THE AIR POWER JOURNAL

MULTI-DOMAIN OPERATIONS, ARTIFICIAL INTELLIGENCE AND INFORMATION DOMINANCE

FALL 2021

Acknowledgements
This read ahead is a SPPS product realized in collaboration with the authors of the articles contained herein. SPPS would like to thank the numerous authors who took the time to contribute to this product in an effort to advance this topic for discussion.

Disclaimer
The views and opinions expressed in this publication are solely those of the authors and do not represent the opinions, official policies or position of SPPS, any agency or any government and are designed to provide an independent overview, analysis and food for thought regarding possible ways ahead on this subject. Examples of analysis performed within this article are only examples and based only on limited and open source information. Assumptions made within the analysis are not reflective of the position of any government entity or to the organizations where the authors are employed or associated.

Published and distributed in November 2021 by
Strategic Planning and Project Management Services
102, The Offices at Ibn Battuta Gate
Dubai, UAE

Foreword

The character of warfare is changing in fundamental ways and the ramifications of these changes are especially profound for air power. Multi-domain integration prepositions a sequence of transformations for air—and, increasingly—space power over the coming years which relate not only to technology but to the strategic and operational concepts that air forces are organized by and conduct their planning and operations through.

The impending—and inevitable—movement towards multi-domain operations appears to be such a glaringly logical evolution for air power that it may provoke the question: Why were we not thinking and developing operating concepts along these lines much earlier? After all, the search for optimization, operational synergies and economy of force is enduring in air power. It may be argued that air forces and its sister services *have* in fact attempted to operate in the multi-domain context, in some way or form, over the years. However, efforts to generate the operational synergies and effects across a multi-domain battlespace at a force-wide or even theatre-wide level proposed by early concept of operations (CONCOPS) for multi-domain operations (MDO) are unprecedented.

Constructs such as Joint All Domain Command and Control (JADC2) articulate a combat cloud-enabled future of warfare where the mission command and battlespace management are effectively *implied* across the fighting force and where the observe-orient-decide-act (OODA) loop is expedited to the speed of edge computing. Sensor and communications networks determine the functional capacity of the air force to undertake almost the entire spectrum of its traditional mission profiles. Data and data flows will become more critical than—and effectively the strategic enabler of—the air force's traditional reliance on freedom of maneuver. Air power will increasingly become about networks rather than platforms and data rather than weapons systems.

Mission success and failure has always been dictated by the level of situational awareness available to commanders and operators. In emerging operational paradigm, the air force's ability to collect, process, and exploit data in near real-time speeds effectively makes data the greatest tool and the most coveted weapon. The gathering, processing,

aggregation, analysis, fusion and dissemination of immense amounts of data, information and knowledge will need to occur as fast as the speed of events in contested battlespaces of the future. The digitization of warfare now underway will lead to an adoption of 'big data' into operational processes broadly in the next few years. The space domain will have a significantly enlarged role to play in enabling continuous, assured and secure communications on a global scale, used as a transportation layer for such in addition to its more traditional utilization for long-range surveillance.

The pursuit of information dominance will extend the competition continuum in new and uncertain ways across the physical, electromagnetic and virtual worlds. New risks, vulnerabilities and failure points will be introduced as air forces develop their usage of combat clouds with embedded artificial intelligence (AI) tools and applications. The collection of articles and insights from leading thinkers around world in this publication provide in-depth perspectives on some of the most pertinent issues for the framing and conceptualization of multi-domain integration and information superiority in air power. The perspectives and discussions featured here reflect the most current thinking on and for a variety of strategic, command and operational levels of consideration which readers will find enriching for their broader understanding.

The expert outlooks featured here are neither optimistic nor pessimistic in themselves—what is confirmed, as we would expect, is that various new technology-enabled 'leap-ahead' opportunities are forming over-the-horizon but their effective exploitation bring complex and disruptive new challenges. Highlighting some of these key challenges and the need for these to be better understood, there are, as is usually the case, no quick fixes or readily available solutions. However, there are compelling reasons to assume that the numerous challenges foreseen today appear to be theoretically and technically surmountable – some even within the coming few years. Among the many uncertainties that exist about the future, what can be said for certain is that air power *will* be radically redefined.

Sabahat Khan ***PMP MA BA PgDip PgCert***
Independent Advisor

Table of Contents

The AI Wave and the Future of Airpower

1

Dr. Michael Raska

Assistant Professor, S. Rajaratnam School of International Studies

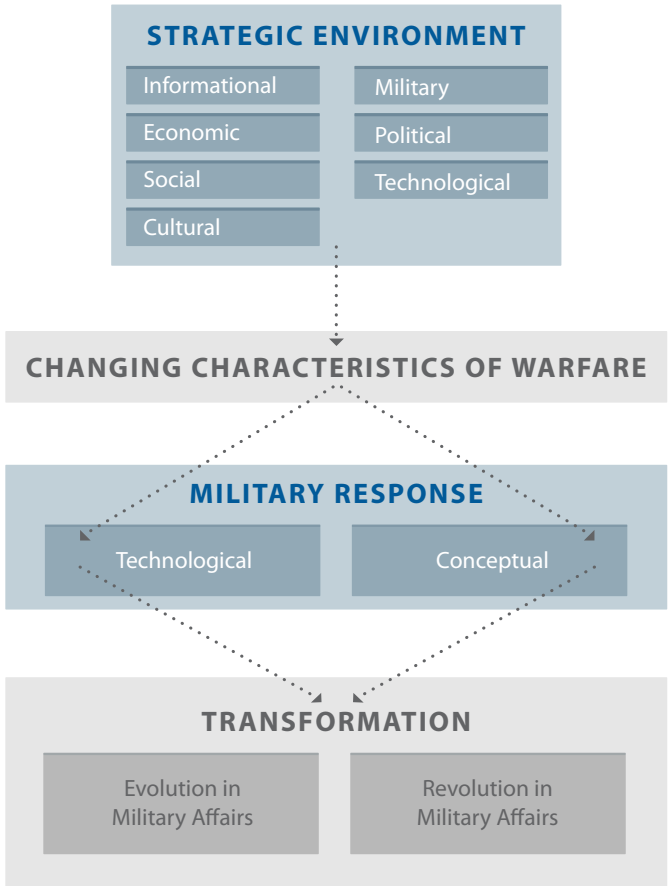
In the 2020s, airpower debates increasingly focus on the impact of emerging technologies on defense innovation and future character of warfare. The convergence of advanced novel technologies such as artificial intelligence (AI) systems, robotics, additive manufacturing (or 3D printing), quantum computing, directed energy, and other 'disruptive' technologies, defined under the commercial umbrella of the 4th Industrial Revolution (4IR), promises new and potentially significant opportunities for defense applications and, in turn, for increasing one's military edge over potential rivals. Much of the current debate arguably portrays the "next-frontier" technologies as synonymous with a "discontinuous" or "disruptive" military innovation in the character and conduct of warfare—from the "industrial-age" toward "information-age warfare" and now increasingly toward "automation-age warfare" (Raska, 2021). For example, advanced sensor technologies such as hyperspectral imagery, computational photography, and compact sensor design aim to improve target detection, recognition, and tracking capabilities and overcome traditional line-of-sight interference (Freitas et al., 2018). Advanced materials such as composites, ceramics, and nanomaterials with adaptive properties will make military equipment lighter but more resistant to the environment (Burnett et al., 2018). Emerging photonics technologies, including high-power lasers and optoelectronic devices,

may provide new levels of secure communications based on quantum computing and quantum cryptography (IISS, 2019).

The convergence of emerging technologies—i.e. robotics, artificial intelligence and learning machines, modular platforms with advanced sensor technologies, novel materials and protective systems, cyber defenses and technologies that blur the lines between the physical, cyber, and biological domains, is widely seen as having profound implications on the character of future warfare. In the context of airpower, the application of novel machine-learning algorithms to diverse problems also promises to provide unprecedented capabilities in terms of speed of information processing, automation for a mix of manned/unmanned weapons platforms and surveillance systems, and ultimately, command and control (C2) decision-making (Horowitz, 2018; Cummings, 2017).

> *Large military-industrial primes are no longer the only drivers of technological innovation; instead, advanced technologies with a dual-use potential are being developed in the commercial sectors and then being 'spun on' to military applications.*

Notwithstanding the varying strategic contexts, however, the diffusion of these emerging technologies is also prompting theoretical and policy-prescriptive questions similar to those posed over the past four decades: Does the diffusion of emerging technologies really signify a 'disruptive' shift in warfare, or is it a mere evolutionary change? If emerging technologies stipulate a disruptive change in warfare, what are defense resource allocation imperatives, including force structure and weapons procurement requirements? How can military organizations, including air forces, exploit emerging technologies to their advantage? Furthermore, how effective are emerging technologies to counter security threats and challenges of the 21st century, characterized by volatility, uncertainty, complexity, and ambiguity?



Four Decades of Disruptive Narratives

Driven largely by the quantum leaps in information technologies, the trajectory of 'disruptive' military innovation narratives and debates have been defined in the context of IT-driven Revolution in Military Affairs (IT-RMA), which have progressed through at least five stages: (1) the initial conceptual discovery of the Military-Technical Revolution by Soviet strategic thinkers in the early 1980s, (2) the conceptual adaptation, modification, and integration by in the U.S. strategic thought during the early 1990s, (3) the technophilic RMA debate during the

mid-to-late 1990s, (4) a shift to the broader "defense transformation" and it partial empirical investigation in the early 2000s, and (5) critical reversal questioning the disruptive narrative from 2005 onwards (Gray, 2006). Since the mid-2010s, however, with the accelerating diffusion of novel technologies such as AI and autonomous systems, one could argue that a new AI-RMA—or the sixth RMA wave—has emerged (Raska, 2021).

In retrospect, however, the implementation of IT-RMA over the past four decades has also arguably followed a distinctly less than revolutionary or disruptive path, consisting of incremental, often near-continuous, improvements in existing capabilities (Ross, 2010). While major, large-scale, and simultaneous military innovation in defense technologies, organizations, and doctrines have been a rare phenomenon, military organizations have largely progressed through a *sustained* spectrum of military innovations ranging from small-scale to large-scale innovation that shaped their conduct of warfare (Goldman, 1999). While many military innovations during this era, such as concepts of Network-Centric Warfare, have matured, the ambitious narratives of impending 'disruptive military transformation' have nearly always surpassed available technological, organizational, and budgetary capabilities. Moreover, the varying conceptual, technological, organizational, and operational innovations focused primarily on integrating digital information technologies into *existing* conventional platforms and systems (Raska, 2016).

> ***Both state and non-state actors may use this so-called adversarial machine learning to deceive opposing sides, using incorrect data to generate wrong conclusions, and in doing so, alter the decision-making processes.***

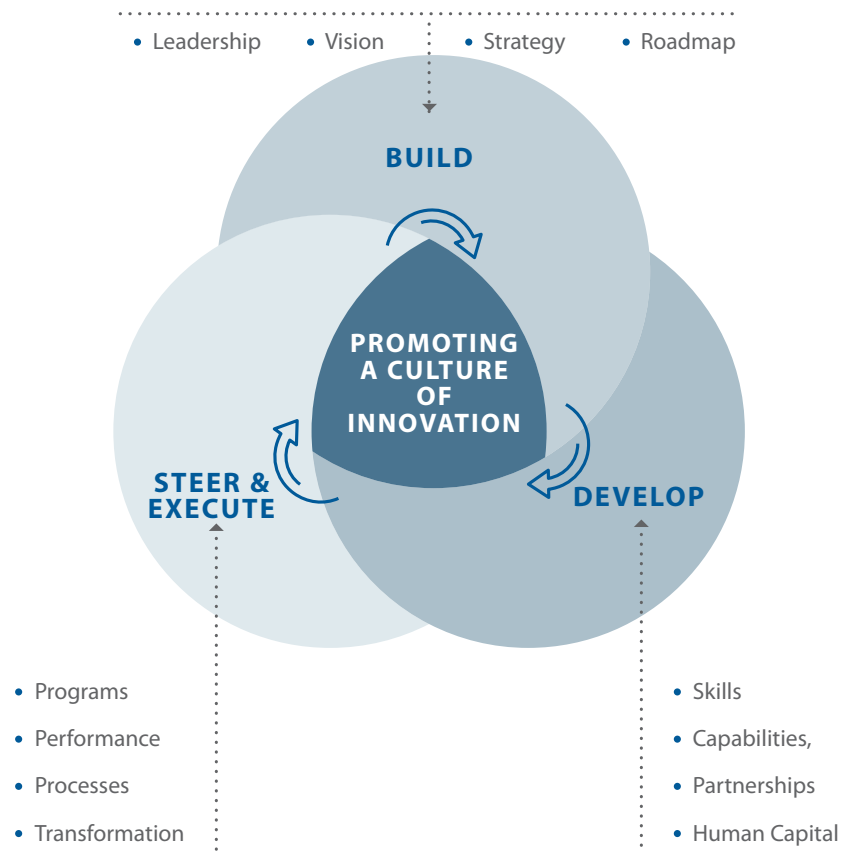
For example, in the U.S. strategic thought, the narratives of disruptive military innovation have gradually waned from 2005 onwards with operational challenges and experiences in wars in Iraq and Afghanistan. More critical voices pointed toward unfulfilled promises of 'disruptive' defense transformations. The rationale for 'new way of thinking and a new way of fighting' justifying virtually every defense initiative or proposal, signaled disorientation rather than a clear strategy (Freedman, 2006). Defense transformation sceptics also cautioned about

the flawed logic in solving complex strategic challenges through technology, while discarding the adaptive capacity of potential enemies or rivals. In short, disruptive narratives of impending defense transformations have turned into an ambiguous idea, propelled by the budgetary requirements and unrealistic capability sets rather than actual strategic and operational logic (Reynolds, 2006).

Why the AI-Wave Differs?

The new 'AI-enabled' defense innovation wave, however, differs from the past IT-led waves in several ways. First, the diffusion of AI-enabled military innovation proceeds at a much faster pace, through multiple dimensions, notably through the accelerating geostrategic competition between great powers—the United States, China, and to a lesser degree Russia. Strategic competitions between great powers are not new; they have been deeply rooted in history—from the Athenian and Spartan grand strategies during the Peloponnesian War in the third century BCE, to the bipolar divide of the Cold War during the second half of the twentieth century. The character of the emerging strategic competition, however, differs from analogies of previous strategic competitions. In the 21st century, the paths and patterns of the strategic competition are more complex and diverse, reflecting multiple competitions under different or overlapping sets of rules in which long-term economic interdependencies co-exist with core strategic challenges (Lee, 2017). In a contest over future supremacy, however, technological innovation is portrayed as a central source of international influence and national power—generating economic competitiveness, political legitimacy, and military power (Mahnken, 2012). Specifically, for the first time in decades, the U.S. faces a strategic peer-competitor, China, capable of pursuing and implementing its own AI-RMA. Accordingly, the main question is not whether the AI-RMA wave is 'the one' that will bring about a fundamental discontinuity in warfare, and if so, how and why? Instead, it is whether the U.S. AI-RMA can be nullified—or at least weakened—by corresponding Chinese or Russian AI-RMAs? In other words, the margins of technological superiority are effectively narrowing, which effectively accelerates the strategic necessity for novel technologies as a source of military advantage.

The convergence of emerging technologies—i.e. robotics, artificial intelligence and learning machines, modular platforms with advanced sensor technologies, novel materials and protective systems, cyber defenses and technologies that blur the lines between the physical, cyber, and biological domains, is widely seen as having profound implications on the character of future warfare.



Second, contrary to previous decades, which, admittedly, utilized *some* dual-use technologies to develop major weapons platforms and systems, the current

AI-enabled wave differs in the magnitude and impact of the commercial-technological innovation as the source of military innovation (Raska, 2020). Large military-industrial primes are no longer the only drivers of technological innovation; instead, advanced technologies with a dual-use potential are being developed in the commercial sectors and then being 'spun on' to military applications. In this context, the diffusion of emerging technologies, including additive manufacturing (3D printing), nanotechnology, space and space-like capabilities, artificial intelligence, and drones, are not confined solely to the great powers (Hammes, 2016). The diffusion of AI-enabled sensors and autonomous weapon systems is also reflected in defense trajectories of select advanced small states and middle powers such as Singapore, South Korea, Israel, and others. These have now the potential to develop niche emerging technologies to advance their defense capabilities and their economic competitiveness, political influence, and status in the international arena (Barsade and Horowitz, 2018).

Third, the diffusion of autonomous and AI-enabled autonomous weapons systems, coupled with novel operational constructs and force structures, challenge the direction and character of human involvement in future warfare—in which algorithms may shape human decision-making, and future combat is envisioned in the use of Lethal Autonomous Weapons Systems (LAWS). Advanced militaries, including air forces, are experimenting with varying man-machine technologies that rely on data analytics and automation in warfare. These technologies are increasingly permeating future warfare experimentation and capability development programs (Jensen and Pashkewitz, 2019). In the U.S., for example, select priority research and development areas focus on the development of AI-systems and autonomous weapons in various human-machine type collaborations—such as, for example, AI-enabled early warning systems and command and control networks, space and electronic warfare systems, cyber capabilities, lethal autonomous weapons systems, and others.

> *AI systems will be increasingly capable to streamline C2 and decision-making processes in every step of the John Boyd's Observe-Orient-Decide-Act (OODA) loop*

The convergence of the three drivers—strategic competition, dual-use emerging technological innovation, and changing character of human-machine interactions in warfare propel a new set of conditions that define the AI-RMA wave. Its diffusion trajectory inherently also poses new challenges and questions concerning strategic stability, alliance relationships, arms control, ethics and governance, and ultimately, the conduct of combat operations (Stanley-Lockman, 2021a). International normative debates on the role of AI systems in the use of force, for example, increasingly focus on the diffusion of LAWS and the ability of states to conform to principles of international humanitarian law. As technological advancements move from the realm of science fiction to technical realities, states also have different views on whether the introduction of LAWS would defy or reinforce international legal principles. Facing contending legal and ethical implications of military AI applications, military establishments increasingly recognize the need to address questions related to safety, ethics, and governance, which are crucial to building trust in new capabilities, managing risk escalation, and revitalizing arms control. Still, there is a tension between how much defense ministries and militaries focus their ethics efforts narrowly on LAWS or more broadly on the gamut of AI-enabled systems. Hence, militaries, including air forces, need to track the evolving perspectives on AI and autonomy and debates on implications to the strategic and operational environment of the 2020s and beyond (Stanley-Lockman, 2021b).

Implications for Airpower

At the operational level, air forces aim to accelerate the integration of varying AI-related systems and technologies such as multi-domain combat cloud systems, which collect big-data from a variety of sources, creating a real-time operational picture, and essentially, automate and accelerate command and control (C2) processes (Robinson, 2021). In doing so, AI-enabled combat clouds are posed to identify targets and allocate them to the most relevant "shooters" in any domain, whether airborne, surface or underwater—which some air forces conceptualize as Joint All-Domain Command and Control (JADC2). Select air forces are also experimenting with AI algorithms as 'virtual backseaters', which effec-

tively control the aircraft's sensors and navigation, finding adversary targets, and in doing so, reduce the aircrew's workload (Everstine, 2020). In this context, the key argument is that advances in AI systems—broadly programs that can sense, reason, act, and adapt, including Machine Learning (ML) systems—algorithms whose performance improves with increasing data interactions over time, and Deep Learning (DL) systems—in which multilayered neural networks learn from vast amounts of data—have the potential "to transform air combat operations and the way airpower is conceived and used" (Davis, 2021).

Specifically, according to a recent RAND study (Lingel et al., 2020), there are currently six categories of applied AI/ML research and development that have implications for future warfare, including airpower:

(1) Computer vision—image recognition—detecting and classifying objects in the visual world that could be used to process multisource intelligence and data fusion;
(2) Natural language processing (NLP)—ability to successfully understand human speech and text recognition patterns, including translation, that could be used to extract intelligence from speech and text, but also monitor friendly communications and direct relevant information to alert individuals or units in need;
(3) Expert systems or rule-based systems—collecting large amounts of data to recommend particular actions to achieve operational and tactical objectives;
(4) Planning systems—using data to solve scheduling and resource allocation problems, which could coordinate select air, space, and cyber assets against targets and to generate recommended time-phased actions;
(5) Machine learning systems—acquiring knowledge from data interactions with the environment, which could be used in conjunction with other categories of AI, i.e. to enable C2 systems to learn how to perform tasks when expert knowledge is not available or when optimal tactics, techniques, and procedures (TTPs) are unknown;

(6) Robotics and autonomous systems—combining AI/ML methods from all or select preceding categories that would enable unmanned systems interactions with their environment;

These AI-related categories are applicable into nearly every aspect of airpower, potentially shaping new forms of automated warfare: from C2 decision support and planning, in which AI/ML could provide recommended options or proposals in increasingly constrained times; ISR support through data mining capabilities; logistics and predictive maintenance to ensure the safety of forces and availability of platforms and units; training and simulation; cyberspace operations to detect and counter advanced cyber-attacks; robotics and autonomous systems such as drones that are utilized across various missions from ISR to the tip of the spear missions such as suppression of enemy air defenses and collaborative combat that integrates the varying manned and unmanned platforms in air and land strike operations. In other words, the argument here is that AI systems will be increasingly capable to streamline C2 and decision-making processes in every step of the John Boyd's Observe-Orient-Decide-Act (OODA) loop: collecting, processing, and translating data into a unified situational awareness view, while providing options for a recommended course of actions, and ultimately, helping humans to act (Fawkes and Menzel, 2018).

However, integrating AI systems into airpower platforms, systems, and organizations to transform computers from tools into problem-solving "thinking" machines will continue to present a range of complex technological, organizational, and operational challenges (Raska et al, 2021). These may include developing algorithms that will enable these systems to better adapt to changes in their environment, learn from unanticipated tactics and apply them on the battlefield. It would also call for designing ethical codes and safeguards for these thinking machines. Another challenge is that technological advances, especially in military systems, are a continuous, dynamic process; breakthroughs are always occurring, and their impact on military effectiveness and comparative advantage could be significant and hard to predict at their nascent stages.

Most importantly, however, the critical question is how much we can trust AI systems, particularly in the areas of safety-critical systems? As Missy Cummings warns, "history is replete with examples of how similar promises of operational readiness ended in costly system failures and these cases should serve as a cautionary tale" (Cummings, 2021). Furthermore, a growing field of research focuses on how to deceive AI systems into making wrong predictions by generating false data. Both state and non-state actors may use this so-called adversarial machine learning to deceive opposing sides, using incorrect data to generate wrong conclusions, and in doing so, alter the decision-making processes. The overall strategic impact of adversarial machine learning might be even more disruptive than the technology itself (Knight, 2019; Danks, 2020).

> *AI-enabled combat clouds are posed to identify targets and allocate them to the most relevant "shooters" in any domain, whether airborne, surface or underwater—which some air forces conceptualize as Joint All-Domain Command and Control (JADC2).*

From a tactical and operational perspective, many of these complex AI systems also need to be linked together—not only technologically but organizationally and operationally. For many air forces, this is an ongoing challenge—they must be able to effectively (in real-time) integrate AI-enabled sensor-to-shooter loops and data streams between the various services and platforms. This means effectively linking the diverse Air Force, Army, Navy, and Cyber battle management; C2, communications and networks; ISR; electronic warfare; positioning, navigation, and timing; with precision munitions. While select AI/ML systems may mitigate some of the challenges, the same systems create another set of new problems related to ensuring trusted AI. Accordingly, one may argue that the direction and character of AI trajectories in future airpower will depend on corresponding strategic, organizational and operational agility, particularly how these technologies interact with current and emerging operational constructs and force structures.

In this context, the level of human involvement in the future of warfare, the need to alter traditional force structures and recruitment patterns and in what

domains force will be used are all matters that are being challenged by new technologies. Air forces are developing their own and often diverse solutions to these issues. As in the past, their effectiveness will depend on many factors that are linked to the enduring principles of *strategy*—the ends, ways, and means to "convert" available defense resources into novel military capabilities, and in doing so, create and sustain air forces with operational competencies to tackle a wide range of contingencies. The main factors for successful implementation will not be technological innovations per se, but the combined effect of sustained funding, organizational expertise (i.e. sizeable and effective R&D bases, both military and commercial) and institutional agility to implement defense innovation (Cheung, 2021). For the future of airpower, this means having the people, processes and systems capable of delivering innovative solutions while maintaining existing core capabilities that would provide viable policy options in an increasingly complex strategic environment.

References:

Barsade, I. and Horowitz, M. (2018). Artificial intelligence beyond the superpowers. *Bulletin of the Atomic Scientists*. 16 August. Available from: *https://thebulletin.org/2018/08/the-ai-arms-race-and-the-rest-of-the-world/*

Burnett, M. et. al. (2018). Advanced materials and manufacturing—implications for defence to 2040. *Defence Science and Technology Group Report*. Australia Department of Defence. Available from: *https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-GD-1022.pdf*

Cheung, T. (2021). A conceptual framework of defence innovation. *Journal of Strategic Studies*, DOI: 10.1080/01402390.2021.1939689.

Cummings, M. (2017). Artificial intelligence and the future of warfare. *Chatham house research paper*. Available from: *https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf*

Cummings, M. (2021). Rethinking the maturity of artificial intelligence in safety-critical settings. *AI Magazine*, 42(1), pp.6-15. Available from: *https://ojs.aaai.org/index.php/aimagazine/article/view/7394*

Danks, D. (2020). How adversarial attacks could destabilize military AI systems. *IEEE Spectrum*. Available from: *https://spectrum.ieee.org/adversarial-attacks-and-ai-systems*

Davis, M. (2021). The artificial intelligence 'backseater' in future air combat. *ASPI Strategist*. Available from: *https://www.aspistrategist.org.au/the-artificial-intelligence-backseater-in-future-air-combat/*

Everstine, B. (2020). U-2 flies with artificial intelligence as its co-pilot. Air Force Magazine. Available from: *https://www.airforcemag.com/u-2-flies-with-artificial-intelligence-as-its-co-pilot/*

Fawkes, J. and Menzel, M. (2018). The future role of artificial intelligence—military opportunities and challenges. *The Journal of the JAPCC*, 27. pp.70-77. Available from: *https://www.japcc.org/wp-content/uploads/JAPCC_J27_screen.pdf*

Freedman, L. (2006). *The transformation of strategic affairs*. London: International Institute of Strategic Studies.

Freitas, S. Silva, H., Almeida, J. and Silva, E. (2018). Hyperspectral imaging for real-time unmanned aerial vehicle maritime target detection. *Journal of Intelligent and Robotic Systems*. 90, pp.551-570.

Goldman, E. (1999). Mission possible: organizational learning in peacetime. In: Trubowitz, P., Goldman, E., and Rhodes, E. *The politics of strategic adjustment: ideas, institutions, and interests*. New York: Columbia University Press, pp.233-266.

Gray, C. (2006). *Strategy and history: essays on theory and practice*. London: Routledge, pp.113-120.

Hammes, T.X. (2016). Technologies converge and power diffuses: the evolution of small, smart, and cheap weapons. *CATO Institute Policy Analysis*. 786. Available from: *https://www.cato.org/policy-analysis/technologies-converge-power-diffuses-evolution-small-smart-cheap-weapons*

Horowitz, M. (2018). The promise and peril of military applications of artificial intelligence. *Bulletin of the Atomic Scientists*. Available from: *https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/*

International Institute for Strategic Studies. (2019). Quantum computing and defence. In: IISS. *The military balance*. London: Routledge, pp. 18-20.

Jensen, B. and Pashkewitz, J. (2019). Mosaic warfare: small and scalable are beautiful. *War on the Rocks*. Available from: *https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/*

Knight, W. (2019). Military artificial intelligence can be easily and dangerously fooled. MIT Technology Review. Available from: *https://www.technologyreview.com/2019/10/21/132277/military-artificial-intelligence-can-be-easily-and-dangerously-fooled/*

Lee, CM. (2016). *Fault lines in a rising Asia*. Washington D.C.: Carnegie Endowment for International Peace, pp. 119-175. Available from: *https://carnegieendowment.org/2016/04/20/fault-lines-in-rising-asia-pub-63365*

Lingel, S. et. al. (2020). Joint all-domain command and control for modern warfare—an analytic framework for identifying and developing artificial intelligence applications. *RAND Corporation Project Air Force Report*. Available from: *https://www.rand.org/pubs/research_reports/RR4408z1.html*

Mahnken, T. (ed.). (2012). *Competitive strategies for the 21st century: theory, history, and practice*. Stanford: Stanford University Press, pp.3-12.

Raska, M. (2016). *Military innovation in small states: creating a reverse asymmetry*. New York: Routledge. Available from: *https://www.routledge.com/Military-Innovation-in-Small-States-Creating-a-Reverse-Asymmetry/Raska/p/book/9780367668617*

Raska, M. (2020). Strategic competition for emerging military technologies: comparative paths and patterns. *Prism—Journal of Complex Operations*. 8(3), pp.64-81. Available from: *https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Raska_64-81.pdf*

Raska, M. (2021). The sixth RMA wave: disruption in military affairs? *Journal of Strategic Studies*. 44(4), pp.456-479.

Raynolds, K. (2006). *Defence transformation: to what? for what?* Carlisle: Strategic Studies Institute.

Robinson, T. (2021). The air force of 2040—synthetically-trained, cloud-networked, space-enabled and NetZero? Royal Aeronautical Society, 10 August. Available from: *https://www.aerosociety.com/news/the-air-force-of-2040-synthetically-trained-cloud-networked-space-enabled-and-netzero/*

Ross, A. (2010). On military innovation: toward an analytical framework. *IGCC Policy Brief*. 1, pp.14-17. Available from: *https://escholarship.org/uc/item/3d0795p8*

Stanley-Lockman. Z. (2021(a)). Responsible and ethical military AI: allies and allied perspectives. *Center for Security and Emerging Technology Issue Brief*. Available from: *https://cset.georgetown.edu/publication/responsible-and-ethical-military-ai/*

Stanley-Lockman, Z. (2021(b)). Military AI cooperation toolbox: modernizing defense science and technology partnerships for the digital age. *Center for Security and Emerging Technology Issue Brief*. Available from: *https://cset.georgetown.edu/publication/military-ai-cooperation-toolbox/*

A New Battle Command Architecture for Air Force–Led All Domain Operations

2

David Deptula, Lieutenant General (Retired), United States Air Force

Dean, Mitchell Institute of Aerospace Studies

Introduction

The U.S. Chairman of the Joint Chiefs of Staff (CJCS) recently testified to Congress about the U.S. military's new joint warfighting concept (JWC) and the importance of the associated new Joint All Domain Command and Control (JADC2) framework to its realization. Specifically, he stated to the U.S. House of Representatives on June 23, 2021:

> The JWC is a multi-year effort to develop a comprehensive approach for joint operations against future threats and provide a guide for future force design and development. Supporting concepts to the JWC describe key warfighting functions. They are fires, logistics, C2, and information advantage. The Joint All Domain Command and Control (JADC2) framework enables the holistic development and realization of the JWC and Supporting Concepts.

The fundamental basis of the JWC is the notion of all domain operations. This is the next evolution in the U.S. military's journey to optimize the synergy of effects that accrues from operating in an integrated fashion across all the domains of air, space, sea, land, and the electromagnetic spectrum. The journey began with

the passage of the Goldwater-Nichols Act of 1986 that aimed to improve the ability of U.S. armed forces to conduct joint (interservice) and combined (interallied) operations. If developed and implemented properly, the JWC will yield a far more decisive, powerful set of combat outcomes than today's "joint" operations that in many cases simply involve service component deconfliction vice integration. For this to happen, the U.S. Department of Defense (DOD) needs to get serious about turning theory into reality. That means taking incremental but concrete steps toward meeting the objectives of JADC2, not waiting for a complete solution before implementing. JADC2 will require much time to engineer as it involves a mammoth conversion of existing concepts, capabilities, and service perspectives. However, accelerating these endeavors can be accomplished through rapid evolution of current command and control paradigms. Specifically, it is time to move beyond large, centralized, static C2 facilities to mobile, distributed C2, with the capability to handle the same volume and diversity of information of a regional combined air and space operations center (CAOC).

As it seeks all domain synergy, embracing complementary vice merely additive employment of capabilities from different domains, the goal of JADC2 is to seek interdependency that enhances effectiveness, and compensates for individual vulnerabilities of each of the domains. Desired military effects will increasingly be generated by the interaction of systems that share information and empower one another. Instead of a set of disconnected, singularly focused combat systems in each of the domains, this JADC2 vision sees assets combined through digital connective "glue" to become a "weapon system" to conduct disaggregated, distributed operations over an entire operational area. This will require treating every platform as a sensor as well as an "effector." It will require a new battle command architecture and command and control paradigm that enables automatic linking, as does cellular phone technology today. It will also need to transfer data securely, reliably, and seamlessly, without need for human interaction.

The Envisioned Transformation

The overarching goal of actualizing JADC2 with the degree of integration required to achieve a self-forming, self-healing complex into reality will require a significant effort and will not be easy. Every military service will be involved as will every combatant command. It will require overcoming several major obstacles in organization; culture; training; acquisition; and policy. It will require connecting, decision-making, and responding at speed. It will require resilient networks and a degree of sharing among service components and allies not yet achieved.

These are numerous and multifaceted challenges that are being addressed across our militaries, services, and combatant commands. However, due to their complexity it will take many years—if not decades—before the ultimate vision of integrated, interdependent, self-forming, self-healing all domain joint and combined operations are a reality. Yet, the threats facing us are growing and demand solutions today. Accordingly, it is time to move out on those elements of JADC2 that can be changed now in order to meet the challenges of the threats we face today.

Each of the service components and combatant commands have well established operating command and control concepts, facilities, and procedures that have proven workable in conflicts of the past. However, each of the variety of C2 architectures that currently exist will require extensive modification in order to survive—much less operate—against the kind of modern threats that have now emerged.

> *Growing accessibility to information requires the restructure of command and control hierarchies to facilitate rapid engagement of perishable targets and capitalize on our technological capability. Information synthesis and execution authority must be shifted to the lowest possible levels while senior commanders and staffs must discipline themselves to stay at the appropriate level of war.*

A central prerequisite to successful operations in all the domains is control of the aerospace environment. Once established, it facilitates the freedom of action and movement for all other joint and combined forces—without it, effective joint and/or combined operations are not possible. Accordingly, effective command and control of aerospace operations are critical functions that must be a priority.

Our ability to command and control (C2) air and space forces is affected by three major elements: threats, technology, and the velocity of information. The changes in these three areas since the design, establishment, and operation of the U.S. Air Force's air and space operations center (AOC)—the AN/USQ-163 Falconer—have been dramatic and continue to accelerate. Therefore, it is time to determine whether we can achieve success in future operations by evolving our current concepts of operation, organizations, and acquisition processes for modernization, or must we seek fundamental change to each of these elements that affect the current theater air and space control system. Before providing an answer, let's take a brief look at each of the trends affecting our ability to effectively command and control aerospace operations.

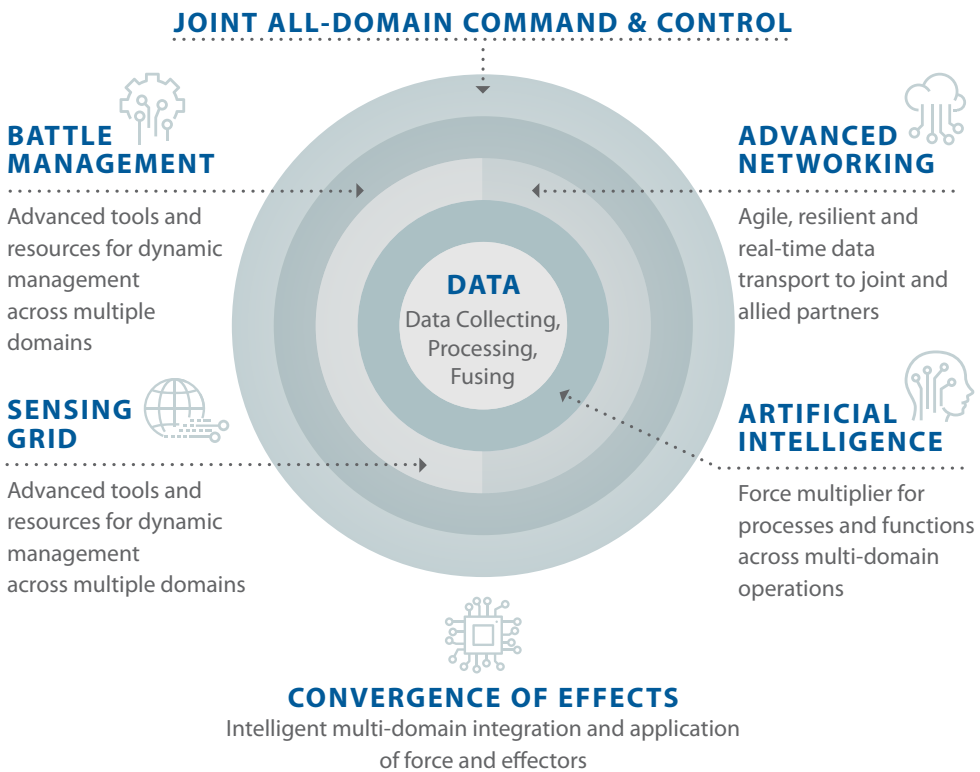
Future Threats and the Operational Environment

Threats

Today, peer threats hold current means of C2 at unacceptable risk when attempting to operate inside the A2/AD environment. For over 30 years we have essentially been on a C2 holiday having the luxury of not being contested in the aerospace domains. Those days are over. Military competitors have accomplished modernization on an unprecedented scale. They have rapidly closed the gap with the U.S., allies, and friendly militaries across a broad spectrum of capabilities including aircraft, spacecraft, missiles, weapons, cyber, command and control, jammers, electronic warfare, data links, and others. Potential adversaries have also studied the American way of war and have determined that it is better to keep us out of their neighborhood rather than face our combat power. They

have adopted and are proliferating anti-access and area denial (A2/AD) capabilities designed to deny U.S. and her allies freedom of action. Mitigating these A2/AD capabilities pose significant challenges driving us to operate with greater risk and farther away from potential areas of conflict.

Foundations of JADC2



A2/AD capabilities threaten our ability to command and control air and space operations in three ways. Near peer adversaries can employ kinetic and non-kinetic weapons to deny us communications and intelligence, surveillance, and reconnaissance (ISR) from our space-based assets thereby isolating our forces

and blinding our view. Cyber attacks are becoming more sophisticated and can disrupt operations at our well-established combined air and space operations centers. Accurate long-range cruise and ballistic missiles now threaten these facilities that are large, fixed, and vulnerable. As the factory for generating strategy, plans, and the tasking orders for air and space assets, the CAOC has become an extremely lucrative target.

Technology

New technologies are enabling new capabilities to optimize C2 mechanisms to facilitate accomplishing desired effects. We need to think beyond the constraints that traditional culture imposes on new technology. For example, next generation aircraft may be still labeled in traditional nomenclature as fighters, bombers, airlifters, etc., but technologically they have the capability to perform multiple missions due to the miniaturization of sensors, processing power, weapons, energy production, and other capabilities. They are in reality flying "sensor-effectors" that can form the basis of highly resilient networks of redundant nodes and multiple kill paths to minimize the critical system value of current highly centralized and limited C2 nodes—like CAOCs—that an enemy could easily target.

> *JADC2 will require much time to engineer as it involves a mammoth conversion of existing concepts, capabilities, and service perspectives. However, accelerating these endeavors can be accomplished through rapid evolution of current command and control paradigms.*

This will require leading-edge networking capabilities, assured communications, and different approaches to solving our data bandwidth challenges. For example, to solve the explosion in data growth from advanced sensors, instead of building bigger pipes to transmit all the collected data, increases in processing power now enables the processing of data on-board and the off boarding of only what is of interest to the users. This approach inverts the way we do

ISR processing today. Rapid exchange of information is especially important at the forward edge of combat, for the value of actual data is often transitory and diminishes as time and circumstance pass. The development of a technological approach to share information automatically and rapidly among diverse users and across multiple classifications and allied nations will be a key to creating the future force.

The old adage, "Speed is life" is no longer just about flying—it is also about rapidly evolving software tools to fight and win. We have to think outside of the organizational constructs that history has etched into our collective psyche. Network-centric, interdependent, and functionally integrated operations are the keys to future military success.

Velocity of Information

Significant advancements in telecommunications, sensors, data storage, and processing power are emerging every day. As a result, the targeting cycle has evolved from weeks to days to minutes, and from multiple, specialized, and separate aircraft to the ability to "find, fix, and finish" from one aircraft in minutes. Growing accessibility to information requires the restructure of command and control hierarchies to facilitate rapid engagement of perishable targets and capitalize on our technological capability. Information synthesis and execution authority must be shifted to the lowest possible levels while senior commanders and staffs must discipline themselves to stay at the appropriate level of war.

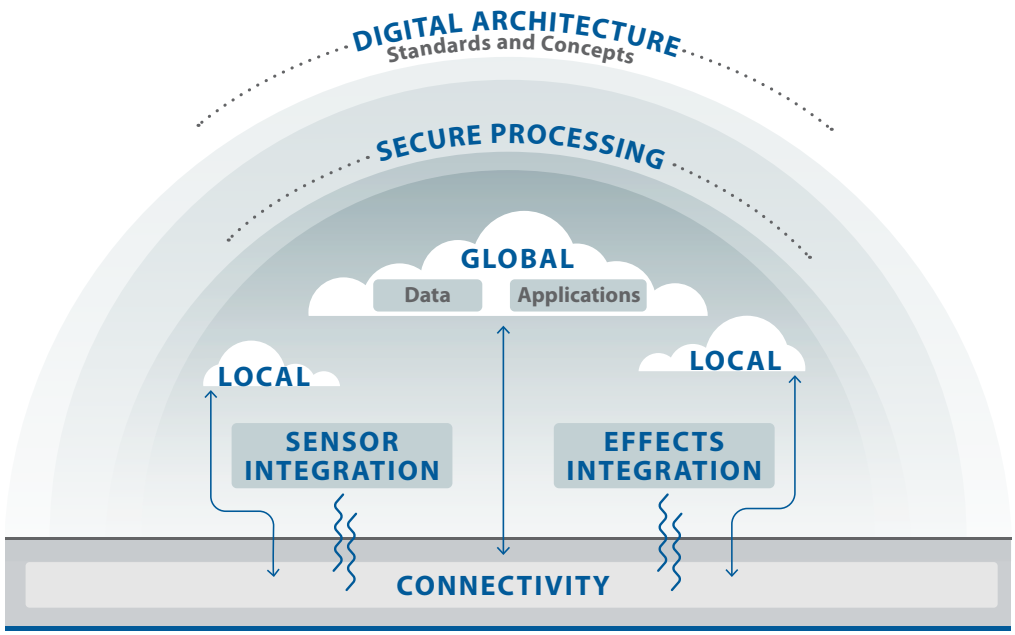
To move beyond large, centralized, static C2 facilities to mobile, distributed C2, with the capability to handle the same volume and diversity of information of a regional CAOC today will require a reappraisal of how we deal with information flow. The two most important aspects of this future capability will be the "command" metamorphosis it will enable through the synchronizing "control" it will provide. The "art of command" will morph to realize Metcalfe law network values (Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system). While the

"science of control" will continue to apply Moore's law expanding technology to extend human capacity. The path for optimal growth of both is found through a focus upon gaining and maintaining a decision cycle advantage as the critical path guide.

The Need for a New Architecture for Aerospace C2—Rapidly

We are now at a juncture where threats, technology, and the velocity of information, require a change in the established architectures to command and control aerospace forces. All the U.S. military services have recognized this and have initiated actions to take appropriate action to develop new concepts of operation for their respective domains. The challenge will be how to assure the integration of each of the individual service concepts of operation into a unified joint all domain command and control architecture. Developed with the idea of creating an ISR, strike, maneuver, and sustainment complex that uses information age technologies to conduct highly interconnected, distributed operations, this "combat cloud" will usher in an entirely different architecture for the conduct of war**.** The fundamental basis of JADC2 is to push accurate, decision-quality information down to the lowest information node to achieve a desired effect, regardless of service, domain, or platform. The U.S. Air Force approach to this goal is their efforts to design and develop an advanced battle management system (ABMS). However, while the elements of the ABMS have been defined, they have yet to be developed into an executable C2 architecture. To get to the desired end state of the ubiquitous and seamless sharing of information across the battlespace in a secure, reliable, and robust fashion for both JADC2 and ABMS will take many years. Given the rapid evolution of significant threats and the vulnerability of current C2 facilities, modification to the current C2 construct for aerospace forces is required now.

Advanced Battle Management System



The fundamental basis of JADC2 is to push accurate, decision-quality information down to the lowest information node to achieve a desired effect, regardless of service, domain, or platform.

What is needed is a new architecture to support an operating concept that actualizes the C2 paradigm that has recently been ensconced in U.S. Air Force Doctrine of centralized command; distributed control; and decentralized execution. No breakthroughs in technology are required to institute a new battle command architecture as the technology already exists to deal with the immediate challenge of distributing C2 functions so that they cannot be eliminated with a few strikes on a few critical C2 nodes.

The U.S. Air Force has been developing a supporting concept of operations to their new doctrine known as agile combat employment or ACE. ACE is a concept that disperses forces and assets to multiple separated locations on short notice to complicate adversary planning. With an appropriate C2 system it can hold adversary targets at risk from many locations that are defensible, sustainable, and relocatable. The details for application of the concept are unique depending on the theater of use, but fundamentally the idea is the same, and C2 is fundamental to the concept's success.

While the CAOC will remain a viable means to conduct C2 operations during periods of less than major regional conflict, to achieve the objectives of JADC2 we will have to deliver information to warfighters at the edge of the battlespace without having to rely on the traditional CAOC model of hundreds of people organized in stovepiped divisions around segregated mission areas. Accordingly, we need to rapidly evolve beyond the large, centralized CAOC structures we rely on today to a much more agile and dispersible set of processes and C2 structures. At the same time this new architecture must be adaptable to ABMS and JADC2 developments. However, given the slow evolution of these programs, we simply cannot wait to begin changing the architecture for C2 of aerospace forces.

Options for this new architecture are many: build hardened CAOCs and remote the functions to assigned units; distribute the planning functions currently incorporated in COACs among multiple locations and network the resultant plans; create processes and procedures to be executed based on the degree of degradation of connectivity between combat units and their respective command elements by shifting execution authority corresponding to levels of connectivity; and there are many others. Regardless of the option(s) selected for development one thing is certain, we must undertake a determined effort to distribute the C2 functions necessary to assure the effective use of aerospace forces in a contested environment—and that effort must begin now.

Developing a Concept of Operations for Joint All-Domain Command and Control with an Embedded Role for Artificial Intelligence Applications

3

Sherrill Lingel

Senior Engineer, RAND Corporation

Before one can leverage artificial intelligence (AI) and machine learning (ML) for multi-domain operations (MDOs) as part of Joint All-Domain Command and Control (JADC2), one must do the grunt work of laying an "information foundation." Laying this foundation—in which data are tagged, securely stored and transported, and easily accessible—requires the mundane and ongoing work of organizing and safeguarding all the information the military needs for C2 across domains, services, and echelons. This same body of information will be the input for AI and ML algorithms. Absent such an information foundation, little progress can be made.

Although recent successes in AI/ML have been encouraging in the field of gaming, employing similar techniques for some C2 functions will remain challenging given the real-world barriers of incomplete information, poor data quality, and adversary actions. Other AI/ML techniques, such as those for predicting the status of aircraft in theater, will be more readily applicable. Reaching JADC2 goals will depend on both identifying the C2 needs of core military mission sets and establishing software development plans that are achievable in the near and far terms.

The remainder of this paper describes the need for JADC2 with embedded AI/ML, offers a cautionary note about the lure of AI/ML, outlines the AI/ML barriers to overcome, and suggests a path forward. In general, investments in people and resources will be needed to move beyond today's man-power intensive C2 paradigm. Improving upon current planning processes with automation and *some* AI/ML is a realistic goal that is worthy of working toward.

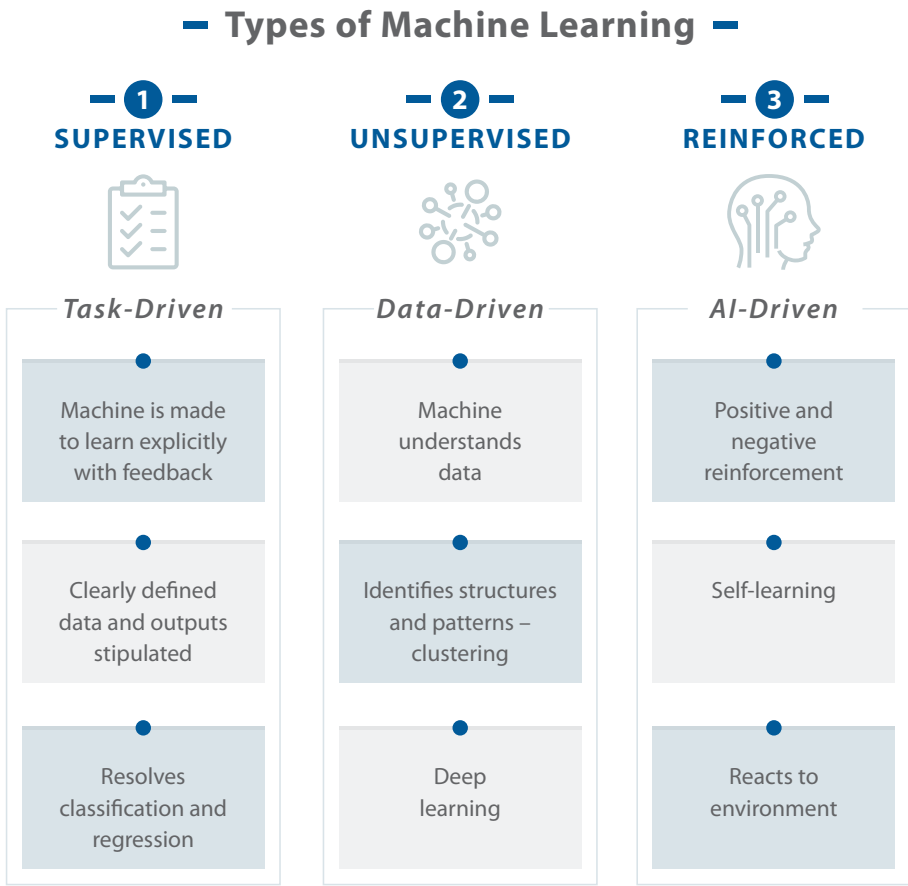
Given the increased complexity of MDO planning, the reduced timescales, and the greater data requirements, military planners will require new tools, including those based on AI/ML.

