it is extremely difficult to jump an air gap (not even to speak of an air gap of several kilometers) and develop targeted malware for specific systems, one has to wonder how an adversary would technically exploit a

[200] *Ibid*.

[201] Isaac R. Porche III et al., "Redefining Information Warfare Boundaries for an Army in a wireless World," RAND Corporation, 2013, https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf, p. 53-54

[202] Fred Kaplan, "Dark Territory: The Secret History of Cyber War," Simon & Schuster, 2017, p. 113

[203] *Ibid*.

[204] *Ibid*. 114

[205] Inspector General, US Department of Defense, "(U) Audit of Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle," DODIG-2021-051, 10.02.2021, https://media.defense.gov/2021/Feb/12/2002581936/-1/-1/1/DODIG-2021-051.PDF, p. 16

[206] *Ibid*., p. 17

[207] *Ibid*., p. 19

vulnerability in an AC-130J moving at 400km/h at an altitude of 10,000 feet, or an AARGM that is locked onto its target. But apparently, the vulnerabilities in those weapon systems are deemed serious enough within the Pentagon's risk assessment that these systems are subjected to penetration testing and vulnerabilities are fixed based on foreign intelligence collection. On the one hand, this could indicate that the US military has likely developed CEMA capabilities that is able to touch and breach an AC-130J or AARGM deployed in the field. On the other hand, it might show that US adversaries are developing exploits for a range of US military systems, and might theoretically be able to touch them in the field.

Without relevant insights into the realities of offensive cyber and electronic warfare capabilities targeting military systems on the battlefield, the true extent and nature of CEMA currently remains closed to the outside observer.

5 Outlook for Switzerland

Through the Armed Forces Command Support Organisation (AFCSO) the Swiss Armed Forces have recognized the potential synergies and parallels between EW, SIGINT and the cyber domain. Notably, in 2015, the Center for Electronic Operations (CEOP) was stood up within the FUB. And on 31 March 2021, the Federal Council decided that AFCSO will be developed into a Cyber Command by early 2024.[208]

In terms of CEMA, three general pathways can be envisioned: (1) continue AFCSO's efforts to bringing together EW and cyber operators within the new Cyber Command; (2) replicate US Army experimentations by standing up dedicated CEMA units; and/or (3) focus on bringing cyber and information warfare capabilities closer together.

On (1): The creation of the Swiss Cyber Command ought to offer a unique opportunity to rethink how EW and cyber operators can be brought closer together to cooperate in and off the battlefield. While the creation of an offensive expeditionary CEMA unit might currently not be in the interest of the Swiss Armed Forces, future conflict scenarios will certainly demand that militaries are able to reliably and continuously bridge air gaps to reach adversarial systems. In that sense, CEMA is a continuous process that evolves in lockstep with the digitalization of the Swiss Armed Forces itself, as well as the infrastructure and systems deployed by adversaries in the field. At the same time, CEMA will require much closer cooperation with partners and industry, and will necessitate an even greater focus on the knowledge and competence of both operators and engineers than merely on acquiring "turnkey" systems.

On (2): An offensive expeditionary CEMA unit could be an attractive approach within the context of special forces units. Open source is unclear as to whether this has already been implemented, and to what degree offensive cyber and EW capabilities are integrated within Swiss special forces units. Notably, CEMA experimentation has been taking place in US special operations forces (SOF) prior to the Army adopting CEMA.[209] As Col. Joshe Raetz, chief of staff 1st Special Forces Command, explained at Technet Augusta on 17 August 2021, "our role as the SOF task force integrating information, electronic warfare, intelligence and other special operations activities is the key to achieving the information advantage […]. The critical piece here is the importance of moving data and information at speed, scale while protecting the integrity of our command and control structures."[210] Army General Richard Clarke, commander of US Special Forces Command, put it even more bluntly in 2020 when he said that, "we need coders […]. We've been having discussions internally that the most important person on the mission is no longer the operator kicking down the door, but the cyber operator who the team has to actually get to the environment so he or she can work their cyber tools into the fight."[211]

Despite such indications and impressions of the pioneering role of US SOF in the adoption of CEMA, this report did not touch upon the specifics of the US SOF approach to CEMA for several reasons. First, there is little to no documentation as to how it was implemented. And secondly, it is unclear whether US SOF actually adopted CEMA or merely expanded to include separate tactical cyber and electronic warfare tools. In particular, it is unclear how US SOF are harnessing the synergies between cyber and EW in their missions.

