FEATURE

Waging Information Warfare for Asymmetric Advantage

Increasing Multi-Domain Speed, Survivability, and Lethality in the Indo-Pacific

Maj Brandon Spader, USAF

Abstract

This article presents the Converged Effects Cells (CEC) theoretical model to organize and employ information warfare (IW) capabilities in the Indo-Pacific necessary for the success of Agile Combat Employment (ACE) and Joint All-Domain Command and Control (JADC2).[1],[2] This construct operationalizes the ideas of Lt Gen Timothy Haugh and Brig Gen George Reynolds to achieve convergence against strategic power competitors and overcome current limitations in waging IW in modern, contested environments. The CEC construct is based off the global exploitation model deployed in early 2016 by elements of United States Special Operations Command (USSOCOM). It also incorporates the operational realities of the cryptologic enterprise and offensive cyber-operations (OCO) in US Indo-Pacific Command (USINDOPACOM). Inherent to this model is the (1) Central Security Service's revitalization (i.e., P2/P3 integration), (2) 16 Air Force's reorganizing organic capabilities, (3) joint force, interagency (IA), intelligence community (IC), and allied partner integration, (4) persistent operations across the entire competition continuum, and (5) over-the-horizon targeting and fires. This model creates a dynamic, scalable capability that blurs the line between kinetic and nonkinetic operations while simultaneously adding flexibility, resilience, and lethality to the current vulnerable and static IW architecture in the Indo-Pacific.

***

While the United States government has no official definition of information warfare (IW), this article defines IW as kinetic and nonkinetic operations conducted domain agnostic that create lethal or nonlethal effects. While this broad statement can easily apply to most military operations, IW influences, disrupts, corrupts, paralyzes, and usurps the decision-making capabilities of adversaries, either cognitively or via physical manifesta-

tion, to gain a competitive advantage across the entire spectrum of the competition continuum. The synchronous and integrated employment of cyberspace, intelligence, surveillance, and reconnaissance (ISR), electromagnetic warfare (EW), information operations (IO), and other support elements such as weather, public affairs, and law enforcement (LE) define converged IW. In addition, the manifestation of converged IW outcomes presents a holistic warfighting capability that can be layered with additional military, diplomatic, and economic instruments of national power to create an asymmetric advantage against both state and nonstate actors.[3] Specific to the Indo-Pacific, the successful application of IW is paramount to overcome geographic, quantitative, and qualitative advantages of our adversaries and is a vital American offset for advantage against strategic competitors.

The Current Areas of Risk for Joint Force Commanders in Waging IW

The current alignment of IW units in US Indo-Pacific Command (USINDOPACOM) is disparate and housed in no fewer than four wings. While this alone is not necessarily problematic, the lack of converged training, deployment, and mission execution is an area of concern that limits the effective execution of converged IW operations.[4] While the establishment of Task Force Skyraider signals 16 Air Force's (AF) intention to present converged IW capabilities to USINDOPACOM, 16 AF lacks a unified operational construct that provides synchronized kinetic and nonkinetic operations spanning the requirements intrinsic in the competition continuum.

Inherent in this non-unified execution model is the lack of combined mission authorities and signals intelligence (SIGINT) accesses (i.e., Title 10, Title 50, querying approvals, security read-ons) that fail to achieve the aggregate of the units' capabilities for combatant commands and service components. Comprising these units are Airmen from different program element codes (PEC) (i.e., P2 and P3) that are limited in their ability to effectively integrate warfighting capabilities. Thus, these Airmen are not utilized to their full operational potential, based on the current interpretation of The Economy Act (31 U.S.C.1535).

Additionally, these units are consolidated at major cryptologic and operational hubs. This in turn presents the adversary with a small target list that, if struck, would cripple the United States' ability to generate IW effects. These large, static hubs primarily require the integration of the warfighter at the stationary facilities to produce converged IW effects. The hubs have limited capability in presenting IW outcomes to the warfighter in the battlespace. In addition to not being surviv-

able, this construct does not take advantage of secured geography and time that can be exploited and leveraged for IW placement and access which is the cornerstone of the Air Force's ACE concept. Holistically, the United States lacks a model for executing converged IW operations in a dynamic environment that is survivable against enemy targeting, effective in a denied, disrupted, intermittent, limited (D-DIL) communications environment, and lethal in supporting both kinetic and nonkinetic fires.

Integrating Cryptologic Airmen Across the Enterprise

For any IW capability developed and deployed with a focus on convergence, the enduring challenge of integrating all cryptologic Airmen and overcoming the legal and bureaucratic restraints (i.e., achieving P2/P3 integration) must be addressed. The complexities inherent with 16 AF units is that they have personnel operating on common missions under different PECs. This leads to concerns about meeting the legal requirements per The Economy Act (31 U.S.C.1535) and currently limit 16 AF in achieving a truly integrated cryptologic force that taps the full potential in generating IW effects. To achieve integration of cryptologic Airmen, the problem must be tackled from a short-term and a long-term perspective.

In the immediate, short term, the National Security Agency's (NSA) Cryptologic Support Team (CST) construct used in the Global War on Terror (GWOT) provides a blueprint to streamline cryptologic Airmen integration. Evolving the old CST construct, the establishment of *Integrated Cryptologic Elements* at the cryptologic centers creates a model in which 16 AF mans the billets that comprise an NSA capability (i.e., Title 50) tasked to support military operations (i.e., Title 10).[5] With 16 AF comprising the NSA capability, and with that NSA capability being tasked to support military operations, the Integrated Cryptologic Element, while a Title 50 asset, would operate nearly identical to a Title 10 element in regards to capability presentation.