The Need for JADC2 in Support of MDO

Modern warfare has expanded beyond the traditional domains of land, air, and sea, requiring military commanders and their staffs to plan, command, and control forces not only in these traditional domains but also now in those of space and cyber and across the electromagnetic spectrum. To complicate matters further, activities across all these domains have expanded beyond traditional warfare to shape the competitive environment in which most nations live today—prior to open hostilities. A military must be able to integrate across these domains not only in warfare, but also in competition. Today's military operations already require resilient and secure means of communicating and sharing data across echelons, domains, organizations, and geographic regions. Tomorrow's all-domain warfare and competition will place even higher premiums on the scale and speed of access to information, on understanding that information, and on rapid decisionmaking—key elements of an effective JADC2 capability (Lingel et al., 2020).

However, today's legacy systems and infrastructure for planning, scheduling, and execution monitoring military missions are incongruent with the modern, all-domain world in which militaries must compete. Given the increased complexity of MDO planning, the reduced timescales, and the greater data requirements, military planners will require new tools, including those based on AI/ML.

A proper prioritization of investment in these tools requires an understanding of their capabilities, their barriers, and their potential fulfillment of the emerging C2 needs for MDOs.



The Lure of Artificial Intelligence/Machine Learning (AI/ML)

The appeal of AI/ML stems in part from recent demonstrations of AI/ML systems achieving super-human performance in increasingly complex games, combined with growing recognition of the operational demands of future high-end

conflicts. The recent success of AlphaStar, an AI/ML system trained to play the real-time strategy game StarCraft, hints at future applications of supervised and reinforcement learning for tactical and operational C2.[1] However, significant research is still needed to transition these technologies from gaming to warfighting.

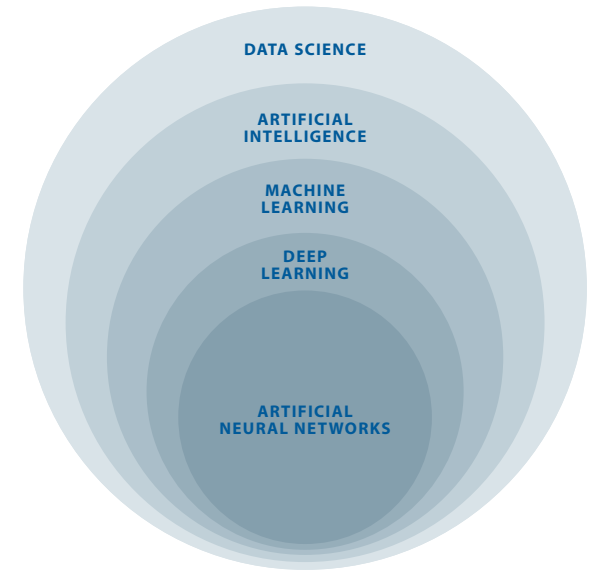
> *All-domain warfare and competition will place even higher premiums on the scale and speed of access to information, on understanding that information, and on rapid decisionmaking*

As AI algorithms are developed for real-world, dynamic, multi-domain, large-scale, and high-tempo operations, important metrics will need to be selected, evaluated, and monitored to gauge algorithm performance, effectiveness, and suitability. Key algorithm metrics will include the following: efficiency (the time and memory needed to compute), soundness (whether the algorithm produces valid results), optimality (whether the algorithm provides a best result for a given objective), robustness (whether the algorithm degrades gracefully under unanticipated cases), explainability (whether a human can understand the "why" of the results), and assuredness (whether the algorithm operates as intended) (Walsh et al., 2021).

Because there is no direct application of commercial and academic AI/ML systems to military missions, the technologies will need to be transitioned to a military setting before they can provide an operational advantage. To decide which AI/ML technologies to pursue, the military must first understand the operational demands the technologies will need to support (e.g., air superiority, air defense, tanker support, etc.). The operational demands will then determine the C2 processes (e.g., situational awareness, airspace deconfliction, etc.) needed to enable the operational missions. Understanding the limitations of the AI/ML technologies, particularly the difficulty they encounter in reasoning under con-

1 Reinforcement, supervised, and unsupervised learning are three types of ML. Reinforcement learning algorithms learn from mistakes by trial and error.

ditions of uncertainty, will be equally important.[2] Otherwise, the technologies may fall short of expectations.



AI/ML Barriers to Overcome

Several barriers to realizing the promise of AI/ML for military applications exist. One barrier is military culture, which is often risk-averse (lives are at risk) in contrast with that of the commercial world, where taking big risks can pay big monetary rewards. A related cultural difference is in sharing data. The military tends to be concerned with securing information (for only those with "the need to know"), whereas the commercial world values open access to data ("sharing widely") for application development and other monetary benefits. Therefore, it will be important to incorporate *security* concerns in military software development and information technology (IT) operations—known as DevSecOps—to thwart adversaries and bad actors who might seek to degrade C2 through cyber means. Perhaps one of the greatest challenges not yet fully faced is to ensure

2 Algorithms are challenged by situations where there are: (1) incomplete information; (2) noisy inputs; and (3) a lack of historical data or a suitable simulation environment to train from.

the suitability of AI/ML algorithms for real-world military situations in which the "fog of war," incomplete information, and adversary actions represent distinct contrasts from a gaming environment.

Another barrier is data inaccessibility within the military itself. To move forward, the military will need a unified data management policy and sufficient IT to make large amounts of data accessible to C2 forces to support their AI-assisted decisionmaking. In other words, there must be an AI ecosystem that supports collecting, tagging, storing, securing, and sharing data. This ecosystem will rely on common data standards, clearly designated authorities, integrity checks, and intrusion safeguards. Cloud computing and data lakes will be key components. A cloud-based data lake can be leveraged for distributed computing, redundant storage, and enterprise-wide connectivity. Building out an environment like this to provide large amounts of data in a secure way across domains and security levels will present challenges for JADC2 given existing military policies, cultures, authorities, budgets, and acquisition paths.

A third barrier is the need to restructure military operations centers and the training of personnel who run them. An increase in machine-to-machine communication, combined with the automation of C2 processes, will likely induce both physical changes and staffing changes in the operations centers, freeing up human operators to engage in more cognitive tasks, such as evaluating and refining potential courses of action. The adoption of AI/ML technologies will create new roles and responsibilities. Operators will need to be trained to manage and navigate the AI ecosystem, all while acting as responsible data stewards to ensure the quality and completeness of the data captured and stored in that ecosystem. Additionally, whereas planners and decisionmakers of today are trained to think within a single domain, new roles will likely emerge requiring personnel to be trained to think in multiple domains all at once.

A fourth barrier is the existence of military subcultures. Integrating AI capabilities across just the air, space, and cyber domains even within just one military service may be difficult given the differences in subcultures among operators, the variations in planning timelines, and the dissimilar distributions of authori-

ties for achieving different operational effects. Still, the need for all-domain C2 is pressing and increasingly pervasive. For this reason, all these barriers—military culture, cyber security concerns, algorithms applied to problems with poor knowledge quality, data inaccessibility, operations center restructuring and training, and military subcultures—must be faced and overcome to embed AI applications in JADC2.

Effectively Moving Forward

The picture may appear grim. Many barriers exist, and a pressing need to move forward quickly demands change now. Yet progress can be made if steps toward the goal are broken down into tractable problems and if the military keeps its "eyes wide open" to technological possibilities and limitations alike. The goal should not be complete automation of C2, but rather effective human-machine teaming for C2. The steps toward that end should include, first, the continuous development and prioritization of JADC2 concepts of operation (CONOPs) and, second, the identification of corresponding needs and opportunities for AI/ML augmentation in the enabling C2 processes.

> *Whereas planners and decisionmakers of today are trained to think within a single domain, new roles will likely emerge requiring personnel to be trained to think in multiple domains all at once.*

At the same time, it will be necessary to set the conditions for a data-driven AI ecosystem, which means placing weapons systems and related data into multi-domain data lakes for use by those who ought to have access to the data while also applying "zero-trust" and other security principles to ensure resilient and secure management of that data. As AI software applications are developed, it will be necessary to experiment with them in operational testbed environments, integrate them with C2 systems, and then deploy them to operations centers. There will likely be iterations of capabilities—first putting limited capabilities into operations centers, then generating user feedback, and then rapidly updat-

ing the software applications. Analysts and technologists will want to explore CONOPs to facilitate human-machine teaming, build human trust in the AI algorithms, and improve algorithm explainability. Targeted military investments will likely be needed in areas where commercial demand is lower, such as AI algorithms for learning where data are scarce or for defending against attacks against those very algorithms.

Current AI/ML techniques need data from which to learn. Given the (fortunate) lack of real-world data to inform the refinement of these techniques for war, the military could leverage modeling, simulation, and exercises to generate training data for AI/ML algorithms. Such algorithms could then assist in the development of, for example, weapon-target pairing. Supervised or reinforcement learning algorithms could support this C2 function, akin to the learning algorithms recently applied to commercial games. But military algorithms must also account for uncertainty in real-world situations—a major difficulty for both humans and algorithms.

As the U.S. Air Force Chief of Staff said in August 2020, "Accelerate change or lose." Making timely progress toward JADC2 is an imperative for modern warfare and doing so "within the competitors' fielding timelines" (Brown, Jr, 2020) is required. The demand is real but setting realistic expectations for AI/ML is important. There is room for improvement in existing C2 processes with automation and, in some cases, AL/ML; in contrast, other C2 processes will remain hard for both humans and algorithms. As U.S. House Armed Services Committee Chairman and Representative Adam Smith, D-Wash., said of JADC2 in September 2021, "The goal is correct, but do not underestimate the difficulty of achieving it (Harper, 2021)."

References:

Lingel, S., Hagen, J., Hastings, E., Lee, M., Sargent, M., Walsh, M., Zhang, L.A. and Blancett, D. (2020). *Joint All-domain Command and Control for Modern Warfare: An Analytical Framework for Identifying and Developing Artificial Intelligence Applications*. Volume I: Artificial Intelligence Applications for Joint All-Domain Command and Control, Santa Monica, Calif.: RAND Corporation, RR-4408/1-AF.

Walsh, M., Menthe, L., Geist, E., Hastings, E., Kerrigan, J., Léveillé, J., Margolis, J., Martin, N. and Donnelly, B.P. (2021). *Exploring the feasibility and utility of machine learning-assisted command and control. Volume 1, Findings and recommendations*, RAND Report RR-A263-1.

Brown, C. Q. Jr., Accelerate *Change or Lose*, [online]. (2020). Available from: *https://www.af.mil/Portals/1/documents/2020SAF/ACOL_booklet_FINAL_13_Nov_1006_WEB.pdf*

Harper, J. (2021). Will the Military Waste Billions on JADC2 Efforts?. *National Defense* [online], September. Available from: *https://www.nationaldefensemagazine.org/articles/2021/9/29/will-the-military-waste-billions-on-jadc2-efforts*

Future Options for Artificial Intelligence and Machine Learning Assisted Decision-Making in Air Warfare

4

Dr. Peter Layton

Visiting Fellow, Griffith Asia Institute

Introduction

Air warfare both involves and is shaped by technology. The technologies used bound the possible actions air forces can potentially take, both empowering and constraining force employment options. Given this, emerging major new technologies always attract great interest and today this is focussed on artificial intelligence (AI).

For the foreseeable future, this is narrow AI technology, not general. Narrow AI equals or exceeds human intelligence for specific tasks within a particular domain. In contrast, general AI equals the full range of human performance for any task in any domain. General AI appears several decades away (Gruetzemacher, 2019).

The global military interest for the near-to-medium term is in how narrow AI technologies could be employed in the modern battlefield. Such AI can be applied in multifarious ways and may be considered as a general purpose technology that as, in wider society, will become pervasive and incorporated into most military machines. (Trajtenberg 2018)

This article restricts its gaze to considering AI in decision-making and in particular in air warfare. The article initially discusses the technology, before noting operational constructs and finishing with considering three alternative approaches for AI and machine learning assisted decision-making in air warfare.

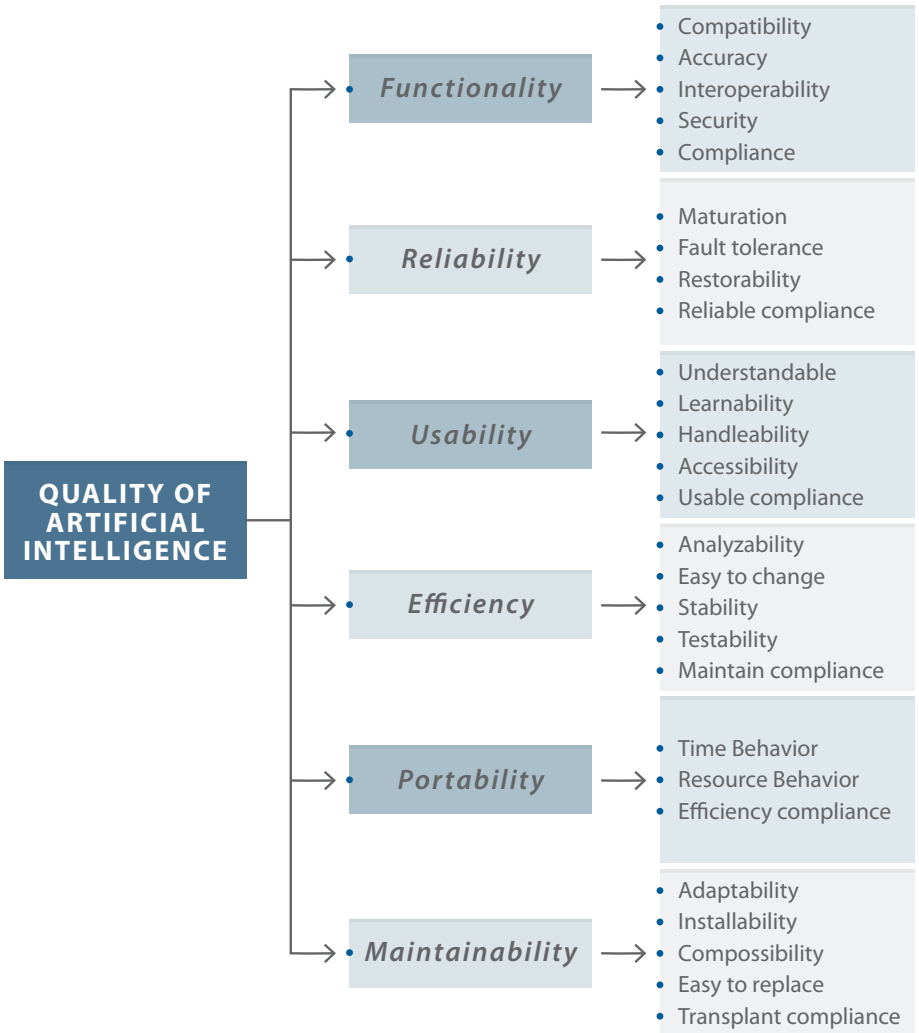
Technology Matters

Modern AI has evolved to meet the needs of the commercial domain and especially consumers. A key advance was when low cost Graphics Processing Units (GPUs) became readily available, mainly to meet video gaming demand. With their massive parallel processing, GPUs can readily run machine learning software. Machine learning is an old concept but it needed the combination of GPUs and access to 'big data' troves to make practical and affordable on a large scale.

In machine learning, the computer's algorithms not external human computer programmers, creates the sequence of instructions and rules that the AI then uses to solve problems. In general, the more data used to train the algorithm the better the rules and instructions devised. Given this, AI with machine learning can potentially teach itself while 'on the job', getting progressively better at a task as it steadily gains more experience in it.

In many cases, this data comes from a large-scale network of interconnected devices that collect information from the field and then transmit this through a wireless 'cloud' into a remote AI computer for processing. In the military sector, the Internet of Battlefield Things (IoBT) network features fixed and mobile devices, including drones able to collaborate with each other in swarms. Such IoBT networks allow remote sensing and control but generate vast amounts of data. A way around this is to connect the network to an edge device that can assess the data in real-time, forward the most important information into the cloud and delete the remainder, thereby saving on storage and bandwidth.

Most edge computing is now done using AI chips. These are physically small, relatively inexpensive, use minimal power, and generate little heat allowing them to be readily integrated into handheld devices such as smartphones and non-consumer devices such as industrial robots. Even so, in many applications AI is used in a hybrid fashion: some portion on-device and some remotely in a distant fusion centre accessed via the cloud.



Operational Constructs

Several important operational concepts are emerging relevant to future air warfare. Operations are moving from being joint into now being multi-domain, that is across land, sea, air, cyber and space. The intent under a follow-on concept called "convergence" is that friendly forces should be able to attack hostile units across and in any domain (Wesley 2020, 4-5). For example, land units will now be able to engage ships at sea, air forces attack space assets and cyber everywhere, simultaneously and in contested environments.

Such an operational concept abandons the traditional, single domain linear kill chains to embrace multi-domain ones that leverage alternate or multiple pathways. The emerging associated "mosaic" construct envisages the data flow across the large IoBT field creating a kill web, where the best path to achieve a task is determined and used in near real-time. The use made of the IoBT field is then fluid and constantly varying, not a fixed data flow as the older kill-chain model implies. The outcome is that the mosaic concept provides highly resilient networks of redundant nodes and multiple kill paths. (Clark 2020, 27-32) This cross domain thinking is now evolving further into notions of "expanded maneuver." (Vergun 2021)

The complexity of implementing these interlocking operational concepts against peer adversaries during a major conflict is readily apparent. To make multi-domain operations involving convergence, mosaic and expanded maneuver operations practical requires the use of automated systems using AI with machine learning.

In the near-to-medium term, AI's principal attraction for decision making involving such complex constructs will its ability to quickly identify patterns and detect items hidden within the large data troves collected by the IoBT. The principal consequence of this is that AI will make it much easier to detect, localise and identify objects across the battlespace. Hiding will become increasingly difficult and targeting much easier. On the other hand, AI is not perfect. It has well known problems in being able to be fooled, in being brittle, being unable

to transfer knowledge gained in one task to another and being dependent on data. (Layton 2021, pp. 13-15)

AI's warfighting principal utility then becomes 'find and fool'. AI with its machine learning is excellent at finding items hidden within a high clutter background however, in being able to be fooled, lacks robustness.

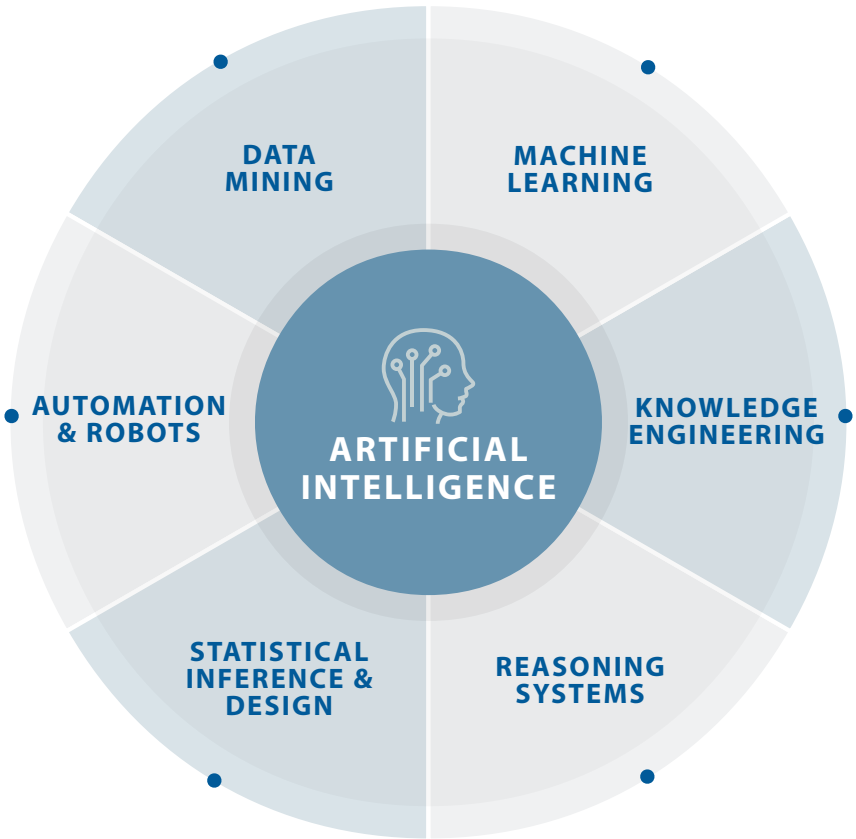
The 'find' starting point is placing many low cost IoBT sensors in the optimum land, sea, air, space and cyber locations in those areas across which hostile forces may transit. A future battlespace might feature hundreds, possibly thousands, of small-to-medium stationary and mobile AI-enabled surveillance and reconnaissance systems operating across all domains. Simultaneously, there may be an equivalent number of AI-enabled jamming and deception systems acting in concert trying to create in the adversary's mind a false and deliberately misleading impression of the battlefield.

Alternative Decision-Making Options

The AI and machine learning decision-making options possible will be influenced both by the technologies and the needs of the desired operational concepts. The alternatives discussed here are to use technology to be able to react to an adversary's actions much faster, to get in front of the adversary through technology driven pre-emption, or to slow adversary decision making down significantly.

Option 1: Hyperwar

AI offers up visions of war at machine speed. John Allen and Amir Husain see AI allowing hyperwar where: "The speed of battle at the tactical end of the warfare spectrum will accelerate enormously, collapsing the decision-action cycle to fractions of a second, giving the decisive edge to the side with the more autonomous decision-action concurrency." (Allen 2017)



In the case of air warfare decision-making, the well-known Observe-Orient-Decide-Action (OODA) model provides a useful framework to appreciate this idea. The model's designer, John Boyd, advocated making decisions faster so as to get inside the adversary's decision-making cycle. This would disrupt the enemy commander's thinking, create a seemingly menacing situation and hinder their adaption to a now too-rapidly changing environment. (Fadok 1997, p.364-368)

In the 'Observe' function, AI would be used for edge computing in most of the IoBT's devices then again in the central command centre that fused the incom-

ing IoBT data into a single comprehensive picture. For 'Orient', AI would play an important part in the battle management system.(Westwood 2020, 22) AI would not only produce a comprehensive near-real time air picture but also predict the enemy air courses of action and movements.

The next AI layer handling 'Decide' in being aware of friendly air defence units availability would pass to the human commander for approval a prioritised list of approaching hostile air targets to engage, the optimum types of multi-domain attack to employ, the timings involved and any deconfliction considerations. Humans would remain in-the-loop or on-the-loop control as necessary, not just for law of armed conflict reasons but as AI can make mistakes and needs checking before any irreversible decisions are made. After human approval, the 'Action' AI layer would assign the preferred weapons to each target passing the requisite targeting data automatically, ensure deconfliction with friendly forces, confirming when the target was engaged and potentially ordering weapon resupply.

Option 2: Beyond OODA

AI technology is rapidly proliferating making it likely both friendly and adversary forces will be equally capable of hyperwar. The OODA model of decision making may then need to change. Under it, an Observation cannot be made until after the event has occurred; the model inherently looks backwards in time. AI could bring a subtle shift. Combining suitable digital models of the environment and the opposing forces with high-quality 'find' data from the IoBT, AI could predict the range of future actions an adversary could conceivably take and from this, the actions the friendly force might best take to counter these.

An AI and machine learning assisted decision making model might then be 'Sense–Predict–Agree–Act': AI senses the environment to find adversary and friendly forces; AI predicts what adversary forces might do in the immediate future and advises on the best friendly force response; the human part of the human–machine team agrees; and AI acts by sending machine-to-machine in-

structions to the diverse array of AI-enabled systems deployed across the battlespace. Under this decision-making option, friendly forces would aim to seize the initiative and act before adversary forces do. It is a highly calculated form of on-going, tactical level pre-emption.

> *AI will make it much easier to detect, localise and identify objects across the battlespace. Hiding will become increasingly difficult and targeting much easier.*

Option 3: Stop Others Decision-Making

An alternative to trying to make friendly force decisions faster is to try to slow the adversary's decision-making down. In air warfare an attacker needs considerable information about the target and its defences to mount successful air raids.

To prevent this, AI-enabled 'fool' systems could be dispersed across the battlespace, both physically and in cyberspace. Small, mobile, edge computing systems widely dispersed could create complicated electronic decoy patterns by transmitting a range of signals of varying fidelity. These systems might be mounted on drones for the greatest mobility, although uncrewed ground vehicles using the road network may also be useful for specific functions such as pretending to be mobile SAM systems. The intent is to defeat the adversary's 'find' systems by building up a misleading or at least a confused picture of the battlefield.

AI-enabled 'fool' systems may also be used in conjunction with a sophisticated deception campaign. For example, several drones all actively transmitting a noisy facsimile of the electronic signature of friendly force fighters could take off when they do. With seemingly, very large numbers of fighter aircraft suddenly airborne, the adversary will be unsure which are real or not.

Conclusion

The three options present real choices in terms of decision-making. Perhaps at odds with initial perceptions, the hyperwar concept is most likely to involve a series of multi-domain salvo or spasm attacks rather than a continuous flowing action. Physical constraints mean that it would take time to rearm, refuel and reposition own-force machines for follow-on attacks.

On the other hand, the beyond OODA option, can be much more of a continuous action as it is effectively following a detailed plan albeit informed by IoBT battlespace sensing. Such a decision-making construct might suit an active defence that absorbed the first attack, learnt from it, and then attacked in a predetermined manner. Given AI's processing speeds the response would be determined immediately before being launched, allowing the greatest value to be made from AI's 'on the job' machine learning.

Lastly, the stopping others decision-making option offers great promise for defenders but requires a good knowledge of the adversary in terms of both the surveillance and reconnaissance systems in use and the cognition of the humans involved. It seems best suited for frozen conflict situations where the 'fool' systems can be optimally placed, the environment very well understood and a single adversary is faced. This option may be less suitable for forces that deploy into distant combat zones quickly and have only a limited comprehension of the situation.

The option preferred will depend on the context but highlights that not all using AI in a conflict may use the same technology in the same way, even in the narrow area of decision-making. There is no doubt that AI will significantly change air warfare decision-making and importantly, in the near term. The choice for each air force today is which way is best for them. Now is the time to start thinking deeply about the issue.

References:

Allen, J.R., and Husain, A. (2017). 'On hyperwar', *USNI Proceedings Magazine*, vol. 143, no. 7.

Clark, B., Patt, D., Schramm, H., (2020). Mosaic Warfare Exploiting Artificial Intelligence And Autonomous Systems To Implement Decision-Centric Operations, Center for Strategic and Budgetary Assessments, Washington.

Fadok, D.S. (1997). *John Boyd and John Warden: Airpower's Quest for Strategic Paralysis*, pp. 357-398 in Phillip S. Meilinger (ed.), The Paths of Heaven The Evolution of Airpower Theory, Air University Press, USAF Maxwell Air Force Base.

Gruetzemacher, R., Paradice, D. and Lee, K.B. (2019). Forecasting transformative AI: an expert survey, Computers and Society: Cornell University. Available from: https://arxiv.org/abs/1901.08579 [16 September 2021].

Layton, P. (2021). *Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars,* Joint Studies Paper Series No. 4, Department of Defence, Canberra.

Trajtenberg, M. (2018). *AI as the next GPT: a political-economy perspective*, National Bureau Of Economic Research, Cambridge.

Vergun, D. (2021). *DOD Focuses on Aspirational Challenges in Future Warfighting*, DOD News, Available from: *https://www.defense.gov/Explore/News/Article/Article/2707633/dod-focuses-on-aspirational-challenges-in-future-warfighting/#DCT* [17 September 2021].

Wesley, E.J., and Simpson, R.H. (2020). *Expanding the battlefield: an important fundamental of multi-domain operations*, Association Of The United States Army, Arlington.

Westwood, C. (2020), *5th Generation Air Battle Management,* Air Power Development Centre, Canberra.

De-Centralized Command and Control in Air Operations: Implications for Air Battle Management and Mission Command

5

Justin Bronk

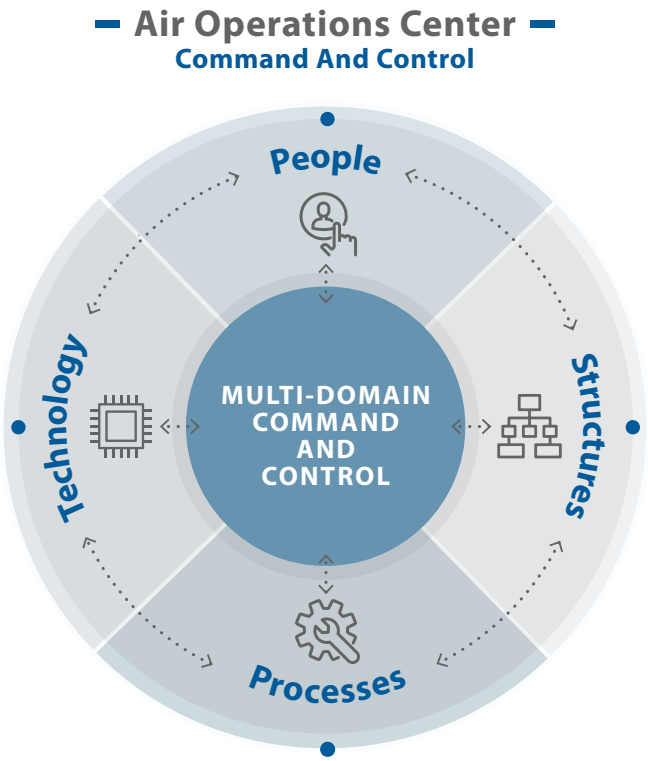
Research Fellow, Royal United Services Institute

Introduction

Air forces around the world which are focusing on peer or near-peer military competition are increasingly aware of the need to adopt decentralised mission command and control (C2) architectures. However, important cultural and political resistance will need to be overcome to allow this to happen. Decentralised C2 will require a reintroduction of traditional notions of mission command where decision-making authorities and permissions are increasingly delegated to relatively junior combat leaders at the tactical level. Nevertheless, most future C2 architectures are being developed with at least some degree of decentralisation in order to make it harder for opposing forces to find, target and degrade key airborne and ground-based nodes. Leading airpower nations are exploring combinations for distributed orbital assets and unmanned aerial vehicles (UAV) to displace legacy processing, exploitation, and dissemination (PED) and C2 platforms.

The future shape of the orbital domain as part of distributed C2 and ISTAR architectures remains uncertain because rapid advances in space-based sensor capabilities, communications bandwidth and robustness suggest a sharp increase

in their role, however, the use of these assets is also likely be highly contested or even denied in the future. UAVs offer potential for long endurance without the same predictable and potentially vulnerable trajectories as satellites in orbit. The viability of fifth generation platforms such as the F-35 and very low observable UAVs as building blocks in a next-generation distributed C2 and ISTAR architecture requires not only secure and inconspicuous datalinks and sensors, but also dynamic edge processing capacity to reduce bandwidth requirements and automatically identify and pass relevant data to other assets. For the foreseeable future, therefore, air forces may well remain reliant on centralised C2 based on obsolescent wide-bodied legacy systems.



The Future Environment

The future combat air environment is characterised by the increasingly ubiquitous development of long-range surface to air missile (SAM) systems (Bronk, 2020a), very long-range air-to-air missiles (VLRAAMs) and very low observable (VLO) fighter and interceptor aircraft (Bronk, 2020b). This new generation of threat systems is steadily increasing the risk level to conventional air operations which rely heavily on centralised command and control assets such as the E-3 AWACS. Long range SAM systems, VLRAAMs and VLO fighter threats will increasingly force traditional command and control (C2) and intelligence, surveillance, target acquisition and reconnaissance (ISTAR) aircraft to operate so far away from hostile territory that their on-board sensors and communications hub capabilities will give greatly reduced operational utility. At the same time, the availability of long-range precision strike systems and offensive cyber tools continue to increase the threat which modern states can pose to each other's centralised ground-based command and control facilities such as combined air operations centres (CAOCs) (Kaushal, Macy and Stickings, 2019). As such, two of the central pillars of early 21st Century Western air power face a potentially existential challenge.

Since the late 1980s, Western air forces have relied heavily on air power to enable joint force operations to be conducted with significantly smaller ground and maritime components than would otherwise have been necessary. The striking success of this model in multiple conflicts during the 1990s and 2000s led to force design across armies and navies which assumed the availability of air support and air-enabled C2 and ISTAR. As such, the ability to provide on-demand ISTAR and fire support from the air is now an essential prerequisite for many Western nations to employ military power. The reliance on coalition operations to generate mass and political legitimacy has also created integration, deconfliction and permissions and oversight requirements as part of everyday air operations. This combination of reliance on air power for joint operations, and coalition integration as a constant requirement, has created an extremely centralised C2 model with the combined air operations centre (CAOC) construct as the focal point.

Legacy Models for C2 and CAOCs

Within a CAOC, the 72-hour Air Tasking Order (ATO) is generated with reference to the various joint force taskings, ISTAR products, multinational contingent permissions processes and enablers such as tankers. This process requires hundreds of specialist professionals, large, fixed facilities and excellent communications links—making CAOCs an extremely valuable and obvious target for hostile states in any major war. The closer a CAOC is to the area of operations, the more potentially vulnerable it becomes to hostile kinetic long range precision strike capabilities. However, the further removed it is, the greater the operational dependence on potentially vulnerable buried, line-of-sight, beyond-line-of-sight and orbital communications links.

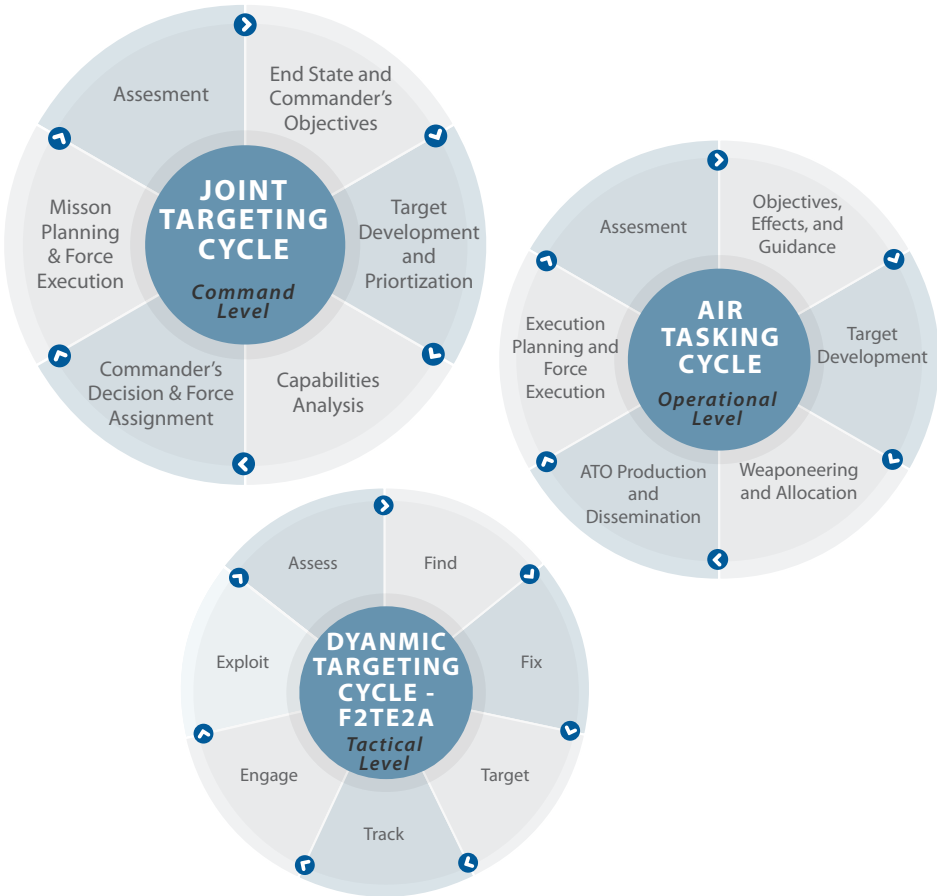
Some future concepts feature smaller scale, more distributed air operations centres (AOCs) to reduce the vulnerability of the joint force to decapitation style attacks on its C2. However, relying on more numerous, distributed AOCs rather than large COACs could create duplication of tasks and thereby increase the burden placed on already overstretched intelligence and command staff personnel. C2 distribution could also increase the dependency on assured communications links, since each AOC is only able to perform some functions of a full scale COAC even with a significant automation of necessary processes. Therefore, if kinetic or non-kinetic tools were to sever or even seriously contest these links then both centralised COACs or smaller distributed AOCs may stand to lose the ability to tactically coordinate ISTAR, strike and enabler assets in-theatre.

Furthermore, a habit of senior commanders exerting direct control and supervision over tactical operations has been allowed to emerge during several decades of largely uncontested air operations. This has partially been prompted by the increased availability of real-time full motion video feeds, allowing CAOC commanders the perception of tactical situational awareness. It has also been fed by a significantly curtailed tolerance for risk at the political level during what have often been seen as discretionary and unpopular conflicts. This, in turn, has increased the desire to avoid delegating control and permissions to the tactical level. Such existing command practices further increase centralisation, reduce

operational tempo and introduce a range of potential bandwidth bottlenecks and electromagnetic vulnerabilities into air operations. Despite discretionary conflicts being the context within which authorities have been held at higher levels, the move back towards planning for high-end conflicts may be unlikely to produce a natural reversal of this trend. Senior politicians and military leaders in many countries are likely to view the much higher geopolitical stakes involved in a peer conflict as a reason to continue to centrally manage tactical decision-making. However, this approach is almost certain to fail in practice against peer and near peer opponents due to the slow operational tempo it entails, and the beyond-line-of-sight connectivity and bandwidth it requires. To be suitable for future state-on-state conflicts, the tactical air commander culture must change to avoid operational paralysis as kinetic, electromagnetic and cyber attacks on the CAOC construct and its supporting communications links cut off commanders from frontline assets.

Future Architectures for Decentralized C2

It is clear to many air forces that traditional airborne C2 and ISTAR nodes derived from wide-bodied airliners such as the E-3 AWACS and E-8 J-STARS are no longer optimal for future conflict scenarios. These assets have very limited self-defence capabilities and must emit large amounts of easily detectable electromagnetic signals in order to function effectively, which makes them easy to locate and track. Such platforms also represent a serious source of potential casualties, since they carry large, highly trained mission systems crews to carry out the key task of processing, exploitation, and dissemination (PED), as well as air battle management functions. Wide-bodied ISTAR and C2 aircraft must stand off so far from hostile SAM systems and VLRAAMs today as to be largely ineffective in terms of their primary sensor picture in the early stages of a conflict with technologically advanced competitors.



The fifth generation F-35 is significantly less dependent on such C2 and ISTAR enablers due to its own ability to supply its pilots with multi-spectral wide-area situation awareness. This ability to organically build situational awareness inside hostile airspace has led many to plan on exploiting the F-35 as a primary building block in a next-generation distributed C2 and ISTAR network (Bronk, 2020c). However, in its present form the F-35 cannot transmit the full sensor picture which it creates for its pilots to other force elements due to bandwidth, software architecture and emissions-control limitations. Furthermore, as a tactical strike fighter, F-35s have limited endurance compared to traditional ISTAR and

C2 nodes, and the limited numbers of F-35s available are also already committed to strike, SEAD/DEAD and interdiction mission sets. Platforms such as the F35, therefore, offer only a partial solution to the increasing obsolescence of traditional C2 and ISTAR enabler assets and networks.

Decentralised airborne C2 and ISTAR architectures under development require changes in equipment to enable air forces to field a larger number of smaller platforms. Alongside network-enabled combat assets such as the F-35, a range of smaller, crewed C2 and ISTAR platforms may still offer the option to carry a small mission system crew to enable on-board PED and air battle management. However, several leading airpower nations are already exploring combinations of distributed orbital assets and unmanned aerial vehicles (UAV) which would displace the PED and C2 functions to remote ground stations.

The future shape of the orbital domain as part of distributed C2 and ISTAR architectures is currently unclear due to a range of competing trends. On the one hand, rapid advances in sensor capabilities, space/weight/power requirements for equipment, communications bandwidth and robustness through MIMO-type arrays and falling cost of launch capacity all point to a sharp increase in the role orbital assets are able to play in future distributed ISTAR and C2 networks. At the same time however a proliferation of kinetic and soft-kill ASAT capabilities, orbital assets capable of Rendezvous, offensive proximity operations and an increasingly contested electromagnetic spectrum render orbital assets and the uplink/downlink capabilities required to utilise them increasingly likely to be denied or at least highly contested in any future war.

The ability to provide on-demand ISTAR and fire support from the air is now an essential prerequisite

UAVs offer the potential for much longer endurance on station than assets which rely on a human flight and mission system crew, without the same predictable and potentially vulnerable trajectories as satellites in orbit. Large UAVs such as the US Air Force RQ-4 Global Hawk and Chinese Divine Eagle have already demonstrated the ability to fly at very high altitudes for more than 24

hours at a time—a hugely desirable attribute for any decentralised airborne C2 or ISTAR node. To make them better able to persist in the face of peer threats, high-altitude, long endurance (HALE) type UAVs with very-low observable (VLO) shapes and materials offer new potential. The suitability of VLO UAVs for C2 and ISTAR tasks within a decentralised system would depend on the development of cutting-edge datalinks, sensors and SATCOMs which could perform their mission functions without revealing the airframe to hostile passive sensors. To complete such tasks, there are promising technologies on the horizon which exist at various degrees of technological maturity but remain expensive and are held at a high level of classification and security sensitivity by the nations which field them. This means that large scale deployment will be challenging, especially on unmanned platforms close to hostile territory.

Connecting Assets is Not Enough

Whilst uncrewed VLO, HALE airframes could be deployed and persist closer to hostile forces than current generation airliner-derived solutions, their ability to replace traditional airborne C2 and ISTAR nodes depends on automated data-sharing and edge processing technologies. Modern ISTAR assets, especially those with multi-spectral sensor suites such as on the F-35, create huge volumes of data as they construct a wide-area picture of the battlespace around them. During this process, they will collect information that could potentially be of high or even critical value to a wide range of other assets across all domains. However, physics-based bandwidth limitations restrict the ability to offload or share all the data collected, even in a non-contested electromagnetic environment (Watling, 2020). In a state-on-state conflict scenario, where the ISTAR (and C2) platforms will be competing for limited and contested spectrum access and potentially operating under emission-controlled conditions to reduce their vulnerability to detection and attack, edge processing to reduce the data volumes which need to be shared will be essential.

Human mission crews can (subject to mental capacity and workload) make the required subjective and situationally-dependent priority and relevance judge-

ments about what information might or might not be worth passing to other assets. Crucially, however, automated systems cannot currently do this except in specific, rigidly defined circumstances. The same goes for the often reactive and judgement-dependent task of air battle management, which is a core part of the AWACS mission set. Replacing centralised C2 and ISTAR nodes in the air domain with an architecture of datalinks and decentralised network nodes primarily mounted on HALE type UAVs and penetrating combat assets is impossible without a suitable answer to these problems.

The components for a highly automated, decentralised airborne C2 and data-sharing network such as that being pursued under the US Joint All-Domain Command and Control (JADC2) programme are within the reach of airframe designers (Congressional Research Service, 2021). However, this ambition is beyond the capacity of currently viable artificial intelligence and autonomy technology. The requirement for such a system is clear, since the bulk of the combat mass in air forces around the world will still be provided by advanced fourth-generation fighters and standoff munitions until at least the mid-2030s. These weapons systems will not be able to perform the roles required of them in high intensity conflicts without being fed real time situational awareness, targeting and weapons cueing from across the battlespace. However, without the subjective judgement and prioritisation capabilities required to allow automated edge processing to truly replace human mission crews in the air battle management and ISTAR PED tasks, air forces may well remain dependent on centralised airborne architecture based on obsolescent wide-bodied legacy systems.

References:

Bronk, J., (2020(a)). 'Modern Russian and Chinese Integrated Air Defence Systems: The Nature of the Threat, Growth Trajectory and Western Options', *RUSI Occasional Papers*, available at *https://static.rusi.org/20191118_iads_bronk_web_final.pdf*

Bronk, J., (2020(b)). 'Russian and Chinese Combat Air Trends: Current Capabilities and Future Threat Outlook', *RUSI Whitehall Reports*, available at *https://static.rusi.org/russian_and_chinese_combat_air_trends_whr_final_web_version.pdf*

Bronk, J., (2020(c)). 'Combat Air Choices for the UK Government', *RUSI Occasional Papers*, available at *https://rusi.org/explore-our-research/publications/occasional-papers/combat-air-choices-uk-government*

Congressional Research Service, *Joint All-Domain Command and Control (JADC2)*, Report, (2021). Available at: *https://crsreports.congress.gov/product/pdf/IF/IF11493*

Kaushal, S., Macy, A. and Stickings, A. (2021). 'The Future of NATO's Air and Missile Defence', *RUSI Occasional Papers*. Available at: *https://static.rusi.org/NATOMissileDefence2021.pdf*

Watling, J. (2020). 'From Multirole to Modularity', *RUSI Defence Systems*. Available at: *https://rusi.org/explore-our-research/publications/rusi-defence-systems/multirole-modularity*

Integration and Interoperability for Multi-Domain Operations in the Coalition Environment: Challenges for European Air Combat Fleets

6

Professor Olivier Zajec

Director, Institute of Strategic and Defense Studies (IESD), Lyon University

Multi-Domain Operations and Interoperability between Air Forces

Strategic thinking in the airpower community is evolving dramatically under the influence of the multi-domain operations (MDO) concept. Until the 1990s, armed forces were broadly engaged in 'transformation' efforts with the aim of improving coordination between military services. By the 2000s, the goal and objectives of transformation efforts evolved and the desire for improved coordination gave way to efforts for deeper operational integration between military services and coalition partners. MDO advances the transformation objective towards an eventual fusion of capabilities among the operational domains in order to be able to deliver simultaneous effects at a much faster pace of operations (Jamieson and Calabrese, 2015). However not all countries are clear on how precisely to adopt the American vision for MDO into their own doctrines and concept of operations or how to resolve the likely integration and interoperability challenges which are generated (Townsend, 2019).

The intended goal of MDO is to accelerate the pace of military operations and allow a more synergistic coordination of effects to be produced in the opera-

tional environment. Multi-domain integration promises to optimize operational advantages in order to pressure the decision-making loops of opposing forces. At the same time MDO also implies a considerable evolution of and necessary changes in approaches to joint operations so its impact will readily affect friendly forces just as profoundly. As noted by Major General Louis Pena, Deputy Commander of the French Air Defense and Air Operations Command (CDAOA), MDO represents "an opportunity to think about how air forces will plan and conduct air operations in the future" (Pena, 2020). It is certain that MDO will be a powerful factor in shaping the future concept of operations for air combat and transformation efforts however there are complex conceptual, technical and strategic challenges that will need to be overcome.

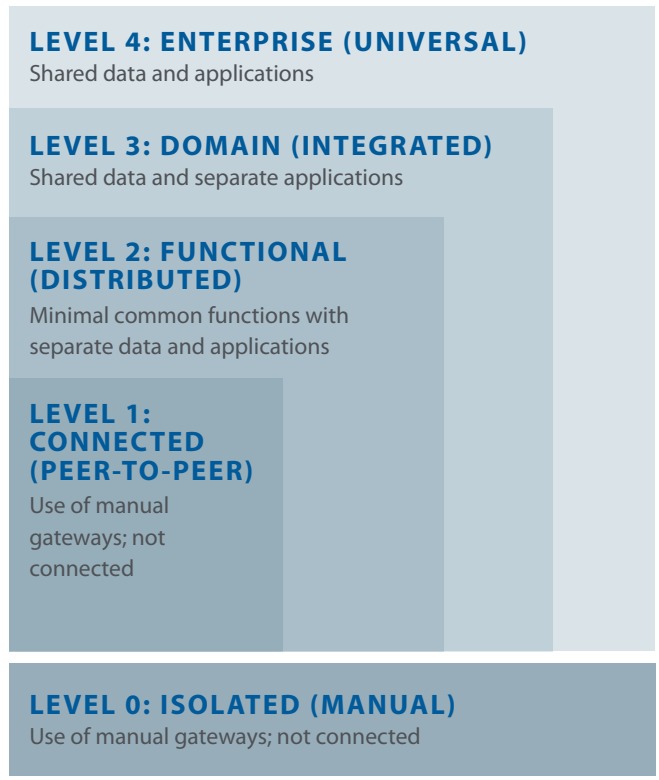
Connectivity and Future Air Combat

Future combat aircraft are envisioned to function and perform as 'connectivity centers' and 'airborne data fusion servers,' linked with a combat cloud providing real-time multi-domain information to distributed elements of joint or coalition forces. These next generation combat aircraft are prepositioned to assume the same roles currently assigned by air forces to airborne warning and control (AWAC) aircraft. AWACS have become a key nodal function in air operations since the arrival of Link 16 which has proven instrumental for Western air superiority in recent decades by enabling radically improved situational awareness and command, control and communications (C3) capabilities in joint and coalition campaigns.

> *The challenge of interoperability in coalition environments is being reframed and will take a new direction with the introduction of new combat aircraft and platforms but there are no clear or readily available solutions to bridge differences in doctrine and concept of operations on the one hand, or for technical integration in a coalition environment where constituent air forces each bring their own set of capabilities, tools and platforms to the fight.*

In the future, data fusion and relay functions will become more distributed and increasingly transferred to combat aircraft themselves, which will be able to orchestrate drone swarms to, for example, penetrate enemy air defenses or deliver kinetic effects. Empowered by new tools and faster decision-making through next generation data and communication networks, combat aircraft will operate in a multi-domain space as key command and control (C2) nodes themselves. Air combat operations will therefore no longer correlate to a set of sequenced tasks but rather to a single continuum of de-compartmentalized maneuvers and effects based on and highly responsive to activity by opposing forces.