On (3): In contrast to Switzerland, the US has been both on the sending and receiving end of significant information warfare operations over the past five years.

[208] Der Bundesrat, "Kommando Cyber der Armee: Bundesrat fällt personelle Entscheide," admin.ch, 31.03.2021, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-82928.html

[209] Mark Pomerleau, "Army Special Forces want to integrate more with other military units on info warfare," C4ISR.net, 19.08.2021, https://www.c4isrnet.com/smr/technet-augusta/2021/08/19/army-special-forces-want-to-integrate-more-with-other-military-units-on-info-warfare/

[210] Mark Pomerleau, "Army Special Forces want to integrate more with other military units on info warfare," C4ISR.net, 19.08.2021, https://www.c4isrnet.com/smr/technet-augusta/2021/08/19/army-special-forces-want-to-integrate-more-with-other-military-units-on-info-warfare/

[211] Jared Keller, "SOCOM chief: Door-kickers are out, cyber operators are in," Task & Purpose, 12.05.2020, https://taskandpurpose.com/news/special-operations-forces-cyber-warfare/

Russia's interference in the 2016 US Presidential Election was an eye opener on the defensive end. And Joint Task Force-Ares proved – with Operation Glowing Symphony against the Islamic State's propaganda team – that offensive cyber operations can achieve tangible results.

Unsurprisingly, the synergies between cyber and information warfare have been of growing interest to the US Army. At AFCEA 2019, Commander of US Army Cyber Command Fogarty finally announced that US Army Cyber Command will be transformed into the "Army Information Warfare Operations Command" by 2028.[212] This is also why ARCYBER's mission statement currently reads: "U.S. Army Cyber Command integrates and conducts cyberspace operations, electromagnetic warfare, and information operations […]."[213] In the summer of 2020, Fogarty qualified his comment in an article for the Cyber Defense Review, explaining that "the Army is currently evaluating whether [operations in the information environment], [information warfare], or some other concept should replace [information operations] to describe an expanded Army mission in the [information environment]. We are likewise considering whether Army Cyber Command (ARCYBER) should change its name to more accurately reflect the full spectrum of its mission portfolio."[214]

To a large degree, the US Army is essentially trying to harness the synergies between cyber and information warfare by replicating a CEMA-esque process. This means that tactical experimentation will inform doctrine and concepts, which in turn will help set new capabilities requirements to stand-up new units that can dominate the intersection of cyber-IW. US Special Forces Command has been on a similar trajectory, by currently building an Information Warfare Center that aims to "consolidate the command's psychological operations capabilities and will wrap around other information related capabilities such as cyber and space."[215] Special Forces Command is also trying to reduce the digital footprint of its personnel on social media, fitness tracking apps, and other databases that can be used to identify US bases, individual operators, and their families.[216]

When it comes to the question as to whether the synergies between cyber and IW are more important and impactful than the battlefield synergies of CEMA, then the answer is a resounding: We do not know. In both areas, we are still at the very beginning of figuring out what kind of direct and cascading effects we can tactically achieve on the battlefield, as well as create within and against the civilian population and infrastructure of an adversarial state. For the Swiss Armed Forces, the question whether to focus on cyber and IW or cyber and EW largely depends upon what kind of conflicts and missions the Swiss Armed Forces are preparing for to fight and defend against in the future.

[212] Kimberly Underwood, "Army Cyber to Become an Information Warfare Command," AFCEA, 14.03.2019, https://www.afcea.org/content/army-cyber-become-information-warfare-command

[213] US Army Cyber Command, "Our Mission," n.d., https://www.arcyber.army.mil/

[214] Stephen G. Fogarty & Bryan N. Sparling, "Enabling the Army in an Era of Information Warfare," Cyber Defense Review, Summer 2020, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fogarty_Sparling_CDR%20V5N2%20Summer%202020.pdf, p. 18

[215] Mark Pomerleau, "Special Forces to build 'influence artillery' for online campaigns," C4ISR.net, 18.02.2021, https://www.c4isrnet.com/information-warfare/2021/02/18/special-forces-to-build-influence-artillery-for-online-campaigns/