The Integrated Cryptologic Element does not require any additional manning from either 16 AF or NSA but would code existing 16 AF-presented billets within NSA to specific cryptologic offices operating under established authorities and operational approvals. Additionally, the Integrated Cryptologic Element does not place any additional mission "tax" on the NSA but solely codifies billets at the cryptologic centers that would directly support the combatant commander, via the National Cryptologic Representative (NCR) at the Combatant Command, while also providing a quick reaction force for holistic cryptologic support on behalf of NSA. This construct arms NSA to better serve as a *combat support agency* by presenting a cryptologic capability that can operate

away from the cryptologic center that is trained to immediately integrate with combat elements during a contingency.

These personnel in the Integrated Cryptologic Element have all their Title 50 authorities, querying approvals, and security read-ons required by NSA to conduct their cryptologic mission at the cryptologic center. The Integrated Cryptologic Element would be responsible for existing daily tasks in their respective cryptologic offices; however, they would also be responsible for integration and coordination with warfighting elements in collaboration with the NCR. This responsibility for direct warfighter support, as was the case in GWOT, opens the aperture for consistent training and operational employment with other 16 AF units and their capabilities.[6] The Integrated Cryptologic Element serves as the cryptologic enterprise's expeditionary force charged with supporting forward military forces and the conduct of their operations.

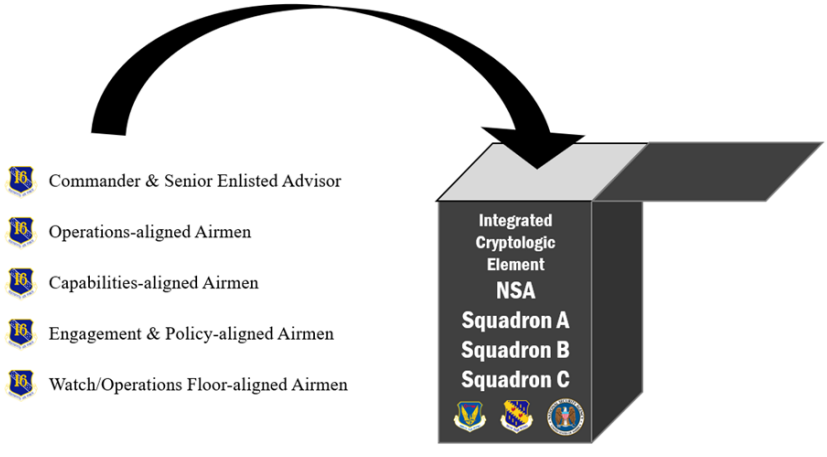

Figure 1. Composition of 16 Air Force-manned Integrated Cryptologic Element from NSA organizational elements operating under Title 50 authorities.[7] The Integrated Cryptologic Element concept uses the Airmen under the operational control (OPCON) of NSA with the explicit task of supporting military operations. Based off the CST used in GWOT, this construct has proven effective to bring NSA-capabilities to the warfighter at speeds and via mechanisms customized to meet the operational environment and military end-user.

While the above construct provides a short-term solution, a long-term solution requires a new model that reinvigorates the virtually static Central Security Service (CSS). 16 AF, along with the other service cryptologic elements, should work with NSA/CSS to develop a holistic service cryptologic strategy.[8] In this strategy, entire mission areas that are currently in NSA's portfolio would be presented to the individual services to lead by leveraging their SIGINT Operational Tasking Authority and responsibilities per the CSS. This model allows for the integration

of cryptologic Airmen, as well as NSA-civilians, to execute problem-centric ISR and would look to the specific service to lead a federated mission across the cryptologic enterprise. In the case of the Indo-Pacific, 16 AF would execute the service-led mission under a federated mission concept against a target country's specific capability (e.g., integrated air defense system (IADS)), which is congruent with the tasking of Task Force Skyraider. This model, in development by the Air Force Cryptologic Office, is the Converged Air Force Enterprise Mission (CAFEM) and is reliant on a service cryptologic strategy that outlines missions led by each service and corresponding querying authorities to allow access to the required data for exploitation, analysis, and dissemination.

Overlaying the short-term solution of building the Integrated Cryptologic Element with the long-term solution of 16 AF executing a traditional NSA mission under an approved service cryptologic strategy overcomes the historical bureaucratic and legal problems associated with the Economy Act (31 U.S.C.1535) and integrates P2 and P3 Airmen. Additionally, 16 AF would be armed with a service-led expeditionary capability to inject tactical SIGINT collect, cyber-ISR data, and OCO-derived intelligence data into the larger cryptologic enterprise—a model proven successful by United States Cyber Command (USCYBERCOM) and the NSA with a similar initiative. In its totality, to achieve the integration of all cryptologic Airmen, 16 AF should leverage the NSA-approved CST-model to create the Integrated Cryptologic Element and inject the long-term authorities and mission management of the CAFEM to create a solution that arms the entirety of the cryptologic enterprise with never-before seen capabilities and resources.