Level of Information System Interoperability (LISI) Model



Air combat will feature a more informed and intelligent application of economy of force to overwhelm opposing forces using a combination of velocity, saturation and stealth ("V2S"—velocity, saturation, stealth) to achieve battlespace superiority. These future concepts rely on a system-of-systems approach with a command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISTAR) core and where each individual force vector functions both as a sensor and as an effector at the same time. Capabilities relating to data fusion, automation, robotics and artificial intelligence (AI) will be critical to realizing 'Spectrum Dominance'—superiority across the operational spectrum.

Air combat will progressively become more dependent on multi-domain awareness and information dominance. The prospect of a singular, overarching combat cloud functioning as central library or brain however presents complex issues in a coalition environment: Permanent connectivity to such a combat cloud generates obvious vulnerabilities for coalition force components. While offering advantages in terms of force concentration and efficiency, the same concentration of power and reliance towards one central cloud generates the prospects of a catastrophic loss in freedom of action. Opposing forces will be aim to hinder communications and employ decoys against sensor networks and in such a context of benign cyberspace and electromagnetic warfare a "One Ring" combat cloud may lead to operational paralysis across its subscribed user base.

In considering such risks, there are serious questions around the maturity of key enabling technologies for the notion of the combat cloud. Information systems and technologies that collect, analyze, store and transmit data are all subject to intrusive threats and replication by opposing forces in order to advance the effectiveness of their anti-access/area denial(A2AD) (Orlin, 2021). 'Big data,' a fundamental requisite for any Common Recognized Operational Picture (CROP) between distributed C2 elements, cannot be properly exploited without AI, the use of which remains problematic given its susceptibility to manipulation and deception.

Predictive maintenance, which is native to future air combat platforms and will be continuously communicated over the network, offers a new attack vulner-

ability in the warfare space and is likely to be heavily targeted (Hitchens, 2020). The exploitation of potential software flaws and limitations will create opportunities for opposing forces in terms of deception, circumvention and surprise operations. Advanced jamming targeting communications and sensor networks, offensive cyber warfare operations directed at the combat cloud (Gros, 2019), and dependence on space assets presents serious risks in scenarios where ground-based or space assets are destroyed or critical data-links become compromised (French Defense and National Security Strategic Review, 2017).

The proliferation of drone technology and digitization of combat systems is already compelling air forces and their sister services Europe to focus investments in cyberspace countermeasures and to 'harden' platforms, assets and operations infrastructure to ensure communications nodes and transmitters are not compromised. Such efforts will accelerate and intensify as military competitors target data and data connectivity capabilities across a wider attack surface that extends the coalition or allied force which are all connected to the same cloud. Such inherent risks to multi-domain combat grids therefore emphasize needs to consider the development of future combat clouds for MDO in coalition environments outside a 'One Ring' design.

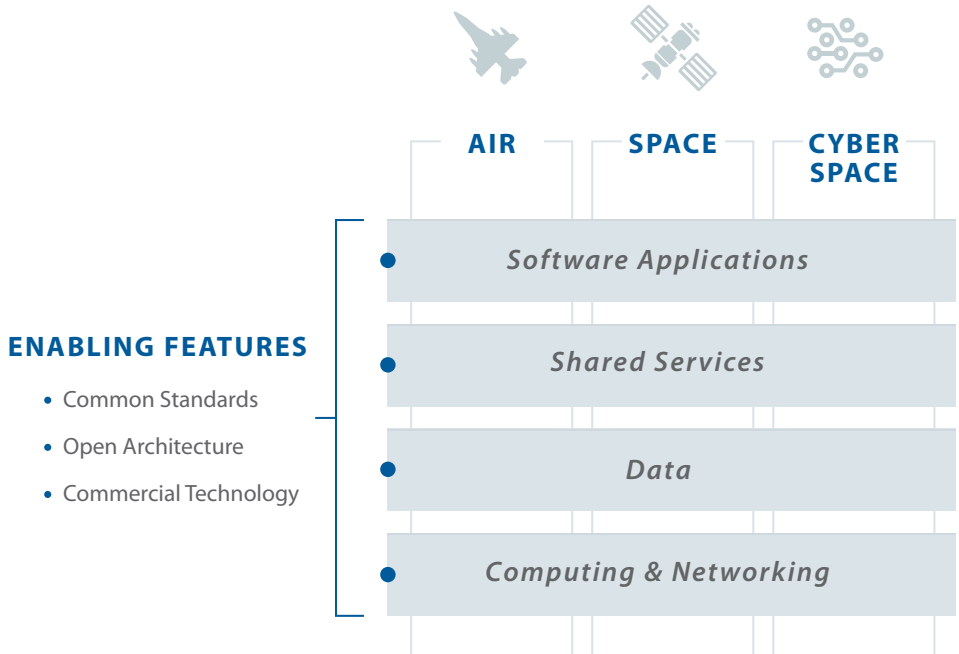
Europe's Combat Air Fleets: The Current and Future Landscape

In Europe, operational integration between air forces has been progressing steadily—the NATO factor has been an important one but is by no means the only driver for the progress achieved in enhancing interoperability between European air forces. Yet the European airpower landscape remains marked by considerable diversity, as illustrated by the diverse typology of the more than 1,900 combat aircraft currently in service.

The American-led F-35 program has brought together a number of European nations including the United Kingdom, the Netherlands, Denmark, Norway, Belgium and Italy. The F-35 as a fifth-generation combat aircraft introduces a new

model and standard for interoperability for Europe which will, together with its operators, play a powerful role in shaping interoperability efforts and programs across European air forces over the coming years. However, most F-35 users continue to maintain wider combat fleets—the Eurofighter Typhoon for example is likely to remain indispensable to the United Kingdom because of the F-35's limitations in air superiority missions. For similar reasons, the Typhoon will likely continue to be operated by Italy, Germany and Spain and similar considerations may extend to F-16 operators such as Belgium, Denmark, Greece, the Netherlands, Norway, Portugal and Turkey.

Elements of Interoperability in Future Networked Multi-Domain Operations



Other European air forces have acquired combat aircraft such as the Gripen-E and Rafale which, with its AESA radar and data fusion capabilities, could be con-

sidered as the de facto future European standard for interoperability. Finland is pursuing its HX Fighter program with five combat aircraft platforms actively involved in the competition. Looking out to 2040 and beyond, Europe is likely to continue seeing the indigenous development of next generation combat aircraft and, with them, new standards for interoperability being inserted into both the acquisition and operational planning frames. Consider the development of the FCAS (Future Combat Air System) and the British Tempest as cases in example—both platforms will be coupled with remotely operated and autonomous systems and relays, and operate inside cloud-based multi-domain data exchange networks.

> *Air combat operations will therefore no longer correlate to a set of sequenced tasks but rather to a single continuum of de-compartmentalized maneuvers and effects based on and highly responsive to activity by opposing forces.*

The existing and likely future diversity of European air combat fleets may prima facie suggest an unnecessary duplication of capabilities however these same differences in approaches and capabilities also provide greater resilience at the operational and strategic levels. In the coalition environment, it is unclear to what extent Europe's air combat fleets will be interoperable with, for example, F35s entering operational service in Europe now. The same questions will theoretically apply to the FCAS or Tempest and these questions around compatibility and interoperability will extend into the future particularly in relation to MDO.

The challenge of interoperability in coalition environments is being reframed and will take a new direction with the introduction of new combat aircraft and platforms but there are no clear or readily available solutions to bridge differences in doctrine and concept of operations on the one hand, or for technical integration in a coalition environment where constituent air forces each bring their own set of capabilities, tools and platforms to the fight. The irony is that the basic premise and purpose of multi-domain integration is to resolve the lack of or low compatibility and synergies between different types of platforms, across

different domains, which are developed using different technical standards and systems engineering approaches.

The Political Dimensions of Integration and Interoperability

The evolution towards MDO implies new challenges for the air force by introducing new sets of dynamics into and for joint parallel planning in the coalition environment. It also presents a need to adapt or replace existing mechanisms which have been developed to enable the necessary levels of integration and interoperability between coalition partners which allow them to operate together effectively. As the movement towards MDO accelerates, it begs the basic question: Is interoperability possible when air forces belonging to coalitions and alliances have adopted different standards in systems and network design owing to contrasting industrial and political considerations?

This question highlights uncertainties related to interoperability in the future timeframe looking out to 2040 and beyond as well as to current air combat fleets which, in the European landscape, already face similar challenges. European air forces will need to contend with requirements for joint integration and fusion at an operational level which will need to be balanced against higher level policy considerations that extend into the realm of national strategy, to include freedom of action and strategic autonomy. In this context, European air forces will need to interact with and plan capability programs and interoperability goals in line with national or European policy directions which are shaped by a complex milieu of institutional factors and agendas.

It is a reasonable argument that the likely benefits of distributivity and data fusion between air forces in coalition environments outweighs the associated risks created by shared combat clouds or the likelihood of operational paralysis occurring. However, beyond purely operational considerations, there are important policy issues which are shaped by grand strategy and political outlooks. Even between allies and partners that share similar worldviews and which fre-

quently operate or cooperate closely in coalition and joint operations, national policies can diverge—particularly with regards to military activity in crisis situations.

There are compelling and historical justifications for continuing to work towards achieving interoperability between coalition and allied partners, including however that would be implied in the context of combat clouds. These efforts however must be balanced with the need to preserve strategic autonomy and the ability to make independent assessments or military activity (Binnendjik and Vershbow, 2021). Diverging approaches which are sometimes viewed as leading to "capability duplication" and a wastage of financial resources in another way offer advantages through the creation of natural firewalls and resilience for joint national and joint coalition operations.

In view of current and future developments in coalition air combat models, preserving a level of autonomy may be as important as securing emerging combat clouds themselves. This will be particularly true in the European context where the combined combat fleet will likely be comprised of a range of platform types, each developed according to different systems engineering, technical and interoperability standards, which link to industrial and political considerations. The same baseline challenges may be transposable to other parts of the world, such as the Middle East or Asia. Rather than attempting to segment air combat fleets into "first" and "second" tier capabilities, coalition and allied partners will need to focus attention towards overcoming challenges and generating the integration enablers and interoperability solutions for MDO in traditional coalition environments (Binnendjik et al, 2021).

References:

Jamieson, V. and Calabrese, M. (2015). An ISR Perspective on Fusion Warfare. *The Mitchell Forum*. 1, p. 5.

Townsend, S. (2019). Defining the 'Domain' in Multi-Domain. Joint Air and Space Power Conference 2019:

Shaping NATO for Multi-Domain Operations of the Future [online], pp. 7-12. Available from: *https://www.japcc.org/wpcontent/uploads/JAPCC_Read_Ahead_2019.pdf* [12 October 2021].

Pena, L. (2020). Le MDC2 : l'occasion de rénover notre C2. *Défense et sécurité international*. 147, pp. 94.

Orlin, S. (2021). *Why the military needs a dynamic network infrastructure*. Defense Systems [online]. Available from: *https://defensesystems.com/articles/2021/06/02/dynamic-network-infrastructure.aspx*

Hitchens, T. (2020). *Air Force Expands AI-based Predictive Maintenance* [online]. Breaking Defense.

Gros, P. (2019). *The tactical cloud, a key element of the future combat air system* [online]. Fondation pour la recherche stratégique. Note n°08, p. 9.

French Defense and National Security Strategic Review [online]. (2017). DICoD—Bureau des éditions, p.90. Available from: *https://franceintheus.org/IMG/pdf/defense_and_national_security_strategic_review_2017.pdf*

Binnendjik, H., and Vershbow, A. (2021). *Needed: A transatlantic agreement on European strategic autonomy*. Defense News. Available from: *https://www.defensenews.com/global/europe/2021/10/10/needed-a-transatlantic-agreement-on-european-strategic-autonomy/*

Binnendjik. A et al. (2021). *At the Vanguard. European Contributions to NATO's Future Combat Airpower*. Available from: *https://www.rand.org/pubs/research_reports/RRA311-1.html*

The Emerging Spectrum of Threats to the Military Use of Space and Implications for Capability Planning

7

Patrick Bolder, Lieutenant Colonel (Retired), Royal Netherlands Air Force

Subject Matter Expert, Hague Centre for Strategic Studies

Introduction

Future military operations between peer competitors will be characterized by Multi-Domain Operations (MDO) approach, which will feature the integrated and parallel use of Air, Sea, Land, Cyberspace and Space. Across the spectrum of military operations, from low-tempo peace-keeping missions and security force assistance to high-intensity, high-tempo warfighting operations, the military will make use of all operational domains—but particularly the space domain. Space has become vital to modern military activity as the speed and tempo of operations have increased and led to compressed time-cycles for decision-making at the command and control (C2) and tactical levels.

In addition, military activity is more closely scrutinized today given the accelerating and widening access to open-source information in the public domain among civil society actors. One consequence of this has been to intensify the need for more rapid but also more accurate intelligence to inform decision-making in military campaigns. Information from an expanding set of sources and origins has become the ways and means for decision-making and the space do-

main has figured centrally to this evolution of military planning and operations across the range of missions that militaries are expected to routinely undertake.

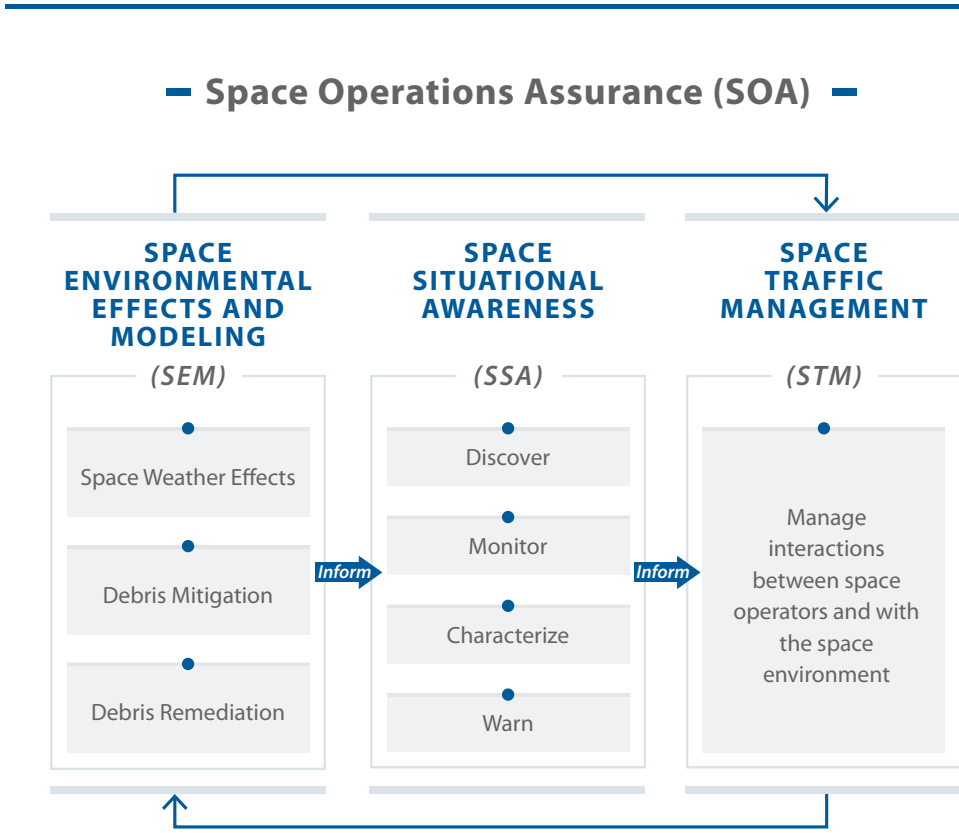
The space domain is the only way to ensure continuous, cross-border intelligence and situational awareness today and facilitate vital communications. This reality necessitates greater attention to be focused on the security of space assets and capability planning for space applications in the future. As it stands, the space domain still does not garner the strategic attention around the world that it already warrants. However, the military's use of space will not only remain on the agenda of defense organizations and military capability planners for years to come but will increase in importance.

The Geopolitics of Earth, Space and the Widening Threat Spectrum

It could be argued that as far back as World War II, the use of space was witnessed in warfighting when Germany lobbed V2 rockets with ballistic trajectories towards Britain. In more recent times, the first military campaign where the space domain played a crucial role occurred during the First Gulf War in 1991. Without the use of satellite-enabled GPS, which provided precision navigation and targeting for kinetic effects and space-based observation of the conflict theatre for situational awareness, the US and its coalition partners may not have achieved the same outcomes of Operation Desert Storm that they did.

Since the end of the First Gulf War, Western militaries have gradually expanded their use and efforts in leveraging the space domain as a way to introduce operational advantages. This growing dependency or addiction on the space domain has however also created—and enlarged—new types of vulnerabilities for military operations which opponents are increasingly capable of exploiting. In this emerging context it is vital that militaries begin to refocus attention on their use of space in terms of planning and developing space capabilities relative to emerging new threats and strategic vulnerabilities.

This is a challenge that needs to be undertaken at a time when few can doubt that great power competition is back on the global stage. As global dynamics have evolved, the United States has been rebalancing its global posture with a pivot to Asia. Falling energy reliance on the Middle East for the United States has also triggered discussion around its long term regional role. For Europe, any future unrest and instability from its eastern and southern borders may lead to unprecedented challenges with refugees and displaced persons. In managing the security impact of such risks, European militaries could well face a new reality where reliance on or the availability of American space assets cannot be taken for granted.



At the same time, Europe's own resolve for strategic autonomy and sovereignty may grow stronger and extend to its future space strategy. Geopolitical factors and lower barriers of entry are likely to continue introducing new players into the frame, pursuing the strategic and tactical use of space, operating satellites and developing ground-based enabling infrastructure. Whilst space cannot be divided into civilian and military spaces, the area of 'military space' will feature the traditional powers of US, Russia and China but also see the addition of new players such as the European Union (EU), India, the UAE and others.

The risks of using and reliance on space for military operations are increasing rapidly as the number of space actors expands. Congestion is a serious threat in space, particularly in Low Earth Orbit (LEO)—the altitude which spans 400-1500 km above the earth—where satellites risk becoming obliterated. LEO is becoming saturated not only by military users but also a growing range of commercial operators producing and launching high numbers of small satellites to serve the rapidly growing commercial space industry.

The risks of growing space congestion are real—since the widely studied collision of Iridium-33 and Kosmos 2251 in February 2009, in March 2021, the collision between Yunhai 1-02 and the fragments (also the result of a knock-off) from Russia's Zenit-2 rocket, which itself was launched in September 1996, reinforced the risks to satellite operations. These recent collisions were most probably accidents but close proximity maneuvers by satellites towards other satellites have been observed recently and such close encounters can be the result of offensive intent designed to render satellites unreliable, untrustworthy or even completely unusable.

> *Securing data and information flows through optical communication, cryptology, frequency hopping or pinpointed radio transmission will need to feature as vital a capability design parameter.*

Recently observed close proximity encounters and operations do not appear to have inflicted any visible damage but these incidents have triggered military ac-

tors in space to rethink their postures and consider mechanisms for enhancing the protection of their assets—including, potentially, through weaponization. In December 2019, NATO explicitly acknowledged space as a military operations domain. Anti-satellite (ASAT) weapons are known to have been experimented with widely and are likely to be developed more readily as a way to introduce the logic of deterrence and denial into the space domain against opponents which may seek to exploit legacy space system vulnerabilities.

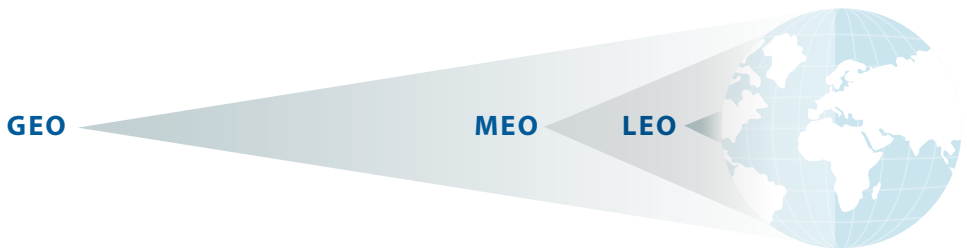
There are major implications for such trajectories because of the unintended consequences and secondary effects such developments would generate at the lowest level, simply through the risk of space debris spreading across significant swathes of space. Opponents in space will also seek to target the critical communications relays between satellites and supporting ground infrastructure or command centers. Technologically less advanced opponents could attack or disrupt ground-based infrastructure supporting space operations such as by simply denying physical access, cutting power cables or even physical attacks and destruction.

The widening spectrum of threats in space are not all-encompassing—for the time being, these mainly relate to space assets in LEO. Here, there are a series of defensive responses from military planners available which focus on the LEO environment—for example, the hardening of supporting and enabling terrestrial infrastructure, earth-to-space (and vice versa) communication channels and also space-based assets themselves. Additionally, military planners will need to generate new ways and means for improved space situational awareness, space traffic management, maneuverability in space, responsiveness and payload adaptability as well as, crucially, international cooperation and efforts towards creating a rules-based order in space.

Terrestrial, Communications and Satellite Hardening

The easiest ways for opponents to target space capabilities supporting military operations is to focus on the terrestrially-based supporting and enabling infrastructure. Fortunately, these elements of space capability are the easiest to defend and, if necessary, repair or replace. Whilst this may initially seem a less sophisticated and low-cost response to reducing vulnerabilities for military space operations, it is vital to not allow this element of future space power and capability planning to escape the strategic design and planning process.

GEO, MEO, and LEO Satellites



	Geostationary Earth Orbit **GEO** *(~36,000 km)*	*Medium Earth Orbit* **MEO** *(~8,000 km)*	*Low Earth Orbit* **LEO** *(~1,000 km)*
• ***Latency***	Higher	Medium	Low
• ***Global Network Coverage***	3 satellites (99%)	6 satellites (96%)	1000s (100%)
• ***Data Gateways***	Few, fixed	Several, flexible	Numerous, local
• ***Technology Readiness***	Proven	Proven	Emerging
• ***Life Cycle***	15 years	12 years	7 years

The widening spectrum of threats in space are not all-encompassing—for the time being, these mainly relate to space assets in LEO.

As cyberspace meets space, a dual vulnerability is introduced, particularly for military communications. The command and control (C2) and information channels between ground and space-based assets are highly sensitive to spoofing, disturbance, jamming and other forms of interference. Securing data and information flows through optical communication, cryptology, frequency hopping or pinpointed radio transmission will need to feature as vital a capability design parameter.

Satellites are also increasingly likely to themselves become the subject of offensive maneuvers and actions to render them less useful or even useless. Military actors in space must begin to consider and address how space-based assets will be protected against physical attacks, exposure to high energy radiation, electromagnetic tampering and a range of emerging new threats from earth. Special coatings and layers, sensors that detect tampering and the enhancement of defensive and appropriate countermeasures will need to be developed and implemented.

Improved Space Situational Awareness (SSA), Space Traffic Management and Maneuverability

SSA underpins an accurate real-time picture of the space domain and makes possible insights into unexpected or unusual occurrences. With SSA, satellite operators can better monitor and control the proximity of their assets to potential threats and collision risks—particularly as it applies to navigating space debris in LEO. The necessary configuration of sensors and data processing technologies will be able to provide early warning against the possible intrusion of satellite safe bubbles as well as make attribution possible. In the emerging scenario, deniability of offensive maneuvers and actions will be out of the question

as accurate attribution is made possible and, logically, a more robust model of deterrence can be enforced.

By making possible a more accurate picture of space and proximity calculations, it will become possible to determine appropriate actions to consider and pursue in more timely ways as well as effectively developing a space traffic management system. Improved SSA will lead to the reduction of a satellite's safe bubble as it is constituted and in turn this will reduce the propensity for evasive maneuvering while offering safer ways to achieve and maintain safe navigation and mobility in space. By also enabling space traffic management, the security of space-based systems will be enhanced, prolonging satellite lifespans and support better planning for replacements, upgrades and new insertions.

Enhancing the maneuverability of satellites is an imperative defensive measure to enhance their protection and survivability. The same benefit of maneuverability as it applies to ground units where mobility will enhance the protection but where a more complex set of challenges will need to be addressed, such as fueling, on station-time and tactics, techniques and procedures (TTPs).

Design, Responsiveness and Payload Adaptability

In the event of losing satellites as a result of offensive actions by an opponent or natural circumstances and even accident, it will be critical to replace any lost capability in the shortest time possible—with a like-for-like or improved system. Indeed, the future of satellites lies with micro or nano-satellites which are less costly to build and launch in comparison to legacy space systems. Where the need for new functionalities and requirements emerge, new space technologies will create new ways to deliver these in more responsive ways. Responsiveness in design, manufacture, testing, procedures and launch will need to be key criterions for space capability planning and will need to be supported by close and continuous cooperation with industry and knowledge partners.

In the design of new satellites and space systems, the development of new applications may need to be spread out in order to build and launch satellites more rapidly and cost effectively. Implementing new and constantly evolving requirements through development programs is unreasonable and militaries must become better at pushing these towards future iterations. Constant change and modifications to space development programs can add huge cost and time delays. Instead, the focus must be on making satellites more modular or adaptable so that their functionality can be modified without great cost or complexity. If high modularity and adaptability is built into the current generation of satellites under development, their usability and lifespans would be enhanced enormously.

> *Geopolitical factors and lower barriers of entry are likely to continue introducing new players into the frame, pursuing the strategic and tactical use of space, operating satellites and developing ground-based enabling infrastructure.*

International Cooperation and a Rules-Based Order in Space

For smaller militaries and particularly those which cooperate under a common security umbrella, burden-sharing through a division of responsibilities and capabilities is strategically compelling. The pooling and shared use of assets and capabilities will be a crucial feature of developing space capabilities that will rest on successful outcomes in international cooperation. International cooperation regarding the use of space will also need to address the wide range of freedom that currently exists for any actor in space in the absence of rules on behavior. Until now it appears that the limited number of nations with advanced space capabilities have been reluctant in creating more concrete frameworks and developing long-term rules between themselves to avoid hampering the future range of strategic possibilities. Yet with increasing congestion in LEO, the emergence of new military actors in space and its evolution as a contested op-

erational domain, space should no longer be accessed and exploited in the absence of a minimum set of rules and acceptable risk.

Conclusion

The widening spectrum of threats—increasingly cross-domain in nature—and the acceleration in military decision-making required given massive increases in data produced or becoming available exacerbates future challenges for warfighters. Hybrid warfare and military competition below the threshold of open conflict will need systems which support the military planners and operators with early warning, superior situational awareness and prompt decision-making. Rapid access to information where integrity is guaranteed will be crucial to strategic success. Across all of these strategic imperatives, the space domain will have a vital role to play.

Access to the space domain comes with enough challenges on its own but in the context of the military use of space, even more must be considered. Nonetheless, dependency on and use of the space domain is inescapable and capability planning for it must apply fundamental considerations for delivering technical solutions which generate new strategic and operational advantages and by forwarding the goal of international cooperation to allow the unobtrusive use of space. Ultimately, though, it should not be lost on militaries to think about how the loss of access to critical space infrastructure will be negotiated. At a time where access to space is taken for granted, the military arts of map and compass reading, field orientation, navigation and operating without communications may need to be preserved for longer yet.

Information Warfare and the Connected Battlefield

8

Dr. Brett van Niekerk

Senior Lecturer, University of KwaZulu-Natal

Introduction

The Fourth Industrial Revolution (4IR) extends the information revolution (Third Industrial Revolution) with increasing degrees of integration amongst cyber, physical and biological systems. The 4IR is predicted to impact on all sectors, including the nature of conflict (Schwab, 2016). Key concepts that form part of 4IR include (but are not limited to):

- Data science and big data analytics, often driven and/or automated by artificial intelligence and machine learning;
- Cloud computing, providing remotely accessible computing resources;
- Internet of Things (IoT), where hyper-connected devices can act as sensors and actuators to produce large amounts of information and cyber-physical interconnections;
- Augmented reality, overlaying information on glasses, map, or image;
- Cyber-security, due to vulnerabilities introduced by connecting insecure 'non-traditional' devices onto networks.

Some of the 4IR concepts have been present in the military setting in some form, such as augmented reality similar to head up displays, and the IoT concept evolves network centric warfare (or as Wassel (2018) calls it, 'data warfare') into what has become known as the 'Internet of Battlefield Things' (IoBT) or the 'Internet of Military Things' (IoMT) (Castiglione, Choo, Nappi, and Ricciardi, 2017). IoT implementations in the military have the potential to support command and control (C2) of Multi-Domain Operations (MDO) in a range of areas (Seffers, 2017). As such, MDO in the future can be considered to include a hyper-connected battlefield which results in an increased attack surface for information warfare (IW) (Cenciotti, 2017; van Niekerk, Pretorius, Ramluckan and Patrick, 2018). This paper will consider IW in the context of both MDO and the IoBT.

Multi-domain Operations and Information Warfare

The traditional 'physical' domains of military operations include land, sea, air, and space; however, there is increasing need to dominate in the electromagnetic spectrum (EMS), cyber, and the broader information environment (Ween, Dortmans, Thakur, and Rowe, 2019). The MDO approach has been described as a "joint warfighting concept that will bring to bear all of the firepower, both kinetic and non-kinetic" to provide superiority across the battlespace in an unprecedented way (South, 2019).

Figure 1 illustrates multiple operational domains: the four 'physical' domains are illustrated in the centre of the figure; these domains usually are mobile and communicate through broadcast mediums at various frequencies (the EMS). Cyberspace becomes an extension of this, providing the data and information transfer mechanisms, such as networking protocols. Whilst the contemporary information domain is considered almost identical to cyberspace, the information environment is broader and includes printed and cognitive information as well. These all support the human element, which encompasses strategic and tactical decision-making processes (for example, command and control) for the warfighters and commanders but extend more widely to society, the economy, and politics.

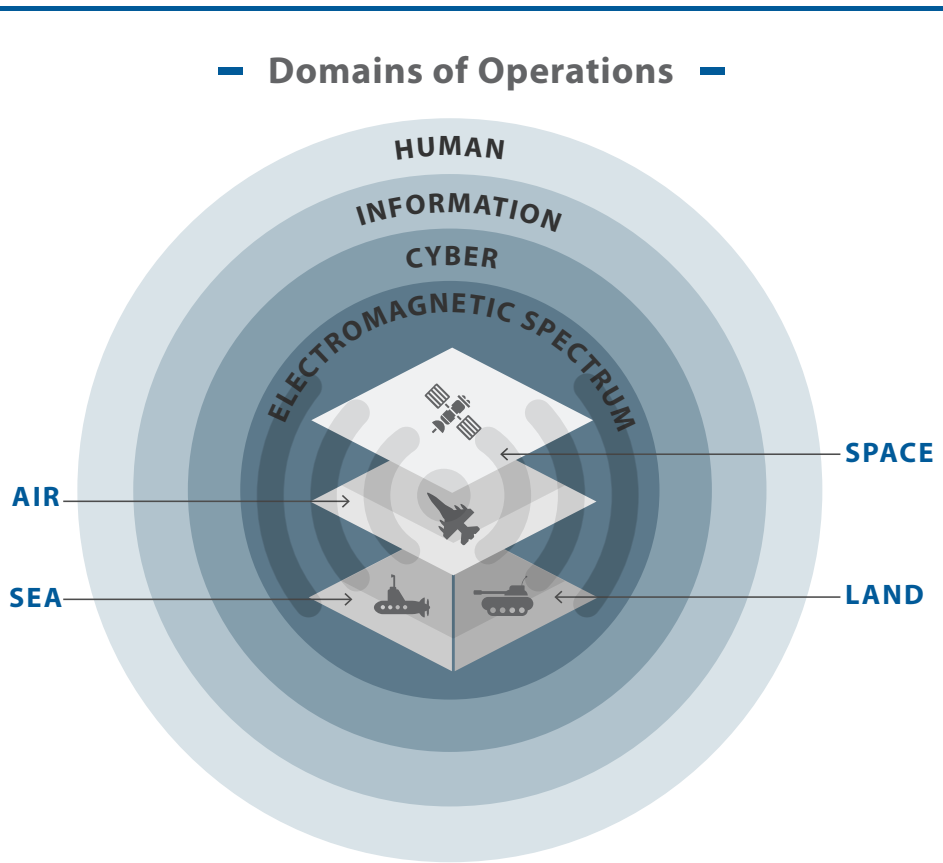


Figure 1: *Domains of Operations*

Information warfare, in its earlier form, comprised operations that could affect and/or protect information across the physical, virtual and cognitive domains (Brazzoli, 2007; Waltz, 1998). These 'pillars' of IW included electronic warfare (EW), cyber-operations, psychological operations (PSYOP), intelligence, network centric warfare or information infrastructure warfare, and command and control warfare (C2W) (Brazzoli, 2007).

Figure 2: *'Pillars' of Information Warfare*

Modern use of the term 'information warfare' tends to refer more to the cognitive aspects, such as disinformation and influence campaigns, often driven by social media and instant messaging (Stengel, 2019). Emerging discussions focus on the 'convergence' of EW and cyber in what is known as cyber electromagnetic activities (CEMA) (UK Ministry of Defence, 2018; US Department of the Army, 2014). However, a greater convergence of IW pillars can be argued particularly given the apparent success of coordinated information and physical operations in Ukraine, despite not providing a 'decisive' victory (Valeriano, Jensen, and Maness, 2008; van Niekerk, 2015).

Offensive IW typically has one of the '"5 Ds": deny, degrade, disrupt, deceive, or destroy' (Sterling, 2019) as a strategic or operational objective; however, others have also proposed objectives such as:

- Disrupt, deny, destroy, manipulate, and steal (Hutchinson and Warren, 2001);
- Degrade, deny, corrupt, and exploit (Borden, 1999; Kopp, 2000);
- Interrupt, modify, fabricate, and intercept (Pfleeger and Pfleeger, 2003).

Ultimately human decision making is targeted at tactical, operational and strategic levels; however, conflict through cyberspace and the information environment is increasingly targeting societal, political and economic decision making as well as military operations or operators. With the growing focus on disinformation and influence campaigns by state and non-state actors, particularly through online 'news' websites and social media, the more objectives of IW at the higher strategic level have been rephrased to the 4 Ds: dismiss, distort, distract, and dismay (White, 2016). Such types of operations target the 'will' of a population or politicians and, combined with the more operationally focused elements of IW in a given battlespace, aim to reduce or remove popular or political support towards a conflict or its military objectives.

IoBT and Information Warfare

Castiglione, Choo, Nappi, and Ricciardi (2017: 16) indicate that the battlefield has seen "an increasing number of ubiquitous sensing and computing devices worn by military personnel and embedded within military equipment". It was reported that NATO was investigating the potential benefits of IoT to the military in areas such as situational awareness, surveillance, logistics, medical applications, base operations and energy management (Seffers, 2017; Stone, 2018; Wassel, 2018). IoBT/IoMT also has a vast potential to support C2 in MDO through "combined operations logistics support; tactical-level situational awareness; targeting; monitoring of vehicle and soldier status; battlefield medical care and even environmental monitoring" (Seffers, 2017).

Ren and Hou (2018) propose a "Combat Cloud-Fog" architecture with three tiers. A 'combat resource' tier includes the military equipment such as platforms and sensors in the traditional four physical domains. Cenciotti (2017) uses the ex-

ample of an F-35 aircraft that has sensors to collect information about its environments and potential threats; it also has internal sensors to monitor its performance and therefore can be seen as both a 'thing' on the Internet, but also as a group of sensors. Valeriano, Jensen, and Maness (2008) consider the F-35 equivalent to a computer server. This indicates the growing complexity of modern military systems, the reliance of digital information, and the amount of data that can be generated (relating to concepts associated with 'big data').

The second tier of Ren and Hou's (2018) architecture includes a 'fog layer', for localised distributed computing and storage. The third layer then comprises of cloud computing, with greater storage and comprising of multiple 'fog network' links. The fog network can be thought of serving the tactical and operational levels of C2, whereas the cloud network serves the operational and strategic levels of C2. Given the scope of MDO, it is wise to extend the sensors of the "Combat Cloud-Fog" architecture to include sensors in the EM domain as part of the combat resource set.

> *The potential for the algorithms to be 'tricked' is of particular concern to those needing to make command decisions based on analysed data being presented to them: can the information about the battlespace be trusted? At a far more tactical level, can a pilot or control station on a warship trust the information being displayed? Any hesitancy or incorrect decision is ultimately the objective of information warfare.*

Monitoring also needs to be provided in the cyber domain throughout the Combat Cloud architecture to aid in cyber-security. There have been recorded incidents of 'connected' military units and/or equipment being affected by cyber-incidents: in 2009 was reported that malware had affected warships and a military airfield (Page, 2009; Willsher, 2009), mobile malware was used to track artillery units (Volz, 2016) and there are now growing concerns over cyber and electromagnetic threats to satellites and space-based systems (Garner, 2020; Rajagopalan, 2019). Compromised IoT devices have been used to launch distribut-

ed denial-of-service (DDoS) cyber-attacks were some of the largest recorded at the time they occurred (Fruhlinger, 2018).

Such incidents and wider concerns related to information systems and security point to the inherent risk of highly interconnected systems. Van Niekerk, Pretorius, Ramluckan, and Patrick (2018) illustrate how information warfare can be used to target IoT and humans through vulnerable IoT. Numerous such theoretical attacks can be applied to military scenarios, such as:

- Wiper malware or ransomware that destroys data and system software can create catastrophic effects for aircrafts or submerged submarines, for example;
- Injecting PSYOP messages to heads-up-displays of pilots can distract and dismay the pilot by suggesting the aircraft systems are compromised and adversely impact time-critical decision-making;
- Cyber-attacks manipulating sensor arrays (for example, sonar array or air defence radar) randomly to provide false targets and hide actual targets, thereby distorting the view of the battlespace;
- Using malware and social media on the phones of military personnel to determine deployments and thereby generate intelligence relating to operations.

Table 1 illustrates possible 'generic' IW threats relevant to the cloud-fog IoBT architecture.

Table 1: *IW threats to the IoBT*

Cloud-Fog Architecture	Domain	IW threats
Tier 3: cloud	Physical	Destruction of cloud network infrastructure
	Cyber	DDoS to overload the cloud network
		Network intrusion to steal information
		Network intrusion to manipulate information
		Network intrusion to destroy information

Cloud-Fog Architecture	Domain	IW threats
Tier 2: fog network	Physical	Destruction of fog network infrastructure
	Electromagnetic	Jamming of wireless receivers to the fog network
	Cyber	DDoS to overload the fog network
		Network intrusion to steal information
		Network intrusion to manipulate information
		Network intrusion to destroy information
Tier 1: combat resource	Physical	Destruction of sensors / equipment
	Electromagnetic	Jamming of wireless links amongst devices
		Directed energy to destroy electronic devices
	Cyber	Malware on devices to track units
		Malware to degrade equipment performance
		System intrusion to manipulate sensor information
	Cognitive	PSYOP messages transmitted to devices

In general, the IoBT may result in a congested EM spectrum and network due to the increasing number of EM signals and the quantity of data being transferred. This in turn may increase the susceptibility to EW and DDoS attacks as each signal could present itself as 'noise' to each other, and jamming will increase this 'noise' level to degrade or disrupt the effectiveness of the communication links. In a similar manner, the closer to the 'threshold' of a network the data quantity is, the more susceptible it will be to being flooded and overwhelmed by malicious traffic.

> *The fog network can be thought of serving the tactical and operational levels of C2, whereas the cloud network serves the operational and strategic levels of C2. Given the scope of MDO, it is wise to extend the sensors of the "Combat Cloud-Fog" architecture to include sensors in the EM domain as part of the combat resource set.*

IoBT will possibly contribute to the 'convergence' of cyber, EW, and PSYOP at the tactical level; van Niekerk, Pretorius, Ramluckan and Patrick (2018) discuss some

aspects of this convergence in a general context. Above the possibility of cyber being used to inject a PSYOP message to target pilots is mentioned; similarly EW could be used to 'overpower' radio communications to transmit PSYOP messages to personnel. This convergence can be thought of as a layered model of IW: EW targets the physical layer of the network, cyber targets the higher layers and protocols, and a payload option for the cyber component is the distribution of PSYOP messages.

Another aspect to consider are the algorithms that are implemented for data analysis and for the functioning of military equipment. Due to the quantity of data produced by modern equipment, it is impossible for humans to analyze all of it and a degree of automation is needed, usually implemented with Artificial Intelligence (AI). However, there have been instances illustrating that modified inputs have resulted in AI providing an incorrect classification (Field, 2017; Lemos, 2021). Often new technologies are implemented without taking security into account, and it is no different with AI. In the academic space, there is a sharp increase in the amount of research investigating attacks on AI systems including adversarial attacks to induce incorrect outputs, as well as data poisoning (also known as model poisoning) which corrupts the training data to produce a flawed model (Constantin, 2021; Lemos, 2021). The potential for the algorithms to be 'tricked' is of particular concern to those needing to make command decisions based on analysed data being presented to them: can the information about the battlespace be trusted? At a far more tactical level, can a pilot or control station on a warship trust the information being displayed? Any hesitancy or incorrect decision is ultimately the objective of information warfare.

Conclusion

Multi-domain operations encompass all physical environments and can extend into the electromagnetic and cyber domains as well. The Internet of Battlefield Things provides a mechanism to achieve multi-domain operations through embedded sensors providing a common picture of the operating environment(s). However, IoT in general has been seen to be vulnerable to compromise, and

a hyper-connected battlespace could increase the attack surface for information warfare across the physical, electromagnetic, cyber and cognitive domains. Attacks could target the physical infrastructure, the signals, network protocols, algorithms, data, and the human psychology.

References:

Borden, A. (1999). What is Information Warfare? *Air & Space Power Journal*, November 2. Available from: *http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html [*2 July 2009].

Brazzoli, M. S. (2007). Future Prospects of Information Warfare and Particularly Psychological Operations. In L. le Roux, *South African Army Vision 2020* (pp. 217-232). Pretoria: Institute for Security Studies.

Cenciotti, D. (2017). Cybersecurity In The Sky: Internet of Things Capabilities Making Aircraft More Exposed To Cyber Threats Than Ever Before, The Aviationist, 20 June. Available from *https://theaviationist.com/2017/06/20/cybersecurity-in-the-sky-internet-of-things-capabilities-to-make-aircraft-more-exposed-to-cyber-threats-than-ever-before/ [*26 September 2021].

Constantin, L. (2021). How data poisoning attacks corrupt machine learning models, *CSO Online*, 12 April. Available from *https://www.csoonline.com/article/3613932/how-data-poisoning-attacks-corrupt-machine-learning-models.html* [5 October 2021].

Field, M. (2017). Graffiti on stop signs could trick driverless cars into driving dangerously, *The Telegraph*, 7 August. Available from *https://www.telegraph.co.uk/technology/2017/08/07/graffiti-road-signs-could-trick-driverless-cars-driving-dangerously/* [5 October 2021].

Fruhlinger, J. (2018). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet, CSO Online, 9 March. Available from *https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html* [29 September 2021].

Garner, T. (2020). Why Satellite Cybersecurity Must Be Prioritized in the New Frontier, *NextGov*, 1 May. Available from *https://www.nextgov.com/ideas/2020/05/*

why-satellite-cybersecurity-must-be-prioritized-new-frontier/164977/ [10 September 2021].

Hutchinson, W., and Warren, M. (2001). *Information Warfare: Corporate Attack and Defense in a Digital World*. Oxford & Auckland: Butterworth Heinemann.

Kopp, C. (2000). A Fundamental Paradigm of Infowar, *Systems: Enterprise Computing Monthly*, Sydney:Auscom Publishing, 46-55.

Lemos, R. (2021). Expect an Increase in Attacks on AI Systems, *Dark Reading*, 27 April. Available from *https://www.darkreading.com/vulnerabilities---threats/advanced-threats/expect-an-increase-in-attacks-on-ai-systems/d/d-id/1340833* [5 October 2021].

Page, L. (2009). MoD networks still malware-plagued after two weeks, *The Register*, 20 January. Available from *https://www.theregister.com/2009/01/20/mod_malware_still_going_strong/* [10 September 2021].

Pfleeger, P., and Pfleeger, S. (2003). *Security in Computing*, 3rd Edition. Upper Saddle River, New Jersey: Prentice Hall.

Rajagopalan, R.P. (2019). Electronic and Cyber Warfare in Outer Space, The United Nations Institute for Disarmament Research. Available from *https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf* [10 September 2021].

Schwab, K. (2016). The Fourth Industrial Revolution: what it means, how to respond, World Economic Forum, 14 January. Available from *https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/* [25 September 2021].

Seffers, G. I. (2017). NATO Studying Military IoT Applications, *Signal*, 1 March. Available from *https://www.afcea.org/content/Article-nato-studying-military-iot-applications* [25 September 2021].

South, T. (2019). This 3-star Army general explains what multi-domain operations mean for you, Army Time, 11 August. Available from *https://www.armytimes.com/news/your-army/2019/08/11/this-3-star-army-general-explains-what-multi-domain-operations-mean-for-you/* [25 September 2021].

Stengel, R. (2019). *Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do about It*. London: Atlantic Books.

Sterling, B. (2019). Deny, degrade, disrupt, deceive, or destroy, Wired, 4 May. Available from *https://www.wired.com/beyond-the-beyond/2019/04/deny-degrade-disrupt-deceive-destroy/* [24 September 2021].

Stone, A. (2018). The answer to battlefield logistics problems could be IoT, C4ISRnet, 12 October. Available from *https://www.c4isrnet.com/it-networks/2018/10/12/the-answer-to-battlefield-logistics-problems-could-be-iot/* [25 September 2021].

UK Ministry of Defence. (2018). Cyber and Electromagnetic Activities, Joint Doctrine Note 1/18. Available from *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf* [24 September 2021].

US Department of the Army. (2014). Cyber Electromagnetic Activities, FM3-38. Available from *https://irp.fas.org/doddir/army/fm3-38.pdf* [24 September 2021].

Valeriano, B., Jensen, B., and Maness, R. C., (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.

van Niekerk, B. (2015). "Information Warfare in the 2013-2014 Ukraine Crisis", in: Richet, J. (ed.), Cybersecurity Policies and Strategies for Cyberwarfare Prevention. Hershey, PA: IGI Global, pp. 307-339.

van Niekerk, B., Pretorius, B., Ramluckan, T., and Patrick, H. (2018). "The Impact of IoT on Information Warfare", in: Fields, Z. (ed.), *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, Hershey, PA:IGI, pp. 141-164.

Volz, D. (2016). Russian hackers tracked Ukrainian artillery units using Android implant: report, Reuters, 22 December. Available from *https://www.reuters.com/article/us-cyber-ukraine-idUSKBN14B0CU* [29 September 2021].

Waltz, E. (1998). *Information Warfare: Principles and Operations*. Boston & London: Artech House.

Wassel, P. (2018). 3 Military Applications of The Internet of Things, Augmate, 27 April. Available from *https://www.augmate.io/3-military-applications-of-the-internet-of-things/* [25 September 2021].

Ween, A., Dortmans, P., Thakur, N., and Rowe, C. (2019). Framing cyber warfare: an analyst's perspective, *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 16(3), 335–345.

White, J. (2016). Dismiss, Distort, Distract, and Dismay: Continuity and Change in Russian Disinformation, Policy Brief 2017/13, Institute for European Studies. Available from *https://www.ies.be/node/3689* [25 September 2021].

Willsher, K. (2009). French fighter planes grounded by computer virus, *The Telegraph*, 7 February. Available from *http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computervirus.html* [26 September 2021].

The Competition Continuum for Information Dominance: The Evolution and Future of Information Warfare for the Joint Force

9

Dr. Edwin "Leigh" Armistead

Chief Editor, Journal of Information Warfare

IW and the Joint Force

It is universally understood today that information is power and while this well-known axiom may seem trite, the Joint Force has experienced rapidly changing circumstances in the information warfare (IW) environment in recent years. Military assets are vested with the Joint Force or its component services increasingly with force-wide or inter-services connectivity enabled by emerging tools in the cyberspace domain and with the notion of combat clouds. The objective of achieving dominance in the information environment, which is accessible to virtually anyone, poses new and complex challenges in an emerging reality of hyperconnectivity that spans the physical and virtual worlds. The dichotomy of the Joint Force not having sole responsibility or authority to IW, both offensive and defensive, is especially acute in the emerging operational context where an increasing expanse of actors and players is more and more apparent. Future approaches to IW in joint and distributed cross-domain operations will therefore need be fundamentally altered and realigned to reflect these fundamental shifts in the nature and scope of the Joint Force's operational spaces.

The ability of Joint Force to adapt systems, networks and operational approaches to compete effectively in the future competition continuum warrants a re-conceptualization of what is inferred by taxonomies such as the 'information environment' and 'IW' itself. Even today, we should ask ourselves, what is IW, how is it different than the Joint Force's traditional military operations and activities, and how will it affect constructs for all-domain command and control? Where is IW positioned in the broader efforts for building an agile and resilient fighting force for the future, to include the cyberspace domain? These are vexing questions which must consider how vital elements of 'power' have changed as a result of the information revolution. Rethinking grand strategy in today's world is key to understanding the ways in which the Joint Force must adapt its future approach with regards to doctrine, planning and operations. Increasingly, IW has been tested and employed in new and novel ways and there is a growing frequency and sophistication in the use of IW by the Joint Force that will only accelerate.

Information is power that is dispersed

There is tremendous power inherent in information and while 'traditional' military approaches emphasize and search for 'new' options for IW effects, these may not reflect the best solutions for the Joint Force or deliver the necessary advantages necessary for achieving the information dominance it desire in an emerging operational environment where a fusion of cyberspace into the planning and operations cycle is well underway. The scope, nature and characteristics of IW has grown, however IW remains a nebulous and ill-defined concept in terms of tactics, techniques and procedures (TTPs) as well as at the level of grand strategy itself. The information revolution has led to the formation of new organisations and actors as well as a growing significance for commercial and even non-state actors into the operational domain of the Joint Force 'virtually'. As a consequence, there is a growing need to bring together this growing and disparate set of stakeholders and actors which are active across the information environment and cyberspace spectrum and which ultimately influence and affect how successfully the Joint Force will be able to conduct its missions.

The goal to become more dynamic and responsive will require that the Joint Force generates a more 'true' strategic and operational picture of IW threats and risks across the information environment it interacts with and influences—or is influenced by. The movement of the security paradigm away from a military-dominated landscape to a new one where that is more dispersed and spans a greater depth and breadth of stakeholders and partners illustrates the disjointedness of IW at the strategic but also operational level of warfare. To truly understand changes now underway within the strategic and operational environment it is critical to understand the tremendous shifts that have occurred in national in power structures over recent years. The irony is that rarely is there a formal government department or agency or operational unit focused solely on information power and which is tasked with the control and distribution of such. The reality is that information power is diluted across a wide array of agencies and organizations.