[216] Jeremy Hsu, "The Strava Heat Map and the End of Secrets," Wired, 29.01.2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/; M. DeLaTorre, "As ISIS threats online persist, military families rethink online lives," Oklahoma News 4, 25.03.2015, https://kfor.com/news/as-isis-threats-online-persist-military-families-rethink-online-lives/; Mark Pomerleau, "Special Forces to build 'influence artillery' for online campaigns," C4ISR.net, 18.02.2021, https://www.c4isrnet.com/information-warfare/2021/02/18/special-forces-to-build-influence-artillery-for-online-campaigns/

Abbreviations

A2/AD	Anti-access/Area denial
AARGM	Advanced Anti-Radiation Guided Missile
ACOIC	Army Cyberspace Operation and Integration Center
ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
AEHF	Advanced Extremely High Frequency
AFCEA	Armed Forces Communications and Electronics Association
AFCSO	Swiss Armed Forces Command Support Organisation
ARCYBER	Army Cyber Command
ARFORCYBER	Army Force Cyber Command
ASB	Air Sea Battle
ATP	Army Techniques Publication
BCT	Brigade Combat Teams
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CCOE	Cyber Center of Excellence
CEMA	Cyber Electromagnetic Activities
CENTCOM	US Central Command
CEWO	Cyber Electronic Warfare Officer
CIG	CEMA Capability Integration Group
CNA	Computer Network Attack
CO	Cyberspace Operations
CREW	Counter radio-controlled improvised explosive device electronic warfare
CSCB	Cyber Support to Corps and Below
CSCB	CEMA Support to Corps and Below
CTC	Combat Training Centers
CWB	Cyberspace Warfare Battalion
DAMO-CY	Department of the Army's Management Office – Cyber
DAMO-SO	Department of the Army's Management Office – Strategic Operations
DCDC	UK Development, Concepts and Doctrine Centre
DoD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
ECT	Expeditionary CEMA Teams
ELINT	Electronic Intelligence
EM	Electromagnetic
EMS	Electromagnetic Spectrum
EW	Electronic Warfare
EWO	Electronic Warfare Officer
FM	Field Manual
FTX	Field Training Exercise
HF	High Frequency
I2CEWS	Intelligence, Information, Cyber, Electronic Warfare and Space
IED	Improvised Explosive Device
IFRI	Institut français des relations internationales
IIA	Inform and Influence Activities
INEW	Integrated Network Electronic Warfare
IO	Information Operations

IoT	Internet of Things
IPb	*informatsionnoye protivoborstvo*
IRC	Information-Related Capabilities
ISR	Intelligence, Surveillance, and Reconnaissance
JCG	Joint Cyber and Electromagnetic Activities Group
JCN	Joint Concept Note
JDN	Joint Doctrine Note
JEMSO	Joint Electromagnetic Spectrum Operations
JFC	Joint Forces Command
JFCC-NW	Joint Functional Component Command - Network Warfare
JP	Joint Publication
JRTC	Joint Readiness Training Center
MDO	Multi-Domain Operations
MDTF	Multi-domain Task Force
MoD	Ministry of Defense
MUTC	Muscatatuck Urban Training Center
NCF	National Cyber Force
NKOCC	Non-Kinetic Operations Coordination Cell
NSA	National Security Agency
NTC	National Training Center
OCO	Offensive Cyber Operations
OIE	Operations in the Information Environment
PLA	People's Liberations Army
RAAF	Royal Australian Air Force
RF	Radio Frequency
SIGINT	Signals Intelligence
SMO	Spectrum Management Operations
SOF	Special Operations Forces
SOP	Standard Operating Procedure
TRADOC	US Army Training and Doctrine Command
UAV	Unmanned Aerial Vehicle
USCYBERCOM	US Cyber Command
USMC	US Marine Corps

About the Author

Stefan Soesanto is a Senior Researcher in the Cyberdefense Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich. Stefan works closely with the Swiss Defense Department. His writings have been published by the Cyber Defense Review, Lawfare, the Royal Institute Elcano, the Konrad-Adenauer Stiftung, Defense One, and the Council on Foreign Relations.

CSS
ETH Zürich

The **Center for Security Studies (CSS)** at ETH Zürich is a center of competence for Swiss and international security policy It offers security policy expertise in research, teaching, and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.