Integrating 16 AF IW Units

With 16 AF manning the Integrated Cryptologic Element and the capability to present holistic cryptologic capabilities to the warfighter, the first critical piece of a converged IW construct emerges. Leveraging the 2020-established Task Force Skyraider operational order, an opportunity presents itself to merge the Title 50 Integrated Cryptologic Element with the various Title 10 capabilities present across 16 AF. Injecting capabilities such as cyber-ISR, weather, National Tactical Integration (NTI), Distributed Common Ground Station (DCGS) Analysis & Exploitation Teams (AET), Air Forces Cyber (AFCYBER)-retained Cyber Combat Mission Teams (CMT), Air Force Computer Network Exploitation (CNE), communications infrastructure, targeting analysis, and flying unit intelligence creates a construct that exercises Title 10 and Title 50 authorities in unison while simultaneously providing converged IW effects to the strategic commander and tactical warfighter.

This construct ensures converged daily operations and training events integrating Intelligence Squadrons, Operational Weather Squadrons, Cyberspace Operations Squadrons, Intelligence Support Squadrons, and various levels of staff, with the end goal of arming 16 AF with a "fight tonight" IW competence that is target-focused and leverages the holistic 16 AF warfighting capability. The construct allows for simultaneous intelligence collection, exploitation, and fires to satisfy both intelligence and nonkinetic targeting requirements, while simultaneously supporting kinetic operations. In its totality, the integration of Title 10 and Title 50 capabilities from the various 16 AF organizations atop the TF Skyraider construct, and merged with the Integrated Cryptologic Element, forms the *Converged Effects Cell* (CEC).

The CEC serves as a self-sustained capability that operates independently or as part of a cellular network dependent on the permissibility of the communications environment. With the Operational Weather Squadron providing environmental updates to factors that can affect active and passive operations, the Intelligence Squadron develops and enacts collection management strategies to exploit the operational environment for the specified area. From forward-exploited intelligence by the DCGS AET, the Intelligence Squadrons also provide NTI to ensure tactical units are armed with strategic cryptologic capabilities and insight, while also executing derivative active intelligence collection operations via cyberspace. Simultaneously, the Cyberspace Operations Squadron's CMTs leverage the intelligence provided by the Intelligence Squadrons and the Integrated Cryptologic Element and overlay it with the operational weather forecast to plan and deliver nonkinetic fires in coordination with the targeting analysts. While the Cyberspace Operations Squadron manages the infrastructure and weapons system used for nonkinetic fires, the Intelligence Support Squadron manages the infrastructure used for intelligence operations. Providing post-strike battle damage assessments (BDA), the Air Force CNE operators in collaboration with the CMTs assess the effectiveness of the fires and the impact on the target. The self-sustaining processes within the CEC allows for converged IW operations in a D-DIL communications environment with planning, execution, and deconfliction being conducted internally with limited external communication requirements.

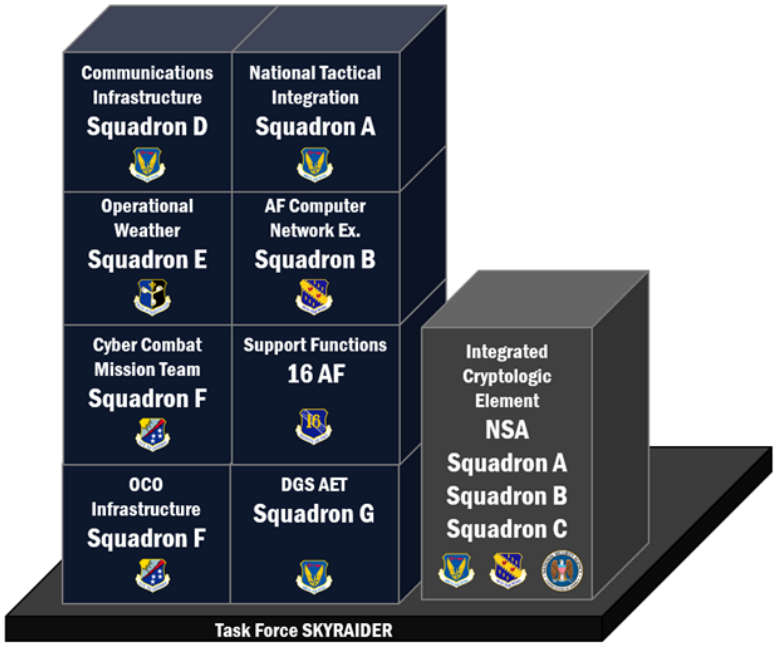

Figure 2. Composition of notional Converged Effects Cell. Each block denotes a unique capability, as well as the associated 16 AF squadron(s).

Cyber-Operations & Persistent Engagement in the Converged Effects Cell

As part of the CEC, the AFCYBER-owned CMT provides 16 AF with an OCO fires capability that operationalizes the exploitation derived from the collocated elements and the broader enterprise. While CMTs have primarily fallen under the OPCON of theater Joint Force Headquarters–Cyber commands, the precedence set by GEN Paul Nakasone, Commander, USCYBERCOM, breaks that mold. General Nakasone's alignment of a non-Joint Force Headquarters–Cyber (JFHQ-C) (Navy) unit to the USINDOPACOM target-set in 2020 provides a template to apply to AFCYBER and USINDOPACOM.