> ***As the Joint Force transforms towards integrated cross-domain operational capabilities, which are intrinsically enabled by the information domain, a domain which is by its nature one that is opaque and blurs the physical and virtual worlds, there is a growing need to recognize IW at the same level as air or land warfare.***

Attempts to now claim or set boundaries around what are elements of information power will be futile, for the Joint Force and, similarly, for others. There are convincing reasons for this, namely dealing with taxonomy and organizational relationships as well as the inability to set clear boundaries and funding for IW missions. Taskings against a growing set of government and military agencies will only impede the development of a coherent, integrated national strategy for information dominance within which the military at large and the Joint Force in particular are one among multiple components. Where once the operational C2 of the Joint Force or its components was solely under 'their' respective commands which had their 'own' communications systems, this is not necessarily the case anymore. Ask, for example, who controls information power and information resources at the strategic level? If it is not the Joint Force, how can the Joint Force be the key C2 authority for IW?

Refocusing IW for the Joint Force

If it was a mission of the air, land and sea forces to counter actions by hostile forces, how would they approach such missions today given the expanded nature and scope for IW that impacts 'their' operations? Combat networks are designed to be dependable, resilient and rigorous, and in some situations, they are the only means of communicating, but there are many more aspects of IW that adversarial forces can target efforts toward in a multi-domain context in order to disrupt, degrade or delay operations today—such as logistics and supply chain, for example. As the Joint Force transforms towards integrated cross-domain operational capabilities, which are intrinsically enabled by the information domain, a domain which is by its nature one that is opaque and blurs the physical and virtual worlds, there is a growing need to recognize IW at the same level as air or land warfare.

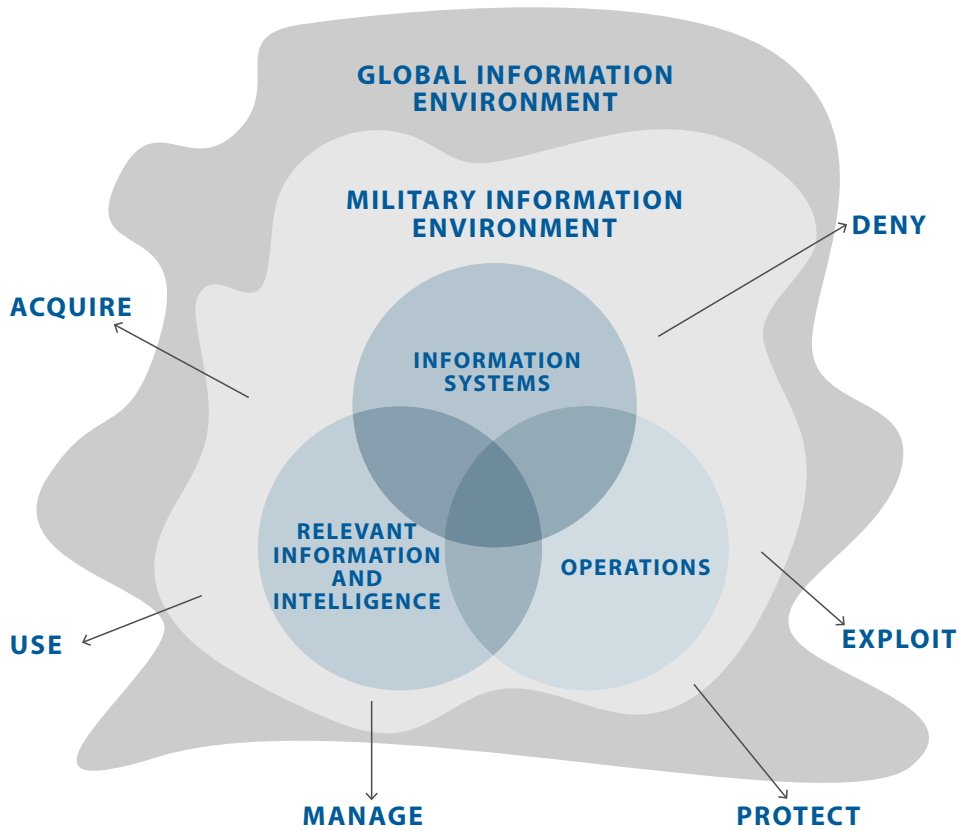
This is especially true as most Joint Force operations are anticipated take place in highly contested and distributed environments where IW will be an inherent feature of the competition space. Yet, with constraining budgets, threats on the rise, and more actors present in these same very spaces, Joint Force commanders find themselves at a critical decision point. The Joint Force will need to generate new ways, means and ends for processing vast amounts of information rapidly and to do so together with a wider set of partners, customers and consumers of these same information resources and databases. As part of IW, information management, connectivity and flows will become core mission elements and the Joint Force will need to transform towards a more integrated and interdependent reality to incorporate new operationally critical elements and layers of the information domain into their planning and operations cycle.

> *The scope, nature and characteristics of IW has grown, however IW remains a nebulous and ill-defined concept in terms of tactics, techniques and procedures (TTPs) as well as at the level of grand strategy itself.*

External interplay and linkage in the search for information dominance

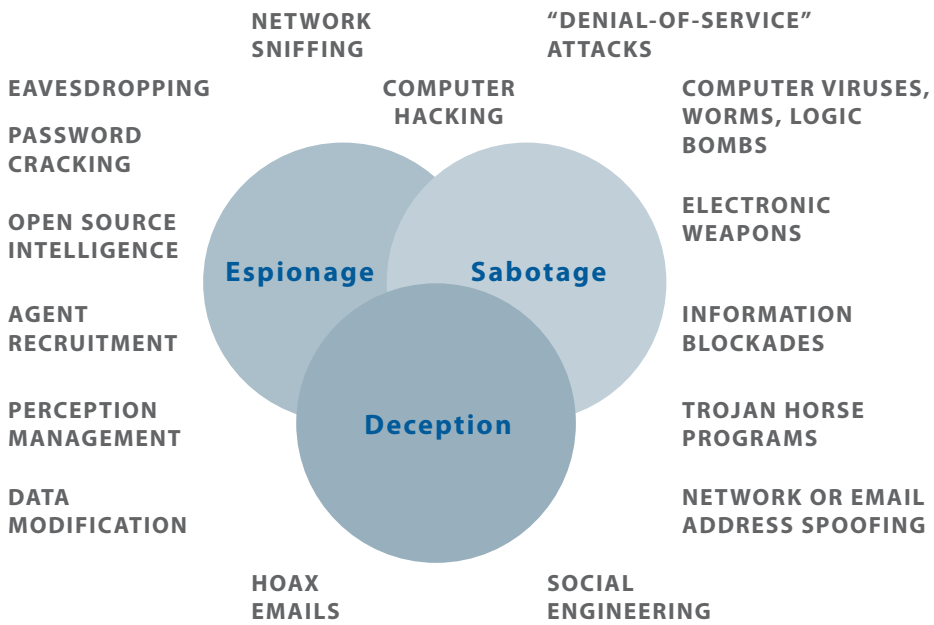
It will be vital for the Joint Force to address the question of whether its focus ought to be more on offensive or defensive IW. Many would agree that the Joint Force should develop and maintain a balance of offensive and defensive IW capabilities however there are more limitations to the former. Ultimately, the Joint Force will need to address these questions by developing clarity on the scope of its future IW goals, capabilities and objectives, considering long-term strategic requirements but understanding what it is that is absolutely essential tactically for it to execute operational missions effectively in the short-term.

The Strategic Environment for IW



IW campaigns will increasingly use or rely on or interact in important ways with commercial networks. Such networks and tools will hinder the Joint Force in utilizing traditional electronic warfare tools and cyber warfare operations. Operational planners will need to contend with an entirely new spectrum of players, networks, systems and other factors in respect to IW. Instead of planning missions in a vacuum, the Joint Force will increasingly need to understand, be aware of and coordinate operationally with more agencies and commercial actors than ever before. This will be a highly complex challenge to develop the necessary frameworks for cooperation to allow the effective coordination and flow of information to and from the Joint Force with, for example, intelligence agencies, third party logistics suppliers, various force elements of coalition partners, and so on.

IW at the Operational Level



There are many ways to think of the factors which will influence the future direction of IW. To begin, is there a truly operational element of IW? If so, who owns it, what is there span of control and influence? Any Joint Force IW strategy should not just be a subset of a nation's power instruments but be totally integrated with it, crossing all domains including land, sea, air and space. As the Joint Force learns to synchronize effects more seamlessly, dominance of the information environment will become crucial to its overall success. IW will need to become embedded in all activities from the onset of planning—not 'added on' at the end or planned in isolation. The Joint Force will need to look at what effects it intends to generate and then pick the appropriate weapon or action for this. Truly full spectrum targeting across domains should theoretically provide a choice of kinetic or even purely informational effects to be used as alternatives.

How this affects C2 in joint warfare environments and the goal of connecting the fighting force in a way that is cognizant of the evolving reality, scope and demands of IW and the capabilities needed for it is crucial. The hard question to ask is: What exactly can we not control with respect to IW? Here we need to consider the growing role and significance of cyber operations by foreign and domestic groups and the reality of IW actually being a transformational concept rather than a fixed one. IW cannot be stove-piped and will need to be distributed across all elements of the security and intelligence architecture with which the Joint Force interacts and operates together with. The need for such an approach is demonstrated by new taxonomies once again: Instead of calling activities as IW, for example, why not instead label them just as operations? The use of information as an element of power or a weapon is not new and although it is a relatively new tool in the Joint Force commander's arsenal this is a weapon that will need to be used just like any other tool if the battlefield has been properly prepared.

Conclusion

The information age promises hyper connectivity not just between sensors and shooters, manned and unmanned vehicles but much more vastly, to include

logistics, intelligence and civilian populations themselves, so moving forwards, what should the Joint Force expect to encounter in respect to capability planning for and in IW environments? The Joint Force's objective to achieve information dominance in multi- or all-domain operations will require the utilization of complex new approaches and tools in IW as part of a wider ecosystem of information resources and information power. IW conducted by the Joint Force will need to be coordinated more closely with partners in, for example, mounting deception and cyber operations and indeed even with fake news and propaganda campaigns.

Threats like ransomware will extend to supply chain partners at one end to ideologically-motivated non-state actors at another. This bifurcation of the information environment into ever smaller and smaller sub-groups creates massive challenges in attempting to develop IW in a total vacuum, for the Joint Force and in practice for other instruments of power a nation has. It has been shown, and it will continue to be emphasized over the next few years, that IW is a vital to the Joint Force's operational and C2 effectiveness, particularly in a combat cloud-enabled environment. The deployment and employment of military power in the future will require the Joint Force's planners and operators to be more situationally aware, more collaborative and more dependent on partners in the information environment if they are to go beyond traditional 'in house' approaches and generate the optimum solutions for IW effects.

Mosaic Warfare: The March towards Interconnectivity in US, UK, and European Airpower

10

Anika Torruella

Senior Analyst, Janes

Information and data-sharing networks have changed the landscape of defence operations. Great-power actors have been investing in technology that enables high-speed connectivity between a growing number of warfighters, networks, and autonomous or manned machines that can interact in a highly complex and increasingly unpredictable battle environment. At the same time there is an emerging drive to link a growing number of sensors, mobile land platforms, aircraft, mission systems, unmanned systems, man-portable devices, human-wearable devices, weapons, munitions, software, and other technology to become a single information network. The overall objective is to create a dynamic and adaptive matrix that enables real-time, actionable, and predictive analytics for decision making, command and control (C2), and other in-theatre capabilities.

The end goal is to shift warfighting from linear decision making to a web of actionable outcomes to deny, deter, and defeat adversaries. The US Defense Advanced Research Projects Agency (DARPA) calls this a shift to 'mosaic warfare' as traditional asymmetric technologies, such as bespoke satellites, stealth aircraft, and precision munitions, offer reduced strategic value in modern warfare due to growing global access to commercially available advanced technology and

components. This mosaic warfare concept is intended to move beyond individual system designs and unique interoperability standards to develop processes and tools dependent on trusted connections between known entities that offer limitless possibilities for creating effects at the tactical, operational, and strategic decision-making levels.

Intelligent interaction

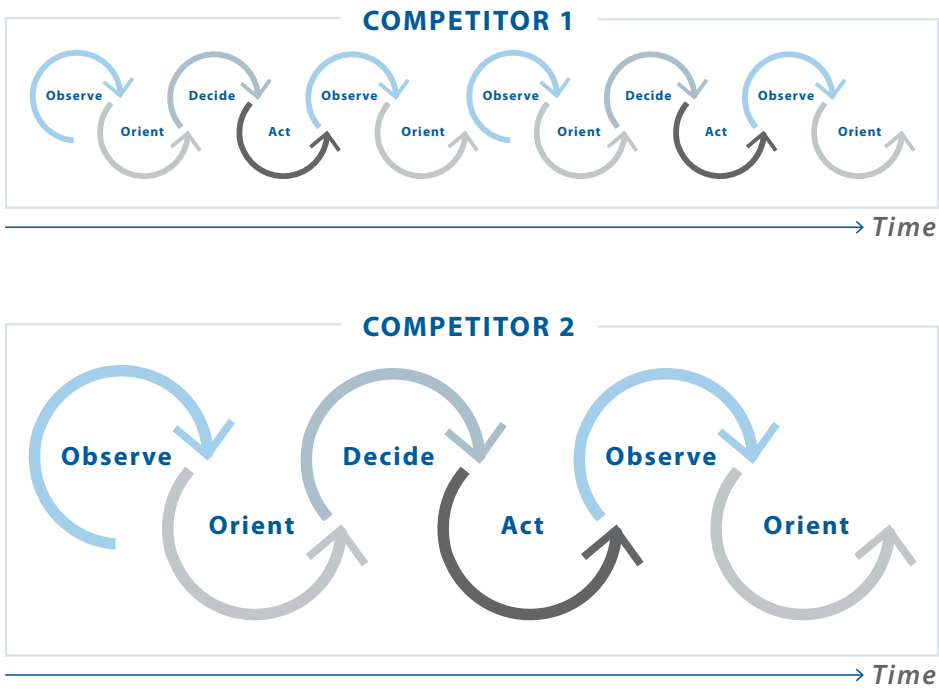
The Internet of Things (IoT) has been used to describe communication and information sharing between large numbers of 'smart' technology nodes. These can then be categorised into data-carrying devices, which are attached indirectly to physical things with communication networks; data-capturing devices, which are reader-/writer-type devices that are capable of interacting with physical things indirectly via data-carrying devices or directly via data carriers attached to physical things; sensing and actuating devices, which detect or measure information in the surrounding environment and convert it into digital signals; and general devices, which have embedded processing and communication capabilities and may include equipment and appliances for different IoT applications (International Telecommunication Union 2012).

IoT can describe city networks, industrial grids, cloud computing, and mobile networks, while its applications have boosted data and information gathering and services when introduced to biomedical, security, and commercial and industrial infrastructure systems. However, due to the relationship between the industrial-commercial complex and defence and military services, applications of IoT technology to modern warfare strategies have come under greater scrutiny. The Internet of Military Things (IoMT), or Internet of Battlefield Things (IoBT), describes technology that enables intelligent interaction among warfighters and their equipment within battlespaces.

Other defence usage of IoMT describes sets of interdependent and networked elements that not only include sensors and devices, but also infrastructure such as storage and data processing equipment, the network used to interconnect

devices and nodes, and the software and machine-learning algorithms that govern them. This incorporates a wide range of military integrated sensors, devices, and platforms capable of intelligent sensing, machine learning, and actuation via cyberspace nodes and human-machine interfaces. These interactions are intended to increase situational awareness and reduce time for processing data, risk assessment, strategic planning, actioning information, and executing objectives. Under a broad definition 'things' could include tanks, warships, aircraft, unmanned aeriel vehicles (UAVs), forward operating bases (FOBs), logistic equipment, transportation and building infrastructure systems, warfighters themselves, or anything that can be integrated with sensing, processing, and transmission capabilities (Russell and Abdelzaher 2018).

Accelerating the OODA Loop for Operational Advantage



In this way IoMT represents the convergence of warfighting domains: their networks, embedded hardware, electromagnetic emissions, communication nodes, mobile processing hardware, software architectures, information management, and data analytics. Just as digital twins mitigate the threat of equipment malfunction, failure, and cyber-based intrusion through simultaneous modelling and continuous prediction of maintenance and performance capabilities, the data collected from the pervasive sensing and communication promised by IoMT can be used for dynamic system optimisation, fault detection, and monitoring and prediction. In addition, IoMT provides the pervasive analysis, management, and C2 needed for a new type of information warfare: one that is decision centric by relying on faster and better decision making, as well as shorter actionable response times.

> *Fault tolerance is low and failures in communication nodes are catastrophic. Back-ups, digital twins, and alternative communication pathways must be established and secured.*

Unmanned and uncrewed (optionally piloted) aircraft have entered the landscape and proven to be a force multiplier, especially for data gathering and air strikes in long-range, difficult to reach, and/or anti-access/area-denial (A2/AD) regions. They have become the workhorses for in-theatre intelligence, reconnaissance, and surveillance (ISR) and are already performing a wide range of military mission roles. A number of countries are developing future-combat air systems (FCAS) programmes that envision high-performance, network-enabled, unmanned aircraft that fly in concert with manned combat aircraft—either in swarms or as a 'loyal wingman'—to close this gap.

Loyal wingman concepts operate as an extension of the sensors and other systems of manned aircraft, with capabilities to disrupt, damage, or destroy target air-defences while surviving in contested A2/AD environments. These teamings seek to create overmatch by shifting traditional manned combat aircraft formations to new mixes of manned and unmanned platforms that create more agile, stealthy, and lethal weapons delivery. If the awareness-to-decision-to-response chain of modern warfare is to accelerate to cyber speed, machine-human team-

ing with AI-boosted analysis and edge computing in-theatre is required. The interconnected technology of mosaic warfare will leverage unmanned systems with machine intelligence self-aware enough to assess the status, goals, and vulnerabilities of missions to counteract disruptions in real time.

JADC2 and Advanced Battle Management System in the United States

The USAF the Advanced Battle Management System (ABMS) is part of a wider plan by the US military to create a Joint All-Domain Command and Control (JADC2) concept, which is looking to build an IoMT by connecting sensors from all across all US services into a single collaborative network. Previous efforts saw each service develop its own tactical network, although these were incompatible with each other. According to the US Congressional Research Service, with interoperability based on a common multi-domain IoMT the US DoD seeks to transform "the current multi-day process to analyse the operating environment and issue commands" into a process that takes "hours, minutes, or potentially seconds" for future conflicts and operating environments. The US DoD has also stated that the existing C2 architecture is insufficient to meet the demands of the US National Defense Strategy (NDS).

The US Air Force's (USAF's) IoMT programme, the ABMS, was originally envisioned to replace the USAF's E-3 Sentry Airborne Warning and Control System (AWACS) platforms. However, it took on a broader scope when former assistant secretary of the Air Force for Acquisition Will Roper stated that the contested environment envisioned by the 2018 US National Defense Strategy had forced the air force to restructure ABMS. Roper directed that ABMS become less focused on command centres and aircraft while refocusing on creating digital technologies, such as secure cloud environments, to share data across multiple weapon systems.

The ABMS IoMT is now intended to encompass a family of systems that includes hardware and software designed to improve anti-access/area denial (A2/AD) management and enable USAF elements to co-ordinate with and conduct joint

operations with the US Navy (USN), US Marine Corps (USMC), and US Army. According to the US Congressional Research Service, the USAF has performed five events to demonstrate the new C2 capabilities it intends ABMS to field. In December 2019 the air force showed the capability to transmit data from a US Army radar (an air-defence sensor and firing unit) and a USN destroyer (the Arleigh Burke-class guided missile destroyer USS Thomas Hudner , deployed in the Gulf of Mexico) to Lockheed Martin F-22 Raptor and F-35A and F-35C Lightning II Joint Strike Fighter combat aircraft, in addition to the US Space Force Unified Data Library (UDL), which is a cloud environment combining space- and ground-based sensors to track satellites.

In September 2020 ABMS detected and defeated a simulated US-bound cruise missile using hypervelocity weapons. ABMS also exhibited capabilities to "detect and defeat efforts to disrupt US operations in space". In the same month the USAF used a KC-46 tanker aircraft to perform tactical C2 by relaying data from fourth-generation fighters to fifth-generation aircraft, such as the F-22 Raptor, during Exercise 'Valiant Shield' at Joint Base Pearl Harbor-Hickam in Hawaii. In February an abbreviated demonstration was held in Europe that linked allied nations, including the Netherlands, Poland, and the United Kingdom, into combined air operations. According to General Jeffery Harrigan, commander of USAF Europe, the event tested US and allied capabilities to perform long-range strike missions with F-15E aircraft launching AGM-158 Joint Air-to-Surface Standoff Missiles (JASSMs) while using US and allied F-35s for airbase defence missions. In May the USAF stated that procuring a communications pod for the KC-46 would be the first capability release for the ABMS programme.

IoMT in the UK and Europe

Concepts for a programme similar to ABMS were published in April by the UK Ministry of Defence's (MoD's) Digital Strategy for Defence effort. This is intended to create a secure, singular, and modern 'digital backbone' connecting "sensors, effectors, and deciders across military and business domains and with partners, driving integration and interoperability across domains and platforms" by 2025.

"We have too often traded out technology refresh and have not driven sufficient integration and commonality," the MoD warned. "Continuing down this path will prevent us from exploiting emerging technologies at the pace and scale required to deliver the Defence Purpose."

The UK Digital Strategy went on to highlight that access to, and control of, the electromagnetic spectrum (EMS) is essential to all operations and the functioning of the digital backbone, adding that with the advent of 5G and IoT the cyber domain would grow "far faster and wider in the next few years. As such, data and architectural standards, as well as management of the EMS, will secure operational advantage and freedom of manoeuvre."

The UK's loyal wingman platform, Mosquito, for the Tempest optionally piloted future fighter jet is under a programme known as the Lightweight Affordable Novel Combat Aircraft (LANCA). Mosquitos will be compatible with UK aircraft carriers and will be able to perform a range of roles, such as weapons carriers and/or decoys or serve as weapons themselves. The UK FCAS programme also includes Alvina swarming drones and other legacy platforms networked together by a combat cloud, with uncrewed aircraft expected to replace UK Typhoon aircraft air-to-air combat capability by the mid-2030s.

European IoMT initiatives include the Wireless Sensor Networks for Urban Local Areas Surveillance (WINLAS) and Cloud Intelligence for Decision Making Support and Analysis (CLAUDIA) projects, which fall within the scope of the European Defence Agency (EDA). The WINLAS programme researches large sensor networks of heterogeneous devices for urban warfare, energy systems, and information management in large-scale soldier modernisation systems. The research from this project builds partly on the results of the EDA's Information Interoperability and Intelligence Interoperability by Statistics, Agents, Reasoning, and Semantics (IN4STARS) programme, which is intended to improve situational awareness in urban areas by using AI, sensors, and energy harvesting to prolong network operation.

The main objective of CLAUDIA is to develop modular software analysis platforms to support the analysis and assessment of military scenarios, especially those exercised during hybrid warfare. CLAUDIA is intended to support the needs of commanders in terms of analysis, decision making, and planning. Its platforms will collect, process, and analyse data from heterogeneous information sources to provide situational awareness and a comprehensive common operational picture (COP) to support planning, decision-making processes, and co-ordination of EU member states.

On the other hand, France, Germany, and Spain have agreed to jointly develop the Next-Generation Weapon System (NGWS) element of their Système de Combat Aérien Futur (SCAF) FCAS programme, called Remote Carriers. First flight demonstrations of the European SCAF/FCAS programme are intended to occur in 2027 and the final proposed design is slated to be frozen in 2030 ahead of a proposed in-service date of between 2040 and 2045. The programme will include the Eurodrone (also called the EuroMALE—European Medium-Altitude Long-Endurance [MALE] Remotely Piloted Aircraft System [RPAS]), an ultra-low observable unmanned combat aerial vehicle (UCAV), future cruise missiles, and legacy platforms operating in the future battlespace.

Operational vulnerability

Implementing IoMT is not without substantial challenges. Complexity arises from the increasing scale, functionalities, and interdependence of the networked elements, as well as from the speed and volume of data collection and production of new information. The new speed of war—driven by automated battle networks and increased computing power—is cyber speed, where network attacks and electronic warfare dominate the information landscape. In addition, despite the capabilities that IoMT offers to defence applications, operational vulnerability is the most critical concern.

Another challenge presented by interconnecting different types of weapons and warfighters is that battlefield scenarios require real-time decisions and re-

sponses. Fault tolerance is low and failures in communication nodes are catastrophic. Back-ups, digital twins, and alternative communication pathways must be established and secured. In addition to 'things' and IoMTs that forces own and control, they may also need to use military, commercial, industrial, or adversary IoTs that they do not own or fully control. Authentication would need to accommodate deceptive data and counter advanced persistent threats (APTs). New elements would need to be secured and updated regularly to prevent APT incursions, which are increasingly frequent, complex, and subtle.

> *If the awareness-to-decision-to-response chain of modern warfare is to accelerate to cyber speed, machine-human teaming with AI-boosted analysis and edge computing in-theatre is required.*

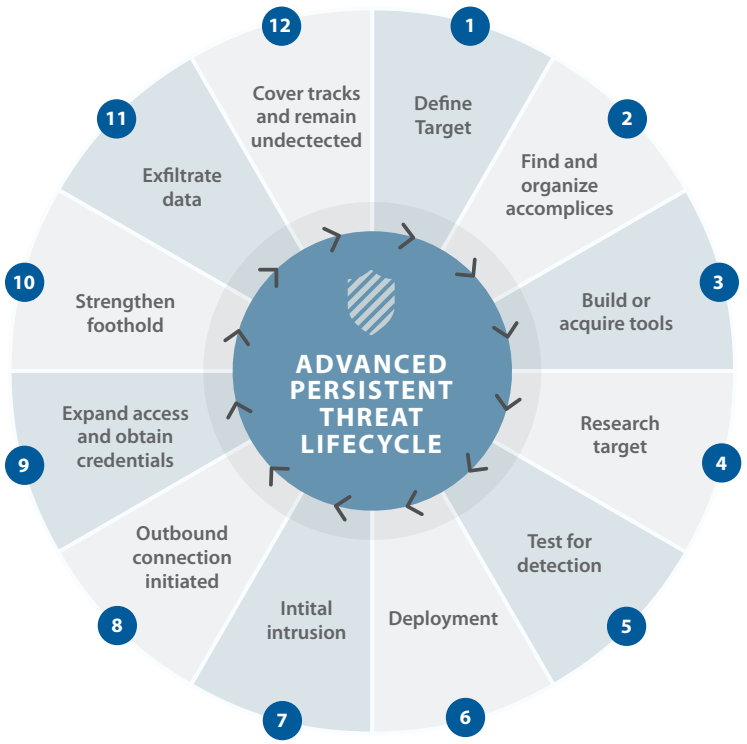
In addition, with IoMT implementation the number of battlefield interactions between constituent things will increase over time. Commercial and industrial protocols that are useful for scaling are unlikely to be effective in the resource-restricted environment of a battlespace where throughput may be limited. The processing and computational requirements are also likely to increase, which makes real-time responses and outputs more unlikely.

Interoperability, energy efficiency, and quality of service are also considerations. The dynamic nature of interoperability—whether between US forces or EU member states—is challenged not only by the different applications and devices used in the battlefield, but also the diverse operational and equipment standards that stem from the devices of different manufacturers of various allies, all of which may not be operating at the same level of technological advancement.

Developing a small form factor for wearable devices without degrading user experience is another challenge, especially since reducing size and weight generally also reduces battery capacity as well as charging and cooling capabilities. The US Army has noted its interest in IoMT for diverse and dynamic missions that will require rapid deployment and adaptation in environments with high mobility, resource constraints, and extreme heterogeneity in very dense and

sparse environments. Degraded transmission quality or drops in real-time analysis would indicate a failure of the entire matrix.

Advanced Persistent Threat (APT) Lifecycle



Conclusion

Despite all the challenges, the march towards interconnectivity seems inexorable. Such disruptive shifts in military thinking coincide with the offset strategy that drove nuclear superiority in the 1950s (First Offset) or the military overmatch provided by guided munitions and battle networks during the 1970s and 1980s (Second Offset). When the US DoD started to think about a Third Offset strategy in 2014, AI, autonomous systems, and human-machine teams were recognised as critical to gaining tempo. As strike velocities and ranges

increase alongside the speed and volume of accessible data, pervasive interconnectivity, interoperable networks, and improved standards of unmanned/manned coordinated behaviour will set new foundations for achieving air power superiority.

References:

International Telecommunication Union. 2012. Series Y.2060: *Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks: Next Generation Networks—Frameworks and functional architecture models: Overview of the Internet of things* [online]. Y.2060. Available from: *https://www.itu.int/rec/TREC-Y.2060-201206-I* [accessed 26 October 2021].

Russell, S, and Abdelzaher, T. 2018. The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making In: *MILCOM 2018—2018 IEEE Military Communications Conference (MILCOM)*. Oct 29-31, Los Angeles. IEEE.

Biographies of Authors

Dr. Edwin "Leigh" Armistead is a retired Naval Officer, who wrote his PhD on Information Operations (IO), and has written/edited three books on this important topic. In 2006, he participated in the establishment of the International Conference of Cyber Warfare and Security (ICCWS), *https://www.academic-conferences.org/conferences/iccws/*, an annual event providing academics, researchers and practitioners of this field, at micro or macro levels, a networking platform and forum for discussion, exploration and development of both theoretical and practical aspects of information warfare and security. He is also the Vice-Chair Working Group 9.10, ICT Uses in Peace and War and the Chief Editor of the Journal of Information Warfare (JIW)—the sole double-blind, peer-reviewed academic journal on Information Warfare (IW) in the United States.

Patrick Bolder, Lieutenant Colonel (Retired), Royal Netherlands Air Force, specializes in plans and policy and strategic thinking. Upon the culmination of his military career, he was seconded to the Hague Centre for Strategic Studies (HCSS), where he works on projects commissioned by the armed forces and the MOD. He has published and co-authored papers in the field of unmanned systems, artificial intelligence and the military aspects of the space domain. He has conducted lectures and presentations for various audiences and continues to expand his knowledge and proficiency in the military application of unmanned and space systems. He gained his education from Wageningen University, Higher Command and Staff College and NATO Defence College.

Justin Bronk is the Research Fellow for Airpower and Technology in the Military Sciences team at RUSI. He is also Editor of the RUSI Defence Systems online journal. His particular areas of expertise include the modern combat air environment, Russian and Chinese ground-based air defences and fast jet capabilities, unmanned combat aerial vehicles and novel weapons technology. He has written extensively for RUSI and a variety of external publications, as well as appearing regularly in the international media. He is a part-time doctoral candidate at the Defence Studies Department of Kings College London and holds an MSc in the History of International Relations from the London School of Economics and Political Science, and a BA (Hons) in History from York University.

David A. Deptula, Lieutenant General (Ret.), United States Air Force, is the Dean of the Mitchell Institute for Aerospace Studies in Arlington, Virginia, and also a Senior Military Scholar at the U.S. Air Force Academy. He was the principal attack planner for the 1991 Operation Desert Storm air campaign; commander of no-fly-zone operations over Iraq in the late 1990s; director of the air campaign over Afghanistan in 2001; twice a joint task force commander; and was the air commander for the 2005 South Asia tsunami relief operations. He is a fighter pilot with more than 3,000 flying hours—400 in combat—including multiple command assignments in the F-15. He was as the Air Force's first three-star chief of intelligence, surveillance, and reconnaissance (ISR), where he transformed America's military ISR and drone enterprises.

Dr. Peter Layton is a Visiting Fellow at the Griffith Asia Institute, Griffith University, a RUSI Associate Fellow and a Visiting Fellow at the Royal Australian Air Force Air and Space Power Centre. He has extensive aviation and defence experience including, flying fast jets and maritime patrol aircraft, force development, major equipment projects and as a defence attaché. For his work at the Pentagon on force structure matters, he was awarded the US Secretary of Defense's Exceptional Public Service Medal. His research interests include grand strategy, national security policies particularly relating to middle powers, defence force structure concepts and the impacts of emerging technology. He has a doctorate from the University of New South Wales on grand strategy.

Sherrill Lingel is a Senior Engineer at the RAND Corporation. Most recently, she conducted research on Joint All-Domain Command and Control (JADC2) for Agile Combat Employment (ACE) in Europe, preceded by work on ACE in a contested electromagnetic spectrum environment. She also led a research team on artificial intelligence applications for JADC2 for the U.S. Air Forces Air Combat Command (ACC). Her research includes complexity in great power competition and warfare, multi-domain operations, JADC2, ACE, capabilities for highly contested environments, and air and missile defense. She earned a B.S. in Aeronautical Engineering from the University of Virginia, an M.S. in Aeronautics and Astronautics Engineering from the University of Washington, and a Ph.D. in Civil Engineering from the University of Washington.

Dr. Brett van Niekerk is a Senior Lecturer at the University of KwaZulu-Natal, and serves as chair for the International Federation of Information Processing Working Group on ICT in Peace and War, and the co-Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He has numerous years of information security and cyber security experience in both academia and industry, and has contributed to the ISO/IEC information security standards and international working groups. He has over 70 publications and presentations to his name. In 2012 he graduated with his PhD focusing on information operations and critical infrastructure protection. He is also holds a MSC in electronic engineering and is CISM certified.

Dr. Michael Raska is an Assistant Professor and Coordinator of the Military Transformations Programme at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. His research interests focus on defence and military innovation, strategic competition, and cyber warfare in East Asia. He is the author of *Military Innovation and Small States: Creating Reverse Asymmetry* (Routledge, 2016) and co-editor of *Defence Innovation and the 4th Industrial Revolution: Security Challenges, Emerging Technologies, and Military Implications* (Routledge, 2022). He holds a BA in International Studies from the Missouri Southern State University, MA in International Relations from Yonsei University, and a PhD from the Lee Kuan Yew School of Public Policy, National

University of Singapore, where he was a recipient of the NUS President's Graduate Fellowship.

Anika Torruella is a Senior Analyst at Janes, covering naval electronic warfare, C2 systems, and sonar technology, with extensive further expertise in artificial intelligence, robotics, naval warfare, space, future computing, nanotechnology, and new materials. Over the past two decades Anika has also worked with the World Bank, Access Intelligence, and National Geographic. Anika graduated with a BA in Physics from Bryn Mawr College in Pennsylvania, where she studied Mathematics and Astronomy and was a Research Fellow.

Olivier Zajec, a graduate of Saint-Cyr Military Academy and of Sciences-Po Paris, is Professor of Political Science as well as Director of the IESD (Institute of Strategic and Defense Studies) at Jean Moulin University, Lyon. He is a research fellow at both the EA 4586 laboratory and the Institut de Stratégie Comparée (ISC) in Paris. He also teaches strategic theory at the French Joint War College. His current research interests focus on the realist theory of international relations, transatlantic defense policies, nuclear policy and strategies, and geopolitical theories. He regularly contributes to various defense and international relations publications: Le Monde diplomatique, Defense and international security (DSI), Res Militaris, Monde Chinois, Conflits, La Revue de Défense nationale.

2012. وهو حاصل أيضًا على ماجستير في الهندسة الإلكترونية واصبح مدير أمن المعلومات المعتمد (CISM).

د. مايكل راسكا هو أستاذ مساعد ومنسق برنامج التحولات العسكرية في مدرسة س. راجاراتنام للدراسات الدولية، جامعة نانيانغ للتكنولوجيا، سنغافورة. تركزت اهتماماته البحثية على الدفاع والابتكار العسكري والمنافسة الاستراتيجية والحرب الإلكترونية في شرق آسيا. وهو مؤلف كتاب "الابتكار العسكري والدول الصغيرة: إنشاء عدم تناسق عكسي" (روتليدج ، 2016)
(Military Innovation and Small States: Creating Reverse Asymmetry (Routledge, 2016))
ومحرر مشارك في "ابتكار الدفاع والثورة الصناعية الرابعة: التحديات الأمنية والتقنيات الناشئة والتداعيات العسكرية" (روتليدج ، 2022)
(Defence Innovation and the 4th Industrial Revolution: Security Challenges, Emerging Technologies, and Military Implications (Routledge, 2022))
حصل على بكالوريوس في الدراسات الدولية من جامعة ولاية ميسوري الجنوبية، وماجستير في العلاقات الدولية من جامعة يونسي، ودكتوراه من كلية لي كوان يو للسياسة العامة، جامعة سنغافورة الوطنية، حيث حصل على زمالة الخريجين بجامعة سنغافورة الوطنية.

أنيكا توروبلا هي محللة كبيرة في مجلة جاينس، تغطي المواضيع المتعلقة بالحرب الإلكترونية البحرية وأنظمة ،وتكنولوجيا السونار، مع خبرة واسعة في الذكاء الاصطناعي، والروبوتات، والحرب البحرية القيادة والتحكم المستقبلية، وتكنولوجيا النانو، والمواد الجديدة .على مدار العقدين الماضيين، عملت (C2) والفضاء، والحوسبة أنيكا أيضًا مع البنك الدولي و ومخابرات الوصول و ناشيونال جيوغرافيك .حصلت أنيكا على درجة البكالوريوس في الفيزياء من كلية برين ماور في ولاية بنسلفانيا ، حيث درست الرياضيات وعلم الفلك وكانت .زميلة أبحاث

بروفيسور أوليفييه زاجيك، خريج أكاديمية سانت سير العسكرية ومعهد الدراسات السياسية في باريس، هو أستاذ العلوم السياسية ومدير IESD (معهد الدراسات الاستراتيجية والدفاعية) في جامعة جان مولان، ليون. يشغل زاجيك منصب زميل باحث في كل من مختبر EA 4586 ومعهد الإستراتيجية المقارنة (ISC) في باريس. كما يقوم بتدريس النظرية الإستراتيجية في الكلية الحربية الفرنسية المشتركة. تركز اهتماماته البحثية الحالية على النظرية الواقعية للعلاقات الدولية، وسياسات الدفاع عبر الأطلسي، والسياسة والاستراتيجيات النووية، والنظريات الجيوسياسية. يساهم بانتظام في العديد من منشورات الدفاع والعلاقات الدولية: العالم الدبلوماسي (Le Monde diplomatique) الدفاع والأمن الدولي (DSI) الشؤون العسكرية (Res Militaris) العالم الصيني (Monde Chinois) الصراعات (Conflits) ومجلة الدفاع الوطني. (La Revue de Défense nationale).

ديفيد أ. ديبتولا، الفريق (متقاعد)، القوات الجوية للولايات المتحدة، هو عميد معهد ميتشل لدراسات الفضاء في أرلينغتون، فيرجينيا، وهو أيضًا باحث عسكري أول في أكاديمية القوات الجوية الأمريكية. كان المخطط الرئيسي للهجوم في الحملة الجوية لعملية عاصفة الصحراء عام 1991.هو قائد عمليات منطقة حظر الطيران فوق العراق في أواخر التسعينيات. عمل كمدير الحملة الجوية على أفغانستان عام 2001؛ وكقائد فرقة عمل مشتركة مرتين ؛ وكان القائد الجوي لعمليات الإغاثة من كارثة تسونامي في جنوب آسيا عام 2005. إنه طيار مقاتل لديه أكثر من 3000 ساعة طيران - 400 ساعة في القتال - بما في ذلك مهام قيادة متعددة على متن طائرة اف-15 (F-15). كان أول رئيس من فئة ثلاث نجوم للاستخبارات والمراقبة والاستطلاع (ISR) في سلاح الجو، حيث قام بتحويل مؤسسات الاستخبارات والمراقبة والاستطلاع العسكرية الأمريكية والطائرات بدون طيار.

د. بيتر لايتون هو زميل زائر في معهد جريفيث آسيا، جامعة جريفيث، زميل مشارك في معهد الخدمات المتحدة الملكي (RUSI) وزميل زائر في سلاح الجو الملكي الاسترالي وفي مركز القوة الجوية والفضائية. يتمتع بخبرة واسعة في مجال الطيران والدفاع بما في ذلك قيادة الطائرات النفاثة السريعة وطائرات الدوريات البحرية وتطوير القوات ومشاريع المعدات الرئيسية وكملحق دفاعي. حصل على وسام الخدمة العامة الاستثنائية لوزير الدفاع الأمريكي لعمله في البنتاغون في مسائل هيكل القوة. تشمل اهتماماته البحثية الاستراتيجية الكبرى، وسياسات الأمن القومي، وخاصة في ما يتعلق بالقوى الوسطى، ومفاهيم هيكل القوة الدفاعية وتأثيرات التكنولوجيا الناشئة. حصل على درجة الدكتوراه من جامعة نيو ساوث ويلز في الاستراتيجية الكبرى.

شيريل لينغيل مهندسة أعلى في مؤسسة راند (RAND). في الآونة الأخيرة، أجرت بحثًا حول القيادة والتحكم المشترك لجميع المجالات (JADC2) من أجل التوظيف القتالي السريع (ACE) في أوروبا، سبقها العمل على التوظيف القتالي السريع (ACE) في بيئة الطيف الكهرومغناطيسي المتنازع عليها. كما قادت فريقًا بحثيًا حول تطبيقات الذكاء الاصطناعي للقيادة والتحكم المشترك لجميع المجالات (JADC2) لقيادة القتال الجوي للقوات الجوية الأمريكية (ACC). تتضمن أبحاثها التعقيد في المنافسة بين القوى العظمى والحرب، والعمليات متعددة المجالات، والقيادة والتحكم المشترك لجميع المجالات (JADC2)، والتوظيف القتالي السريع (ACE)، وإمكانيات البيئات المتنازع عليها بشدة، والدفاع الجوي والصاروخي. حصلت على بكالوريوس العلوم في هندسة الطيران من جامعة فيرجينيا. كما حصلت على ماجستير في هندسة الملاحة الجوية والفضائية من جامعة واشنطن، و شهادة الدكتوراه في الهندسة المدنية من جامعة واشنطن.

د. بريت فان نيكيرك أستاذ محاضر كبير في جامعة كوازولو ناتال، ويشغل منصب رئيس الاتحاد الدولي لفريق عمل معالجة المعلومات حول تكنولوجيا المعلومات والاتصالات في السلام والحرب، ورئيس التحرير المشارك للمجلة الدولية للحرب السيبرانية والإرهاب. يمتلك سنوات عديدة من الخبرة في مجال المعلومات/ الأمن السيبراني في كل من الأوساط الأكاديمية والصناعية، وقد ساهم في معايير أمن معلومات المنظمة الدولية للمقاييس/اللجنة الكهرتقنية الدولية (ISO / IEC) ومجموعات العمل الدولية. له أكثر من 70 منشورًا وعرضًا تقديميًا باسمه. تخرج بدرجة الدكتوراه التي تتركزعلى عمليات المعلومات وحماية البنية التحتية الحيوية في عام

السير الذاتية للكُتّاب

د. ادوين "لي" أرميستيد هو ضابط بحري متقاعد، كتب أطروحة الدكتوراه الخاصة به عن عمليات المعلومات (IO)، وقد كتب وحرر ثلاثة كتب حول هذا الموضوع المهم. شارك في تأسيس المؤتمر الدولي للحرب السيبرانية والأمن (ICCWS) في عام 2006 https://www.academic-conferences.org/conferences/iccws/ وهو حدث سنوي يوفر للأكاديميين والباحثين والممارسين في هذا المجال على المستويين الجزئي أو الكلي، منصة شبكية ومنتدى لمناقشة واستكشاف وتطوير الجوانب النظرية والعملية لحرب المعلومات والأمن. وهو أيضًا نائب رئيس الفريق العامل 9.10 ، لاستخدامات تكنولوجيا المعلومات والاتصالات في السلام والحرب ورئيس تحرير مجلة حرب المعلومات (JIW) - المجلة الأكاديمية الوحيدة مزدوجة التعمية والمراجعة من قبل الأقران حول حرب المعلومات (IW) في الولايات المتحدة الأمريكية

باتريك بولدر هو مقدم متقاعد حديثًا في سلاح الجو الملكي الهولندي ومتخصص في التخطيط والسياسات والتفكير الاستراتيجي. في ذروة مسيرته العسكرية، تم اعتماده في مركز لاهاي للدراسات الاستراتيجية (HCSS)، حيث يعمل في مشاريع بتكليف من القوات المسلحة ووزارة الدفاع. نشر وشارك في تأليف أوراق بحثية في مجال الأنظمة غير المأهولة والذكاء الاصطناعي والجوانب العسكرية لمجال الفضاء. ألقى محاضرات وعروضًا تقديمية لمختلف الجماهير كما ويواصل توسيع معرفته وكفاءته في التطبيق العسكري للأنظمة غير المأهولة والفضائية. تابع تعليمه في جامعة واغنينغن وكلية القيادة العليا والأركان وكلية الدفاع التابعة لحلف الناتو.

جاستن برونك هو زميل باحث في القوة الجوية والتكنولوجيا في فريق العلوم العسكرية في في معهد الخدمات المتحدة الملكي (RUSI). وهو أيضًا محرر في مجلة أنظمة دفاع في معهد الخدمات المتحدة الملكي لأنظمة الدفاع (RUSI)على الإنترنت. تشمل مجالات خبرته الخاصة البيئة الجوية القتالية الحديثة، والدفاعات الجوية الأرضية الروسية والصينية، والقدرات النفاثة السريعة، والمركبات الجوية القتالية غير المأهولة وتكنولوجيا الأسلحة الجديدة. كتب على نطاق واسع لمعهد معهد الخدمات المتحدة الملكي لأنظمة الدفاع (RUSI) ومجموعة متنوعة من المنشورات الخارجية، فضلاً عن ظهوره بانتظام في وسائل الإعلام الدولية. وهو مرشح دكتوراه بدوام جزئي في قسم الدراسات الدفاعية في كينجز كوليدج بلندن وحاصل على ماجستير في تاريخ العلاقات الدولية من كلية لندن للاقتصاد والعلوم السياسية، ودرجة البكالوريوس (مع مرتبة الشرف) في التاريخ من جامعة يورك.

المراجع

الاتحاد الدولي للاتصالات. 2012. السلسلة Y.2060: البنية التحتية العالمية، جوانب بروتوكول الإنترنت وشبكات الجيل التالي: شبكات الجيل التالي - الأطر ونماذج البنية الوظيفية: نظرة عامة على إنترنت الأشياء [عبر الإنترنت]. Y.2060. متاح من:
https://www.itu.int/rec/TREC-Y.2060-201206-I [تم الدخول في 26 أكتوبر 2021].

Russell, S, and Abdelzaher .T. 2018. إنترنت أشياء ساحة المعركة: الجيل القادم من القيادة والسيطرة والاتصالات والاستخبارات (C3I) اتخاذ القرار في:
MILCOM 2018 - 2018 IEEE Military Communications Conference
(MILCOM). 29-31 أكتوبر ، لوس أنجلوس. IEEE.

وتكييفًا في بيئات ذات قدرة عالية على الحركة، قيود على الموارد وعدم تجانس شديد في بيئات شديدة الكثافة والمتفرقة. قد يشير تدهور جودة الإرسال أو الانخفاض في التحليل في الوقت الفعلي إلى فشل المصفوفة بأكملها.

الخاتمة

على الرغم من كل التحديات، يبدو أن المسيرة نحو الترابط لا هوادة فيها. تتزامن هذه التحولات التخريبية في التفكير العسكري مع استراتيجية الإزاحة التي قادت التفوق النووي في الخمسينيات (الإزاحة الأولى) أو المبالغة العسكرية التي قدمتها الذخائر الموجهة وشبكات المعارك خلال السبعينيات والثمانينيات (الإزاحة الثانية). عندما بدأت وزارة الدفاع الأمريكية في التفكير في إستراتيجية الإزاحة الثالثة في عام 2014 ، تم الاعتراف بالذكاء الاصطناعي والأنظمة المستقلة وفرق الإنسان والآلة على أنها ضرورية لاكتساب الإيقاع. مع زيادة سرعات ونطاقات الضربات جنبًا إلى جنب مع سرعة وحجم البيانات التي يمكن الوصول إليها، فإن الترابط المنتشر والشبكات القابلة للتشغيل البيني وتحسين معايير السلوك المنسق غير المأهول/المأهول سيضع أسسًا جديدة لتحقيق تفوق القوة الجوية.

دورة حياة التهديد المستمر المتقدم (APT)

التوسع فعالة في بيئة محدودة الموارد في ساحة المعركة حيث قد تكون الإنتاجية محدودة. من المرجح أيضًا أن تزداد متطلبات المعالجة والحساب، مما يجعل الاستجابات والنواتج في الوقت الفعلي أكثر احتمالًا.

تعد قابلية التشغيل البيني وكفاءة الطاقة وجودة الخدمة من الاعتبارات أيضًا. إنّ الطبيعة الديناميكية لقابلية التشغيل البيني - سواء بين القوات الأمريكية أو الدول الأعضاء في الاتحاد الأوروبي - تواجه تحديًا ليس من خلال التطبيقات والأجهزة المختلفة المستخدمة في ساحة المعركة فحسب، بل من خلال المعايير التشغيلية والتجهيزات المتنوعة أيضًا والتي تنبع من أجهزة الشركات المصنعة المختلفة لمختلف الحلفاء، قد لا تعمل جميعها على نفس المستوى من التقدم التكنولوجي.

يعد تطوير عامل شكل صغير للأجهزة القابلة للارتداء دون تجربة المستخدم المهينة تحديًا آخر، خاصة وأن تقليل الحجم والوزن بشكل عام يقلل أيضًا من سعة البطارية بالإضافة إلى قدرات الشحن والتبريد. لاحظ الجيش الأمريكي اهتمامه بإنترنت الأشياء العسكرية (IoMT) للمهام المتنوعة والديناميكية التي ستتطلب نشرًا سريعًا

من ناحية أخرى ، وافقت فرنسا وألمانيا وإسبانيا على التطوير المشترك لعنصر نظام الأسلحة من الجيل التالي (NGWS) من برنامج نظام القتال الجوي المستقبلي (SCAF / FCAS)، المسمى الناقلين عن بعد (Remote Carriers). من المقرر أن تحدث عروض الطيران الأولى لبرنامج SCAF / FCAS الأوروبي في عام 2027 ومن المقرر تجميد التصميم النهائي المقترح في عام 2030 قبل الموعد المقترح للخدمة بين 2040 و 2045. وسيشمل البرنامج يورودرون (Eurodrone) (أيضًا يُطلق عليها EuroMALE - نظام الطائرات الأوروبية على ارتفاعات متوسطة طويلة التحمل [MALE] نظام الطائرات الموجهة عن بُعد [RPAS])، وهي مركبة جوية قتالية بدون طيار منخفضة للغاية يمكن ملاحظتها (UCAV)، وصواريخ كروز مستقبلية، ومنصات قديمة تعمل في ساحة المعركة المستقبلية.

الضعف التشغيلي

لا يخلو تطبيق إنترنت الأشياء العسكرية (IoMT) من تحديات كبيرة. ينشأ التعقيد من الحجم المتزايد والوظائف والترابط بين العناصر الشبكية، وكذلك من سرعة وحجم جمع البيانات وإنتاج معلومات جديدة. السرعة الجديدة للحرب- مدفوعة بشبكات المعارك الآلية وزيادة قوة الحوسبة- هي السرعة الإلكترونية، حيث تهيمن هجمات الشبكات والحرب الإلكترونية على مشهد المعلومات. بالإضافة إلى ذلك، على الرغم من الإمكانات التي يوفرها تطبيق إنترنت الأشياء العسكرية (IoMT) للتطبيقات الدفاعية، فإن الضعف التشغيلي هو الشاغل الأكثر أهمية.

يتمثل التحدي الآخر الذي يمثله الربط بين أنواع مختلفة من الأسلحة ورجال الحرب في أن سيناريوهات ساحة المعركة تتطلب قرارات واستجابات في الوقت الفعلي. إن تحمّل الأخطاء منخفض وإن الفشل في عقد الاتصال كارثي. يجب إنشاء وتأمين النسخ الاحتياطية والتوائم الرقمية ومسارات الاتصال البديلة. بالإضافة إلى "الأشياء" و إنترنت الأشياء العسكرية (IoMT) التي تمتلكها القوات وتسيطر عليها، قد يحتاجون أيضًا إلى استخدام تقنيات إنترنت الأشياء العسكرية (IoMT) أو التجارية أو الصناعية أو المعادية التي لا يمتلكونها أو يتحكمون فيها بشكل كامل. ستحتاج المصادقة إلى استيعاب البيانات الخادعة ومواجهة التهديدات المستمرة المتقدمة (APTs). يجب تأمين العناصر الجديدة وتحديثها بانتظام لمنع توغلات التهديدات المستمرة المتقدمة (APT)، والتي تزداد تكراراً وتعقيدًا ودقة.

> إذا كانت سلسلة الوعي بالقرار إلى الاستجابة للحرب الحديثة تهدف إلى الإسراع إلى السرعة الإلكترونية، فإن التعاون بين الإنسان والآلة مع التحليل المعزز بالذكاء الاصطناعي والحوسبة المتطورة في مسرح العمليات مطلوب.

بالإضافة إلى ذلك، مع تطبيق إنترنت الأشياء العسكرية (IoMT)، سيزداد عدد التفاعلات في ساحة المعركة بين العناصر المكونة بمرور الوقت. من غير المحتمل أن تكون البروتوكولات التجارية والصناعية المفيدة في

إلى التكامل والتشغيل البيني عبر المجالات والأنظمة الأساسية" بحلول عام 2025. حذرت وزارة الدفاع قائلةً " لقد تداولنا في كثير من الأحيان تحديث التكنولوجيا ولم يؤد إلى تكامل كافٍ وقواسم مشتركة كافية ". "الاستمرار في هذا المسار سيمنعنا من استغلال التقنيات الناشئة بالسرعة والنطاق المطلوبين لتحقيق الغرض الدفاعي."

استمرت الاستراتيجية الرقمية في المملكة المتحدة في تسليط الضوء على أن الوصول إلى الطيف الكهرومغناطيسي (EMS) والتحكم فيه ضروري لجميع العمليات لعمل العمود الفقري الرقمي، مضيفًا أنه مع ظهور تقنية الجيل الخامس وإنترنت الأشياء(IoT)، سينمو المجال السيبراني "أسرع بكثير وأوسع نطاقًا في السنوات القليلة المقبلة. على هذا النحو، ستؤمن البيانات والمعايير المعمارية، بالإضافة إلى إدارة الطيف الكهرومغناطيسي (EMS)، الميزة التشغيلية وحرية المناورة".

منصة طيار الجناح الموالية للمملكة المتحدة، موسكيتو (Mosquito)، لطائرة تامبست (Tempest) النفاثة المقاتلة المستقبلية التي يتم تجريبها بشكل اختياري، تخضع لبرنامج يُعرف باسم الطائرات المقاتلة خفيفة الوزن ذات الأسعار المعقولة (LANCA). ستكون منصة طيار الجناح الموالية للمملكة المتحدة، موسكيتو (Mosquito) متوافقةً مع حاملات الطائرات البريطانية وستكون قادرةً على أداء مجموعة من الأدوار، مثل حاملات الأسلحة و/أو الأفخاخ أو العمل كأسلحة بأنفسهم. يشتمل برنامج أنظمة جوية قتالية مستقبلية (FCAS) في المملكة المتحدة أيضًا على طائرات بدون طيار من طراز Alvina ومنصات قديمة أخرى مرتبطة ببعضها البعض بواسطة سحابة قتالية، ومن المتوقع أن تحل الطائرات غير المأهولة محل القدرة القتالية الجوية لطائرات تايفون (Typhoon) البريطانية بحلول منتصف عام 2030.

تشمل مبادرات إنترنت الأشياء العسكرية (IoMT) الأوروبية شبكات الاستشعار اللاسلكية لمراقبة المناطق الحضرية المحلية (WINLAS) ومشاريع الذكاء السحابي لدعم اتخاذ القرار والتحليل (CLAUDIA) ، والتي تقع ضمن نطاق وكالة الدفاع الأوروبية (EDA). يبحث برنامج شبكات الاستشعار اللاسلكية لمراقبة المناطق الحضرية المحلية (WINLAS) عن شبكات استشعار كبيرة من الأجهزة غير المتجانسة لحرب المدن وأنظمة الطاقة وإدارة المعلومات في أنظمة تحديث الجندي على نطاق واسع. يعتمد البحث من هذا المشروع جزئيًا على نتائج التشغيل البيني للمعلومات والتشغيل البيني الاستخباراتي التابع لوكالة الدفاع الأوروبية (EDA) من خلال برنامج الإحصاء والوكلاء والاستدلال والدلالات (IN4STARS)، والذي يهدف إلى تحسين الوعي بالظروف في المناطق الحضرية باستخدام الذكاء الاصطناعي، وأجهزة الاستشعار، وحصاد الطاقة لإطالة تشغيل الشبكة.

يتمحور الهدف الرئيسي من مشاريع الذكاء السحابي لدعم اتخاذ القرار والتحليل (CLAUDIA) هو حول تطوير منصات تحليل برمجية معيارية لدعم تحليل وتقييم السيناريوهات العسكرية، وخاصة تلك التي تمارَس أثناء الحرب المختلطة. تهدف مشاريع الذكاء السحابي لدعم اتخاذ القرار والتحليل (CLAUDIA) إلى دعم احتياجات القادة من حيث التحليل واتخاذ القرار والتخطيط. ستقوم منصاتها بجمع ومعالجة وتحليل البيانات من مصادر المعلومات غير المتجانسة لتوفير الوعي الظرفي وصورة تشغيلية مشتركة شاملة (COP) لدعم التخطيط وعمليات صنع القرار والتنسيق بين الدول الأعضاء في الاتحاد الأوروبي.

القيادة والطائرات مع إعادة التركيز على إنشاء تقنيات رقمية ، مثل البيئات السحابية الآمنة، لمشاركة البيانات عبر أنظمة أسلحة متعددة.

يهدف نظام إدارة المعارك المتقدم لإنترنت الأشياء العسكرية (ABMS) (IoMT) الآن إلى تضمين مجموعة من الأنظمة التي تتضمن الأجهزة والبرامج المصممة لتحسين إدارة منع الولوج والمناطق المحرّمة (A2/AD) وتمكين عناصر القوات الجوية الأمريكية من التنسيق مع البحرية الأمريكية وإجرائها (USN)، مشاة البحرية الأمريكية (USMC)، والجيش الأمريكي. وفقًا لخدمة أبحاث الكونجرس الأمريكية، أجرت القوات الجوية الأمريكية خمسة أحداث لإثبات قدرات القيادة والتحكم (C2) الجديدة التي يعتزم نظام إدارة المعارك المتقدم (ABMS) إدخالها في المجال. أظهر سلاح الجو القدرة على نقل البيانات من رادار للجيش الأمريكي في ديسمبر 2019 (جهاز استشعار للدفاع الجوي ووحدة إطلاق نار) ومدمرة البحرية الأمريكية (USN) (المدمرة آرلي بيرك Arleigh Burke من فئة الصواريخ الموجهة يو إس إس توماس هودنر *Thomas Hudner* USS، المنتشرة في خليج المكسيك) إلى طائرات مقاتلة من نوع اف-22 رابتور من لوكهيد مارتن (F-22 Raptor) واف-35 ايه (F-35A) ومقاتلة اف-35سي (F-35C)، بالإضافة إلى مكتبة البيانات الموحدة للقوات الفضائية الأمريكية (UDL)، وهي بيئة سحابية تجمع بين أجهزة الاستشعار الفضائية والأرضية لتتبع الأقمار الصناعية.

في سبتمبر 2020، اكتشف نظام إدارة المعارك المتقدم (ABMS) وهزم صاروخ كروز افتراضي متجهًا إلى الولايات المتحدة باستخدام أسلحة فائقة السرعة. كما عرض نظام إدارة المعارك المتقدم (ABMS) أيضًا قدرات "للكشف عن الجهود المبذولة لتعطيل العمليات الأمريكية في الفضاء وإلحاق الهزيمة بها". في نفس الشهر، استخدمت القوات الجوية الأمريكية طائرة ناقلة من طراز كي سي-46 (KC-46) لأداء القيادة والتحكم (C2) التكتيكي من خلال نقل البيانات من مقاتلات الجيل الرابع إلى طائرات الجيل الخامس، مثل F-22 Raptor ، أثناء تمرين "الدرع الشجاع" في قاعدة بيرل هاربور - هيكام المشتركة في هاواي. في فبراير، تم تنظيم تمرين مختصر في أوروبا ربط الدول الحليفة، بما في ذلك هولندا وبولندا والمملكة المتحدة، في عمليات جوية مشتركة. وفقًا للجنرال جيفري هاريجان، قائد القوات الجوية الأمريكية في أوروبا، اختبر الحدث قدرات الولايات المتحدة والحلفاء لأداء مهام هجومية بعيدة المدى باستخدام طائرة من طراز اف-15اي F-15E تطلق صواريخ المواجهة الجوية المشتركة إيه جي إم-158 (AGM-158)أثناء استخدام الولايات المتحدة وحلفائها مقاتلات اف-35 (F-35) لمهام الدفاع الجوي. في مايو، صرح سلاح الجو الأمريكي (USAF) أن شراء حجرة اتصالات لـ KC-46 سيكون أول إصدار للقدرة لبرنامج نظام إدارة المعارك المتقدم (ABMS).

إنترنت الأشياء العسكرية (IoMT) في المملكة المتحدة وأوروبا

تم نشر مفاهيم لبرنامج مشابه لنظام إدارة المعارك المتقدم (ABMS) في أبريل من قبل الاستراتيجية الرقمية لوزارة الدفاع البريطانية (MoD) لجهود الدفاع. ويهدف هذا إلى إنشاء "عمود فقري رقمي" آمن وفريد وحديث يربط بين "أجهزة الاستشعار والمؤثرات والمقررين عبر المجالات العسكرية والتجارية ومع الشركاء، مما يؤدي

> إن تحمّل الأخطاء منخفض وإن الفشل في عقد الاتصال كارثي. يجب إنشاء وتأمين النسخ الاحتياطية والتوائم الرقمية ومسارات الاتصال البديلة.

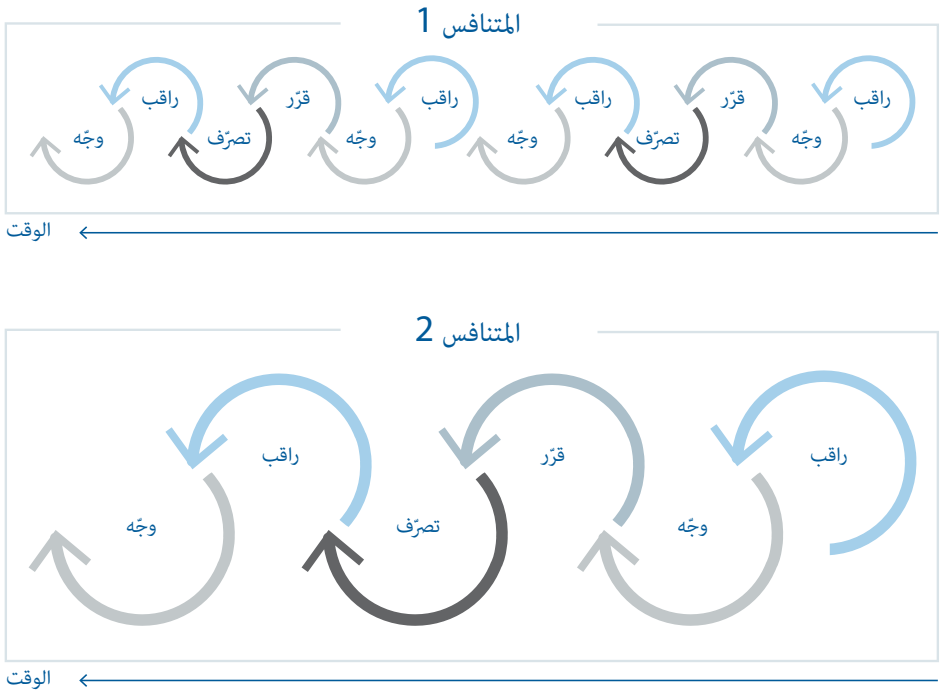
تعمل مفاهيم الجناح الموالي كامتداد لأجهزة الاستشعار والأنظمة الأخرى للطائرات المأهولة، مع القدرة على تعطيل أو إتلاف أو تدمير الدفاعات الجوية المستهدفة أثناء البقاء على قيد الحياة في بيئات منع الولوج والمناطق المحرّمة (A2/AD) المتنازع عليها. تسعى هذه الفرق إلى رفع مستوى التنافس عن طريق تحويل تشكيلات الطائرات المقاتلة المأهولة التقليدية إلى مزيج جديد من المنصات المأهولة وغير المأهولة التي تخلق تسليمًا أكثر رشاقةً وخبثًا وفتاكًا للأسلحة. إذا كانت سلسلة الوعي بالقرار إلى الاستجابة للحرب الحديثة تهدف إلى الإسراع إلى السرعة الإلكترونية، فإن التعاون بين الإنسان والآلة مع التحليل المعزز بالذكاء الاصطناعي والحوسبة المتطورة في مسرح العمليات مطلوب. ستعمل التكنولوجيا المترابطة لحرب الفسيفساء على الاستفادة من الأنظمة غير المأهولة ذات الإدراك الذاتي للذكاء الآلي بما يكفي لتقييم حالة وأهداف ونقاط ضعف البعثات لمواجهة الاضطرابات في الوقت الفعلي.

مفهوم مشترك للقيادة والتحكم (JADC2) ونظام إدارة المعركة المتقدم في الولايات المتحدة

يعتبر نظام إدارة المعارك المتقدم (ABMS) التابع للقوات الجوية الأمريكية جزءًا من خطة أوسع من قبل الجيش الأمريكي لإنشاء مفهوم مشترك للقيادة والتحكم (JADC2) ، والذي يتطلع إلى بناء إنترنت الأشياء العسكرية (IoMT) من خلال توصيل أجهزة الاستشعار من جميع أنحاء الولايات المتحدة في شبكة تعاونية واحدة. شهدت الجهود السابقة تطوير كل خدمة لشبكتها التكتيكية الخاصة، على الرغم من عدم توافقها مع بعضها البعض. وفقًا لخدمة أبحاث الكونجرس الأمريكية، مع إمكانية التشغيل المتداخل استنادا إلى إنترنت الأشياء العسكرية (IoMT) المتعددة المجالات الشائعة، تسعى وزارة الدفاع الأمريكية إلى تحويل "العملية الحالية متعددة الأيام لتحليل بيئة التشغيل وإصدار الأوامر" إلى عملية تستغرق "ساعات ودقائق، أو ثوانٍ محتملة" للصراعات وبيئات التشغيل المستقبلية. صرّحت وزارة الدفاع الأمريكية أيضًا أن بنية القيادة والتحكم (C2) الحالية غير كافية لتلبية متطلبات استراتيجية الدفاع الوطني الأمريكية (NDS).

تم تصور برنامج إنترنت الأشياء العسكرية (IoMT) التابع لسلاح الجو الأمريكي (USAF)، المجلس الأمريكي للتخصصات الطبية (ABMS) ، في الأصل ليحل محل منصات نظام الإنذار والتحكم المحمولة جواً (AWACS) لطائرات السلاح الجو الأمريكي إيه-3 (E-3). ومع ذلك، فقد اتخذ نطاقًا أوسع عندما صرح ويل روبر، مساعد وزير الدفاع السابق للقوات الجوية للاستحواذ، أن البيئة المتنازع عليها التي تصورتها استراتيجية الدفاع الوطني الأمريكية لعام 2018 قد أجبرت القوات الجوية على إعادة هيكلة أنظمة نظام إدارة المعارك المتقدم (ABMS). وعمل روبر على أن يصبح نظام إدارة المعارك المتقدم (ABMS) أقل تركيزًا على مراكز

تسريع حلقة نموذج راقب، وجّه، قرّر، تصرّف
للميزة التشغيلية (OODA)



الأشياء العسكرية (IoMT) التحليل الشامل والإدارة والقيادة والتحكم (C2) اللازمة لنوع جديد من حرب المعلومات: حرب تتمحور حول القرار من خلال الاعتماد على اتخاذ قرارات أسرع وأفضل، بالإضافة إلى أوقات استجابة أقصر قابلة للتنفيذ.

دخلت الطائرات دون طيار و الطائرات غير المأهولة (التي يتم توجيهها اختياريًا) إلى المشهد وأثبتت أنها مضاعفة القوة، خاصةً لجمع البيانات والضربات الجوية بعيدة المدى، ويصعب الوصول إلى مناطق و/أو منع الولوج والمناطق المحرّمة (A2/AD). لقد أصبحوا بمثابة عمالة للاستخبارات والاستطلاع والمراقبة في مسرح العمليات (ISR) ويقومون بالفعل بأداء مجموعة واسعة من المهام العسكرية. يعمل عدد من البلدان على تطوير برامج أنظمة جوية قتالية مستقبلية (FCAS) التي تصوّر طائرات بدون طيار عالية الأداء وممكّنة للشبكة والتي تطير بالتنسيق مع الطائرات المقاتلة المأهولة - إما في أسراب أو كـ" جناح موالي" – لسد هذه الفجوة.

تفاعل ذكي

تم استخدام إنترنت الأشياء (IoT) لوصف الاتصال ومشاركة المعلومات بين عدد كبير من عقد التكنولوجيا "الذكية". يمكن بعد ذلك تصنيفها إلى أجهزة تحمل البيانات، والتي يتم ربطها بشكل غير مباشر بالأشياء المادية بشبكات الاتصال؛ أجهزة التقاط البيانات، وهي أجهزة من نوع القارئ/ الكاتب قادرة على التفاعل مع الأشياء المادية بشكل غير مباشر عبر الأجهزة التي تحمل البيانات أو مباشرة عبر ناقلات البيانات المرتبطة بأشياء مادية؛ أجهزة الاستشعار والتشغيل، التي تكتشف أو تقيس المعلومات في البيئة المحيطة وتحولها إلى إشارات رقمية؛ والأجهزة العامة، التي تحتوي على إمكانات معالجة واتصالات مضمنة وقد تتضمن معدات وأجهزة لتطبيقات إنترنت الأشياء المختلفة (International Telecommunication Union 2012).

يمكن لإنترنت الأشياء (IoT) أن تصف شبكات المدن، والشبكات الصناعية، والحوسبة السحابية، وشبكات الهاتف المحمول، بينما عززت تطبيقاتها جمع البيانات والمعلومات والخدمات عند تقديمها لأنظمة البنية التحتية الطبية الحيوية والأمن والتجارية والصناعية. ومع ذلك، نظرًا للعلاقة بين المجمع الصناعي التجاري والخدمات العسكرية والدفاعية، فقد خضعت تطبيقات إنترنت الأشياء (IoT) لاستراتيجيات الحرب الحديثة لمزيد من التدقيق. يصف إنترنت الأشياء العسكرية (IoMT) أو إنترنت الأشياء في ساحة المعركة (IoBT) التكنولوجيا التي تتيح التفاعل الذكي بين المقاتلين ومعداتهم في ساحات المعارك.

يصف الاستخدام الدفاعي الآخر لإنترنت الأشياء العسكرية (IoMT) مجموعات من العناصر المترابطة والمتصلة بالشبكة والتي لا تشمل المستشعرات والأجهزة فحسب، بل تشمل أيضًا البنية التحتية مثل معدات التخزين ومعالجة البيانات، والشبكة المستخدمة لربط الأجهزة والعقد، والبرامج وخوارزميات التعلم الآلي التي تحكم معهم. يتضمن هذا مجموعة واسعة من أجهزة الاستشعار العسكرية المتكاملة والأجهزة والمنصات القادرة على الاستشعار الذكي والتعلم الآلي والتشغيل عبر عقد الفضاء الإلكتروني وواجهات الإنسان والآلة. تهدف هذه التفاعلات إلى زيادة الوعي الظرفي وتقليل الوقت اللازم لمعالجة البيانات وتقييم المخاطر والتخطيط الاستراتيجي ومعلومات العمل وتنفيذ الأهداف. بموجب التعريف الواسع، يمكن أن تشمل " الأشياء" الدبابات، والسفن الحربية، والطائرات، والمركبات الجوية غير المأهولة (UAVs)، وقواعد العمليات الأمامية (FOBs)، والمعدات اللوجستية، وأنظمة النقل وبناء البنية التحتية، والمقاتلين أنفسهم، أو أي شيء يمكن دمجه مع نظام الاستشعار، وقدرات المعالجة والإرسال (راسل اند عبدالظاهر 2018).

وبهذه الطريقة، تمثل إنترنت الأشياء العسكرية (IoMT) التقارب بين مجالات القتال: شبكاتها، والأجهزة المضمنة، والانبعاثات الكهرومغناطيسية، وعقد الاتصال، وأجهزة معالجة الأجهزة المحمولة، وهندسة البرمجيات، وإدارة المعلومات، وتحليلات البيانات. تمامًا كما تخفف التوائم الرقمية من خطر تعطل المعدات والفشل والتطفل الإلكتروني من خلال النمذجة المتزامنة والتنبؤ المستمر بقدرات الصيانة وقدرات الأداء، يمكن استخدام البيانات التي تم جمعها من الاستشعار والاتصال المنتشر الذي وعدت به إنترنت الأشياء العسكرية (IoMT) لتحسين النظام الديناميكي، والكشف عن الأخطاء والمراقبة والتنبؤ. بالإضافة إلى ذلك، توفر إنترنت

10 حرب الفسيفساء: المسيرة نحو الترابط في الولايات المتحدة والمملكة المتحدة والقوة الجوية الأوروبية

أنيكا توروبلا

محلل أعلى، جاينس

لقد غيرت شبكات تبادل المعلومات والبيانات مشهد العمليات الدفاعية. يستثمر الفاعلون من القوى العظمى في مجال التكنولوجيا التي تتيح الاتصال عالي السرعة بين عدد متزايد من المقاتلين والشبكات والآلات المستقلة أو المأهولة التي يمكن أن تتفاعل في بيئة معركة معقدة للغاية ولا يمكن التنبؤ بها بشكل متزايد. في الوقت نفسه، ثمة دافع ناشئ لربط عدد متزايد من أجهزة الاستشعار، والمنصات الأرضية المتنقلة، والطائرات، وأنظمة المهام، والأنظمة غير المأهولة، والأجهزة المحمولة، والأجهزة المحمولة، والأسلحة والذخائر، والبرامج، وغيرها من التقنيات لتصبح شبكة معلومات واحدة. إنّ الهدف العام هو إنشاء مصفوفة ديناميكية وقابلة للتكيف تتيح تحليلات تنبؤية وقابلة للتنفيذ في الوقت الفعلي لاتخاذ القرار والقيادة والتحكم (C2) وإمكانيات أخرى داخل مسرح القتال.

إنّ الهدف النهائي هو تحويل القتال الحربي من اتخاذ القرار الخطي إلى شبكة من النتائج القابلة للتنفيذ لإنكار وردع وهزيمة الأعداء. تصف وكالة مشاريع الأبحاث الدفاعية المتقدمة الأمريكية (DARPA) هذا بالتحول إلى "حرب الفسيفساء" حيث أن التقنيات التقليدية غير المتماثلة، مثل الأقمار الصناعية المخصصة والطائرات ذات خاصية الشبح والذخائر الدقيقة، تقدم قيمة إستراتيجية منخفضة في الحرب الحديثة بسبب الوصول العالمي المتزايد إلى التكنولوجيا والمكونات المتقدمة المتاحة تجارياً. يهدف مفهوم حرب الفسيفساء هذا إلى تجاوز تصميمات الأنظمة الفردية ومعايير التشغيل البيني الفريدة لتطوير العمليات والأدوات التي تعتمد على الاتصالات الموثوقة بين الكيانات المعروفة التي توفر إمكانيات غير محدودة لإحداث تأثيرات على مستويات صنع القرار التكتيكية والتشغيلية والاستراتيجية.

القوة الأخرى التي تمتلكها الدولة. فلقد تم إثبات أنّ حرب المعلومات أمر حيوي للفعالية التشغيلية ولفعالية القيادة والتحكم للقوات المشتركة، لا سيما في بيئة قتالية تعتمد على السحابة، وسيستمر هذا الواقع على مدى السنوات القليلة القادمة، مما سيتطلب نشر القوة العسكرية وتوظيفها في المستقبل، وأن يكون مخططو ومشغلو القوات المشتركة أكثر وعياً بالموقف وأكثر تعاوناً وأكثر اعتماداً على الشركاء في بيئة المعلومات إذا أرادوا تجاوز المقاربات التقليدية "الداخلية" وإنشاء الحلول المثلى لتأثيرات حرب المعلومات.

أن تكون أي استراتيجية حرب معلومات للقوات المشتركة مجرد مجموعة فرعية من أدوات القوة الخاصة بالدولة، بل يجب أن تتكامل معها تمامًا وتتخطى جميع المجالات بما في ذلك الأرض والبحر والجو والفضاء. ففي الوقت الذي تتعلم فيه القوات المشتركة مزامنة التأثيرات بشكل أكثر سلاسة، ستصبح هيمنة بيئة المعلومات حاسمة لنجاحها بشكل عام، وسوف تحتاج حرب المعلومات إلى أن تصبح جزءًا لا يتجزأ من جميع الأنشطة منذ بداية التخطيط - وليس "مضافًا" في النهاية أو مخططًا بشكل منفصل، كما وستحتاج القوات المشتركة إلى النظر في التأثيرات التي تنوي إحداثها ثم اختيار السلاح أو الإجراء المناسب لذلك، فيما يجب أن يوفر استهداف الطيف الكامل عبر المجالات من الناحية النظرية خيارًا من التأثيرات الحركية أو حتى المعلوماتية البحتة لاستخدامها كبدائل.

إنّ كيفية تأثير هذا على القيادة والتحكم في بيئات الحرب المشتركة وهدف ربط القوة المقاتلة بطريقة تدرك الواقع المتطور ونطاق ومتطلبات حرب المعلومات والقدرات اللازمة لذلك، يُعَد أمر بالغ الأهمية، والسؤال الصعب الذي يجب طرحه هو: ما الذي لا يمكننا التحكم فيه بالضبط في ما يتعلق بحرب المعلومات؟ إننا بحاجة إلى النظر في الدور المتزايد وأهمية العمليات السيبرانية من قبل المجموعات الأجنبية والمحلية، وحقيقة كون حرب المعلومات هي في الواقع مفهوم تحوّلي وليس مفهومًا ثابتًا. لا يمكن أن تكون حرب المعلومات مُنعَزِلة وستحتاج إلى أن يتم توزيعها عبر جميع عناصر هندسة الأمن والاستخبارات التي تتفاعل معها القوات المشتركة وتعمل معها، إذ تظهر الحاجة إلى مثل هذا النهج من خلال التصنيفات الجديدة مرة أخرى: بدلاً من تسمية الأنشطة بحرب المعلومات على سبيل المثال ، لماذا لا نسميها عمليات فحسب؟ إن استخدام المعلومات كعنصر قوة أو سلاح ليس بالأمر الجديد، وعلى الرغم من كونها أداة جديدة نسبيًا في ترسانة قائد القوات المشتركة، إلا أنها سلاح يجب استخدامه تمامًا مثل أي أداة أخرى إذا كانت ساحة المعركة مُعَدّة بشكل مناسب.

الخاتمة

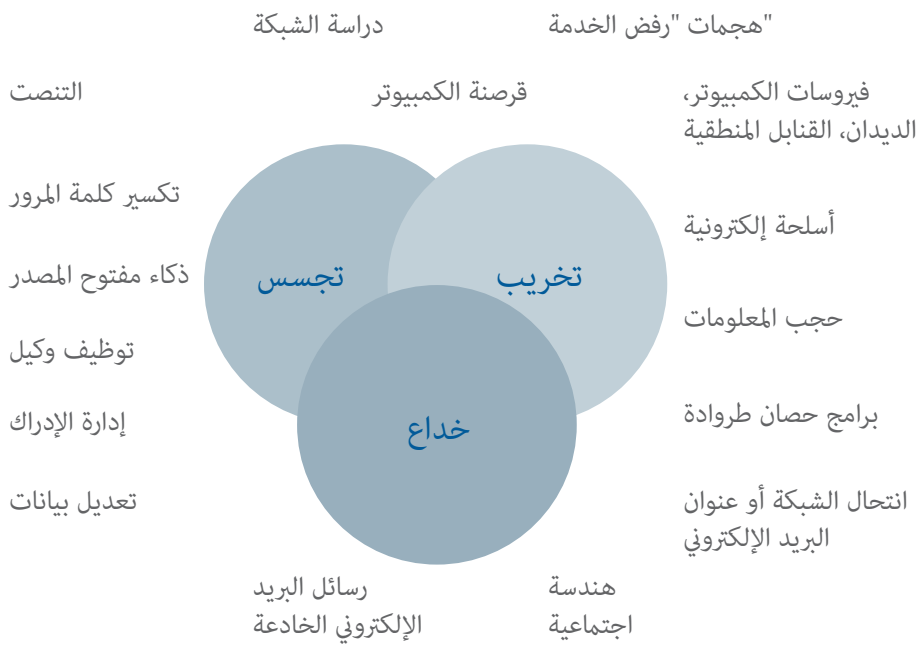
يَعِد عصر المعلومات بالاتصال الفائق ليس بين أجهزة الاستشعار والرماة والمركبات المأهولة وغير المأهولة فحسب، بل على نطاق أوسع بكثير ليشمل اللوجستيات والاستخبارات والسكان المدنيين أنفسهم، لذا، ما الذي يجب أن تتوقع القوات المشتركة مواجهته على مستوى التخطيط للقدرات وفي بيئات حرب المعلومات في إطار المضي قدمًا؟ سيتطلب هدف القوات المشتركة لتحقيق هيمنة المعلومات في العمليات متعددة المجالات أو في العمليات في جميع المجالات، استخدام مناهج وأدوات جديدة معقدة في مجال المعلومات الدولية كجزء من نظام بيئي أوسع لموارد المعلومات وقوة المعلومات، كما وستحتاج القوات المشتركة إلى التنسيق الوثيق مع الشركاء في عمليات الخداع والعمليات الإلكترونية المتصاعدة بل وحتى في الحملات الدعائية والأخبار الوهمية.

وستمتد التهديدات مثل برامج الفدية إلى شركاء سلسلة التوريد من طرف إلى جهات فاعلة غير حكومية ذات دوافع أيديولوجية من جهة أخرى. إنّ هذا التشعب لبيئة المعلومات إلى مجموعات فرعية أصغر وأصغر يخلق تحديات هائلة في محاولة تطوير حرب المعلومات في فراغ كامل للقوات المشتركة وفي الممارسة العملية لأدوات

مع مراعاة المتطلبات الاستراتيجية الطويلة الأجل إلى جانب فهم ما هو ضروري للغاية من الناحية التكتيكية لتنفيذ المهام التشغيلية بفعالية على المدى القصير.

وستستخدم حملات الحرب الإلكترونية بشكل متزايد الشبكات التجارية أو تعتمد عليها أو تتفاعل معها بطرق مهمة، بحيث ستشكل مثل هذه الشبكات والأدوات عائقًا أمام القوات المشتركة على مستوى استخدام أدوات الحرب الإلكترونية التقليدية وعمليات حرب المعلومات، فيما سيحتاج المخططون التشغيليون إلى التعامل مع مجموعة جديدة تمامًا من اللاعبين والشبكات والأنظمة وعوامل أخرى في ما يتعلق بالحرب وبدلاً من التخطيط للبعثات في فراغ، ستحتاج القوات المشتركة بشكل متزايد إلى الفهم والوعي والتنسيق العملي مع المزيد من الوكالات والجهات الفاعلة التجارية أكثر من أي وقت مضى، إذ سيشكل ذلك تحديًا شديد التعقيد لتطوير الأطر اللازمة للتعاون بهدف السماح بالتنسيق الفعال وتدفق المعلومات من وإلى القوات المشتركة مع، على سبيل المثال، وكالات الاستخبارات، وموردي الخدمات اللوجستية، وعناصر القوة المختلفة لشركاء التحالف، وغيرها.

حرب المعلومات على المستوى العملياتي



وثمة طرق عديدة للتفكير في العوامل التي ستؤثر على الاتجاه المستقبلي لحرب المعلومات. في البداية، هل هناك عنصر تشغيلي حقيقي لحرب المعلومات؟ إذا كان الأمر كذلك، فمن يمتلكه، وما مدى السيطرة والتأثير؟ لا ينبغي

إعادة تركيز حرب المعلومات للقوات المشتركة

إذا كانت مهمة القوات الجوية والبرية والبحرية مواجهة الأعمال التي تقوم بها القوات المعادية، فكيف ستتعامل هذه القوات مع مثل هذه المهام اليوم بالنظر إلى الطبيعة والنطاق الموسع لحرب المعلومات التي تؤثر على عملياتهم؟ لقد تم تصميم شبكات القتال لتكون موثوقة ومرنة وصارمة، وفي بعض الحالات، تكون هي الوسيلة الوحيدة للتواصل. ولكن ثمة العديد من جوانب حرب المعلومات التي يمكن للقوى المعادية أن تركز جهودها نحوها في سياق متعدد المجالات من أجل تعطيل العمليات اليوم أو التسبب بتدهورها أو تأخيرها- مثل اللوجستيات وسلسلة التوريد على سبيل المثال؛ فمع تحوّل القوات المشتركة نحو القدرات التشغيلية المدمجة عبر المجالات، والتي يتم تمكينها جوهريًا بواسطة مجال المعلومات، وهو مجال غامض بطبيعته ويجعل العالمين المادي والافتراضي غير واضحَين، ثمة حاجة متزايدة للاعتراف بكون حرب المعلومات بنفس مستوى أهمية الحرب الجوية أو البرية.

ويبدو هذا صحيح بشكل خاص حيث من المتوقع أن تتم معظم عمليات القوات المشتركة في بيئات شديدة التنافس وموزّعة حيث ستكون حرب المعلومات سمة متأصلة في مساحة المنافسة، ومع ذلك، مع الميزانيات المقيّدة والتهديدات المتزايدة ووجود المزيد من الجهات الفاعلة في نفس هذه الأماكن بالذات، يجد قادة القوات المشتركة أنفسهم في نقطة حاسمة لاتخاذ القرار، إذ ستحتاج القوة المشتركة إلى إيجاد طرق ووسائل وغايات جديدة لمعالجة كميات هائلة من المعلومات بسرعة والقيام بذلك جنبًا إلى جنب مع مجموعة أكبر من الشركاء والعملاء والمستهلكين لمصادر المعلومات وقواعد البيانات هذه، وكجزء من حرب المعلومات، ستصبح إدارة المعلومات والاتصال والتدفقات عناصر مهمة أساسية وستحتاج القوة المشتركة إلى التحوّل نحو واقع أكثر تكاملاً وترابطًا لدمج عناصر وطبقات جديدة حاسمة من الناحية التشغيلية في مجال المعلومات في دورة التخطيط والعمليات.

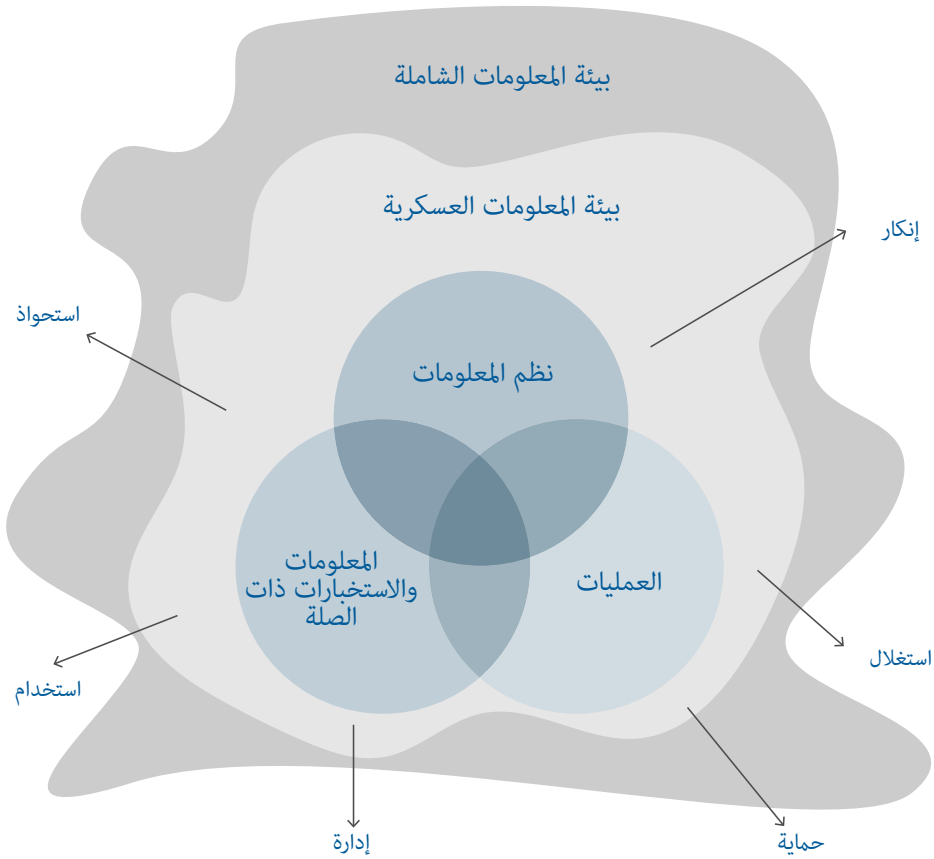
> لقد نمى نطاق حرب المعلومات وطبيعتها وخصائصها، ومع ذلك فهي لا تزال مفهومًا غامضًا وغير محدد المعالم من حيث التكتيكات والتقنيات والإجراءات (TTPs) وكذلك على مستوى الإستراتيجية الكبرى نفسها.

التفاعل والربط الخارجي في البحث عن هيمنة المعلومات

سيكون من الحيوي للقوات المشتركة أن تعالج مسألة ما إذا كان تركيزها يجب أن يكون أكثر على الهجوم أو على الدفاع. يتفق الكثيرون على أنّه يتعيّن على القوات المشتركة أن تطوّر توازن قدرات الحرب الهجومية والدفاعية وتحافظ عليه ولكن ثمة المزيد من القيود على هذه الأخيرة، إذ أنه في نهاية المطاف، ستحتاج القوات المشتركة إلى معالجة هذه المسائل من خلال تطوير مستوى الوضوح المتعلّق بنطاق أهدافها المستقبلية وقدراتها،

عدم القدرة على وضع حدود واضحة وتمويل مهام حرب المعلومات. إن المهام الموجهة ضد مجموعة متنامية من الوكالات الحكومية والعسكرية لن تؤدي إلا إلى إعاقة تطوير استراتيجية وطنية متماسكة ومتكاملة لهيمنة المعلومات التي يكون فيها الجيش بشكل عام والقوات المشتركة بشكل خاص أحد المكونات المتعددة، فعندما كانت قدرات القيادة والتحكم التشغيلية للقوات المشتركة أو مكوّناتها تحت قيادة "كل منهم" التي كان لها أنظمة اتصالات "خاصة بها" ، ولم يعد هذا هو الحال بالضرورة بعد الآن. اسأل على سبيل المثال من يتحكم في قوة المعلومات ومصادر المعلومات على المستوى الاستراتيجي؟ في حال لم تكن القوات المشتركة، فكيف يمكن أن تكون القوة المشتركة هي السلطة الرئيسية للقيادة والتحكم لحرب المعلومات؟

البيئة الإستراتيجية لحرب المعلومات



اختبار حرب المعلومات وتوظيفها بشكل متزايد وبطرق جديدة ومبتكرة، كما أنّه ثمة تواتر متزايد وتطوّر في استخدام حرب المعلومات من قبل القوات المشتركة الذي من شأنه أن يتسارع فحسب.

المعلومات قوة مشتتة

هناك قوة هائلة متأصلة في المعلومات، وبينما تشدد المناهج العسكرية "التقليدية" وتبحث عن خيارات "جديدة" لتأثير حرب المعلومات، فقد لا تعكس هذه الخيارات أفضل الحلول للقوات المشتركة أو تقدم المزايا الضرورية اللازمة لتحقيق السيطرة على المعلومات التي ترغب بها في بيئة تشغيلية ناشئة حيث يجري دمج الفضاء الإلكتروني في دورة التخطيط والعمليات بشكل جيد. لقد نمى نطاق حرب المعلومات وطبيعتها وخصائصها، ومع ذلك فهي لا تزال مفهومًا غامضًا وغير محدد المعالم من حيث التكتيكات والتقنيات والإجراءات (TTPs) وكذلك على مستوى الإستراتيجية الكبرى نفسها. لقد أدت ثورة المعلومات إلى تشكيل منظمات وفاعلين جدد بالإضافة إلى ظهور أهمية متزايدة للجهات الفاعلة التجارية وحتى غير الحكومية في المجال التشغيلي للقوات المشتركة "تقريبًا". نتيجة لذلك ثمة حاجة متزايدة للجمع بين هذه المجموعة المتنامية والمتباينة من أصحاب المصلحة والجهات الفاعلة النشطة عبر بيئة المعلومات وطيف الفضاء الإلكتروني والتي تؤثر في النهاية على مدى نجاح القوات المشتركة في تنفيذ مهامها.

وسيتطلب الوصول لهدف أن تصبح القوات المشتركة أكثر ديناميكية واستجابةً، أن تولّد هذه القوات صورة استراتيجية وتشغيلية "حقيقية" أكثر لتهديدات ومخاطر حرب المعلومات عبر بيئة المعلومات التي تتفاعل معها وتؤثر عليها - أو تتأثر بها. حيث أن تحرك النموذج الأمني بعيدًا عن المشهد الذي يهيمن عليه الجيش إلى مشهد جديد يكون أكثر تشتتًا ويمتد على مجموعة أوسع من أصحاب المصلحة والشركاء يوضح عدم ترابط حرب المعلومات على المستويين الاستراتيجي والتشغيلي للحرب. وبهدف فهم التغييرات الجارية الآن في البيئة الاستراتيجية والتشغيلية فعلًا، من الضروري فهم التحولات الهائلة التي حدثت في هياكل القوة الوطنية على مدى السنوات الأخيرة، إذ يُشار إلى أنّ المفارقة هي أنه نادراً ما تتواجد إدارة حكومية رسمية أو وكالة أو وحدة تشغيلية تركز فقط على قوة المعلومات وهي مكلّفة بمراقبة هذه المعلومات وتوزيعها، وإنّ الحقيقة هي أنّه يتم إضعاف قوة المعلومات عبر مجموعة واسعة من الوكالات والمنظمات.

> فمع تحوّل القوات المشتركة نحو القدرات التشغيلية المدمجة عبر المجالات، والتي يتم تمكينها جوهريًا بواسطة مجال المعلومات، وهو مجال غامض بطبيعته ويجعل العالمين المادي والافتراضي غير واضحَين، ثمة حاجة متزايدة للاعتراف بكون حرب المعلومات بنفس مستوى أهمية الحرب الجوية أو البرية.

إن المحاولات الآن للمطالبة أو وضع حدود حول ماهية عناصر قوة المعلومات ستكون غير مجدية للقوات المشتركة وللآخرين كذلك ثمة أسباب مقنعة لذلك، وهي التعامل مع التصنيف والعلاقات التنظيمية بالإضافة إلى

9

استمرارية المنافسة على هيمنة المعلومات: تطور حرب المعلومات ومستقبلها بالنسبة للقوات المشتركة

د. ادوين "لي" أرميستيد

رئيس تحرير، مجلة حرب المعلومات

من المفهوم عالميًا اليوم أن المعلومات هي القوة؛ وفي وقت قد تبدو هذه البديهية المعروفة مبتذلة، فقد شهدت القوات المشتركة ظروفًا سريعة التغير في بيئة حرب المعلومات (IW) في السنوات الأخيرة. تُمنح الأصول العسكرية للقوات المشتركة أو القطاعات المكوِّنة لها بشكل متزايد من خلال الاتصال على مستوى القوة أو في ما بين القطاعات والذي يتم تمكينه باستخدام الأدوات الناشئة في مجال الفضاء الإلكتروني ومع مفهوم السحب القتالية. ويطرح هدف تحقيق الهيمنة في بيئة المعلومات التي يمكن لأي شخص عمليًا الوصول إليها، تحديات جديدة ومعقدة في واقع ناشئ من الاتصال الفائق الذي يمتد عبر العالمين المادي والافتراضي، إذ يُعَد الانقسام بين القوات المشتركة التي لا تتمتع بمسؤولية أو سلطة فردية تجاه الحرب المعلومات، الهجومية والدفاعية، حاد بشكل خاص في سياق العمليات الناشئة حيث يتضح التوسع المتزايد للجهات الفاعلة واللاعبين أكثر فأكثر. وبالتالي، فإن المناهج المستقبلية لحرب المعلومات في العمليات المشتركة والموزعة عبر المجالات سوف تحتاج إلى تغيير جذري وإعادة موائمتها لتعكس هذه التحولات الأساسية في طبيعة المساحات العمليات للقوات المشتركة ونطاقها.

إن قدرة القوات المشتركة على تكييف الأنظمة والشبكات والأساليب التشغيلية للتنافس بشكل فعال في استمرارية المنافسة المستقبلية تستدعي إعادة تصور ما استنتجته التصنيفات مثل "بيئة المعلومات" و "حرب المعلومات" نفسها. فحتى اليوم ، يجب أن نسأل أنفسنا ما هي حرب المعلومات؟ وبماذا تختلف عن العمليات والأنشطة العسكرية التقليدية للقوات المشتركة؟ وكيف ستؤثر على **الإنشاءات** للقيادة والتحكم في جميع المجالات؟ ما هو موقع حرب المعلومات في الجهود الأوسع لبناء قوة قتالية مرنة وسريعة الحركة في المستقبل لتشمل مجال الفضاء الإلكتروني؟ هذه أسئلة محيّرة يجب أن تأخذ في عين الاعتبار وكيف تغيرت عناصر "القوة" الحيوية نتيجة لثورة المعلومات. إنّ إعادة التفكير في الإستراتيجية الكبرى في عالم اليوم هي المفتاح لفهم الطرق التي يجب على القوة المشتركة تكييف نهجها المستقبلي بحسبها في ما يتعلق بالعقيدة والتخطيط والعمليات. لقد تم

Research on Information والأمن السيبراني في الثورة الصناعية الرابعة ، Hershey، PA: IGI، pp. 141-164.

Volz، D. (2016) .قراصنة روس تعقبوا وحدات مدفعية أوكرانية باستخدام غرسة أندرويد: تقرير ، رويترز ، 22 ديسمبر. تم الوصول إليه في 29 سبتمبر 2021 من https://www.reuters.com/article/us-cyber-ukraine-idUSKBN14B0CU.

والتز ، إي (1998). حرب المعلومات: المبادئ والعمليات. بوسطن ولندن.Artech House

Wassel، P. (2018) 3 Military Applications of Internet of Things ،Augmate ،27 April.تم الوصول إليه في 25 سبتمبر 2021 من

https://www.augmate.io/3-military-applications-of-the-internet-of-things/.

Ween، A.، Dortmans، P.، Thakur، N.، and Rowe، C. (2019) .تأطير الحرب الإلكترونية: منظور محلل ، مجلة نمذجة الدفاع والمحاكاة: التطبيقات ، المنهجية ، التكنولوجيا 16 (3) ، 335– 345.

White، J. (2016) Dismiss، Distort، and Distract and Dismay: Continuity and Change in Russian Disin Information ،Policy Brief 2017/13 ،Institute for European Studies.تم الوصول إليه في 25 سبتمبر 2021 من https://www.ies.be/node/3689.

ويلشر ، ك. (2009). طائرات مقاتلة فرنسية أسقطت بسبب فيروس الكمبيوتر ، التلغراف ، 7 فبراير. تم الوصول إليه في 26 سبتمبر 2021 من http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html.

ساوث، ت. (2019). يشرح جنرال الجيش هذا من فئة 3 نجوم ما تعنيه العمليات متعددة المجالات بالنسبة لك ، وقت الجيش ، 11 أغسطس. تم الوصول إليه في 25 سبتمبر 2021 من https://www.armytimes.com/news/your-army/2019/08/11/this-3-star-army-general-explains-what-multi-domain-operations-mean-for-أنت./

ستينجل ، ر. (2019) حروب المعلومات: كيف خسرنا المعركة العالمية ضد المعلومات المضللة وما يمكننا القيام به حيال ذلك. لندن: كتب الأطلسي.