Augmenting JFHQ-C (Navy) and their subordinate elements in the Indo-Pacific, the realignment of another service's cyber capability without falling subordinate to JFHQ-C (Navy) proved to be a successful model. Based off this success, 16 AF/AFCYBER should use this vignette to retain OPCON of one CMT currently manned by the Indo-Pacific-aligned Cyberspace Operations Squadron. With 16 AF/AFCYBER retaining OPCON of a CMT in the Indo-Pacific, the CEC would support Theater Joint Forces Air Component Commander (TJ-

FACC), USCYBERCOM, USINDOPACOM, and 16 AF/Task Force Skyraider OCO priorities while executing persistent engagement operations.[9]

While postured to conduct Operational Plan (OPLAN) activities in the time of a contingency, the CMT in the CEC can leverage authorities to persistently engage the enemy in day-to-day operations. Operating below the threshold of armed conflict along the competition continuum and weaponizing the intelligence gathered from collocated capabilities in the CEC, the CMT can serve as a 21st Century "Voice of America." For example, publicly highlighting the People's Republic of China's (PRC) predatory lending practices inherent with the Belt Road Initiative, the abuse by high-ranking PRC leaders such as the sexual assault of tennis star Peng Shuai, corruption in the upper echelons in the PRC leadership, and the ongoing human rights violations of Uighurs in Northwest China, the CEC can decrease the competitiveness of the PRC by "weaponizing the truth." From these operations, the PRC is forced to reallocate finite resources to counter negative narratives that would otherwise be used to fund outward expansion. The CEC can inject disinformation into the targeted adversary's society to spur the unwitting propagation of misinformation by its populous.

As the relationship between the United States and the PRC moves closer to that of "conflict" on the competition continuum, the rhetoric would increase in focus toward weakening the adversary—if that is the desired end state. Spreading messages that highlight freedom of speech, freedom to assemble, and a commitment to truth all degrade a nation's ability to domestically control the information space while allowing the injection of pro-American ideals.[10] Further degrading the target nation's ability to control mass media and information, the CMT can target the adversary's technical capabilities required to control their internet media, thus opening periods of time for the population of the target nation to access nongovernment restricted web content. From these sporadic leaks of nonfiltered content, the United States can sow entropy into the regime's ability to govern that can compound over time and create chaos in the target nation.

Similarly, the CEC serves as a "reconnaissance platform" for collecting against the enemy's planning and execution of IW effects against the United States and allied nations. In this role, the CEC collects, exploits, and informs senior leaders of an enemy's malicious IW intentions prior to their launch against US or allied interests. Operating as an indications & warning (I&W) sensor, the CEC supports Cyber Mission Force Defensive Cyberspace Operations and Department of Defense Information Network Operations, while also assisting Cyber National Mission Force and Cyber Protection Force operations.[11] The forward presence of the CEC enables placement and access, as well as opens partnership opportuni-

ties, to key terrain for use in illuminating enemy capabilities and intentions to allow for appropriate measures to be taken.

Learning from Special Operations and the Regional Exploitation Center Model

The CEC finds its origin from the Regional Exploitation Center (REC) model developed by joint special operations forces (SOF) during Operation Inherent Resolve in Iraq and Syria. Subordinate to the regional task force (RTF) commander, the REC provides the RTF commander with a scalable, modular collection and exploitation hub that is custom composed of capabilities to match the operational requirement and environment. The composition of each REC, in which a specific geographic region may have several RECs, differs based upon the unique requirements for the specific operating area, as well as the intended effects-generation requirement. This construct is now codified at United States Special Operations Command (USSOCOM) and forms the basis for global joint identity activities as published in Joint Doctrine Note 1-20.[12]

The REC provides maneuverability to IW and operates in contested and D-DIL communication environments. Through achieving localized superiority, a window in time and space opens that allows the REC to take advantage of fleeting access in support of nonkinetic and kinetic operations. With pre-approved cryptologic administrative actions ready for implementation, there are no extensive administrative routing times, making the deployment of the REC with all required cryptologic authorities expedient.

As geographic access is lost or the risks are deemed too high to operate, the REC collapses into a neighboring, operational REC. Repeating the process of expanding and collapsing with the ebb and flow of the operational environment, the REC is a dynamic entity that is constantly maneuvering. Additionally, the small, custom-built, cellular-construct of the REC provides survivability to the SOF-enterprise as well as line-of-sight (LOS) connectivity to mitigate a D-DIL communications environment with other tactical users. The decentralized execution of IW operations at the REC allows SOF an asymmetric advantage in speed of operationalizing collected data, conducting novel OCO, and enabling operations to seize key terrain. From this key terrain, new accesses are presented for IW effects generation as part of the larger RTF's offense—further continuing the cycle.

The power behind the REC is the ability to integrate the broader Intelligence Community (IC), interagency (IA), and allied partners. Since the REC houses most tactical intelligence access for a particular target, the IA/IC and allied

partners use the REC as the forward injection point for their respective capabilities (e.g., digital forensics, document exploitation (DOMEX), debriefings, LE investigations). With this integration, the REC's Title 10 authorities are enhanced with the various operating authorities inherent with the collocated agencies to create a whole-of-government IW capability that spans all instruments of national power. This approach proved highly effective in combating transregional targets, specifically the foreign terrorist fighter threat and specific technology proliferation.

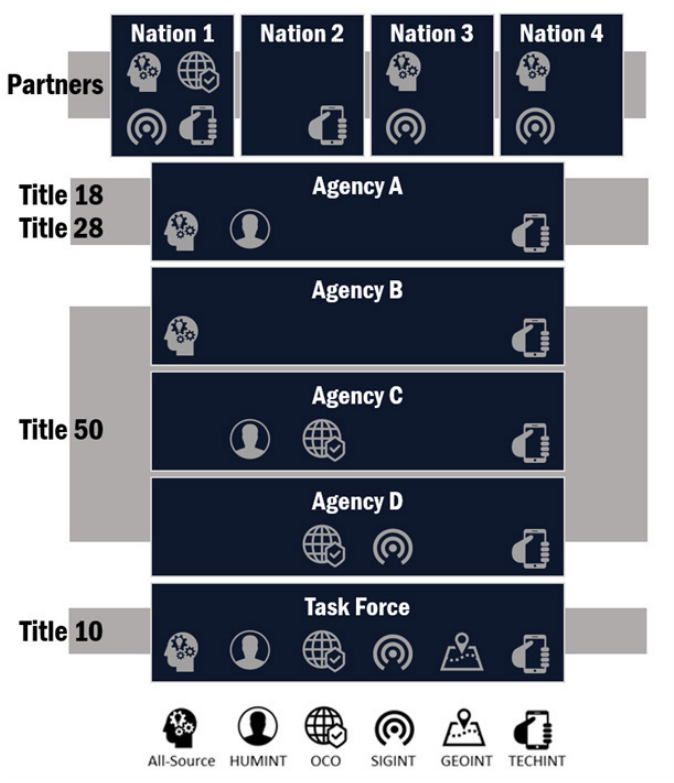

Figure 3. Notional construct of Regional Exploitation Cell capabilities and authorities. Overlapping capabilities of the various IA/IC partners with those of our allied nations provides a holistic force that is suited to meet the operational requirements directed by the joint force commander.

Integrating the Interagency, Intelligence Community, and Allied Partners

For successful and synchronized IW operations across all domains, the joint commander must be armed with a whole-of-government complement of capabilities. The capabilities afforded by the broader IA/IC extends the reach and

impact of the joint commander using complimentary authorities (e.g., Title 28, Title 18, Title 6, and Title 14) to traditional Title 10 and Title 50 operations. Given the global nature of the IW battlespace, leveraging the authorities inherent within the IA/IC are critical to accessing and safeguarding domestic information technology systems vital to the United States, as well as creating novel effects against a target nation. The forward presence of the CEC, along with the Cell's convergence-centric approach to operations, entices the broader IA/IC to integrate. The symbiotic relationship between the joint commander and the IA/IC at the CEC provides the joint commander with additional capabilities to combat the enemy while the IA/IC has forward-edge access to operations and data. From this forward-edge access, the IA/IC can leverage available communication pathways to ingest and export agency-prioritized data to support their organic operations independent of the CEC.

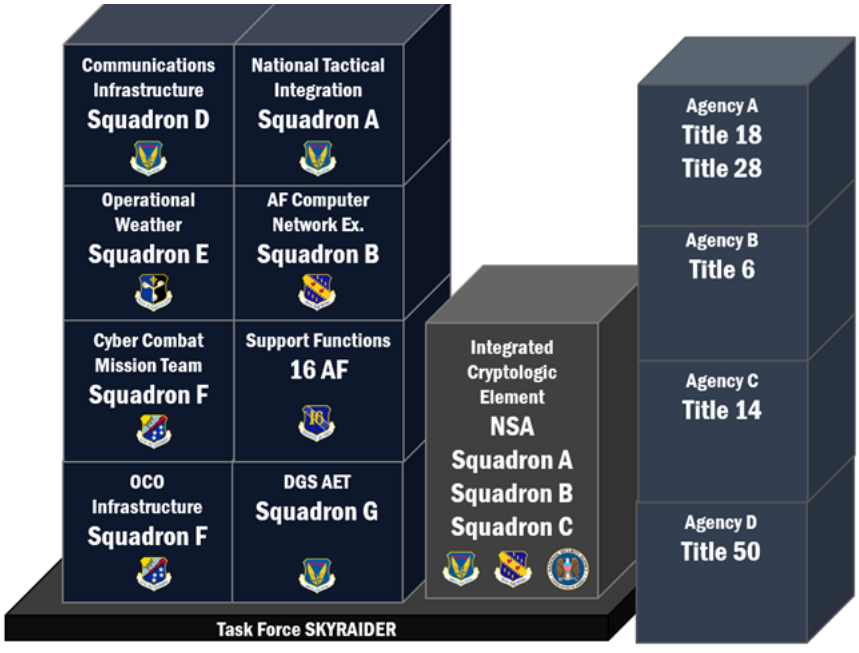

Figure 4. Composition of a notional Converged Effects Cell in the Indo-Pacific with IA/IC integration. Each block denotes a unique capability, as well as the associated 16 AF squadron(s) and associated authorities for operations. Integrating IA/IC elements expands the operational capabilities of the IW construct, writ large.

Given the geographic disparate nature of the CECs and the role of allied forces, integrating foreign partners into the Cells provides multi-order advantages. First, integrating allied forces brings new capabilities, expertise, and novel thinking to the IW fight for the joint commander. As was proven at the REC, certain allied partners have niche skills absent in the US military and by integrating them into

the fight, the aggregate combat power only increases. Second, data derived from the CEC is a currency that the joint commander can use to achieve operational goals. For instance, the joint commander can provide specified data to an allied nation in exchange for permission to deploy a CEC within their borders or allow over-flight rights for aircraft. The CEC is not only a converged IW capability against a targeted nation, but the Cells also serve as a rallying point to strengthen allied bonds against a common threat.

Employing Converged Effects Cells in USINDOPACOM

The CEC, modeled after the RECs used by SOF in semi-permissible environments, encompasses the various 16 AF capabilities, the Integrated Cryptologic Element, and serves as an anchoring point for IA/IC and allied nation integration. While the operational requirements and environment dictate each CEC's composition, the agility of the construct provides a new level of IW maneuverability and subsequent survivability.