ستيرلينغ ب. تم الوصول إليه في 24 سبتمبر 2021 من https://www.wired.com/beyond-the-beyond/2019/04/deny-degrade-disrupt-deceive-destroy/.

Stone، A. (2018) يمكن أن تكون الإجابة على المشكلات اللوجستية في ساحة المعركة هي إنترنت الأشياء C4ISRnet ، 12 أكتوبر. تم الوصول إليه في 25 سبتمبر 2021 من https://www.c4isrnet.com/it-networks/2018/10/12/the-answer-to-battlefield-logistics-problems-could-be-iot/.

وزارة الدفاع البريطانية. (2018) الأنشطة السيبرانية والكهرومغناطيسية ، مذكرة العقيدة المشتركة 18/1. تم الوصول إليه في 24 سبتمبر 2021 من https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.

وزارة الجيش الأمريكية. (2014) الأنشطة الكهرومغناطيسية السيبرانية ، FM3-38. تم الوصول إليه في 24 سبتمبر 2021 من https://irp.fas.org/doddir/army/fm3-38.pdf.

فاليريانو ، بي ، جنسن ، بي ، ومانيس ، آر سي ، (2018) إستراتيجية الإنترنت: الطابع المتطور للقوة والإكراه. أكسفورد: مطبعة جامعة أكسفورد.

van Niekerk، B. (2015) "Information Warfare in the 2013-2014 Ukraine Crisis" ، in: Richet ، J. (ed.) ، Cybersecurity Policies and Strategies for Cyberfare Prevention. هيرشي ، بنسلفانيا: آي جي آي جلوبال ، ص 307-339.

van Niekerk، B. ، Pretorius ، B. ، Ramluckan ، T. ، and Patrick ، H. (2018) "The Impact of IoT on Information Warfare" ، in: Fields ، Z. (ed.) ، Handbook of

الأمن السيبراني للأقمار الصناعية يجب أن يكون ذا أولوية الحدود الجديدة / 164977./

هاتشينسون ، و. ، ووارن ، م. (2001). حرب المعلومات: هجوم الشركات والدفاع في عالم رقمي. أكسفورد وأوكلاند: بتروورث هاينمان.

كوب ، سي (2000). نموذج أساسي من Infowar ، الأنظمة: الحوسبة الشهرية للمؤسسات ، سيدني : Auscom Publishing، 46-55.

ليموس ، ر. (2021). توقع زيادة الهجمات على أنظمة الذكاء الاصطناعي ، القراءة المظلمة ، 27 أبريل. تم الوصول إليه في 5 أكتوبر 2021 من https://www.darkreading.com/vulnerabilities---threats/advanced-threats/expect-an-increase-in-attacks-on-ai-systems/d/d-id/1340833

Page، L. (2009). لا تزال شبكات وزارة الدفاع تعاني من البرامج الضارة بعد أسبوعين ، السجل ، 20 يناير. تم الوصول إليه في 10 سبتمبر 2021 من https://www.theregister.com/2009/01/20/mod_malware_still_going_strong/.

Pfleeger، P.، and Pfleeger، S. (2003). الأمن في الحوسبة ، الإصدار الثالث. نهر السرج العلوي ، نيو جيرسي: برنتيس هول.

Rajagopalan، R.P. (2019) الحرب الإلكترونية والسيبرانية في الفضاء الخارجي ، معهد الأمم المتحدة لبحوث نزع السلاح. تم الوصول إليه في 10 سبتمبر 2021 من https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf.

شواب ، ك. (2016) ، الثورة الصناعية الرابعة: ماذا تعني ، كيف تستجيب ، المنتدى الاقتصادي العالمي ، 14 يناير. تم الوصول إليه في 25 سبتمبر 2021 من https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

Seffers، G. I. (2017) الناتو يدرس تطبيقات إنترنت الأشياء العسكرية ، الإشارة ، 1 مارس. تم الوصول إليه في 25 سبتمبر 2021 من https://www.afcea.org/content/Article-nato-studying-military-iot-applications.

المراجع

بوردن، أ. (1999). ما هي حرب المعلومات؟ مجلة القوة الجوية والفضائية، 2 نوفمبر. تم الوصول إليه في 2 يوليو 2009 من : http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html.

برازول ، إم إس (2007). الآفاق المستقبلية لحرب المعلومات والعمليات النفسية على وجه الخصوص. في L. le Roux، رؤية جيش جنوب إفريقيا 2020 (ص 217 - 232). بريتوريا: معهد الدراسات الأمنية.

Cenciotti، D. (2017) Cybersecurity In the Sky: Internet of Things قدرات تجعل الطائرات أكثر عرضة للتهديدات السيبرانية أكثر من أي وقت مضى ، الطيران ، 20 يونيو. تم الوصول إليه في 26 سبتمبر 2021 من https://theaviationist.com/2017/06/20/cybersecurity-in-the-sky-internet-of-things-capabilities-to-make-aircraft-more-exposed-to-cyber-threats - أكثر مما سبق./

كونستانتين ، إل (2021) كيف يهاجم تسمم البيانات نماذج التعلم الآلي الفاسدة ، CSO Online، 12 أبريل. تم الوصول إليه في 5 أكتوبر 2021 من https://www.csoonline.com/article/3613932/how-data-poisoning-attacks-corrupt-machine-learning-models.html.

فيلد ، إم. (2017) الكتابة على الجدران على لافتات التوقف يمكن أن تخدع السيارات بدون سائق لدفعها بشكل خطير ، التلغراف ، 7 أغسطس. تم الوصول إليه في 5 أكتوبر 2021 من https://www.telegraph.co.uk/technology/2017/08/07/graffiti-road-signs-could-trick-driverless-cars-driving-dangerously/.

Fruhlinger، J. (2018) .شرح الروبوتات في Mirai: كيف أن المحتالين المراهقين وكاميرات الدوائر التلفزيونية المغلقة كادوا يتسببون في تدمير الإنترنت، CSO Online، 9 مارس. تم الوصول إليه في 29 سبتمبر 2021 من https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-bopped-down-the-internet.html .

Garner، T. (2020) لماذا يجب إعطاء الأولوية للأمن السيبراني عبر الأقمار الصناعية في New Frontier، NextGov، 1 مايو. تم الوصول إليه في 10 سبتمبر 2021 من https://www.nextgov.com/ideas/2020/05/w/

> نظرًا لنطاق العمليات متعددة المجالات، فمن الحكمة توسيع مستشعرات بنية "قتال سحابة- ضباب "لتشمل أجهزة استشعار في المجال الكهرومغناطيسي كجزء من مجموعة الموارد القتالية.

من المحتمل أن يساهم إنترنت الأشياء في ساحة المعركة (IoBT) إلى "التقارب" بين الإنترنت والحرب الإلكترونية وجهاز العمليات النفسية على المستوى التكتيكي؛ يناقش فان نيكيرك وبريتوريوس ورامالكان وباتريك (2018) بعض جوانب هذا التقارب في سياق عام. ذكر أعلاه إمكانية استخدام الإنترنت لحقن رسالة عمليات نفسية لاستهداف الطيارين؛ كذلك، يمكن استخدام الحرب الإلكترونية "للتغلب" على الاتصالات اللاسلكية لنقل رسائل عمليات نفسية إلى الأفراد. يمكن اعتبار هذا التقارب كنموذج متعدد الطبقات لحرب المعلومات حيث تستهدف الحرب الإلكترونية الطبقة المادية للشبكة، وتستهدف السيبرانية الطبقات والبروتوكولات الأعلى ، وخيار الحمولة للمكوِّن السيبراني هو توزيع رسائل عمليات نفسية.

ثمة جانب آخر يجب مراعاته وهو الخوارزميات التي يتم تنفيذها لتحليل البيانات وتشغيل المعدات العسكرية. نظرًا لكمية البيانات التي تنتجها المعدات الحديثة، فإنّه من المستحيل على البشر تحليلها بالكامل، وثمة حاجة إلى درجة من الأتمتة، يتم تنفيذها عادةً باستخدام الذكاء الاصطناعي. ومع ذلك، كانت هناك حالات توضح أن المدخلات المعدلة أدت إلى توفير الذكاء الاصطناعي لتصنيف غير صحيح (فيلد، 2017، ليموس، 2021). غالبًا ما يتم تنفيذ التقنيات الجديدة دون مراعاة الأمان، ولا يختلف الأمر مع الذكاء الاصطناعي. في المجال الأكاديمي، ثمة زيادة حادة في كمية الأبحاث التي تحقق في الهجمات على أنظمة الذكاء الاصطناعي بما في ذلك الهجمات العدائية للحث على مخرجات غير صحيحة، بالإضافة إلى تسمم البيانات (المعروف أيضًا باسم تسمم النموذج) الذي يفسد بيانات التدريب لإنتاج نموذج معيب (قسطنطين ، 2021 ؛ ليموس ، 2021). إن احتمال "خداع" الخوارزميات يمثل مصدر قلق خاص لأولئك الذين يحتاجون إلى اتخاذ قرارات القيادة بناءً على البيانات التي تم تحليلها وتقديمها لهم: هل يمكن الوثوق بالمعلومات حول ساحة المعركة؟ على مستوى أكثر تكتيكيًا، هل يمكن لمحطة طيار أو محطة تحكم على سفينة حربية أن تثق في المعلومات التي يتم عرضها؟ إنّ أي تردد أو قرار غير صحيح هو في النهاية هدف حرب المعلومات.

الخاتمة

تشمل العمليات متعددة المجالات جميع البيئات المادية ويمكن أن تمتد إلى المجالات الكهرومغناطيسية والسيبرانية أيضًا. يوفر إنترنت ساحة المعركة آلية لتحقيق عمليات متعددة المجالات من خلال أجهزة استشعار مدمجة توفر صورة مشتركة لبيئة (بيئات) التشغيل. ومع ذلك، فقد نُظر إلى إنترنت الأشياء بشكل عام على أنها عرضة للتسوية، ويمكن أن تؤدي ساحة المعركة شديدة الارتباط إلى زيادة سطح الهجوم لحرب المعلومات عبر المجالات المادية والكهرومغناطيسية والإلكترونية والمعرفية. يمكن أن تستهدف الهجمات البنية التحتية المادية والإشارات وبروتوكولات الشبكة والخوارزميات والبيانات وعلم النفس البشري.

يوضح الجدول 1 تهديدات "حرب المعلومات العامة" المحتملة ذات الصلة ببنية إنترنت الأشياء في ساحة المعركة السحابية.

الجدول 1: تهديدات حرب المعلومات على إنترنت الأشياء العسكرية

تهديدات مجال هندسة السحابة الضبابية
المستوى 3: التدمير المادي للسحابة للبنية التحتية للشبكة السحابية
هجمات حجب الخدمة الموزعة (DDoS) السيبرانية لزيادة التحميل على الشبكة السحابية
اختراق الشبكة لسرقة المعلومات
اختراق الشبكة للتلاعب بالمعلومات
اختراق الشبكة لتدمير المعلومات

المستوى 2: شبكة الضباب التدمير المادي للبنية التحتية لشبكة الضباب
التشويش الكهرومغناطيسي على أجهزة الاستقبال اللاسلكية بشبكة الضباب
هجمات حجب الخدمة الموزعة (DDoS) السيبرانية لزيادة التحميل على شبكة الضباب
اختراق الشبكة لسرقة المعلومات
اختراق الشبكة للتلاعب بالمعلومات
اختراق الشبكة لتدمير المعلومات

المستوى 1: التدمير المادي للمورد القتالي لأجهزة الاستشعار/ المعدات
التشويش الكهرومغناطيسي على الوصلات اللاسلكية بين الأجهزة
الطاقة الموجهة لتدمير الأجهزة الإلكترونية
البرامج الضارة السيبرانية على الأجهزة لتتبع الوحدات
البرامج الضارة لتقليل أداء المعدات
اختراق النظام لمعالجة معلومات المستشعر
إرسال رسائل العمليات النفسية المعرفية إلى الأجهزة

بشكل عام ، قد يؤدي إنترنت الأشياء في ساحة المعركة إلى ازدحام طيف الكهرومغناطيسي وشبكة بسبب زيادة عدد الإشارات الكهرومغناطيسية وكمية البيانات التي يتم نقلها. وهذا بدوره قد يزيد من قابلية التعرض لهجمات الحرب الإلكترونية وهجمات هجمات حجب الخدمة الموزعة(DDoS) حيث يمكن أن تقدم كل إشارة نفسها على أنها "ضوضاء" لبعضها البعض، وسيؤدي التشويش إلى زيادة مستوى "الضوضاء" هذا لتقليل فعالية روابط الاتصال أو تعطيلها. بطريقة مماثلة، كلما اقتربت كمية البيانات من "عتبة" الشبكة، كلما كانت أكثر عرضة للفيضان والارتباك من قبل حركة المرور الضارة.

تشتمل الطبقة الثانية من هندسة رين وهوز (2018) على "طبقة ضبابية" للحوسبة والتخزين الموزع المحلي. تتكون الطبقة الثالثة بعد ذلك من الحوسبة السحابية، مع مساحة تخزين أكبر وتتألف من روابط "شبكة ضبابية" متعددة. يمكن التفكير في أن شبكة الضباب تخدم المستويات التكتيكية والتشغيلية للقيادة والتحكم بينما تخدم الشبكة السحابية المستويات التشغيلية والاستراتيجية للقيادة والتحكم.

نظرًا لنطاق العمليات متعددة المجالات، فمن الحكمة توسيع مستشعرات بنية "قتال سحابة- ضباب "لتشمل أجهزة استشعار في المجال الكهرومغناطيسي كجزء من مجموعة الموارد القتالية.

يجب أيضًا توفير المراقبة في المجال السيبراني عبر بنية سحابة قتال للمساعدة في الأمن السيبراني. تم تسجيل حوادث تتعلق بتأثر الوحدات العسكرية و/ أو المعدات العسكرية "المتصلة" بالحوادث الإلكترونية: في عام 2009 تم الإبلاغ عن أن البرمجيات الخبيثة المتنقلة قد أثرت على السفن الحربية والمطار العسكري (بايدج، 2009؛ ويلشر، 2009)، تم استخدام البرمجيات الخبيثة المتنقلة في وحدات مدفعية المسار (فولز، 2016). وثمة الآن مخاوف متزايدة بشأن التهديدات الإلكترونية والكهرومغناطيسية للأقمار الصناعية والأنظمة الفضائية (غارنر، 2020، راجاغوبالان، 2019). تم استخدام أجهزة إنترنت الأشياء التي تم اختراقها لإطلاق هجمات حجب الخدمة الموزعة (DDoS) وكانت من بين أكبر الهجمات التي تم تسجيلها وقت حدوثها (فروهلنغر، 2018).

تشير مثل هذه الحوادث والمخاوف الأوسع المتعلقة بأنظمة المعلومات والأمن إلى المخاطر الكامنة في الأنظمة شديدة الترابط. يوضح فان نيكيرك، بريتوريوس، راملومان، وباتريك (2018) كيف يمكن استخدام حرب المعلومات لاستهداف إنترنت الأشياء والبشر من خلال إنترنت الأشياء الضعيفة. يمكن تطبيق العديد من هذه الهجمات النظرية على السيناريوهات العسكرية، مثل:

- يمكن أن تؤدي البرامج الضارة الماسحة أو برامج الفدية التي تدمر البيانات وبرامج النظام إلى تأثيرات كارثية على الطائرات أو الغواصات المغمورة، على سبيل المثال ؛
- يمكن أن يؤدي حقن رسائل عمليات نفسية في شاشات العرض العلوية للطيارين إلى تشتيت انتباه الطيار وإرباكه من خلال الإشارة إلى أن أنظمة الطائرات معرضة للخطر وتؤثر سلبًا على عملية اتخاذ القرار ذات الأهمية الزمنية.
- تتلاعب الهجمات الإلكترونية بمصفوفات أجهزة الاستشعار (على سبيل المثال، مجموعة السونار أو رادار الدفاع الجوي) بشكل عشوائي لتوفير أهداف خاطئة وإخفاء أهداف فعلية، وبالتالي تشويه منظر ساحة المعركة ؛
- استخدام البرمجيات الخبيثة ووسائل التواصل الاجتماعي على هواتف الأفراد العسكريين لتحديد عمليات الانتشار وبالتالي توليد المعلومات الاستخبارية المتعلقة بالعمليات.

الوعي الظرفي على المستوى التكتيكي، الاستهداف ؛ مراقبة حالة المركبة والجندي ؛ الرعاية الطبية في ساحة المعركة وحتى المراقبة البيئية (سيفيرز، 2017).

يقترح رين وهو (2018) بنية "قتال سحابة- ضباب" بثلاثة طبقات. تشمل فئة "الموارد القتالية" المعدات العسكرية مثل المنصات وأجهزة الاستشعار في المجالات المادية الأربعة التقليدية. يستخدم شينشيوتي (2017) مثالًا لطائرة F-35 تحمل على متنها مستشعرات لجمع المعلومات حول بيئاتها والتهديدات المحتملة؛ بالإضافة إلى مستشعرات داخلية لمراقبة أدائها، وبالتالي يمكن اعتبارها "شيئًا" على الإنترنت، ولكن أيضًا كمجموعة من أجهزة الاستشعار. يعتبر فاليريانو، جنسن، ومانس (2008) أنطائرة F-35 مكافئة لخادم الكمبيوتر. يشير هذا إلى التعقيد المتزايد للأنظمة العسكرية الحديثة، والاعتماد على المعلومات الرقمية، وكمية البيانات التي يمكن إنشاؤها (المتعلقة بالمفاهيم المرتبطة بـ "البيانات الضخمة").

الشكل 2: "أركان" حرب المعلومات

الواضح للمعلومات المنسّقة والعمليات البدنية في أوكرانيا، على الرغم من عدم تحقيق نصر "حاسم (فاليريانو، جنسن، ومانيس، 2008، فان نيكيرك، 2015).

عادةً ما يكون لحرب المعلومات الهجومية أحد عناصر الخمسة التالية: الحرمان أو التحطيم أو التعطيل أو الخداع أو التدمير (ستيرلينغ، 2019) كهدف استراتيجي أو تشغيلي؛ ومع ذلك، اقترح آخرون أيضًا أهدافًا مثل:

- التعطيل ، والإنكار ، والتدمير ، والتلاعب ، والسرقة (هاتشينسون ووارن، 2001)،
- التحطيم والإنكار والفساد والاستغلال (بوردن، 1999، كوب، 2000)،
- المقاطعة والتعديل والتلفيق والاعتراض (بفيلغير وبفيلغير، 2003)

في نهاية المطاف، يتم استهداف صنع القرار البشري على المستويات التكتيكية والتشغيلية والاستراتيجية؛ ومع ذلك ، فإن الصراع من خلال الفضاء الإلكتروني وبيئة المعلومات يستهدف بشكل متزايد اتخاذ القرارات المجتمعية والسياسية والاقتصادية وكذلك العمليات العسكرية أو المشغلين العسكريين. مع التركيز المتزايد على حملات التضليل والتأثير من قبل الجهات الفاعلة الحكومية وغير الحكومية، لا سيما من خلال مواقع "الأخبار" عبر الإنترنت ووسائل التواصل الاجتماعي، تمت إعادة صياغة المزيد من أهداف حرب المعلومات على المستوى الاستراتيجي الأعلى إلى 4 عناصر: الاستبعاد ، التشويه ، صرف الانتباه والترهيب (وايت، 2016). تستهدف مثل هذه الأنواع من العمليات "إرادة" السكان أو السياسيين، وتهدف ، جنبًا إلى جنب مع العناصر الأكثر تركيزًا على العمليات من الحرب العالمية الثانية في ساحة معركة معيّنة، إلى تقليل أو إزالة الدعم الشعبي أو

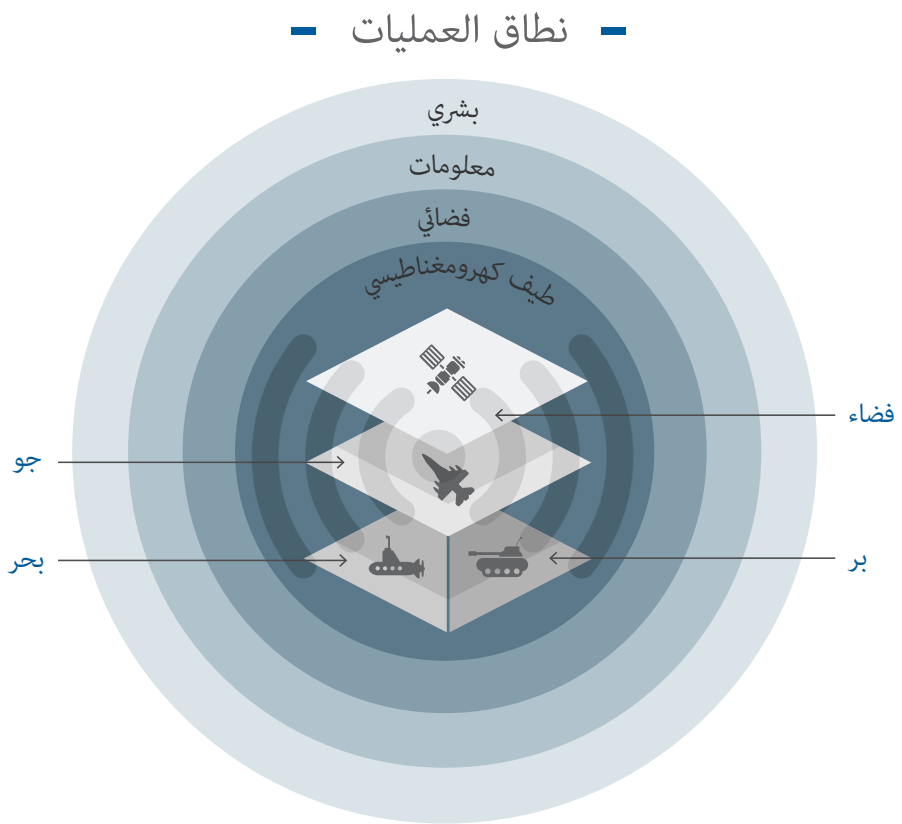
> يمكن التفكير في أن شبكة الضباب تخدم المستويات التكتيكية والتشغيلية للقيادة والتحكم بينما تخدم الشبكة السحابية المستويات التشغيلية والاستراتيجية للقيادة والتحكم.

السياسي تجاه نزاع أو أهدافه العسكرية.

إنترنت الأشياء وحرب المعلومات

يشير وكاستيغلون، شو، نابيوريكيادي (2017: 6) إلى أن ساحة المعركة قد شهدت "عددًا متزايدًا من أجهزة الاستشعار والحاسوب في كل مكان التي يرتديها الأفراد العسكريون والمدمجة في المعدات العسكرية". أفادت التقارير أن الناتو كان يجري تحقيقات حول الفوائد المحتملة لإنترنت الأشياء للجيش في مجالات مثل الوعي الظرفي والمراقبة والخدمات اللوجستية والتطبيقات الطبية والعمليات الأساسية وإدارة الطاقة (سيفيرز، 2017، ستون، 2018، واصل، 2018). تمتلك إنترنت الأشياء العسكرية/ إنترنت الأشياء في ساحة المعركة أيضًا إمكانات هائلة لدعم القيادة والتحكم في العمليات متعددة المهام من خلال "الدعم اللوجستي للعمليات المشتركة؛

تتألف حرب المعلومات ، في شكلها السابق ، من عمليات يمكن أن تؤثر على المعلومات و/ أو تحميها عبر المجالات المادية والافتراضية والمعرفية (برازولي، 2007، والتز، 1998). تضمنت "ركائز" حرب المعلومات الحرب الإلكترونية (EW)، والعمليات الإلكترونية، والعمليات النفسية (PSYOP) والاستخبارات والحرب المتمركزة حول الشبكة أو حرب البنية التحتية للمعلومات، وحرب القيادة والتحكم (برازولي، 2007)



الشكل 1: مجالات العمليات

يميل الاستخدام الحديث لمصطلح "حرب المعلومات" إلى الإشارة أكثر إلى الجوانب المعرفية، مثل المعلومات المضللة وحملات التأثير، والتي غالبًا ما تكون مدفوعة بوسائل التواصل الاجتماعي والرسائل الفورية (ستينغل، 2019). تركز المناقشات الناشئة على "التقارب" بين الحرب الإلكترونية والإنترنت في ما يعرف بالأنشطة الإلكترونية الكهرومغناطيسية (CEMA) (وزارة الدفاع البريطانية، 2018؛ وزارة الجيش الأمريكية، 2014). ومع ذلك ، يمكن مناقشة تقارب أكبر بين ركائز الحرب العالمية الثانية بشكل خاص بالنظر إلى النجاح

(IoBT)أو "إنترنت الأشياء العسكرية" (IoMT) (كاستيغليون، شو، نابي، وريكيادي 2017). إنّ تطبيقات إنترنت الأشياء في الجيش تتمتع بالقدرة على دعم القيادة والتحكم (C2) للعمليات متعددة المجالات (MDO) في مجموعة من المجالات (سيفيرز، 2017). وعليه، يمكن اعتبار أن العمليات متعددة المجالات في المستقبل تشتمل على ساحة معركة شديدة الارتباط تؤدي إلى زيادة سطح الهجوم لحرب المعلومات (سينشيوتي، 2017: فان نيكيرك، بريتوريوس، راملوكان وباتريك، 2018). تتم في هذه المقالة دراسة الحرب الإلكترونية في سياق كل من العمليات متعددة المجالات وإنترنت الأشياء في ساحة المعركة (IoBT).

العمليات متعددة المجالات وحرب المعلومات

تشمل المجالات "المادية" التقليدية للعمليات العسكرية الأرض والبحر والجو والفضاء؛ ومع ذلك ، ثمة حاجة متزايدة للسيطرة على الطيف الكهرومغناطيسي (EMS) ، والبيئة السيبرانية، وبيئة المعلومات الأوسع (وين، دورتمانز، تاكور، وروي، 2019). تم وصف نهج العمليات متعددة المجالات بأنه "مفهوم القتال المشترك الذي سيحمل كل القوة النارية والحركية وغير الحركية على حد سواء" لتوفير التفوق عبر ساحة المعركة بطريقة غير مسبوقة (ساوث، 2019).

يوضح الشكل 1 مجالات تشغيلية متعددة: المجالات "المادية" الأربعة موضحة في وسط الشكل؛ عادة ما تكون هذه المجالات متنقلة وتتواصل من خلال وسائط البث على ترددات مختلفة (EMS). يصبح الفضاء الإلكتروني امتدادًا لذلك، حيث يوفر آليات نقل البيانات والمعلومات، مثل بروتوكولات الشبكات. ففي حين يُعتبر مجال المعلومات المعاصر مطابقًا تقريبًا للفضاء السيبراني، فإن بيئة المعلومات أوسع وتتضمن معلومات مطبوعة ومعرفية أيضًا. تدعم كل هذه العناصر العنصر البشري، الذي يشمل عمليات صنع القرار الإستراتيجي والتكتيكي (على سبيل المثال، القيادة والتحكم) لقادة الحرب والقادة ولكنه يمتد على نطاق أوسع ليشمل المجتمع والاقتصاد والسياسة.

> إن احتمال "خداع" الخوارزميات يمثل مصدر قلق خاص لأولئك الذين يحتاجون إلى اتخاذ قرارات القيادة بناءً على البيانات التي تم تحليلها وتقديمها لهم: هل يمكن الوثوق بالمعلومات حول ساحة المعركة؟ على مستوى أكثر تكتيكيًا، هل يمكن لمحطة طيار أو محطة تحكم على سفينة حربية أن تثق في المعلومات التي يتم عرضها؟ إنّ أي تردد أو قرار غير صحيح هو في النهاية هدف حرب المعلومات.

8 حرب المعلومات وساحة المعركة المتصلة

د. بريت فان نيكيرك
أستاذ محاضر كبير، جامعة كوازولو ناتال

مقدمة

تمتد الثورة الصناعية الرابعة (4IR) من ثورة المعلومات (الثورة الصناعية الثالثة) مع درجات متزايدة من التكامل بين الأنظمة السيبرانية والفيزيائية والبيولوجية. ومن المتوقع أن تؤثر الثورة الصناعية الرابعة على جميع القطاعات، بما في ذلك طبيعة الصراع (شواب، 2016). تتضمن المفاهيم الأساسية التي تشكل جزءًا من الثورة الصناعية الرابعة على سبيل المثال لا الحصر:

- علم البيانات وتحليلات البيانات الضخمة ، التي غالبًا ما تكون مدفوعة و/ أو مؤتمتة بواسطة الذكاء الاصطناعي والتعلم الآلي؛
- الحوسبة السحابية وتوفير موارد حوسبة يمكن الوصول إليها عن بعد؛
- إنترنت الأشياء (IoT) ، حيث يمكن للأجهزة شديدة الاتصال أن تعمل كمستشعرات وكمحركات لإنتاج كميات كبيرة من المعلومات والترابط السيبراني الفيزيائي؛
- الواقع المعزز، تراكب المعلومات على النظارات أو الخريطة أو الصورة؛
- الأمن السيبراني، بسبب نقاط الضعف التي أُدخِلت عن طريق ربط الأجهزة "غير التقليدية" غير الآمنة بالشبكات.

كانت بعض مفاهيم الحرب الصناعية الرابعة موجودة في الإعداد العسكري بشكل ما، مثل الواقع المعزز المشابه لشاشات العرض التي يتم وضعها على الرأس، ويطوّر مفهوم إنترنت الأشياء الحرب المركزية على الشبكة (أو كما يسميها "واصل 2018، " حرب البيانات" وهو ما أصبح يُعرف باسم "إنترنت الأشياء في ساحة المعركة" "

جهات فاعلة عسكرية جديدة في الفضاء وظهوره كمجال تشغيلي متنازع عليه بشكل متزايد، لم يعد من الممكن استغلال الفضاء في غياب مجموعة دنيا من القواعد ضمن مستوى مقبول من المخاطر.

الخاتمة

إن اتساع نطاق التهديدات - عبر المجالات بشكل متزايد في الطبيعة - والتسارع في صنع القرار العسكري المطلوب نظرًا للزيادات الهائلة في البيانات المنتجة أو التي أصبحت متاحة يؤدي إلى تفاقم التحديات المستقبلية للمحاربين. سوف تحتاج الحرب الهجينة والمنافسة العسكرية دون عتبة الصراع المفتوح إلى أنظمة تدعم المخططين والمشغلين العسكريين بالإنذار المبكر والوعي بالأوضاع الفائقة واتخاذ القرار الفوري، وسيكون الوصول السريع إلى المعلومات حيث يتم ضمان النزاهة أمرًا حاسمًا للنجاح الاستراتيجي. يلعب مجال الفضاء دورًا حيويًا من خلال توفير كل هذه الضرورات الاستراتيجية.

ويأتي الوصول إلى مجال الفضاء مع تحديات كافية من تلقاء نفسه ولكن في سياق الاستخدام العسكري للفضاء يجب التفكير في المزيد. ومع ذلك، فإن الاعتماد على المجال الفضائي واستخدامه أمر لا مفر منه، كما ويجب أن يطبق تخطيط القدرة على الفضاء الأساسيات لتقديم حلول تقنية للتحديات الاستراتيجية وتوليد مزايا جديدة من خلال التعاون الدولي الذي يساعد في الاستخدام غير المزعج للفضاء للعمليات العسكرية. ففي نهاية المطاف، وعلى الرغم من ذلك، لا ينبغي أن يضيع على الجيوش التفكير في كيفية التفاوض بشأن فقدان الوصول إلى البنية التحتية الفضائية الحيوية. في الوقت الذي يعتبر فيه الوصول إلى الفضاء أمرًا مفروغًا منه ، قد يلزم الحفاظ على الفنون العسكرية للخريطة وقراءة البوصلة والتوجيه الميداني والملاحة والتشغيل بدون اتصالات لفترة أطول.

التصميم والاستجابة والقدرة على التكيف مع الحمولة

في حالة فقدان الأقمار الصناعية نتيجة الأعمال الهجومية من قبل الخصم أو الظروف الطبيعية وحتى الحوادث فإنّه سيكون من الضروري استبدال أي قدرة مفقودة في أقصر وقت ممكن - بنظام مماثل أو محسّن. في الواقع، يكمن مستقبل الأقمار الصناعية في الأقمار الصناعية الدقيقة أو النانوية التي تكون أقل تكلفة على مستوى بنائها وإطلاقها مقارنة بأنظمة الفضاء القديمة. عندما تظهر الحاجة إلى وظائف ومتطلبات جديدة، ستخلق تقنيات الفضاء الجديدة طرقًا جديدة لتقديمها بطرق أكثر استجابة. يجب أن تكون الاستجابة في التصميم والتصنيع والاختبار والإجراءات والإطلاق معايير أساسية لتخطيط القدرات الفضائية وستحتاج إلى دعم من خلال التعاون الوثيق والمستمر مع شركاء الصناعة والمعرفة.

وعند تصميم الأقمار الصناعية وأنظمة الفضاء الجديدة، قد يحتاج تطوير التطبيقات الجديدة إلى الانتشار من أجل بناء وإطلاق الأقمار الصناعية بشكل أسرع وأكثر فعالية من حيث التكلفة. إن تنفيذ المتطلبات الجديدة والمتطورة باستمرار من خلال برامج التطوير أمر غير معقول ويجب أن تصبح الجيوش أفضل في دفع هذه المتطلبات نحو التكرارات المستقبلية. يمكن أن يؤدي التغيير والتعديل المستمر في برامج تطوير المساحات إلى زيادة التكلفة والتأخير في الوقت. بدلاً من ذلك، يجب أن يكون التركيز على جعل الأقمار الصناعية أكثر نمطية أو قبولًا للتكيف بحيث يمكن تعديل وظائفها دون تكلفة أو وقت أو تعقيد كبير. إذا تم بناء نمطية عالية وقابلية للتكيف في الجيل الحالي من الأقمار الصناعية قيد التطوير، فإنّه سيتم تحسين قابليتها للاستخدام وإطالة عمرها بشكل كبير.

> من المرجح أن تستمر العوامل الجيوسياسية في إدخال لاعبين جدد في الإطار لمتابعة الاستخدام الاستراتيجي والتكتيكي للفضاء وتشغيل الأقمار الصناعية وتطوير البنية التحتية التمكينية الأرضية.

التعاون الدولي والنظام القائم على القواعد في الفضاء

بالنسبة للجيوش الأصغر وخاصة تلك التي تتعاون تحت مظلة أمنية مشتركة ، فإن تقاسم الأعباء من خلال تقسيم المسؤوليات والقدرات أمر مقنع من الناحية الإستراتيجية. سيكون تجميع الأصول والقدرات واستخدامها بشكل مشترك سمة حاسمة لتطوير القدرات الفضائية التي ستعتمد على النتائج الناجحة في التعاون الدولي. سيحتاج التعاون الدولي فيما يتعلق باستخدام الفضاء أيضًا إلى معالجة النطاق الواسع للحرية الموجودة حاليًا لأي فاعل في الفضاء في غياب قواعد السلوك، وحتى الآن، يبدو أن العدد المحدود من الدول ذات القدرات الفضائية المتقدمة كان مترددًا في إنشاء المزيد من الأطر الملموسة ووضع قواعد طويلة الأجل في ما بينها لتجنب إعاقة النطاق المستقبلي للإمكانيات الاستراتيجية. ولكن مع تزايد الازدحام في المدار الأرضي المنخفض، وظهور

من خلال الاتصال البصري أو علم التشفير أو قفز التردد أو الإرسال الراديوي المحدد إلى إبرازها كمعامل حيوي لتصميم القدرة.

ومن المرجح أيضًا أن تصبح الأقمار الصناعية نفسها موضوعًا لمناورات وأعمال هجومية لجعلها أقل فائدة أو حتى عديمة الفائدة. يجب أن تبدأ الجهات العسكرية الفاعلة في الفضاء في النظر في كيفية حماية الأصول الفضائية من الهجمات الفعلية، والتعرض لإشعاع عالي الطاقة، والتلاعب الكهرومغناطيسي، ومجموعة من التهديدات الجديدة الناشئة من الأرض، ومعالجتها. يجب تطوير وتنفيذ الغلافات والطبقات الخاصة وأجهزة الاستشعار التي تكشف أي تلاعب بالأنظمة وتعزّز الإجراءات الدفاعية والمضادة المناسبة.

إدراك الواقع الميداني الفضائي (SSA)، وإدارة حركة المرور في الفضاء والقدرة على المناورة

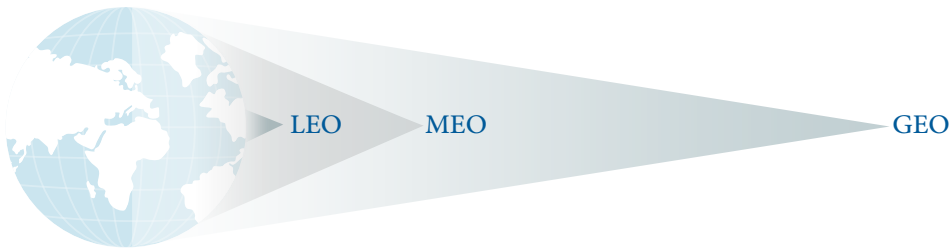
يدعم نظام الواقع الميداني الفضائي (SSA) صورة دقيقة في الوقت الفعلي للمجال الفضائي ويتيح رؤى ممكنة للأحداث غير المتوقعة أو غير العادية. باستخدام نظام الواقع الميداني الفضائي (SSA)، يمكن لمشغلي الأقمار الصناعية مراقبة أصولهم والتحكم بها بشكل أفضل بهدف حمايتها من التهديدات المحتملة ومخاطر الاصطدام- لا سيما لأنها تنطبق على التنقل في الحطام الفضائي في المدار الأرضي المنخفض. سيكون التكوين الضروري لأجهزة الاستشعار وتقنيات معالجة البيانات قادرًا على توفير إنذار مبكر ضد التدخل المحتمل للفقاعات الآمنة للأقمار الصناعية بالإضافة إلى جعل الإسناد ممكنًا، وفي السيناريو الناشئ، سيكون إنكار المناورات والإجراءات الهجومية أمرًا غير وارد نظرًا لأن الإسناد الدقيق أصبح ممكنًا،كما ويمكن من الناحية المنطقية فرض نموذج أقوى للردع.

فمن خلال توفير صورة أكثر دقة لحساب الفضاء والقرب، سيصبح من الممكن تحديد الإجراءات المناسبة للنظر فيها ومتابعتها بطرق أكثر دقة على مستوى الوقت، بالإضافة إلى التطوير الفعال لنظام إدارة الحركة الفضائية. سيؤدي تحسين نظام إدراك الواقع الميداني الفضائي (SSA) إلى تصغير حجم الفقاعة الآمنة للقمر الصناعي عند تكوينها، وهذا بدوره سيقلل من الميل إلى المناورة المراوغة مع توفير طرق أكثر أمانًا لتحقيق التنقل الآمن والتنقل في الفضاء والحفاظ عليهما. يشار إلى أنّه سيتم تعزيز أمن الأنظمة الفضائية وإطالة عمر الأقمار الصناعية ودعم التخطيط الأفضل لعمليات الاستبدال والتحديث والإدماج الجدي، من خلال تمكين إدارة حركة المرور في الفضاء.

إلى ذلك، يعد تعزيز قدرة الأقمار الصناعية على المناورة إجراء دفاعي ضروري لتعزيز حمايتها وقدرتها على البقاء. إنّ نفس مستوى فائدة القدرة على المناورة ينطبق على الوحدات الأرضية حيث سيعزز التنقل الحماية ولكن حيث سيتعين معالجة مجموعة أكثر تعقيدًا من التحديات مثل التزوّد بالوقود، والتكتيكات والتقنيات والإجراءات (TTPs).

وإصلاحها أو استبدالها إذا لزم الأمر. في حين أن هذا قد يبدو في البداية استجابة أقل تعقيدًا ومنخفضة التكلفة لتقليل نقاط الضعف للعمليات الفضائية العسكرية، فمن الضروري عدم السماح لهذا العنصر من القوة الفضائية المستقبلية وتخطيط القدرات بالهروب من التصميم الاستراتيجي وعملية التخطيط.

الأقمار الصناعية MEO, GEO وLEO



	المدار الأرضي الثابت بالنسبة للأرض GEO (~36,000كم)	مدار أرضي متوسط MEO (~8,000كم)	مدار أرضي منخفض LEO (~1,000كم)
وقت الإستجابة	أعلى	متوسط	قليل
تغطية الشبكة العالمية	3 أقمار صناعية (99%)	6 أقمار صناعية (96%)	1000 (100%)
بوابات البيانات	قليل ، ثابت	متعددة ومرنة	عديدة، محلية
الاستعداد التكنولوجي	مثبت	مثبت	مستجدة
دورة الحياة	15 سنة	12 سنة	7 سنة

إنّ الطيف الآخذ في الاتساع من التهديدات في الفضاء ليس شاملاً. في الوقت الحالي، تتعلق هذه التهديدات بشكل أساسي بالأصول الفضائية في المدار الأرضي المنخفض.

عندما يلتقي الفضاء الإلكتروني بالفضاء، تظهر ثغرة مزدوجة، خاصة على مستوى الاتصالات العسكرية. وتعتبر قنوات القيادة والتحكم (C2) والمعلومات بين الأصول الأرضية والفضائية شديدة الحساسية حين يتعلق الأمر بتزوير والاضطراب والتشويش وغير ذلك من أشكال التداخل. سيحتاج تأمين تدفق البيانات والمعلومات

القريبة نتيجة لنيّة هجومية مصمّمة على جعل الأقمار الصناعية غير موثوقة أو غير جديرة بالثقة أو حتى غير صالحة للاستخدام تمامًا.

> سيحتاج تأمين تدفق البيانات والمعلومات من خلال الاتصال البصري أو علم التشفير أو قفز التردد أو الإرسال الراديوي المحدد إلى إبرازها كمعامل حيوي لتصميم القدرة.

لا يبدو أن المواجهات والعمليات عن قرب التي لوحظت مؤخرًا قد أحدثت أي ضرر مرئي ، لكن هذه الحوادث دفعت الجهات العسكرية في الفضاء إلى إعادة التفكير في مواقفها والنظر في آليات تعزيز حماية أصولها - بما في ذلك ، من خلال التسليح المحتمل. في ديسمبر 2019، أقر الناتو صراحةً بالفضاء كمجال للعمليات العسكرية. من المعروف أن الأسلحة المضادة للأقمار الصناعية (ASAT) قد تمت تجربتها على نطاق واسع ومن المرجح أن يتم تطويرها بسهولة أكبر كطريقة لإدخال منطق الردع والحرمان في المجال الفضائي ضد الخصم الذي قد يسعى إلى استغلال الثغرات الأمنية في نظام الفضاء القديم.

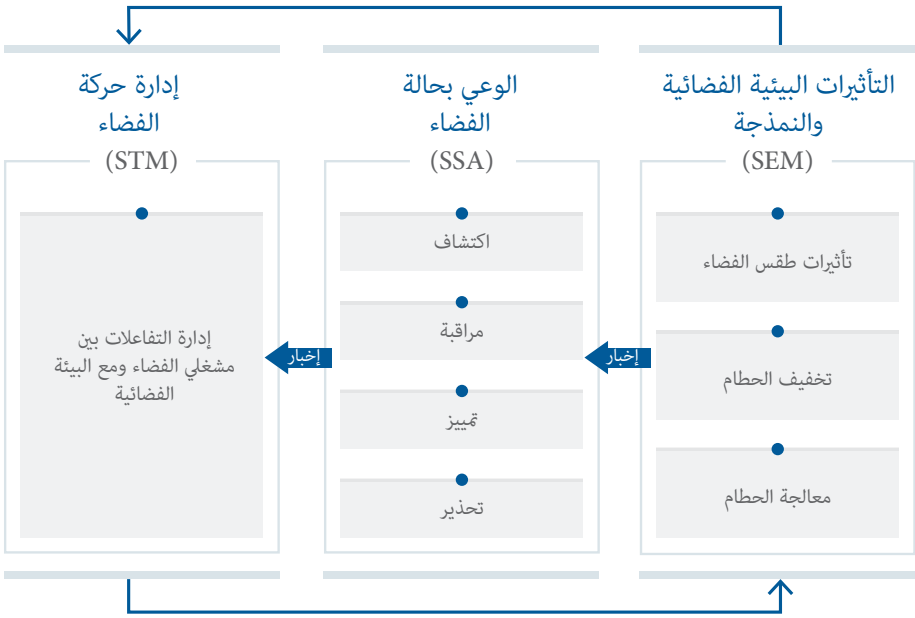
وثمة تداعيات كبيرة على مثل هذه المسارات بسبب العواقب غير المقصودة والآثار الثانوية التي قد تولدها مثل هذه التطورات، على أدنى مستوى من خلال خطر انتشار الحطام الفضائي عبر مساحات كبيرة من الفضاء. سيسعى المعارضون في الفضاء أيضًا إلى استهداف مرحلات الاتصالات الحرجة بين الأقمار الصناعية والبنية التحتية الأرضية الداعمة أو مراكز القيادة. كما ويمكن للخصوم الأقل تقدمًا من الناحية التكنولوجية مهاجمة البنية التحتية الأرضية الداعمة للعمليات الفضائية، مثل منع الوصول الفعلي أو قطع كابلات الطاقة أو حتى الهجمات الفعلية والتدمير أو حتى تعطيل بنيتها.

إنّ الطيف الآخذ في الاتساع من التهديدات في الفضاء ليس شاملاً. في الوقت الحالي، تتعلق هذه التهديدات بشكل أساسي بالأصول الفضائية في المدار الأرضي المنخفض. ثمة سلسلة من الردود الدفاعية المتاحة من المخططين العسكريين والتي تركز على بيئة المدار الأرضي المنخفض، كتشديد دعم البنية التحتية الأرضية، وقنوات الاتصال من الأرض إلى الفضاء (والعكس بالعكس) وكذلك الأصول الموجودة في الفضاء أنفسهم وتمكينها. بالإضافة إلى ذلك، سيحتاج المخططون العسكريون إلى إيجاد طرق ووسائل جديدة لتحسين الواقع الميداني الفضائي، وإدارة حركة المرور في الفضاء، والقدرة على المناورة في الفضاء، والاستجابة والقدرة على التكيف مع الحمولة، وكذلك التعاون الدولي والجهود المبذولة في مجال إنشاء نظام قائم على القواعد في الفضاء.

تصلب الأرض والاتصالات والأقمار الصناعية

إنّ أسهل الطرق للمعارضين لاستهداف القدرات الفضائية الداعمة للعمليات العسكرية هي التركيز على البنية التحتية الداعمة والتمكينية الأرضية. لحسن الحظ، فإن عناصر القدرة الفضائية هذه هي الأسهل للدفاع عنها،

ضمان عمليات الفضاء (SOA)



وتتزايد مخاطر استخدام الفضاء والاعتماد عليه للعمليات العسكرية بسرعة مع ارتفاع عدد الفاعلين في الفضاء. يمثل الازدحام تهديدًا خطيرًا في الفضاء، لا سيما في المدار الأرضي المنخفض (LEO)- الارتفاع الذي يمتد من 400 إلى 1500 كيلومتر فوق الأرض - حيث تتعرض الأقمار الصناعية لخطر الانقراض. أصبح المدار الأرضي المنخفض مشبعًا ليس فقط من قبل المستخدمين العسكريين ولكن أيضًا من قِبل مجموعة متزايدة من المشغلين التجاريين الذين ينتجون ويطلقون أعدادًا كبيرة من الأقمار الصناعية الصغيرة لخدمة سرعة نمو صناعة الفضاء التجارية.

إنّ مخاطر تزايد الازدحام في الفضاء حقيقية - منذ الاصطدام المدروس على نطاق واسع للقمرين الصناعيين إيريديوم 33 وكوزموس 2251 في فبراير 2009، وفي مارس 2021 بين القمر الصناعي يونهاي 1-02 وشظايا (أيضًا نتيجة ضربة قاضية) صاروخ زينيت -2 من روسيا، الذي أُطلق في سبتمبر 1996، عزز المخاطر على عمليات الأقمار الصناعية. كانت هذه الاصطدامات الأخيرة على الأرجح حوادث، ولكن تم رصد مناورات قريبة من الأقمار الصناعية تجاه الأقمار الصناعية الأخرى مؤخرًا ويمكن أن تكون هذه المواجهات

العالم الذي يضمنه بالفعل. ومع ذلك ، فإن الاستخدام العسكري للفضاء لن يظل على جدول أعمال المنظمات الدفاعية ومخططي القدرات العسكرية لسنوات قادمة فحسب، بل ستزداد أهميته.

الجغرافيا السياسية للأرض والفضاء واتساع نطاق التهديد

يمكن القول أنه منذ الحرب العالمية الثانية، ظهر استخدام الفضاء في القتال عندما أطلقت ألمانيا صواريخ في (V2) ذات المسارات الباليستية نحو بريطانيا. في الآونة الأخيرة، حدثت أول حملة عسكرية حيث لعب مجال الفضاء دورًا حاسمًا خلال حرب الخليج الأولى في عام 1991. فبدون استخدام نظام تحديد المواقع العالمي (GPS) الذي يعمل بالأقمار الصناعية، والذي وفر دقة الملاحة والاستهداف للتأثيرات الحركية والمراقبة الفضائية في مسرح الصراع من أجل بلوغ إدراك الواقع الميداني، ربما لم تحقق الولايات المتحدة وشركاؤها في التحالف نفس نتائج التي حققوها خلال عملية عاصفة الصحراء.

منذ نهاية حرب الخليج الأولى، وسعت الجيوش الغربية تدريجياً استخدامها وجهودها في الاستفادة من مجال الفضاء كطريقة لإدخال مزايا تشغيلية. ومع ذلك، فإن هذا الاعتماد المتزايد على مجال الفضاء أو الاتكال عليه قد أوجد أيضًا - ووسع - أنواعًا جديدة من نقاط الضعف للعمليات العسكرية التي يستطيع المعارضون استغلالها بشكل متزايد. في هذا السياق الناشئ، من الضروري أن تبدأ الجيوش في إعادة تركيز الانتباه على استخدامها للفضاء من حيث التخطيط وتطوير القدرات الفضائية بالنسبة للتهديدات الجديدة الناشئة ونقاط الضعف الاستراتيجية.