Each CEC deployed in the Indo-Pacific comprises the capabilities required by the joint commander for the geographic space and time they operate in. While one CEC may have the full complement of IW warfighters, another CEC may not have OCO capability due to a lack of required infrastructure or target access. Just like the personnel manning and the specialty capabilities represented at each CEC, the compute capability and capacity at each CEC represents the unique operational requirements dictated by the joint commander. The CEC provides the joint force commander a tailorable, cellular IW construct that is versed in converged operations and operates either autonomously or as part of the broader network across the entire competition continuum.

The CECs are housed across various domains and within a variety of modalities. From clandestine, covert, and overt terrestrial, surface maritime, subsurface maritime, and airborne platforms, the CECs operating in unison across the various platforms provide the joint force commander a resilient and effective IW effects-generation element. The CEC acts as a truly multi-domain capability that is tailorable to both the blue-force and red-force operating environments.

The CECs operate based upon the geographic environment but also the electromagnetic (EM) environment. Given the nature of IW operations, the CECs must operate at locations with favorable EM environmental factors to enable passive and active operations. Locations include densely populated centers and areas near telecommunications access point. Additionally, the CECs require placement that affords access into the targeted enemy system or network at an acceptable level of risk. This balance requires the CECs to be functional in overt, covert, and

clandestine operating modes that are manned by multi-capable Airmen trained in signature reduction, cover management, and other traditionally absent tradecraft.

The ability for the CECs in the Indo-Pacific to expand and collapse requires an expeditionary-mindedness and employment of IW that has historically been absent from the Air Force. This absence is derived from the preponderance of IW operations historically being conducted from static, cryptologic centers that are minimally integrated into the joint fires scheme of maneuver. Transplanting capabilities from the cryptologic centers to the forward edge of the battlespace presents strategic capabilities to the warfighter at greater speeds, while also adding resilience and survivability to the vulnerable IW enterprise by dispersing IW projection points across a geographic area.

As the operational environment shifts, and localized superiority secures time and space for maneuver, new CECs deploy to exploit the opportunity to create converged IW outcomes. Simultaneously, the CEC's geographic placement presents a "landing pad" for US and allied assets to inject collected data for processing and exploitation. Given the expected contested communications environment in the Indo-Pacific during a contingency operation, long-haul transfer of collected data from intelligence platforms back to continental United States (CONUS) processing sites presents several challenges. However, leveraging the placement of the CEC, LOS communications equipment can be collocated to allow for downlink of collected intelligence from multi-domain assets. Given the composition of the CEC, the downlinked data will be ingested, exploited by the DCGS AET and Integrated Cryptologic Element using manual and machine-aided tradecraft, and then organically operationalized for nonkinetic effects by collocated IW warfighters.[13] Dependent on communication permissibility, stored data can be transported back to niche centers such as USINDOPACOM headquarters, USINDOPACOM Joint Intelligence Operations Center (JIOC), 613th Air and Space Operations Center, National Air and Space Intelligence Center, JFHQ-C, and other IA/IC elements.

Overlayed with the capability to inject downlinked data from multi-domain platforms, the CEC feeds data directly from the tactical collector into the Cell's construct for immediate exploitation and analysis. The attained speed of operationalizing intelligence at the edge provides IW capabilities for the joint force at the tactical level, thus allowing for quicker IW "sortie-generation" and better synchronization with battlefield units. Additionally, the CEC's ability to house edge-processors and automation suites as part of the future Joint All-Domain Command and Control (JADC2) construct creates IW effects at faster speeds. These speeds, attained from taking a process that historically took place at large cryptologic cen-

ters and moving them down to the tactical warfighter, opens new realms of possibilities for bringing IW effects to the contested USINDOPACOM battlespace.

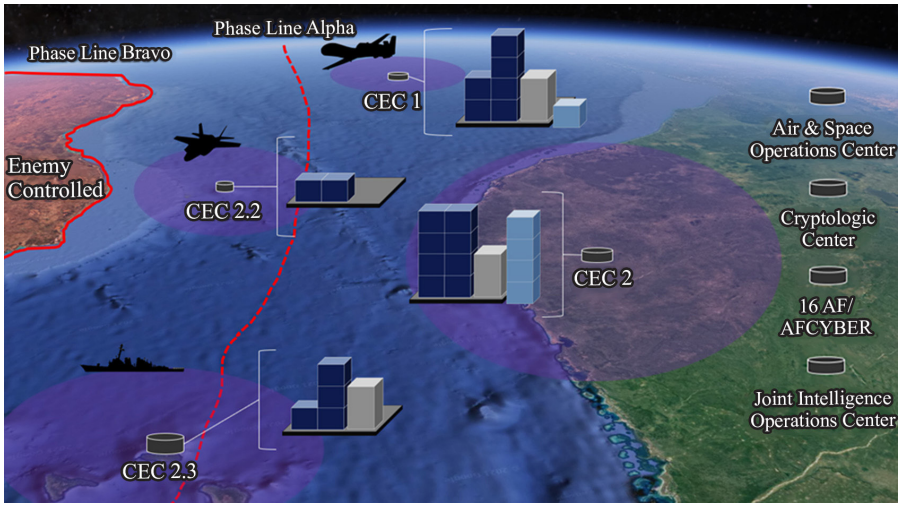

Figure 5. Employment of the Converged Effects Cell construct in a notional environment. From CEC 2, additional CECs 2.2 and 2.3 are established and deployed to take advantage of the semi-permissible environment created by pushing enemy control from Phase Line Alpha to Phase Line Bravo. The CECs house LOS communication systems to integrate IW effects with other users operating across the domains. As the environment becomes more contested and the risk is deemed unacceptable, CECs 2.2 and 2.3 reintegrate back into CEC 1 and 2. The CECs, while designed to operate self-sufficiently in a D-DIL communications environment, are also able to both "push" and "pull" data across the broader warfighting and intelligence community enterprise.