هذا تحد يجب مواجهته في وقت لا يشك فيه سوى قلة من أن منافسة القوى العظمى قد عادت إلى الساحة العالمية. مع تطور الديناميكيات العالمية، عكفت الولايات المتحدة على إعادة التوازن إلى وضعها العالمي مع التركيز المتزايد على آسيا. كما أدى انخفاض الاعتماد على واردات الطاقة من منتجي النفط في الشرق الأوسط للولايات المتحدة إلى إثارة النقاش حول دورها الإقليمي هناك. أما بالنسبة إلى أوروبا، فإن أي اضطرابات وعدم استقرار في المستقبل من حدودها الشرقية والجنوبية قد تؤدي إلى تحديات غير مسبوقة مع اللاجئين والمشردين. وفي إدارة التأثير الأمني لمثل هذه المخاطر، قد تواجه الجيوش الأوروبية واقعًا جديدًا حيث لا يمكن اعتبار الاعتماد على الأصول الفضائية الأمريكية أو توفرها أمرًا مفروغًا منه.

ففي الوقت نفسه، قد يزداد إصرار أوروبا على بلوغ الاستقلال الاستراتيجي والسيادة ويمتد ليشمل إستراتيجيتها الفضائية المستقبلية. من المرجح أن تستمر العوامل الجيوسياسية في إدخال لاعبين جدد في الإطار لمتابعة الاستخدام الاستراتيجي والتكتيكي للفضاء وتشغيل الأقمار الصناعية وتطوير البنية التحتية التمكينية الأرضية. في الوقت الذي لا يمكن تقسيم الفضاء إلى مساحات مدنية وعسكرية، فإن منطقة "الفضاء العسكري" ستبرز القوى التقليدية للولايات المتحدة وروسيا والصين، ولكنها ستشهد أيضًا إضافة لاعبين جدد مثل الاتحاد الأوروبي والهند والإمارات العربية المتحدة وغيرها.

7 الطيف الناشئ من التهديدات على الاستخدام العسكري للفضاء وانعكاساته على التخطيط في مجال القدرات

باتريك بولدر، مقدم (متقاعد)، سلاح الجو الملكي الهولندي
خبير في مركز لاهاي للدراسات الاستراتيجية

مقدمة

ستتميز العمليات العسكرية المستقبلية بين المنافسين الأقران بنهج عمليات متعددة المجالات (MDO)، والتي ستتميز بدورها بالاستخدام المتكامل والمتوازي للجو والبحر والأرض والفضاء السيبراني والفضاء. سيستفيد الجيش من جميع المجالات العملياتية ولكن بشكل خاص مجال الفضاء في كافة مجالات العمليات العسكرية، بدءً بمهام حفظ السلام ذات الإيقاع المنخفض ومساعدة قوات الأمن ووصولًا إلى عمليات القتال الحربية العالية الكثافة والإيقاع. لقد أصبح الفضاء حيويًا للنشاط العسكري الحديث حيث زادت سرعة وتيرة العمليات وأدت إلى دورات زمنية مضغوطة لاتخاذ القرار على مستوى القيادة والتحكم (C2) وعلى المستويات التكتيكية.

فبالإضافة إلى ذلك ، يخضع النشاط العسكري اليوم لمزيد من التدقيق في ضوء تسارع وتوسيع عملية الوصول إلى المعلومات مفتوحة المصدر في المجال العام بين الجهات الفاعلة في المجتمع المدني. ولقد تمثلت إحدى نتائج ذلك بتكثيف الحاجة إلى معلومات استخباراتية أكثر سرعة ولكن أيضًا أكثر دقة لتوجيه عملية صنع القرار في الحملات العسكرية. أصبحت المعلومات من مجموعة موسعة من المصادر والأصول هي سبل صنع القرار والوسائل لتحقيق ذلك، وقد برز مجال الفضاء بشكل مركزي لبلوغ هذا التطور على مستوى التخطيط والعمليات العسكرية عبر مجموعة المهام التي من المتوقع أن تقوم بها الجيوش بشكل روتيني.

إنّ مجال الفضاء هو السبيل الوحيد لضمان استخبارات مستمرة عبر الحدود وإدراك الواقع الميداني اليوم وتسهيل الاتصالات الحيوية. يتطلب هذا الواقع مزيدًا من الاهتمام للتركيز على أمن الأصول الفضائية وتخطيط القدرات للتطبيقات الفضائية في المستقبل. كما هو الحال، لا يزال مجال الفضاء لا يحظى بالاهتمام الاستراتيجي حول

https://www.defensenews.com/global/europe/2021/10/10/needed-a-transatlantic-agreement-on-european-strategic-autonomy/

ايه. بينيندجيك وال. (2021). At the Vanguard. European Contributions to NATO's Future Combat Airpower. متوافر على:
https://www.rand.org/pubs/research_reports/RRA311-1.html

المراجع

جاميسون، في. وكاليبريزي، ام. (2015). مقال An ISR Perspective on Fusion Warfare. منتدى ذي ميتشيل. 1، الصفحة 5.

تاونساند، اس. (2019). Defining the 'Domain' in Multi-Domain. مؤتمر القوة الجوية والفضائية المشترك 2019: Shaping NATO for Multi-Domain Operations of the future (عبر الانترنت)، صفحة 7-12. متوافر على: https://www.japcc.org/wpcontent/uploads/JAPCC_Read_Ahead_2019.pdf [12 October 2021]

بينا، ال. (2020). Le MDC2: l'occasion de rénover notre C2. Défense et sécurité international. 147 الصفحة 94.

اورلين، اس. (2021). Why the military needs a dynamic network infrastructure. Defense Systems (عبر الانترنت). متوافر على: https://defensesystems.com/articles/2021/06/02/dynamic-network-infrastructure.aspx

هيتشنز، تي. (2020). Air Force Expands AI-based Predictive Maintenance (عبر الانترنت). Breaking Defense. شكر لباتريك مونوز (ADIC) للنقاش المثمر حول هذا الموضوع.

غروس، بي. (2019). The tactical cloud, a key element of the future combat air system (عبر الانترنت). Fondation pour la recherche stratégique. ملاحظة رقم 8، ص.9.

French Defense and National Security Strategic Review (عبر الانترنت). (2017). مكتب النشر، ص. 90. متوافر على: https://franceintheus.org/IMG/pdf/defense_and_national_security_strategic_review_2017.pdf

بينيندجيك، اتش. وفيرشبو، ايه. (2021). Needed: A transatlantic agreement on European strategic autonomy. Defense News. متوافر على.

التابعة للتحالفات والأحلاف معايير مختلفة في تصميم الأنظمة والشبكات بسبب الاعتبارات الصناعية والسياسية المتناقضة؟

إنّ هذا السؤال يسلّط الضوء على أوجه عدم اليقين المتعلقة بإمكانية التشغيل البيني في الإطار الزمني المستقبلي الذي يتطلع إلى عام 2040 وما بعده بالإضافة إلى أساطيل القتال الجوي الحالية التي تواجه بالفعل تحديات مماثلة في المشهد الأوروبي. ستحتاج القوات الجوية الأوروبية إلى التعامل مع متطلبات التكامل والاندماج المشترك على المستوى التشغيلي الذي سيحتاج إلى الموازنة مع اعتبارات السياسة ذات المستوى الأعلى التي تمتد إلى مجال الاستراتيجية الوطنية، لتشمل حرية العمل والاستقلال الاستراتيجي. وفي هذا السياق، ستحتاج القوات الجوية الأوروبية إلى التفاعل مع برامج القدرات وأهداف التشغيل البيني وتخطيطها بما يتماشى مع توجهات السياسة الوطنية أو الأوروبية التي تتشكل من خلال بيئة معقدة من العوامل المؤسسية وجداول الأعمال.

إنها حجة منطقية مفادها أن الفوائد المحتملة للتوزيع ودمج البيانات بين القوات الجوية في بيئات التحالف تفوق المخاطر المرتبطة الناتجة عن السحب القتالية المشتركة أو احتمالية حدوث الشلل التشغيلي. ومع ذلك، وبغض النظر عن الاعتبارات التشغيلية البحتة، ثمة قضايا سياسية مهمة تتشكل من خلال الإستراتيجية الكبرى والتوقعات السياسية. حتى بين الحلفاء والشركاء الذين يتشاركون وجهات نظر عالمية متشابهة والذين يعملون بشكل متكرر أو يتعاونون بشكل وثيق في عمليات التحالف والعمليات المشتركة، يمكن أن تتباين السياسات الوطنية، لا سيما في ما يتعلق بالنشاط العسكري في حالات الأزمات.

ثمة مبررات مقنعة وتاريخية لمواصلة العمل من أجل تحقيق قابلية التشغيل البيني بين التحالف والشركاء المتحالفين، ومع ذلك يمكن أن يكون ذلك ضمن سياق السحب القتالية. ولكن يجب أن تكون هذه الجهود متوازنة مع الحاجة إلى الحفاظ على الاستقلال الاستراتيجي والقدرة على إجراء تقييمات مستقلة أو نشاط عسكري (بينيندجيك وفيرشبو، 2021). تقدم المناهج المتباينة التي يُنظر إليها أحيانًا على أنها تؤدي إلى "ازدواجية القدرات" وإهدار الموارد المالية بطريقة أخرى مزايا من خلال إنشاء جدران الحماية الطبيعية والمرونة لعمليات التحالف الوطنية والمشتركة.

وفي ضوء التطورات الحالية والمستقبلية في نماذج القتال الجوي للتحالف، قد يكون الحفاظ على مستوى من الاستقلالية بنفس أهمية تأمين السحب القتالية الناشئة نفسها. سيكون هذا صحيحًا بشكل خاص في السياق الأوروبي حيث من المحتمل أن يتكون الأسطول القتالي المشترك من مجموعة من أنواع المنصات تم تطوير كل منها وفقًا لمعايير هندسة الأنظمة والتقنية وقابلية التشغيل البيني المختلفة، والتي ترتبط بالاعتبارات الصناعية والسياسية. قد تكون تحديات خط الأساس نفسها قابلة للنقل إلى أجزاء أخرى من العالم، مثل الشرق الأوسط أو آسيا. وبدلاً من محاولة تقسيم أساطيل القتال الجوي إلى قدرات من المستوى "الأول" و"الثاني"، سيحتاج التحالف والشركاء المتحالفون إلى تركيز الانتباه على التغلب على التحديات وإنشاء عوامل تمكين التكامل وحلول التشغيل البيني لمفهوم العمليات متعددة المجالات (MDO) في بيئات التحالف التقليدية.

خمس منصات طائرات مقاتلة تشارك بنشاط في المنافسة. وبالنظر إلى عام 2040 وما بعده، من المرجح أن تستمر أوروبا في رؤية التطوير المحلي للطائرات المقاتلة من الجيل التالي، ويتم معها إدراج معايير جديدة للتشغيل البيني في كل من أطر الاستحواذ والتخطيط التشغيلي. أنظر إلى تطوير نظام القتال الجوي المستقبلي (FCAS) ونظام بريتيش تيمبيست (British Tempest) على سبيل المثال - فإنّ كلتي المنصتين ستقترنان بأنظمة ومرحلات تعمل عن بعد ومستقلة، وتعمل داخل شبكات تبادل بيانات متعددة المجالات قائمة على السحابة.

> وبالتالي، لن ترتبط العمليات القتالية الجوية بمجموعة من المهام المتسلسلة، بل سترتبط بسلسلة واحدة من المناورات والتأثيرات غير المجزأة القائمة على نشاط القوات المعادية والاستجابة لها بشكل كبير.

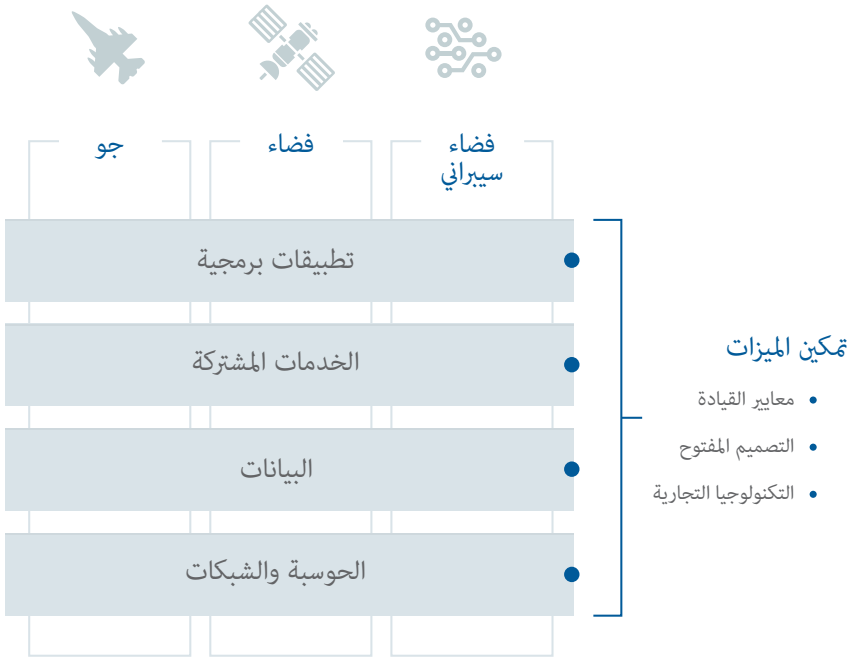
قد يشير التنوع الحالي والمستقبلي المحتمل لأساطيل القتال الجوي الأوروبية للوهلة الأولى إلى تكرار غير ضروري للقدرات، لكن هذه الاختلافات نفسها في الأساليب والقدرات توفر أيضًا مرونة أكبر على المستويين التشغيلي والاستراتيجي. ففي بيئة التحالف، ليس من الواضح إلى أي مدى ستكون أساطيل القتال الجوي في أوروبا قابلة للتشغيل المتبادل مع، على سبيل المثال ، دخول مقاتلة اف-35 إلى الخدمة التشغيلية في أوروبا الآن. سيتم تطبيق نفس الأسئلة نظريًا على نظام القتال الجوي المستقبلي (FCAS) ونظام تيمبيست (Tempest) وستمتد هذه الأسئلة حول التوافق وقابلية التشغيل البيني إلى المستقبل خاصة فيما يتعلق بمفهوم العمليات متعددة المجالات (MDO).

تتم إعادة صياغة التحدي المتمثل في إمكانية التشغيل البيني في بيئات التحالف وسيتخذ اتجاهًا جديدًا مع إدخال طائرات ومنصات مقاتلة جديدة ولكن لا توجد حلول واضحة أو متاحة بسهولة لسد الاختلافات في العقيدة ومفهوم العمليات من ناحية، أو من أجل تحقيق التكامل التقني في بيئة التحالف حيث توفر كل من القوات الجوية المكونة لها مجموعة القدرات والأدوات والمنصات الخاصة بها للقتال. تبقى المفارقة كون الفرضية الأساسية والغرض من التكامل متعدد المجالات هو حل نقص أو انخفاض التوافق والتآزر بين أنواع مختلفة من المنصات، عبر مجالات مختلفة، والتي تم تطويرها باستخدام معايير تقنية مختلفة وأساليب هندسة النظم.

الأبعاد السياسية للتكامل والتشغيل البيني

ينطوي التطور نحو مفهوم العمليات متعددة المجالات (MDO) على تحديات جديدة للقوات الجوية من خلال تقديم مجموعات جديدة من الديناميكيات في التخطيط الموازي المشترك في بيئة التحالف. كما أنه يمثل حاجة إلى تكييف أو استبدال الآليات الحالية التي تم تطويرها لتمكين المستويات الضرورية من التكامل والتشغيل البيني بين شركاء التحالف مما يسمح لهم بالعمل معًا بفعالية. ومع تسارع الحركة نحو مفهوم العمليات متعددة المجالات (MDO)، فإنّ السؤال الأساسي الذي يطرح نفسه هو: هل التشغيل البيني ممكن عندما تتبنى القوات الجوية

عناصر قابلية التشغيل البيني في العمليات متعددة المجالات المتصلة بالشبكة في المستقبل



لقد جمع برنامج اف-35 (F-35) الذي تقوده الولايات المتحدة عددًا من الدول الأوروبية بما في ذلك المملكة المتحدة وهولندا والدنمارك والنرويج وبلجيكا وإيطاليا. تقدم طائرة اف-35 (F-35) لكونها مقاتلة من الجيل الخامس نموذجًا جديدًا ومعيارًا جديدًا للتشغيل البيني لأوروبا والذي سيلعب جنبًا إلى جنب مع مشغليها دورًا قويًا في تشكيل جهود وبرامج التشغيل البيني عبر القوات الجوية الأوروبية خلال السنوات القادمة. ومع ذلك، يستمر معظم مستخدمي مقاتلة اف-35 في الحفاظ على أساطيل قتالية أوسع، ومن المرجح أن تظل يوروفايتر تايفون على سبيل المثال لا غنى عنها بالنسبة للمملكة المتحدة بسبب قيود اف-35 في مهام التفوق الجوي. من المرجح أن تستمر إيطاليا وألمانيا وإسبانيا في تشغيل مقاتلة تايفون لأسباب مماثلة، وقد تمتد اعتبارات مماثلة إلى مشغلي اف-16 (F-16) مثل بلجيكا والدنمارك واليونان وهولندا والنرويج والبرتغال وتركيا.

لقد حصلت القوات الجوية الأوروبية الأخرى على طائرات مقاتلة مثل غريبين-اي (Gripen-E) ورافال (Rafale) والتي يمكن اعتبارها، إلى جانب قدرات رادار المسح الإلكتروني النشط (AESA) ودمج البيانات، المعيار الأوروبي المستقبلي الفعلي للتشغيل البيني. تتابع فنلندا برنامج مقاتلة اتش-اكس (HX Fighter) مع

الكهرومغناطيسية، قد تؤدي سحابة قتالية "الحلقة الواحدة" إلى شلل تشغيلي عبر قاعدة المستخدمين المشتركين بها.

عند النظر في مثل هذه المخاطر، ثمة أسئلة جدية حول نضج تقنيات التمكين الرئيسية لمفهوم السحابة القتالية. فإنّ أنظمة وتقنيات المعلومات التي تجمع البيانات وتحللها وتخزنها وتنقلها تخضع لظهور تهديدات تدخلية وتكرارها من قبل القوى المعارضة من أجل تعزيز فعالية منع الوصول/ منع الوصول (A2AD) (اورلين، 2021). لا يمكن استغلال "البيانات الضخمة"، وهي شرط أساسي لأي صورة تشغيلية مشتركة معروفة (CROP) بين عناصر القيادة والتحكم الموزّعة، بشكل صحيح بدون الذكاء الاصطناعي، والتي لا يزال استخدامها يمثل مشكلة نظرًا لقابليتها للتلاعب والخداع.

توفر الصيانة التنبؤية، التي هي أصلية لمنصات القتال الجوي المستقبلية وسيتم إبلاغها باستمرار عبر الشبكة، ثغرة هجومية جديدة في مساحة الحرب ومن المرجح أن تكون مستهدفة بشكل كبير (هيتشنز، 2020). إن استغلال العيوب والقيود المحتملة في البرامج سيخلق فرصًا للقوى المعارضة من حيث الخداع والتحايل والعمليات المفاجئة. يمثل التشويش المتقدم الذي يستهدف شبكات الاتصالات وأجهزة الاستشعار وعمليات الحرب الإلكترونية الهجومية الموجهة إلى السحابة القتالية (غروس، 2019)، والاعتماد على الأصول الفضائية مخاطر جسيمة في السيناريوهات التي يتم فيها تدمير الأصول الأرضية أو الفضائية أو تعريض روابط البيانات المهمة للخطر (المراجعة الاستراتيجية للدفاع والأمن القومي الفرنسي، 2017).

إن انتشار تكنولوجيا الطائرات بدون طيار ورقمنة أنظمة القتال يجبر بالفعل القوات الجوية والخدمات الشقيقة في أوروبا على تركيز الاستثمارات في الإجراءات المضادة للفضاء السيبراني و"تقوية" المنصات والأصول والبنية التحتية للعمليات لضمان عدم المساس بعقد الاتصالات وأجهزة الإرسال. سوف تتسارع هذه الجهود وتتكثف حيث يستهدف المنافسون العسكريون إمكانات اتصال البيانات عبر سطح هجوم أوسع يوسع التحالف أو القوة المتحالفة التي ترتبط جميعها بنفس السحابة. لذلك تؤكد هذه المخاطر الكامنة على شبكات القتال متعددة المجالات على الحاجة إلى النظر في تطوير سحابات قتالية مستقبلية لمفهوم العمليات متعددة المجالات (MDO) في بيئات التحالف خارج تصميم "الحلقة الواحدة".

الأساطيل الجوية القتالية في أوروبا: المشهد الحالي والمستقبلي

في أوروبا ، كان التكامل العملياتي بين القوات الجوية يتقدم باطراد حيث كان عامل الناتو مهمًا ولكنه ليس بأي حال من الأحوال المحرك الوحيد للتقدم المحرز في تعزيز التشغيل البيني بين القوات الجوية الأوروبية. ومع ذلك، لا يزال مشهد القوة الجوية الأوروبية يتسم بتنوع كبير، كما يتضح من الأنواع المتنوعة لأكثر من 1900 طائرة مقاتلة موضوعة حاليًا في الخدمة.

متجه قوة فردي كمستشعر وكمستجيب في الوقت نفسه. وستكون القدرات المتعلقة بدمج البيانات والأتمتة والروبوتات والذكاء الاصطناعي (AI) ضرورية لتحقيق "هيمنة الطيف" - التفوّق عبر الطيف التشغيلي.

مستوى نموذج قابلية التشغيل البيني لنظام المعلومات (LISI)

سيصبح القتال الجوي بشكل تدريجي أكثر اعتمادًا على الإدراك متعدد المجالات وهيمنة المعلومات. ومع ذلك، فإن احتمالية وجود سحابة قتالية فردية وشاملة تعمل كمكتبة مركزية أو كدماغ تطرح مشكلات معقدة في بيئة التحالف: الاتصال الدائم بمثل هذه السحابة القتالية يولّد نقاط ضعف واضحة لمكوّنات قوات التحالف. إن نفس تركيز القوة والاعتماد على سحابة مركزية واحدة يولّد احتمالات خسارة كارثية في حرية التصرف، في حين يتم توفير مزايا من حيث تركيز القوة وكفاءتها. ستهدف القوى المتعارضة إلى إعاقة الاتصالات واستخدام الشراك الخداعية ضد شبكات الاستشعار وفي مثل هذا السياق من الفضاء السيبراني الحميدة والحرب

كيفية تخطيط القوات الجوية وتنفيذها للعمليات الجوية في المستقبل" (بينا، 2020). من المؤكد أن مفهوم العمليات متعددة المجالات (MDO) سيمثل عاملاً قوياً في تشكيل المفهوم المستقبلي للعمليات للقتال الجوي وجهود التحوّل، ولكن هناك تحديات مفاهيمية وتقنية واستراتيجية معقدة يجب التغلب عليها.

الاتصال والقتال الجوي في المستقبل

من المتصوَّر أن تعمل الطائرات القتالية المستقبلية كـ"مراكز اتصال" و"خوادم لدمج البيانات المحمولة جواً،" مرتبطة بسحابة قتالية توفر معلومات متعددة المجالات في الوقت الفعلي إلى العناصر الموزَّعة من القوات المشتركة أو قوات التحالف. يتم وضع هذه الطائرات المقاتلة من الجيل التالي لتولي نفس الأدوار المعيَّنة حاليًا من قبل القوات الجوية لطائرات الإنذار المبكر والقيادة والسيطرة، المحمولة جواً (AWACS). فقد أصبحت هذه الأنظمة وظيفة أساسية في العمليات الجوية منذ وصول لينك 16 (Link 16) والتي أثبتت فعاليتها في التفوق الجوي الغربي في العقود الأخيرة من خلال تمكين تحسين إدراك الواقع الميداني وقدرات القيادة والسيطرة والاتصالات (C3) بشكل جذري في الحملات المشتركة والتحالف.

> تتم إعادة صياغة التحدي المتمثل في إمكانية التشغيل البيني في بيئات التحالف وسيتخذ اتجاهًا جديدًا مع إدخال طائرات ومنصات مقاتلة جديدة ولكن لا توجد حلول واضحة أو متاحة بسهولة لسد الاختلافات في العقيدة ومفهوم العمليات من ناحية، أو من أجل تحقيق التكامل التقني في بيئة التحالف حيث توفر كل من القوات الجوية المكونة لها مجموعة القدرات والأدوات والمنصات الخاصة بها للقتال.

في المستقبل، ستصبح وظائف دمج البيانات وترحيلها أكثر توزيعًا وإعادة بثها بشكل متزايد إلى الطائرات المقاتلة نفسها والتي ستكون قادرة على تنسيق أسراب الطائرات بدون طيار، على سبيل المثال، لاختراق الدفاعات الجوية للعدو أو إحداث تأثيرات حركية. ستعمل الطائرات المقاتلة في مساحة متعددة المجالات كعقد القيادة والتحكم الرئيسية (C2) نفسها مدعومة بأدوات جديدة واتخاذ قرارات أسرع من خلال شبكات البيانات والاتصالات من الجيل التالي. وبالتالي، لن ترتبط العمليات القتالية الجوية بمجموعة من المهام المتسلسلة، بل سترتبط بسلسلة واحدة من المناورات والتأثيرات غير المجزأة القائمة على نشاط القوات المعادية والاستجابة لها بشكل كبير.

سيشمل القتال الجوي تطبيقًا أكثر استنارة وذكاءًا لاقتصاد القوة للتغلب على القوات المعارضة باستخدام مزيج من السرعة والتشبع والتسلل ("V2S" - السرعة والتشبع والتخفي) لتحقيق التفوّق في ساحة المعركة. تعتمد هذه المفاهيم المستقبلية على نهج نظام الأنظمة مع جوهر القيادة والتحكم والاتصالات وأجهزة القيادة والتحكم والاتصالات والحوسبة والأمن السيبراني والاستخبارات والمراقبة والاستطلاع (C4ISTAR) وحيث يعمل كل

6 التكامل وقابلية التشغيل البيني للعمليات متعددة المجالات في بيئة التحالف: التحديات التي تواجه أساطيل القتال الجوي الأوروبية

بروفيسور أوليفييه زاجيتش
مدير معهد الدراسات الاستراتيجية والدفاع (IESD)، جامعة ليون

العمليات متعددة المجالات وقابلية التشغيل البيني بين القوات الجوية

يتطور التفكير الاستراتيجي في مجتمع القوة الجوية بشكل كبير تحت تأثير مفهوم العمليات متعددة المجالات (MDO). فقد كانت القوات المسلحة حتى التسعينيات منخرطة على نطاق واسع في جهود "التحوّل" بهدف تحسين التنسيق بين الخدمات العسكرية. بحلول العقد الأول من القرن الحادي والعشرين، تطوّر هدف وغايات جهود التحول وأفسحت الرغبة في تحسين التنسيق الطريق أمام الجهود المبذولة من أجل تكامل عملياتي أعمق بين الخدمات العسكرية وشركاء التحالف. يركّز مفهوم العمليات متعددة المجالات (MDO)على تعزيز هدف التحوّل نحو الاندماج النهائي للقدرات بين المجالات التشغيلية من أجل التمكن من تقديم تأثيرات متزامنة بوتيرة أسرع للعمليات (جاميسون وكابريزي، 2015). ومع ذلك، فإنّه ليست كل البلدان واضحة بشأن كيفية تبني الرؤية الأمريكية لمفهوم العمليات متعددة المجالات (MDO) بدقة في عقائدها الخاصة وفي مفهوم العمليات أو كيفية حل تحديات التكامل والتشغيل البيني المحتملة التي تنشأ (تاونسند، 2019).

إنّ الهدف المنشود من مفهوم العمليات متعددة المجالات (MDO) هو تسريع وتيرة العمليات العسكرية والسماح بتنسيق أكثر تآزرًا للتأثيرات التي سيتم إنتاجها في بيئة العمليات. يَعِد التكامل متعدد المجالات بتحسين المزايا التشغيلية من أجل الضغط على حلقات صنع القرار للقوى المعارضة. وفي الوقت نفسه، يشير مفهوم العمليات متعددة المجالات (MDO) أيضًا إلى تطور كبير وتغييرات ضرورية في مناهج العمليات المشتركة بحيث تؤثر بسهولة على القوات الصديقة بنفس القدر من العمق. كما أشار اللواء لويس بينا، نائب قائد الدفاع الجوي الفرنسي وقيادة العمليات الجوية (CDAOA)، يمثل مفهوم العمليات متعددة المجالات (MDO) "فرصة للتفكير في

المراجع:

جاستن برونك، (2020، (ايه))، "أنظمة الدفاع الجوي الروسية والصينية الحديثة المتكاملة: طبيعة التهديد ، مسار النمو والخيارات الغربية" ، أوراق RUSI من حين لآخر، متوافر على https://static.rusi.org/20191118_iads_bronk_web_final.pdf

جاستن برونك،(2020، (بي))، "Russian and Chinese Combat Air Trends: Current Capabilities and Future Threat Outlook"، RUSI Whitehall Reports، متوافر على https://static.rusi.org/russian_and_chinese_combat_air_trends_whr_final_web_version.pdf

جوستين برونك (2020، (سي)) ، ``خيارات القتال الجوي لحكومة المملكة المتحدة "، أوراق RUSI العرضية، متوافر على- https://rusi.org/explore-our-research/publications/occasional-papers/combat-air-choices-uk

خدمة أبحاث الكونغرس، القيادة والتحكم المشترك لجميع المجالات (JADC2) ، تقرير، (2021)، متاح على https://crsreports.congress.gov/product/pdf/IF/IF11493

Kaushal، Sidharth and Macy، Archer and Stickings، Alexandra (2021)، "مستقبل الدفاع الجوي والصاروخي لحلف الناتو"، أوراق RUSI Occasional Papers، متوافر على https://static.rusi.org/NATOMissileDefence2021.pdf

Watling، Jack، "From Multirole to Modularity"، RUSI Defense Systems (2020)، متوافر على- https://rusi.org/explore-our-research/publications/rusi-defence-systems/multirole-modularity

على مجموعات أجهزة استشعار متعددة الأطياف مثل اف-35 (f-35)، كميات هائلة من البيانات لأنها تنشئ صورة واسعة النطاق لساحة المعركة من حولها. خلال هذه العملية، سيقومون بجمع المعلومات التي من المحتمل أن تكون ذات قيمة أو حساسية عالية لمجموعة واسعة من الأصول الأخرى عبر جميع المجالات. ومع ذلك، فإن قيود النطاق الترددي القائمة على الفيزياء تقيّد القدرة على تفريغ أو مشاركة جميع البيانات التي تم جمعها، حتى في بيئة كهرومغناطيسية غير متنازع عليها (والتينغ، 2020). في سيناريو الصراع بين الدول، حيث تتنافس منصات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) والقيادة والتحكم (C2) على الوصول المحدود والمتنازع عليه إلى الطيف، ومن المحتمل أن تعمل في ظل ظروف يتم التحكم فيها بالانبعاثات لتقليل تعرضها للاكتشاف والهجوم، ومعالجة الحدود لتقليل البيانات ستكون المجلدات التي يجب مشاركتها ضرورية.

يمكن لأطقم المهمات البشرية (رهنا بالقدرة العقلية وعبء العمل) جعل الأولوية المطلوبة الذاتية والمعتمدة على الموقف والأحكام ذات الصلة حول المعلومات التي قد تكون أو لا تستحق نقلها إلى أصول أخرى. ومع ذلك، لا تستطيع الأنظمة الآلية حاليًا القيام بذلك بشكل حاسم إلا في ظروف محددة بشكل صارم. وينطبق الشيء نفسه على المهام التفاعلية التي غالبًا ما تعتمد على رد الفعل والحكم لإدارة المعركة الجوية، والتي تعد جزءًا أساسيًا من مجموعة مهام أواكس. من المستحيل استبدال عقدتي الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) والقيادة والتحكم (C2) المركزية في المجال الجوي بهندسة روابط البيانات وعقد الشبكة اللامركزية المثبتة بشكل أساسي على الطائرات بدون طيار من نوع الطائرات ذات مستوى التحمل العالي واختراق الأصول القتالية دون إجابة مناسبة لهذه المشاكل.

إن مكونات شبكة القيادة والتحكم المحمولة جواً اللامركزية والآلية للغاية وشبكة مشاركة البيانات مثل تلك التي تتم متابعتها في إطار برنامج القيادة والتحكم المشترك لجميع المجالات (JADC2) في متناول مصممي هياكل الطائرات (خدمة أبحاث الكونغرس، 2021). ومع ذلك، فإنّ هذا الطموح يفوق قدرة الذكاء الاصطناعي وتقنية الاستقلالية القابلة للتطبيق حاليًا. إن متطلبات مثل هذا النظام واضحة، لأن الجزء الأكبر من الكتلة القتالية في القوات الجوية في جميع أنحاء العالم سيظل يتم توفيره بواسطة مقاتلات الجيل الرابع المتقدمة وذخائر المواجهة حتى منتصف عام 2030 على الأقل. لن تكون أنظمة الأسلحة هذه قادرة على أداء الأدوار المطلوبة منها في النزاعات عالية الحدة دون تغذية إدراك الواقع الميداني في الوقت الحقيقي والاستهداف والإشارة إلى الأسلحة من جميع أنحاء ساحة المعركة. ومع ذلك، بدون الحكم الذاتي وقدرات تحديد الأولويات المطلوبة للسماح بمعالجة الحافة الآلية لاستبدال أطقم المهام البشرية حقًا في إدارة المعركة الجوية ومهام الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) والمعالجة والاستغلال والنشر(PED) ، قد تظل القوات الجوية معتمدة بشكل كبير على بنية مركزية محمولة جواً تعتمد على أنظمة قديمة كبيرة الحجم.

المدارية في شبكات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) و القيادة والتحكم (C2) الموزعة في المستقبل. ومع ذلك، فإن انتشار القدرات الحركية والأسلحة الخفيفة المضادة للسواتل، والأصول المدارية القادرة على الالتقاء وعمليات القرب الهجومية والطيف الكهرومغناطيسي المتنازع عليه بشكل متزايد في الوقت نفسه، تجعل الأصول المدارية وقدرات الوصلة الصاعدة/ الهابطة اللازمة لاستخدامها عرضة بشكل متزايد للرفض أو على الأقل متنازع عليه بشدة في أي حرب مستقبلية.

> فإن القدرة على توفير قدرات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) عند الطلب والدعم الناري من الجو تمثل الآن شرط أساسي مسبق

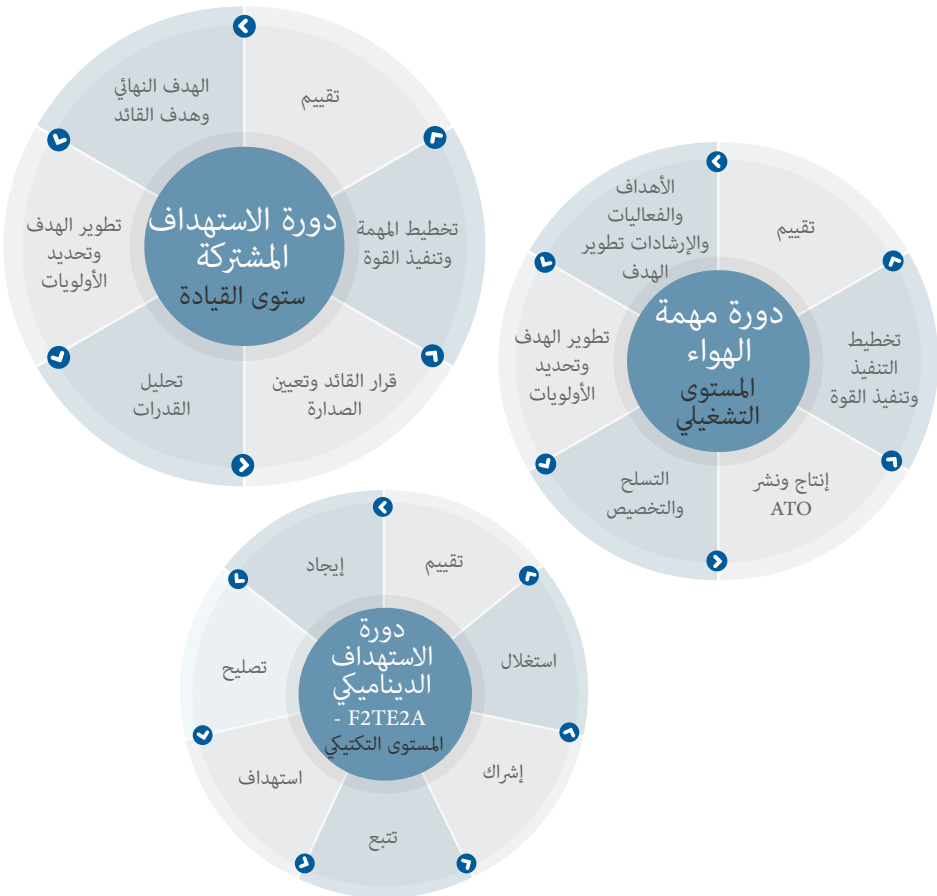
توفر الطائرات دون طيار القدرة على التحمل لفترة أطول في المحطة مقارنة بالأصول التي تعتمد على طاقم نظام الرحلة والبعثات البشرية، دون نفس المسارات التي يمكن التنبؤ بها والتي يحتمل أن تكون معرّضة للخطر مثل الأقمار الصناعية في المدار. لقد أثبتت الطائرات دون طيار الكبيرة مثل الطائرة الأمريكية آر كيو-4 غلوبال هوك (RQ-4 Global Hawk) وديفاين ايغل الصينية (Chinese Divine Eagle) بالفعل القدرة على الطيران على ارتفاعات عالية جدًا لأكثر من 24 ساعة في كل مرة - وهي سمة مرغوبة للغاية لأي عقدة شبكات استخبارات ومراقبة واستحواذ على الهدف والاستطلاع (ISTAR) وقيادة وتحكم (C2) لا مركزية محمولة جواً. بهدف جعلها أكثر قدرة على الاستمرار في مواجهة تهديدات الأقران، توفر الطائرات دون طيار من النوع عالي التحمل (HALE) ذات الأشكال والمواد التي تتميز بمستوى احتمال رصد منخفض جدًا إمكانات جديدة. تعتمد ملاءمة الطائرات دون طيار ذات مستوى احتمال رصد منخفض جدًاوالمعتمدة لمهام شبكات استخبارات ومراقبة واستحواذ على الهدف والاستطلاع (ISTAR) وقيادة وتحكم (C2) داخل نظام لامركزي على تطوير روابط البيانات المتطورة وأجهزة الاستشعار وساتكوم التي يمكن أن تؤدي وظائف مهمتها دون الكشف عن هيكل الطائرة لأجهزة الاستشعار السلبية المعادية. لإنجاز مثل هذه المهام، ثمة تقنيات واعدة في الأفق تتميز بدرجات مختلفة من النضج التكنولوجي ولكنها تظل باهظة الثمن ويتم الاحتفاظ بها على مستوى عالٍ من التصنيف والحساسية الأمنية من قبل الدول التي تعمل بها. هذا يعني أن النشر على نطاق واسع سيكون صعبًا، خاصة على المنصات غير المأهولة بالقرب من المناطق المعادية.

ربط الأصول غير كافٍ

في حين أنّ الطائرات ذات مستوى الملاحظة المنخفض جدًا(VLO) غير المأهولة، يمكن نشر هياكل الطائرات من النوع عالي التحمل والحفاظ عليها بالقرب من القوات المعادية من حلول الجيل الحالي المشتقة من الطائرات، فإن قدرتها على استبدال عقد شبكات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) والقيادة والتحكم (C2) المحمولة جواً التقليدية تعتمد على تبادل البيانات الآلي وتقنيات المعالجة المتطورة. تُنشئ أصول الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) الحديثة، خاصة تلك التي تحتوي

تستكشف بالفعل مجموعات من الأصول المدارية الموزعة والمركبات الجوية غير المأهولة (UAV) والتي من شأنها أن تحل وظائف المعالجة والاستغلال والنشر(PED) و والقيادة والتحكم بهدف التحكم عن بعد بمحطات أرضية بعيدة.

إنّ الشكل المستقبلي للمجال المداري كجزء من تصاميم الاستخبارات والمراقبة والاستحواذ على الهدف



والاستطلاع (ISTAR) و القيادة والتحكم (C2) الموزعة غير واضح حاليًا بسبب مجموعة من الاتجاهات المتنافسة. ومن ناحية أخرى، فإنّ التطورات السريعة على مستوى قدرات أجهزة الاستشعار، ومتطلبات المساحة/ الوزن/ الطاقة للمعدات، وعرض النطاق الترددي للاتصالات والمتانة من خلال المصفوفات المتعددة المدخلات والمخرجات وانخفاض تكلفة قدرة الإطلاق تشير جميعها إلى زيادة حادة في الدور الذي يمكن أن تلعبه الأصول

البنى المستقبلية لأنظمة القيادة والتحكم اللامركزية

من الواضح للعديد من القوات الجوية أن العقد التقليدية المحمولة جواً القيادة والتحكم (C2) والاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) المشتقة من الطائرات ذات الجسم العريض مثل مثل إي-3 أواكس (E-3 AWACS) وإي-8 جي ستارز (E-8 J STARS) لم تعد مثالية لسيناريوهات الصراع في المستقبل. تتمتع هذه الأصول بقدرات دفاع عن النفس محدودة للغاية ويجب أن تصدر كميات كبيرة من الإشارات الكهرومغناطيسية التي يسهل اكتشافها من أجل العمل بفعالية، مما يسهل تحديد موقعها وتعقبها. تمثل هذه المنصات أيضًا مصدرًا خطيرًا للإصابات المحتملة، لأنها تحمل أطقم أنظمة مهام كبيرة مدربة تدريباً عالياً لتنفيذ المهمة الرئيسية للمعالجة والاستغلال والنشر (PED)، فضلاً عن وظائف إدارة المعركة الجوية. يجب أن تقف طائرات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) و القيادة والتحكم (C2) ذات الجسم العريض بعيدًا عن أنظمة صواريخ سطح-جو المعادية وصواريخ جو- جو بعيدة المدى (VLRAAMs) اليوم لأنها غير فعالة إلى حد كبير من حيث صورة المستشعر الأولية في المراحل المبكرة من الصراع مع المنافسين المتقدمين تقنيًا.

إنّ الجيل الخامس من طائرات اف-35 أقل اعتمادًا بشكل كبير على عناصر التمكين مثل أنظمة الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) و القيادة والتحكم (C2) نظرًا لقدرتها على تزويد الطيارين بوعي متعدد الأطياف للوضع على نطاق واسع. أدت هذه القدرة على بناء الوعي بالأوضاع داخل المجال الجوي المعادي إلى قيام الكثيرين بالتخطيط لاستغلال الطائرة اف-35 (F-35) باعتبارها ركيزة أساسية في شبكة الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) و القيادة والتحكم (C2) الموزعة من الجيل التالي (برونك، 2020سي). ومع ذلك، لا يمكن لطائرة اف-35 (F-35) في شكلها الحالي نقل صورة المستشعر الكاملة التي تخلقها لطياريها إلى عناصر قوة أخرى بسبب عرض النطاق الترددي وبنية البرامج وقيود التحكم في الانبعاثات. علاوة على ذلك، تتمتع طائرات اف-35 (F-35) نظرا لكونها مقاتلة قتالية تكتيكية، بقدرة تحمل محدودة مقارنة بعقد أنظمة الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) والقيادة والتحكم (C2) التقليدية، كما أن الأعداد المحدودة من طائرات اف-35 (F-35) المتاحة ملتزمة بالفعل بمجموعات مهام قمع الدفاع الجوي للعدو/ تحطيم الدفاع الجوي للعدو ومجموعات مهام الحظر. تقدم المنصات مثلاف-35 (F-35) حلاً جزئيًا فقط لاعتماد أصول وشبكات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) و القيادة والتحكم (C2) التمكينية التقليدية.

تتطلب تصاميم الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) و القيادة والتحكم (C2) المحمولة جواً واللامركزية التي يتم تطويرها تغييرات في المعدات لتمكين القوات الجوية من نشر عدد أكبر من المنصات الأصغر. إلى جانب الأصول القتالية المدعومة بالشبكة مثل طائرة اف-35 (F-35)، قد لا تزال مجموعة من منصات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) و القيادة والتحكم (C2) الأصغر حجمًا والمأهولة توفر خيارًا لحمل طاقم نظام مهام صغير لتمكين المعالجة والاستغلال والنشر(PED) على متن الطائرة وإدارة المعركة الجوية ومع ذلك، فإن العديد من دول القوة الجوية الرائدة

إزالته، زاد الاعتماد التشغيلي على وصلات الاتصالات المدارية والمدفونة التي هي ضمن خط البصر، والبعيدة عن خط البصر والتي يحتمل أن تكون معرضة للخطر.

تتميز بعض المفاهيم المستقبلية بمراكز عمليات جوية أصغر حجمًا وأكثر توزيعًا (AOCs) لتقليل تعرض القوة المشتركة لهجمات بطريقة قطع الرأس على مراكز القيادة والتحكم التابعة لها. ومع ذلك، يمكن أن يؤدي الاعتماد على عدد أكبر من مراكز العمليات الميدانية الموزعة بدلاً من مراكز عمليات العمليات الجوية المشتركة (CAOC) الكبيرة إلى حدوث ازدواجية في المهام وبالتالي زيادة العبء الواقع على موظفي الاستخبارات والقيادة المرهقين بالفعل. يمكن أن يزيد توزيع قدرات القيادة والحكم أيضًا من الاعتماد على روابط اتصالات مضمونة، نظرًا لأن كل مركز عمليات جوية قادر فقط على أداء بعض وظائف مراكز العمليات الجوية المشتركة على نطاق كامل حتى مع أتمتة كبيرة للعمليات الضرورية. لذلك، إذا كانت الأدوات الحركية أو غير الحركية ستقطع هذه الروابط أو حتى تعارضها بجدية، فقد تفقد كل من مراكز العمليات الجوية المشتركة المركزية أو مراكز العمليات الجوية الموزعة القدرة على التنسيق التكتيكي لأصول قدرات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) وشن الغارات والتمكين في المسرح.

علاوة على ذلك، تم السماح لمجموعة مكن كبار القادة الذين يمارسون السيطرة المباشرة والإشراف على العمليات التكتيكية بالظهور خلال عدة عقود من العمليات الجوية غير المتنازع عليها إلى حد كبير. وقد كان الدافع وراء ذلك جزئيًا هو التوافر المتزايد لتغذية الفيديو بالحركة الكاملة في الوقت الفعلي، مما يسمح لقادة مركز العمليات العسكرية المشتركة (CAOC) بإدراك الموقف التكتيكي. وقد استفاد ذلك أيضا من التقلص الكبير في التسامح مع المخاطر على المستوى السياسي خلال ما كان يُنظر إليه في كثير من الأحيان على أنه صراعات تقديرية وغير شعبية. وقد أدى هذا بدوره إلى زيادة الرغبة في تجنب تفويض السيطرة والأذونات إلى المستوى التكتيكي. تؤدي ممارسات القيادة الحالية إلى زيادة المركزية وتقليل وتيرة التشغيل وتقديم مجموعة من التعقيدات المحتملة على مستوى النطاق الترددي ونقاط الضعف الكهرومغناطيسية في العمليات الجوية. على الرغم من أن النزاعات التقديرية هي السياق الذي تم فيه احتجاز السلطات في مستويات أعلى، فإن العودة نحو التخطيط للنزاعات عالية المستوى قد لا يؤدي إلى انعكاس طبيعي لهذا الاتجاه. من المرجح أن ينظر كبار السياسيين والقادة العسكريين في العديد من البلدان إلى المخاطر الجيوسياسية الأسوء بكثير التي ينطوي عليها صراع الأقران على أنها سبب لمواصلة الإدارة المركزية لصنع القرار التكتيكي. ومع ذلك، فإنّه من شبه المؤكد فشل هذا النهج عمليًا ضد خصوم الأقران والأقران نظرًا لبطء الإيقاع التشغيلي، والاتصال خارج خط البصر والنطاق الترددي الذي يتطلبه. يجب أن تتغير ثقافة القائد الجوي التكتيكي لتجنب الشلل التشغيلي لكي تكون مناسبة للنزاعات المستقبلية بين الدول، حيث إن الهجمات الحركية والكهرومغناطيسية والسيبرانية على بناء مركز العمليات الجوية المشتركة (CAOC)وروابط الاتصالات الداعمة لها تقطع القادة عن أصول الخطوط الأمامية.

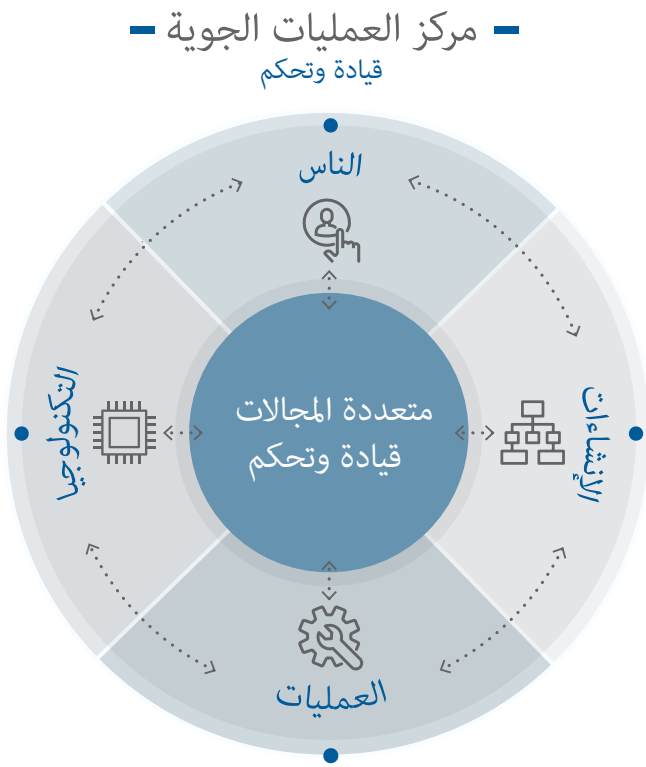
على زيادة مستوى المخاطر بشكل مطرد للعمليات الجوية التقليدية التي تعتمد بشكل كبير على أصول القيادة والتحكم المركزية مثل إي-3 أواكس (E-3 AWACS). ستعمل أنظمة صواريخ السطح- جو بعيدة المدى وصواريخ جو- جو بعيدة المدى (VLRAAMs) والطائرات المقاتلة والاعتراضية ذات مستوى الملاحظة المنخفض جدًا بشكل متزايد على إجبار طائرات القيادة والتحكم التقليدية (C2) والاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) على العمل بعيدًا جدًا عن الأراضي المعادية، ستؤدي أجهزة الاستشعار الموجودة على متنها وقدرات مركز الاتصالات إلى تقليل المنفعة التشغيلية بشكل كبير. في الوقت نفسه، يستمر توافر أنظمة الضربات الدقيقة بعيدة المدى والأدوات الإلكترونية الهجومية في زيادة التهديد الذي يمكن أن تشكّله الدول الحديثة على مرافق القيادة والسيطرة الأرضية المركزية لبعضها البعض مثل مراكز العمليات الجوية المشتركة (كوشال، مايسي وستيكينغز، 2019). وعليه، تواجه اثنتان من الركائز الأساسية للقوة الجوية الغربية في أوائل القرن الحادي والعشرين تحديًا وجوديًا محتملاً.