Critical Information Warfare Component for Agile Combat Employment

Founded on the idea of relying less on large traditional basing points for power projection and using dispersed forward expeditionary locations, ACE "shifts operations from centralized physical infrastructures to a network of smaller, dispersed locations that can complicate adversary planning and provide more options for joint force commanders."[14] The CEC is built on the concept of "distributed operations," where small groups operate independently rather than en masse.[15] The distribution of IW forces counters the enemy's precision strike capabilities and presents the ability to contest the enemy through IW effects, thus attriting enemy strength and their ability to conduct command and control (C2) by creating the "virtues of mass without the vulnerabilities of concentration."[16] In addition, the CEC nests precisely with the Air Force's ACE concept by expanding from the air domain and incorporating the cyber and cognitive domains. As the Air Force further advances and deploys future C2 technologies, the CECs are the

entities that will integrate and harmonize kinetic and nonkinetic environments to achieve synchronized joint all-domain operations (JADO) for warfighting.

Leveraging the concepts underpinning ACE, the tailored IW force packages of the CECs holistically act as an organism to inject entropy via multiple domains and methods culminating in chaos and subsequent paralysis in enemy power projection. The CEC relies on leaders empowered with mission command and armed with mission type orders to execute IW operations through "centralized command, distributed control, and decentralized execution."[17] Through is approach, IW effects are generated in D-DIL communications environments while leveraging the ingenuity and innovative qualities of the multi-capable Airmen. To achieve this, however, the current time-intensive bureaucratic processes associated with conducing OCO and other IW activities must be addressed.

Future Opportunities Presented: Over-the-Horizon Targeting Solutions

With the CECs serving as inject point for both passive and active intelligence collection operations, as well as housing future human-augmenting technologies, over-the-horizon targeting support options materialize. The colocation of data from multi-domain intelligence assets, layered with amplifying analysis from across the US government, allows for automated technical targeting capabilities against dynamic targets. A weapon system can be launched over-the-horizon by US or allied forces prior to being provided targeting coordinates and programmed to "call-back" or "await receipt" of targeting criteria from the CEC's targeting analysts.[18] The CEC, housing an organic capability to fuse and create targeting intelligence, feeds real-time targeting data to the weapon system all the way to the weapon's terminal targeting phase, impact, or loss-of-connection.

The CECs conduct CNE activities to gain access to an enemy's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) network and exfiltrates that data back to US and allied targeting centers. In a D-DIL environment however, the CECs can pass targeting data directly to kinetic weapon systems (e.g., Joint Air-to-Surface Standoff Missile (JASSM) Extreme Range (XR), hypersonic platforms, loitering munitions, pallet-dropped cruise missiles) within LOS.[19], [20] In this model, the CECs provide the joint force commander a mechanism to operationalize cyber-derived intelligence for real-time kinetic strikes to support dynamic targeting, analogous to multi-domain "buddy lasing."

Below is a fictional vignette that temporally depicts potential over-the-horizon targeting support the CECs can provide:

1. Special Operations C-130 based from a forward operating site takes off and launches Rapid Dragon pallet-dropped cruise missile against potential enemy nuclear missile regiment over-the-horizon with preprogrammed flight path to fly within LOS of a CEC.[21]
2. CEC launches CNE operation to gain access to enemy's communication architecture to identify enemy assets and their geographic location.
3. CEC exfiltrates the location of enemy nuclear mobile missile regiment to organic analytic systems, as well as to the crew of the C-130, 613 AOC, and USINDOPACOM J2T if communications allow. However, due to communications jamming by enemy forces, the C-130 crew, 613 AOC, and USINDOPACOM J2T may be unable to receive targeting data for ongoing or future strikes.
4. CEC exploits and processes CNE-derived data with other active and passive intelligence to create a high-fidelity geolocation for the enemy nuclear missile regiment.
5. Cruise missile flies within LOS of CEC allowing for the upload of real-time targeting data, thus overcoming enemy's communication jamming and allowing for the prosecution of the dynamic target.
6. Cruise missile strikes target.
7. CEC conducts CNE operation to provide BDA to see if the nuclear missile regiment is still active in enemy's C4ISR picture.

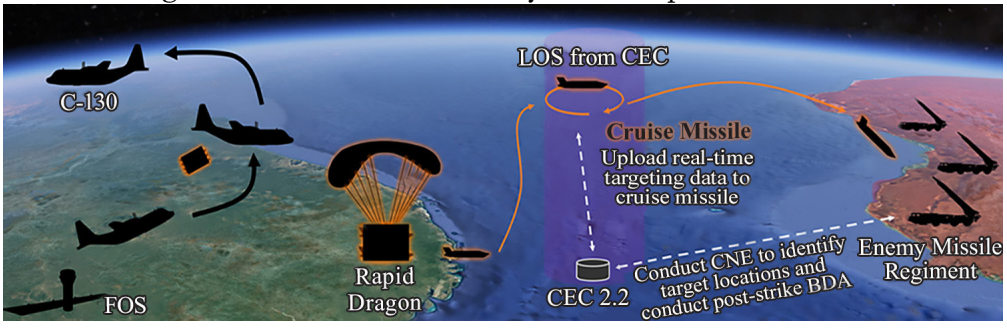

Figure 6. Notional model for a CEC supporting over-the-horizon targeting. CEC 2.2 serves as a mechanism for extracting real-time targeting data via CNE and can upload targeting data derived from organic targeting analysts via LOS communications to a launched munition, thus overcoming aspects of a nonpermissive EM environment. Additionally, the CEC can provide CNE-derived BDA using organically contained capabilities.

Conclusion

For the United States to overcome the geographic, quantitative, and qualitative advantages of our adversaries in the Indo-Pacific, IW must be embraced as a vital American offset for advantage against our strategic competitors. To tap into the

full potential that waging IW offers to the joint force commander, the Indo-Pacific requires a new operational construct to organize and employ IW capabilities across the range of the competition continuum. Through the direct application and synchronization of strategic cryptologic capabilities via the establishment of the Integrated Cryptologic Elements and subsequent integration of organic 16 AF and IA/IC capabilities, the Converged Effects Cell comes to light. The Converged Effects Cell serves as a multi-domain entity, built off the historical success of USSOCOM elements in contested environments, which provides the joint force commander persistent options across the entirety of the competition continuum for creating IW, as well as kinetic effects. From the Converged Effects Cell model, the Indo-Pacific does not take whole-of-government approach, but rather a whole-of-alliance approach to bring to bear the collective IW effects-generation capabilities of the broader alliance. These capabilities manifest and provide never-before-attainable options to the joint force commander that blur the line between kinetic and nonkinetic while reinforcing American speed, survivability, and lethality in the Indo-Pacific. ✪

Maj Brandon Spader, USAF

Major Spader is a 2008 graduate of the United States Air Force Academy. He is a career intelligence officer with four task force deployments in support of Operations Enduring Freedom, Inherent Resolve, and Freedom's Sentinel as part of a special operations task force. He is a graduate of the Joint Officer Cryptologic Career Program (JOCCP) with the National Security Agency/Central Security Service (NSA/CSS) and has served as Technical Exploitation Troop Commander for the Joint Special Operations Command (JSOC) Intelligence Brigade, Commander of a Cyber Combat Mission Team, and Director of Operations of the 37th Intelligence Squadron at Joint Base Pearl Harbor-Hickam, Hawaii.

Notes

1. Joint Doctrine Note 1-19, *Competition Continuum*, 3 June 2019.

2. Air Force Doctrine Note (AFDN) 1-21, *Agile Combat Employment*, 29 September 2021, 1-12.

3. Lt Gen Timothy D. Haugh, Lt Col Nick Hall, and Maj Eugene Fan, USAF, "16th Air Force and Convergence for the Information War," *Cyber Defense Review* 5, no. 2 (Summer 2020): 29–44, https://cyberdefensereview.army.mil/.

4. Brig Gen George M. Reynolds, "Achieving Convergence in the Information Environment: Revising the Air Component Structure," *Air & Space Power Journal* 34, no. 4 (Winter 2020), 7, https://www.airuniversity.af.edu/.

5. James Bamford, "He's in the Backseat!" *The Atlantic*, April 2006, 1, https://www.theatlantic.com/.

6. National Security Agency, *The New Design: Simple. Functional. Effective* (Fort George G. Meade), https://www.nsa.gov/.

7. National Security Agency, *The New Design*.

8. Brian Cook (Air Force Cryptologic Office), interview by the author, 20 November 2021.

9. Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *Institute for Defense Analysis*, May 2018, 2, https://www.ida.org/.

10. Brig Gen Gregory J. Gagnon, "Information Warfare, Cyberspace Objectives, and the US Air Force," *Air & Space Power Journal* 34, no. 3 (Fall 2020), 6, https://www.airuniversity.af.edu/.

11. US Army Cyber Command. "DOD FACT SHEET: Cyber Mission Force," 10 February 2020, https://www.arcyber.army.mil/.

12. Joint Doctrine Note 1-20, *Joint Identity Activities*, 24 November 2020, III-5, https://www.jcs.mil/.

13. Mark Pomerleau, "Air Force Testing How to Do Intelligence in Disconnected Environments." *C4ISRNet*, 20 September 2021, https://www.c4isrnet.com/.

14. Sandeep Mulgund, "Command and Control for Agile Combat Employment," *Wild Blue Yonder*, 30 August 2021, https://www.airuniversity.af.edu/.

15. Mark F. Cancian, "The Marine Corps' Radical Shift toward China," *Center for Strategic & International Studies*, 25 March 2020, 2, https://www.csis.org/.

16. Cancian, "The Marine Corps' Radical Shift toward China."

17. Air Force Doctrine Publication (AFDP) 1, *Air Force*, 10 March 2021, 1–20.

18. Kelsey Atherton. "Loitering Munitions Preview the Autonomous Future of Warfare." *Tech Stream* (blog), 4 August 2021, https://www.brookings.edu/.

19. John Pike, "AGM-158D JASSM-D / JASSM-XR 'Extreme Range," *Global Security*, 7 January 2021, https://www.globalsecurity.org/.

20. John Watts, Christian Trotti, and Mark Massa, "Primer on Hypersonic Weapons in the Indo-Pacific Region," *Atlantic Council: Scowcroft Center for Strategy and Security*, August 2020, 1–26, https://www.atlanticcouncil.org/.

21. Joseph Trevithick, "Special Operations C-130 Hits Target with a 'Rapid Dragon' Pallet-Dropped Cruise Missile (Update)," *The War Zone*, 16 December 2021, https://www.thedrive.com/.