منذ أواخر الثمانينيات، اعتمدت القوات الجوية الغربية بشكل كبير على القوة الجوية لتمكين عمليات القوات المشتركة من إجراء عمليات برية وبحرية أصغر بكثير مما كان يمكن أن يكون ضروريًا لولا ذلك. وقد أدى النجاح المذهل لهذا النموذج في صراعات متعددة خلال التسعينيات والعقد الأول من القرن الحادي والعشرين إلى تصميم القوة عبر الجيوش والبحرية التي افترضت توفر الدعم الجوي وقدرات القيادة والتحكم التقليدية (C2) الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) الممكّنين جواً. وبذلك، فإن القدرة على توفير قدرات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) عند الطلب والدعم الناري من الجو تمثل الآن شرط أساسي مسبق للعديد من الدول الغربية لتوظيف القوة العسكرية. كما أدى الاعتماد على عمليات التحالف لتوليد شرعية جماهيرية وسياسية إلى خلق متطلبات التكامل وعدم التضارب والأذونات والرقابة كجزء من العمليات الجوية اليومية. لقد أدى هذا المزيج من الاعتماد على القوة الجوية للعمليات المشتركة، وتكامل التحالف كمتطلب ثابت، إلى إنشاء نموذج قياة وتحكم (C2) شديد المركزية مع إنشاء مركز العمليات الجوية المشترك (CAOC) كنقطة محورية.

النماذج القديمة لأنظمة القيادة والتحكم (C2) مراكز العمليات الجوية المشتركة (CAOC)

يتم إنشاء أمر المهام الجوية (ATO) ضمن مركز العمليات الجوية المشتركة لمدة 72 ساعة بالرجوع إلى مختلف مهام القوة المشتركة ومنتجات الاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) وعمليات الأذونات الطارئة متعددة الجنسيات والعوامل التمكينية مثل الناقلات. تتطلب هذه العملية مئات من المتخصصين المختصّين، ومرافق كبيرة وثابتة وروابط اتصالات ممتازة، الأمر الذي يجعل مركز العمليات الجوية المشترك (CAOC) هدفًا قيمًا وواضحًا للغاية للدول المعادية في أي حرب كبرى. كلما اقترب المركز من منطقة العمليات، زاد احتمال تعرضه لقدرات الضربة الدقيقة الحركية بعيدة المدى. ومع ذلك، كلما تمت

القيادة والتحكم (C2) والاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) الموزّعة من الجيل التالي لا يتطلّب روابط بيانات وأجهزة استشعار آمنة وغير واضحة فحسب، بل قدرة معالجة ديناميكية أيضًا للحد من متطلبات النطاق الترددي وتحديد البيانات ذات الصلة ونقلها تلقائيًا إلى الأصول الأخرى. لذلك، قد تظل القوات الجوية في المستقبل المنظور معتمدة على قدرات القيادة والتحكم (C2) المركزية على أساس أنظمة قديمة كبيرة الحجم.



بيئة المستقبل

تتميز بيئة القتال الجوية المستقبلية بالتطور المتزايد في كل مكان لأنظمة صواريخ سطح- جو بعيدة المدى (برونك، 2020 أ)، وصواريخ جو- جو بعيدة المدى (VLRAAMs) والطائرات المقاتلة والاعتراضية ذات مستوى الملاحظة المنخفض جدًا (VLO) (برونك ، 2020 ب). يعمل هذا الجيل الجديد من أنظمة التهديد

5 القيادة والسيطرة اللامركزية في العمليات الجوية: الآثار المترتبة على إدارة المعركة الجوية وقيادة المهمة

جاستن برونك

زميل باحث في القوة الجوية،معهد رويال يونايتد للخدمات (RUSI)، لندن

مقدمة

تدرك القوات الجوية في جميع أنحاء العالم التي تركز على المنافسة العسكرية بين الأقران أو شبه الأقران بشكل متزايد الحاجة إلى تبني تصاميم قيادة وتحكم (C2) غير مركزية للمهمة. ولكن، يجب التغلب على مستوى المقاومة الثقافية والسياسية العالي للسماح بتحقيق ذلك. وستتطلب قدرات القيادة والتحكم (C2) اللامركزية إعادة إدخال المفاهيم التقليدية لقيادة المهمة حيث يتم تفويض سلطات صنع القرار والأذونات بشكل متزايد إلى قادة القتال المتوسطي الرتب نسبيًا على المستوى التكتيكي. ومع ذلك، يتم تطوير معظم تصاميم القيادة والتحكم (C2) المستقبلية بدرجة معينة على الأقل من اللامركزية حتى يصبح من الصعب على القوى المعارضة العثور على العقد الرئيسية المحمولة جواً والأرضية واستهدافها وتحطيمها. تستكشف دول القوة الجوية الرائدة مجموعات الأصول المدارية الموزعة والمركبات الجوية غير المأهولة (UAV) لتحل محل عمليات المعالجة والاستغلال والنشر(PED) ومنصات القيادة والتحكم (C2) القديمة.

وفيما لا يزال الشكل المستقبلي للمجال المداري كجزء من هندسات القيادة والتحكم (C2) والاستخبارات والمراقبة والاستحواذ على الهدف والاستطلاع (ISTAR) الموزعة غير مؤكد لأن التقدم السريع على مستوى قدرات أجهزة الاستشعار الفضائية وعرض النطاق الترددي للاتصالات والمتانة تشير إلى زيادة حادة في دورها، ومع ذلك، فإنّه من المحتمل أيضًا أن يكون استخدام هذه الأصول عملية متنازع عليها بشدة أو حتى مرفوضة في المستقبل. توفر الطائرات دون طيار إمكانية التحمل لفترة طويلة دون المسارات نفسها التي يمكن التنبؤ بها والتي يحتمل أن تكون معرّضة للخطر مثل الأقمار الصناعية في المدار. إنّ بقاء منصات الجيل الخامس مثل مقاتلة اف-35 (F-35) والطائرات دون طيار التي تكون إمكانية ملاحظتها منخفضة جدًا مثل أحجار الأساس في بنية

المراجع:

ألي، جي. آر. وحسين، إيه.، 2017، مجلة Proceedings، المعهد البحري الأميركي، المجلد 143، الرقم 7.

كلارك بي.، بات، د.، شرام، إتش.، 2020، Mosaic Warfare Exploiting Artificial Intelligence And Autonomous Systems To Implement Decision-Centric Operations ، مركز التقييمات الإستراتيجية والمتعلقة بالميزانية، واشنطن.

فادوك، دي. اس.، 1997، ' John Boyd and John Warden: Airpower's Quest for Strategic Paralysis'الصفحات 357 و398 في فيليب اس. ميلينغير (محرر)، The Paths of Heaven The Evolution of Airpower Theory, Air University Press، قاعدة ماكسويل الجوية التابعة للقوات الجوية الأمريكية.

غروتزماخر، آر.، باراديس، د. ولي، كاي. بي، 2019، ' Forecasting transformative AI: an expert survey'، حواسيب ومجتمع، جامعة كورنويل، تم الولوج اليها بتاريخ 26 سبتمبر 2021، https://arxiv.org/abs/1901.08579

لايتون، بي.، 2021 Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars'، سلسلة أوراق الدراسات المشتركة رقم 4، قسم الدفاع، كانبيرا.

تراجتنبرغ، ام.، 2018، AI as the next GPT: a political-economy perspective، المكتب الوطني للبحوث الاقتصادية ، كامبريدج.

فيرجون، دي.، 2021 ' DOD Focuses on Aspirational Challenges in Future Warfighting' أخبار وزارة الدفاع، تاريخ الولوج 17 سبتمبر 2021، <https://www.defense.gov/Explore/News/Article/Article/2707633/dod-focuses-on-aspirational-challenges-in-future-warfighting/#DCT>.

ويسلي، ايه. جيه.، وسيمبسون، ار. اتش.، 2020، Expanding the battlefield: an important fundamental of multi-domain operations، رابطة جيش الولايات المتحدة ، أرلينغتون.

ويستوود، سي.، 2020، 5th Generation Air Battle Management، مركز تطوير القوة الجوية ، كانبرا.

متدفق مستمر. تعني القيود المادية أن الأمر سيستغرق وقتًا لإعادة تسليح آلات القوة الخاصة وإعادة تزويدها بالوقود وتغيير موضعها من أجل هجمات المتابعة.

من ناحية أخرى ، يمكن أن يكون خيار ما بعد OODA أكثر من عمل مستمر لأنه يتبع بشكل فعال خطة مفصلة وإن كانت مستنيرة من خلال استشعار ساحة المعركة IoBT. قد يناسب بناء صنع القرار هذا دفاعًا نشطًا امتص الهجوم الأول، وتعلم منه، ثم هاجم بطريقة محددة مسبقًا. بالنظر إلى سرعات معالجة الذكاء الاصطناعي، سيتم تحديد الاستجابة على الفور قبل إطلاقها ، مما يسمح بتحقيق أكبر قيمة من التعلم الآلي للذكاء الاصطناعي "أثناء العمل".

وأخيرًا، يقدم خيار وقف الآخرين عن اتخاذ القرار أملًا كبيرًا للمدافعين ولكنه يتطلب معرفة جيدة بالخصم من حيث أنظمة المراقبة والاستطلاع المستخدمة وإدراك الأشخاص المعنيين. يبدو أنه الأنسب لحالات الصراع المجمدة حيث يمكن وضع الأنظمة "المخادعة" على النحو الأمثل، وفهم البيئة جيدًا ومواجهة خصم واحد. قد يكون هذا الخيار أقل ملائمة للقوات التي تنتشر في مناطق القتال البعيدة بسرعة ولديها فهم محدود للموقف.

سيعتمد الخيار المفضل على السياق ولكنه يسلط الضوء على أنه ليس كل استخدام للذكاء الاصطناعي في نزاع قد يستخدم نفس التكنولوجيا بنفس الطريقة، حتى في المجال الضيق لصنع القرار. ليس هناك شك في أن الذكاء الاصطناعي سيغير بشكل كبير عملية صنع القرار المتعلق بالحرب الجوية، والأهم من ذلك، على المدى القريب. اختيار كل قوة جوية اليوم هو الطريقة الأفضل بالنسبة لهم. حان الوقت الآن لبدء التفكير بعمق في هذه القضية.

قد يكون نموذج اتخاذ القرار بمساعدة الذكاء الاصطناعي والتعلم الآلي هو "استشعر، توقّع، وافق، إعمَل": يستشعر الذكاء الاصطناعي البيئة للعثور على قوى الخصم والقوى الصديقة. يتوقع الذكاء الاصطناعي ما يمكن أن تفعله القوات المعادية في المستقبل القريب ويقدم المشورة بشأن أفضل استجابة للقوات الصديقة ؛ يوافق الجانب البشري من فريق الإنسان والآلة ؛ ويعمل الذكاء الاصطناعي من خلال إرسال تعليمات من آلة إلى آلة إلى مجموعة متنوعة من الأنظمة التي تدعم الذكاء الاصطناعي والمنتشرة في جميع أنحاء ساحة المعركة. في ظل خيار اتخاذ القرار هذا، تهدف القوات الصديقة إلى الاستيلاء على المبادرة والتصرف قبل القوات المعادية. إنه شكل محسوب للغاية من المستوى التكتيكي الاستباقي المستمر.

> الذكاء الاصطناعي سيجعل من الأسهل بكثير اكتشاف الأشياء وتحديد موقعها وتحديدها عبر ساحة المعركة.

الخيار 3: وقف الآخرين عن اتخاذ القرار

إن أحد البدائل لمحاولة اتخاذ قرارات القوة الودية بشكل أسرع هو محاولة إبطاء عملية اتخاذ القرار للخصم. في الحرب الجوية، يحتاج المهاجم إلى معلومات كبيرة حول الهدف ودفاعاته لشن غارات جوية ناجحة.

ولمنع ذلك، يمكن أن تنتشر الأنظمة "الخادعة" التي تدعم الذكاء الاصطناعي عبر ساحة المعركة، سواء على الصعيد المادي أو في الفضاء الإلكتروني. يمكن لأنظمة الحوسبة الصغيرة والمتنقلة والمتناثرة على نطاق واسع أن تخلق أنماطًا إلكترونية معقدة من خلال إرسال مجموعة من الإشارات ذات الدقة المتفاوتة. قد يتم تثبيت هذه الأنظمة على طائرات بدون طيار لأكبر قدر من التنقل، على الرغم من أن المركبات الأرضية غير المأهولة التي تستخدم شبكة الطرق قد تكون مفيدة أيضًا لوظائف محددة مثل التظاهر بأنها أنظمة صواريخ سطح- جو متنقلة، حيث يتمحور القصد من ذلك حول هزيمة أنظمة "البحث" للخصم من خلال بناء صورة مضللة أو على الأقل مشوشة لساحة المعركة.

كما ويمكن أيضًا استخدام الأنظمة "المخادعة" التي تدعم الذكاء الاصطناعي جنبًا إلى جنب مع حملة خداع معقدة. على سبيل المثال، يمكن أن تقلع العديد من الطائرات بدون طيار عندما تقوم بإرسال فاكس صاخب للتوقيع الإلكتروني لمقاتلي القوة الصديقة عندما يفعلون ذلك. مع وجود أعداد كبيرة جدًا من الطائرات المقاتلة التي تحلق فجأة في الجو، فإن الخصم لن يكون متأكدًا مما هو حقيقة ومما هو عكس ذلك.

الخاتمة

تقدم الخيارات الثلاثة خيارات حقيقية من حيث اتخاذ القرار. ربما على خلاف مع التصورات الأولية ، من المرجح أن يتضمن مفهوم الحرب الفائقة سلسلة من الهجمات متعددة المجالات أو هجمات التشنج بدلاً من إجراء

الخيار 1: الحرب المفرطة

يقدم الذكاء الاصطناعي رؤى الحرب بسرعة الآلة. يرى جون ألين وأمير حسين أن الذكاء الاصطناعي يسمح بالحرب المفرطة حيث: "سوف تتزايد سرعة المعركة في النهاية التكتيكية لطيف الحرب بشكل كبير، مما يؤدي إلى انهيار دورة اتخاذ القرار إلى أجزاء من الثانية، مما يمنح الجانب الحاسم التزامن المستقل بين القرار والعمل ". (ألين 2017)

في حالة اتخاذ قرارات الحرب الجوية، يوفر نموذج راقب، وجّه، قرّر، تصرّف (OODA) إطارًا مفيدًا لتقدير هذه الفكرة. دعا مصمم النموذج ، جون بويد ، إلى اتخاذ القرارات بشكل أسرع للدخول في دورة اتخاذ القرار لدى الخصم. إنّ هذا من شأنه أن يعطل تفكير قائد العدو ويخلق موقفًا خطيرًا على ما يبدو ويعيق تكيفهم مع بيئة سريعة التغير الآن. (فدوق 1997 ، ص 364-368)

ففي وظيفة "راقِب"، سيتم استخدام الذكاء الاصطناعي للحوسبة المتطورة في معظم أجهزة شبكة إنترنت أشياء ساحة المعركة (IoBT) ثم مرة أخرى في مركز القيادة المركزي الذي دمج بيانات الشبكة المذكورة والواردة في صورة واحدة شاملة. بالنسبة لوظيفة "وجّه"، سيلعب الذكاء الاصطناعي دورًا مهمًا في نظام إدارة المعركة. (ويستوود 2020 ، 22) لن ينتج الذكاء الاصطناعي صورة جوية شاملة في الوقت الفعلي فحسب، بل سيتنبأ أيضًا بمسارات العدو الجوية وحركاته.

ستنتقل معالجة طبقة الذكاء الاصطناعي التالية "قرّر" في إدراك توفر وحدات الدفاع الجوي الودية إلى القائد البشري للموافقة على قائمة ذات أولوية بالاقتراب من الأهداف الجوية المعادية للاشتباك، والأنواع المثلى للهجوم متعدد المجالات لتوظيفها، والتوقيتات المعنية وأي اعتبارات تتعلق بعدم التضارب. سيبقى البشر في الحلقة أو السيطرة على الحلقة حسب الضرورة، ليس فقط لأسباب تتعلق بقانون النزاع المسلح ولكن لأن الذكاء الاصطناعي يمكن أن يرتكب الأخطاء ويحتاج إلى التحقق قبل اتخاذ أي قرارات لا رجعة فيها. بعد الموافقة البشرية، تتمحور وظيفة "تصرّف" في الذكاء الاصطناعي حول تحديد الأسلحة الأفضل لكل هدف لتمرير بيانات الاستهداف المطلوبة تلقائيًا، كما تضمن عدم التضارب مع القوات الصديقة وتأكيد وقت الاشتباك مع الهدف، كما أنّه من المحتمل أن تطلب إعادة إمداد السلاح.

الخيار 2: ما بعد نموذج راقب، وجّه، قرّر، تصرّف (OODA)

تتكاثر تقنية الذكاء الاصطناعي بسرعة مما يجعل من المحتمل أن تكون القوى الصديقة والقوى المعادية تتمتع بالقدرات نفسها في الحرب الشديدة. قد يحتاج نموذج راقب، وجّه، قرّر، تصرّف (OODA) لاتخاذ القرار بعد ذلك إلى التغيير. وبموجب ذلك، فإنّه لا يمكن إجراء الملاحظة إلا بعد وقوع الحدث. إنّ النموذج بطبيعته ينظر إلى الوراء في الوقت المناسب. يمكن للذكاء الاصطناعي إحداث تحوّل دقيق. من خلال الجمع بين النماذج الرقمية المناسبة للبيئة والقوى المتعارضة مع بيانات "العثور" عالية الجودة من شبكة إنترنت أشياء ساحة المعركة (IoBT)، يمكن للذكاء الاصطناعي أن يتنبأ بمدى الإجراءات المستقبلية التي يمكن أن يتخذها الخصم، ومنها الإجراءات التي قد تتخذها القوة الصديقة بشكل أفضل لمواجهة هؤلاء.

خيارات صنع القرار البديلة

ستتأثر خيارات اتخاذ القرار الممكنة بشأن الذكاء الاصطناعي والتعلم الآلي بكل من التقنيات واحتياجات المفاهيم التشغيلية المرغوبة. إنّ البدائل التي تمت مناقشتها هنا هي استخدام التكنولوجيا ليصبح من الممكن الرد على تصرفات الخصم بشكل أسرع، أو للتصدي للخصم من خلال الإجراءات الاستباقية المدفوعة بالتكنولوجيا، أو لإبطاء عملية اتخاذ القرار للخصم بشكل كبير.

حقل إنترنت أشياء ساحة المعركة (IoBT) الكبير مما يؤدي إلى إنشاء شبكة قتل ، حيث يتم تحديد أفضل مسار لتحقيق مهمة ما واستخدامه في الوقت الفعلي تقريبًا. يصبح استخدام حقل إنترنت أشياء ساحة المعركة (IoBT) مائعًا ومتغيرًا باستمرار، وليس تدفقًا ثابتًا للبيانات كما يوحي نموذج سلسلة القتل الأقدم. إنّ النتيجة هي أن مفهوم الفسيفساء يوفر شبكات عالية المرونة من العقد الزائدة عن الحاجة ومسارات قتل متعددة. (كلارك 2020 ، 27-32) إنّ هذا التفكير عبر المجالات يتطور الآن بشكل أكبر إلى مفاهيم "المناورة الموسعة". (فيرغون 2021)

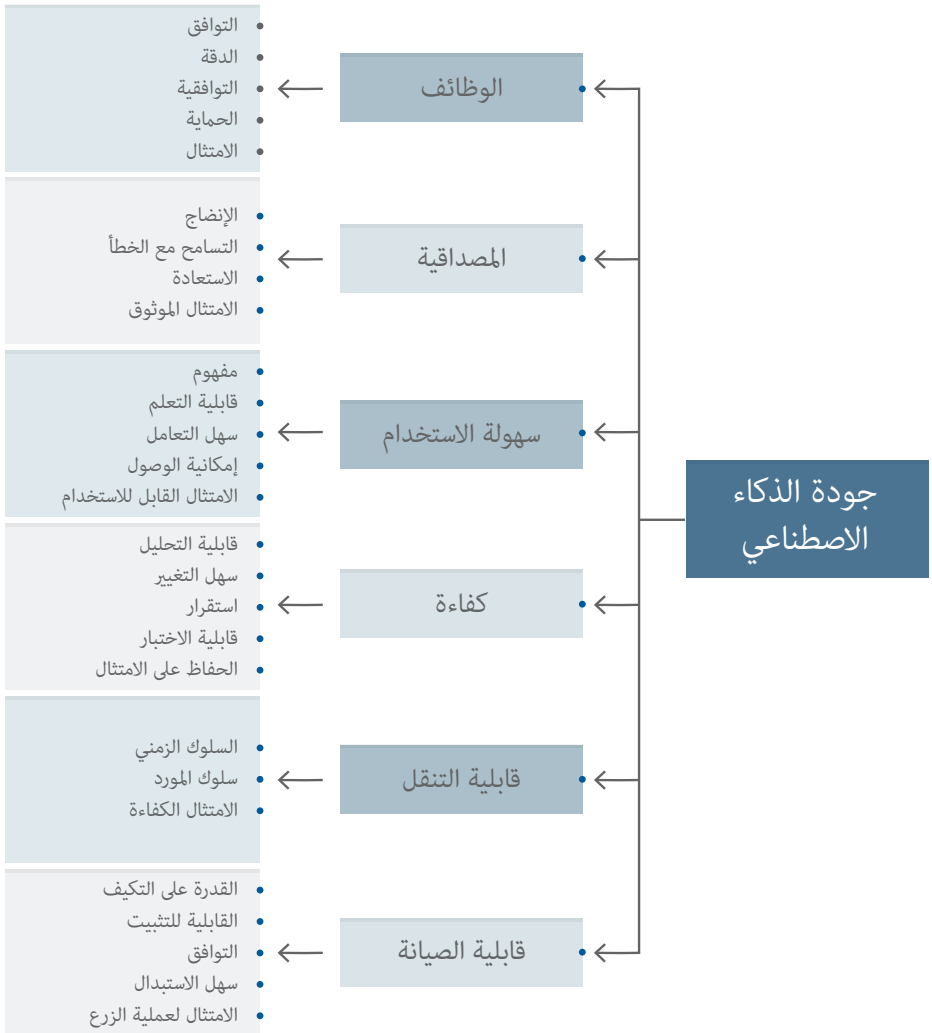
إن تعقيد تنفيذ هذه المفاهيم العملياتية المتشابكة ضد الأعداء الأقران خلال صراع كبير ظاهر بسهولة، بحيث إنّ إجراء عمليات متعددة المجالات تتضمن عمليات تقارب وفسيفساء ومناورة موسعة وعملية تتطلب استخدام أنظمة مؤتمتة تستخدم الذكاء الاصطناعي مع التعلم الآلي.

فعلى المدى القريب إلى المتوسط، فإن عامل الجذب الرئيسي للذكاء الاصطناعي في اتخاذ القرار الذي يتضمن مثل هذه التركيبات المعقدة سيتمثل بقدرته على التعرف السريع على الأنماط واكتشاف العناصر المخبأة داخل مجموعات البيانات الكبيرة التي يجمعها إنترنت الأشياء. أما النتيجة الرئيسية لذلك فهي أن الذكاء الاصطناعي سيجعل من الأسهل بكثير اكتشاف الأشياء وتحديد موقعها وتحديدها عبر ساحة المعركة. سيصبح الاختباء أكثر صعوبة والاستهداف أسهل بكثير. من ناحية أخرى، لا يعد الذكاء الاصطناعي مثاليًا. حيث أنّ به مشاكل معروفة جيدًا في القدرة على الانخداع وهشاشة وعدم قدرة على نقل المعرفة المكتسبة في مهمة إلى أخرى والاعتماد على البيانات. (لايتون 2021 ، ص 13-15)

ثم تصبح الأداة الرئيسية القتالية للذكاء الاصطناعي هي "البحث والخداع". يعد الذكاء الاصطناعي بفضل تعلم الآلة ممتازًا في العثور على العناصر المخبأة داخل خلفية عالية الفوضى. ومع ذلك، فإنّه يفتقر إلى القوة على مستوى القدرة على عدم الانخداع.

إنّ نقطة بداية "البحث" هي وضع العديد من مستشعرات شبكة إنترنت أشياء ساحة المعركة (IoBT) منخفضة التكلفة في أفضل المواقع البرية والبحرية والجوية والفضائية والإلكترونية في تلك المناطق التي قد تمر عبرها القوات المعادية. قد تضم ساحة المعركة المستقبلية المئات، وربما الآلاف، من أنظمة المراقبة والاستطلاع الصغيرة والمتوسطة الثابتة والمتنقلة التي تدعم الذكاء الاصطناعي والتي تعمل في جميع المجالات. في الوقت نفسه، قد يكون ثمة عدد مكافئ من أنظمة التشويش والخداع التي تدعم الذكاء الاصطناعي والتي تعمل بشكل جماعي في محاولة لخلق انطباع خاطئ ومضلل عن عمد عن ساحة المعركة في عقل الخصم.

وفي أي مجال. (ويسلي2020، 4-5) على سبيل المثال، ستتمكن الوحدات البرية الآن من الاشتباك مع السفن في البحر، وستهاجم القوات الجوية الأنظمة الفضائية والإنترنت في كل مكان، في وقت واحد وفي بيئات متنازع عليها.



يتخلى مثل هذا المفهوم التشغيلي عن سلاسل القتل الخطية التقليدية ذات النطاق الفردي لاحتضان تلك المتعددة المجالات التي تستفيد من مسارات بديلة أو متعددة. تتصور بنية "الفسيفساء" المرتبطة الناشئة تدفق البيانات عبر

مسائل التكنولوجيا

تطور الذكاء الاصطناعي الحديث لتلبية احتياجات المجال التجاري وخاصة المستهلكين. وكان التقدم الرئيسي عندما أصبحت وحدات معالجة الرسومات (GPU) المنخفضة التكلفة متاحة بسهولة، وذلك لتلبية الطلب على ألعاب الفيديو بشكل أساسي. بفضل معالجتها المتوازية الضخمة، يمكن لوحدات معالجة الرسومات تشغيل برامج التعلم الآلي بسهولة. يعد التعلم الآلي مفهومًا قديمًا ولكنه يحتاج إلى الجمع بين وحدات معالجة الرسومات والوصول إلى مجموعات "البيانات الضخمة" لجعلها عملية وبأسعار معقولة على نطاق واسع.

في التعلم الآلي، تنتج خوارزميات الكمبيوتر وليس مبرمجي الكمبيوتر البشريين الخارجيين، تسلسل التعليمات والقواعد التي يستخدمها الذكاء الاصطناعي بعد ذلك لحل المشكلات. بشكل عام، كلما زادت البيانات المستخدمة لتدريب الخوارزمية، كانت القواعد والتعليمات الموضوعة أفضل. بالنظر إلى ذلك، يمكن للذكاء الاصطناعي مع التعلم الآلي أن يعلّم نفسه أثناء "العمل" ويتحسن تدريجيًا في مهمة ما لأنه يكتسب باستمرار المزيد من الخبرة فيها.

ففي كثير من الحالات، تأتي هذه البيانات من شبكة واسعة النطاق من الأجهزة المترابطة التي تجمع المعلومات من الميدان ثم تنقلها عبر "سحابة" لاسلكية إلى كمبيوتر بعيد يعمل بالذكاء الاصطناعي لمعالجتها. في القطاع العسكري، تتميز شبكة إنترنت أشياء ساحة المعركة (IoBT) بالأجهزة الثابتة والمتنقلة، بما في ذلك الطائرات بدون طيار القادرة على التعاون مع بعضها البعض ضمن أسراب. كما وتوفر شبكات إنترنت أشياء ساحة المعركة (IoBT) قدرات الاستشعار والتحكم عن بعد ولكنها تولد في الوقت نفسه كميات هائلة من البيانات. تتمثل إحدى الطرق للتغلب على ذلك في توصيل الشبكة بجهاز حديث قادر على تقييم البيانات في الوقت الفعلي وإعادة توجيه أهم المعلومات إلى السحابة وحذف الباقي، وبالتالي توفير مساحة التخزين وعرض النطاق الترددي.

وتتم معظم عمليات الحوسبة المتطورة الآن باستخدام شرائح الذكاء الاصطناعي. تعد هذه الأخيرة صغيرة من حيث الحجم وغير مكلفة نسبيًا، كما أنّها تستخدم الحد الأدنى من الطاقة وتولّد القليل من الحرارة مما يسمح بدمجها بسهولة في الأجهزة المحمولة مثل الهواتف الذكية والأجهزة غير الاستهلاكية مثل الروبوتات الصناعية. ومع ذلك، يتم استخدام الذكاء الاصطناعي في العديد من التطبيقات بطريقة هجينة: جزء منها على الجهاز والبعض الآخر عن بعد في مركز اندماج بعيد يمكن الوصول إليه عبر السحابة.

التركيبات التشغيلية

يظهر العديد من المفاهيم العملياتية الهامة ذات الصلة بالحرب الجوية المستقبلية، حيث تنتقل العمليات من كونها مشتركة إلى كونها متعددة المجالات الآن أي عبر البر والبحر والجو والإنترنت والفضاء. ويُقصَد من مفهوم المتابعة المسمى "التقارب" هو أن القوات الصديقة يجب أن تكون قادرة على مهاجمة الوحدات المعادية عبر

4 خيارات مستقبلية للذكاء الاصطناعي واتخاذ القرار بمساعدة التعلم الآلي في الحرب الجوية

د. بيتر لايتون
زميل زائر، معهد جريفيث آسيا

مقدمة

تتضمن الحرب الجوية التكنولوجيا وتتشكّل منها على حد سواء. لقد ربطت التقنيات المستخدمة الإجراءات المحتملة التي يمكن أن تتخذها القوات الجوية، سواء بهدف تمكين أو تقييد خيارات توظيف القوة. في ضوء ذلك، تجذب التقنيات الجديدة الرئيسية الناشئة دائمًا اهتمامًا كبيرًا، واليوم يركز هذا على الذكاء الاصطناعي (AI).

في المستقبل المنظور، يعد ذلك تقنية ذكاء اصطناعي ضيّقة وليست عامة. ويساوي الذكاء الاصطناعي الضيّق أو يتجاوز الذكاء البشري لمهام محددة ضمن مجال معين. وفي المقابل، فإن الذكاء الاصطناعي العام يساوي النطاق الكامل للأداء البشري لأي مهمة في أي مجال، حيث يظهر الذكاء الاصطناعي العام على بعد عقود عدة. (غروتزيماخر، 2019)

ويتمثل الاهتمام العسكري العالمي على المدى القريب إلى المتوسط في كيفية استخدام تقنيات الذكاء الاصطناعي الضيقة في ساحة المعركة الحديثة، بحيث يمكن تطبيق مثل هذا الذكاء الاصطناعي بطرق متعددة ويمكن اعتباره تقنية للأغراض العامة، إذ سيصبح منتشر ومدمج في معظم الآلات العسكرية كما هو الحال في المجتمع الأوسع. (تراجتنبرج 2018)

تتمحور الفكرة الرئيسية لهذا المقال حول دور الذكاء الاصطناعي في صنع القرار وخاصة في الحرب الجوية، كما ويناقش المقال في البداية التكنولوجيا، قبل الإشارة إلى التركيبات التشغيلية وتنتهي في النظر في ثلاثة مناهج بديلة للذكاء الاصطناعي وصنع القرار بمساعدة التعلم الآلي في الحرب الجوية.

المراجع:

لينجل، شيريل، جيف هاغن، إريك هاستينغز، ماري لي، ماثيو سارجنت، ماثيو والش، لي آنج زانج، ديفيد بلانت، القيادة والتحكم المشتركين في جميع المجالات للحرب الحديثة، المجلد الأول: تطبيقات الذكاء الاصطناعي لجميع إدارة المجال والتحكم فيه، سانتا مونيكا، كاليفورنيا: مؤسسة RAND ،-RR-4408/1 AF، 2020.

التعلم المعزز والإشراف وغير الخاضع للإشراف ثلاثة أنواع من تعلم الآلة. تتعلم خوارزميات التعلم المعزز من الأخطاء عن طريق التجربة والخطأ.

ماثيو والش، لانس مينث، إدوارد جيست، إريك هاستينغز، جوشوا كريجان، جاسمين ليفيلي، جوشوا مارجوليس، نيكولاس مارتن، بريان ب. دونيلي، استكشاف جدوى وفائدة القيادة والتحكم بمساعدة التعلم الآلي. المجلد 1، النتائج والتوصيات، تقرير مؤسسةRAND RR-A263-1 ، 2021.

يتم تحدي الخوارزميات من خلال المواقف التي يوجد فيها: (1) معلومات غير كاملة؛ (2) مدخلات صاخبة؛ و (3) نقص البيانات التاريخية أو بيئة محاكاة مناسبة للتدريب منها.

الجنرال تشارلز كيو براون جونيور ، تسريع التغيير أو الخسارة ، أغسطس 2020. الوصول إليه على https://www.af.mil/Portals/1/documents/2020SAF/ACOL_booklet_FINAL_13_Nov_1006_WEB.pdf

جون هاربر ، هل يهدر الجيش المليارات على جهود JADC2؟ ، 29 سبتمبر 2021 ، الدفاع الوطني. يمكن الوصول إليها على https://www.nationaldefensemagazine.org/articles/2021/9/29/will-the-military-waste-billions-on-jadc2-efforts

الاصطناعي، وتحسين إمكانية شرح الخوارزمية. من المحتمل أن تكون هناك حاجة إلى استثمارات عسكرية موجهة في المناطق التي يكون فيها الطلب التجاري أقل، مثل خوارزميات الذكاء الاصطناعي للتعلم حيث تكون البيانات نادرة أو للدفاع ضد الهجمات ضد تلك الخوارزميات ذاتها.

> بينما يتم تدريب المخططين وصانعي القرار اليوم على التفكير في مجال واحد ، فمن المحتمل أن تظهر أدوار جديدة تتطلب تدريب الأفراد على التفكير في مجالات متعددة في وقت واحد.

وتحتاج تقنيات الذكاء الاصطناعي/ التعلم الآلي الحالية إلى بيانات يمكن التعلم منها. نظرًا للافتقار (المحظوظ) لبيانات العالم الحقيقي للإبلاغ عن صقل هذه التقنيات للحرب، يمكن للجيش الاستفادة من النمذجة والمحاكاة والتمارين لإنشاء بيانات تدريب لخوارزميات الذكاء الاصطناعي/ التعلم الآلي. يمكن أن تساعد هذه الخوارزميات بعد ذلك في تطوير الاقتران بين الأسلحة والهدف على سبيل المثال.

ويمكن أن تدعم خوارزميات التعلم الخاضع للإشراف أو المعزز وظيفة القيادة والتحكم هذه، على غرار خوارزميات التعلم المطبقة مؤخرًا على الألعاب التجارية. لكن يجب أن تأخذ الخوارزميات العسكرية أيضًا في الحسبان عدم اليقين في مواقف العالم الحقيقي - وهي صعوبة كبيرة لكل من البشر والخوارزميات.

وكما قال رئيس أركان القوات الجوية الأمريكية في أغسطس 2020، "تسريع التغيير أو الخسارة". يُعد إحراز تقدم في الوقت المناسب نحو القيادة والتحكم المشترك لجميع المجالات (JADC2) أمرًا حتميًا للحرب الحديثة ، والقيام بذلك "ضمن الجداول الزمنية لميدان المنافسين" مطلوب. إنّ الطلب حقيقي ولكن من المهم تحديد توقعات واقعية للذكاء الاصطناعي/ التعليم الآلي. ثمة مجال للتحسين في عمليات القيادة والحكم الحالية مع الأتمتة، وفي بعض الحالات ، الذكاء الاصطناعي/ التعلم الآلي ؛ في المقابل ، ستظل عمليات القيادة والتحكم الأخرى صعبة لكل من البشر والخوارزميات. كما قال رئيس لجنة القوات المسلحة في مجلس النواب الأمريكي والممثل آدم سميث، دي-واشنطن، عن القيادة والتحكم المشترك لجميع المجالات (JADC2) في سبتمبر 2021 ، "الهدف صحيح، لكن لا تقلل من صعوبة تحقيقه."

التعلم الآلي إلى خلق أدوار ومسؤوليات جديدة. سيحتاج المشغلون إلى التدريب على إدارة النظام البيئي للذكاء الاصطناعي والتنقل فيه، كل ذلك أثناء العمل كمسؤولين عن البيانات لضمان جودة واكتمال البيانات التي تم التقاطها وتخزينها في هذا النظام البيئي. بالإضافة إلى ذلك، بينما يتم تدريب المخططين وصانعي القرار اليوم على التفكير في مجال واحد ، فمن المحتمل أن تظهر أدوار جديدة تتطلب تدريب الأفراد على التفكير في مجالات متعددة في وقت واحد.

أما الحاجز الرابع فهو وجود ثقافات فرعية عسكرية. قد يكون من الصعب دمج قدرات الذكاء الاصطناعي عبر المجالات الجوية والفضائية والسيبرانية حتى ضمن خدمة عسكرية واحدة فحسب، نظرًا للاختلافات في الثقافات الفرعية بين المشغلين، والاختلافات في الجداول الزمنية للتخطيط، والتوزيعات المتباينة للسلطات لتحقيق تأثيرات تشغيلية مختلفة. ومع ذلك، فإن الحاجة إلى قدرات القيادة والتحكم لجميع المجالات ملحة ومنتشرة بشكل متزايد. لهذا السبب، يجب مواجهة جميع هذه العوائق كالثقافة العسكرية، ومخاوف الأمن السيبراني، والخوارزميات المطبقة على مشاكل ضعف جودة المعرفة، وعدم إمكانية الوصول إلى البيانات، وإعادة هيكلة مركز العمليات والتدريب، والثقافات الفرعية العسكرية، وتجاوزها لتضمين تطبيقات الذكاء الاصطناعي في القيادة والتحكم المشترك لجميع المجالات(JADC2) .

المضي قدما بشكل فعال

قد تبدو الصورة قاتمة. ثمة العديد من الحواجز إلى جانب الحاجة الملحة للمضي قدمًا بسرعة والتي تتطلب التغيير الآن. ومع ذلك، يمكن إحراز تقدم إذا تم تقسيم الخطوات نحو الهدف إلى مشاكل يمكن حلها وإذا أبقى الجيش "عينيه مفتوحتين" على الإمكانيات والقيود التكنولوجية على حد سواء. لا ينبغي أن يكون الهدف أتمتة كاملة للقيادة والتحكم، بل يجب أن يكون فريقًا فعالًا بين الإنسان والآلة للقيادة والتحكم. يجب أن تتضمن الخطوات نحو هذه الغاية أولاً التطوير المستمر وتحديد أولويات مفاهيم تشغيل القيادة والتحكم المشترك لجميع المجالات (JADC2)، وثانيًا تحديد الاحتياجات والفرص المقابلة لزيادة الذكاء الاصطناعي/ التعلم الآلي في عمليات التمكين للقيادة والتحكم.

في الوقت نفسه، سيكون من الضروري تحديد الشروط لنظام بيئي للذكاء الاصطناعي يعتمد على البيانات، الأمر الذي يعني وضع أنظمة الأسلحة والبيانات ذات الصلة في بحيرات بيانات متعددة المجالات لاستخدامها من قبل أولئك الذين يجب أن يكون لديهم إمكانية الوصول إلى البيانات أثناء تطبيق "صفر- ثقة" ومبادئ الأمان الأخرى لضمان إدارة مرنة وآمنة لتلك البيانات. أثناء تطوير تطبيقات برامج الذكاء الاصطناعي، سيكون من الضروري تجربتها في بيئات اختبار التشغيل، ودمجها مع أنظمة القيادة والتحكم، ثم نشرها في مراكز العمليات. من المحتمل أن تكون هناك تكرارات للقدرات - أولاً وضع إمكانات محدودة في مراكز العمليات، ثم إنشاء ملاحظات المستخدم، ثم التحديث السريع لتطبيقات البرامج. سيرغب المحللون والتقنيون في استكشاف وتخطيط القدرات ومفهوم العمليات (CONOPS) لتسهيل التعاون بين الإنسان والآلة، وبناء الثقة البشرية في خوارزميات الذكاء

ستضع الحرب والمنافسة في جميع المجالات في الغد علاوات أعلى على نطاق وسرعة الوصول إلى المعلومات، على فهم تلك المعلومات، وعلى اتخاذ القرار السريع

تحديد حواجز الذكاء الاصطناعي/ التعلم الآلي للتغلب عليها

ثمة حواجز عدة أمام تحقيق وعد الذكاء الاصطناعي/ التعلم الآلي للتطبيقات العسكرية. يتمثل أحد العوائق في الثقافة العسكرية والتي غالبًا ما تتجنب المخاطر (الأرواح معرضة للخطر) على عكس العالم التجاري، حيث يمكن أن تؤدي المخاطرة الكبيرة إلى دفع مكافآت مالية كبيرة. ثمة اختلاف ثقافي مرتبط في مشاركة البيانات. يميل الجيش إلى الاهتمام بتأمين المعلومات (فقط لمن لديهم "الحاجة إلى المعرفة")، في حين يقدّر العالم التجاري الوصول المفتوح إلى البيانات ("المشاركة على نطاق واسع") لتطوير التطبيقات والمزايا المالية الأخرى. لذلك، سيكون من المهم دمج المخاوف الأمنية في عمليات تطوير البرامج العسكرية وتكنولوجيا المعلومات (IT)- المعروفة باسم DevSecOps- لإحباط الخصوم والجهات الفاعلة السيئة الذين قد يسعون إلى إضعاف قدرات القيادة والتحكم من خلال الوسائل الإلكترونية. ربما يكون أحد أكبر التحديات التي لم تتم مواجهتها بالكامل بعد هو ضمان ملاءمة خوارزميات الذكاء الاصطناعي/ التعلم الآلي للعالم الحقيقي والمواقف العسكرية التي يمثل فيها "ضباب الحرب" والمعلومات غير المكتملة والإجراءات المعادية تناقضات واضحة عن بيئة الألعاب.

ثمة عائق آخر يتمثل في عدم إمكانية الوصول إلى البيانات داخل الجيش نفسه. بهدف المضي قدمًا، سيحتاج الجيش إلى سياسة موحدة لإدارة البيانات وتكنولوجيا معلومات كافية لإتاحة كميات كبيرة من البيانات لقوات القيادة التحكم لدعم عملية صنع القرار بمساعدة الذكاء الاصطناعي. بمعنى آخر، يجب أن يكون هناك نظام بيئي للذكاء الاصطناعي يدعم جمع البيانات ووضع علامات عليها وتخزينها وتأمينها ومشاركتها. سيعتمد هذا النظام البيئي على معايير البيانات المشتركة، والسلطات المحددة بوضوح، وفحوصات السلامة، وضمانات التطفل. ستكون الحوسبة السحابية وبحيرات البيانات من المكونات الرئيسية. يمكن الاستفادة من بحيرة البيانات المستندة إلى السحابة للحوسبة الموزعة والتخزين الزائد والاتصال على مستوى المؤسسة. إن بناء بيئة كهذه لتوفير كميات كبيرة من البيانات بطريقة آمنة عبر المجالات ومستويات الأمان سيشكل تحديات القيادة والتحكم المشترك لجميع المجالات(JADC2) نظرًا للسياسات العسكرية القائمة، والثقافات، والسلطات، والميزانيات، ومسارات الاستحواذ.

الحاجز الثالث هو الحاجة إلى إعادة هيكلة مراكز العمليات العسكرية وتدريب الأفراد الذين يديرونها. من المرجح أن تؤدي زيادة الاتصال من آلة إلى آلة، جنبًا إلى جنب مع أتمتة عمليات القيادة والتحكم، إلى إحداث تغييرات مادية وتغييرات في التوظيف في مراكز العمليات، الأمر الذي يحرر المشغلين البشريين للانخراط في المزيد من المهام المعرفية مثل تقييم الدورات المحتملة وتنقيحها من العمل. سيؤدي اعتماد تقنيات الذكاء الاصطناعي/

نظرًا للتعقيد المتزايد لتخطيط العمليات متعددة المجالات (MDO)، والنطاقات الزمنية المنخفضة، ومتطلبات البيانات الأكبر، سيحتاج المخططون العسكريون إلى أدوات جديدة، بما في ذلك تلك القائمة على الذكاء الاصطناعي/ التعلم الآلي.

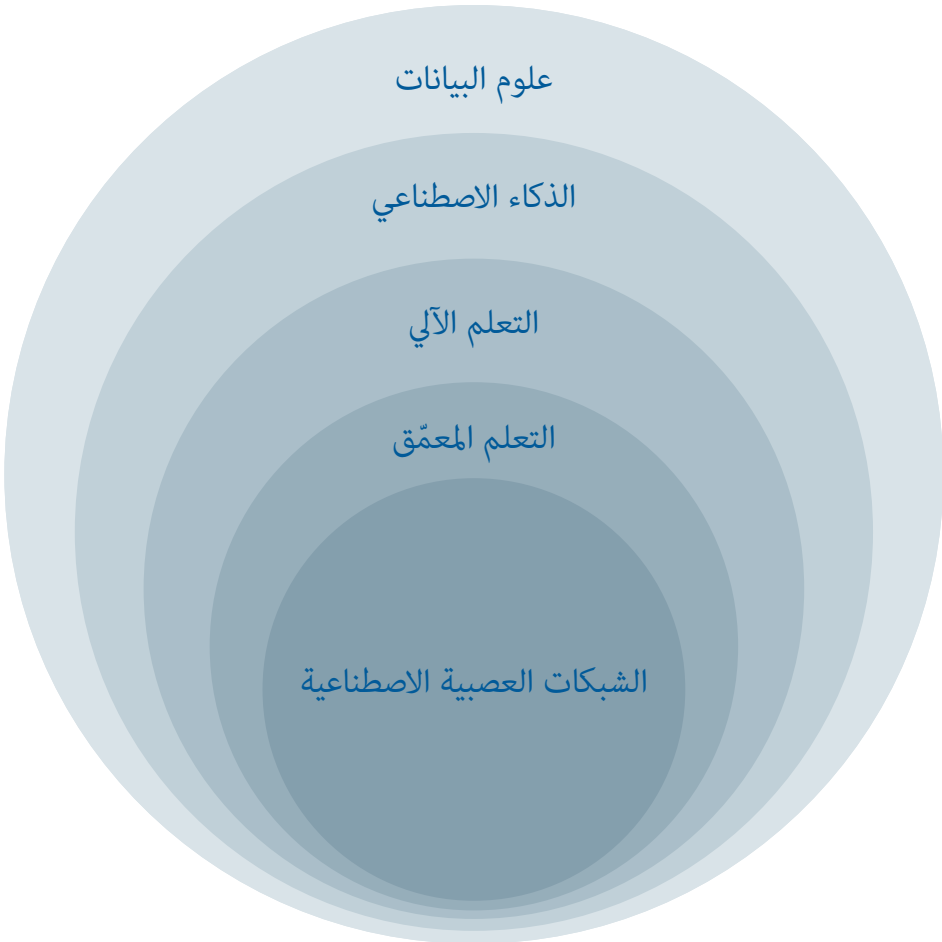
إغراء الذكاء الاصطناعي / التعلم الآلي (AI / ML)

تنبع جاذبية الذكاء الاصطناعي/ التعلم الآلي جزئيًا من العروض الأخيرة لأنظمة الذكاء الاصطناعي/ التعلم الآلي التي تحقق أداءً خارقًا في الألعاب المعقدة بشكل متزايد، جنبًا إلى جنب مع الاعتراف المتزايد بالمطالب التشغيلية للصراعات المتطورة في المستقبل. إنّ النجاح الأخير لألفاستار (AlphaStar)، وهو نظام ذكاء اصطناعي/ تعلم آلي تم تدريبه على أداء لعبة الإستراتيجية ستاركرافت (StarCraft) في الوقت الحقيقي، يلمّح إلى التطبيقات المستقبلية للتعلم الخاضع للإشراف والمعزز للقيادة والتحكم التكتيكي والتشغيلي. ومع ذلك، لا تزال هناك حاجة لأبحاث كبيرة لتحويل هذه التقنيات من الألعاب إلى القتال الحربي.

ونظرًا لأن خوارزميات الذكاء الاصطناعي يتم تطويرها من أجل العمليات الواقعية والديناميكية والمتعددة المجالات والواسعة النطاق وعالية الإيقاع، فستحتاج المقاييس المهمة إلى التحديد والتقييم والمراقبة لقياس أداء الخوارزمية وفعاليتها وملاءمتها. ستشمل مقاييس الخوارزمية الرئيسية ما يلي: الكفاءة (الوقت والذاكرة اللازمتان للحساب)، السلامة (ما إذا كانت الخوارزمية تنتج نتائج صحيحة)، الأداء الأمثل (ما إذا كانت الخوارزمية توفر أفضل نتيجة لهدف معين)، المتانة (ما إذا كانت الخوارزمية تتاثر بسهولة في ظل الحالات غير المتوقعة) ، القابلية للتفسير (ما إذا كان الإنسان يستطيع فهم "سبب" النتائج)، والتأكيد (ما إذا كانت الخوارزمية تعمل على النحو المنشود).

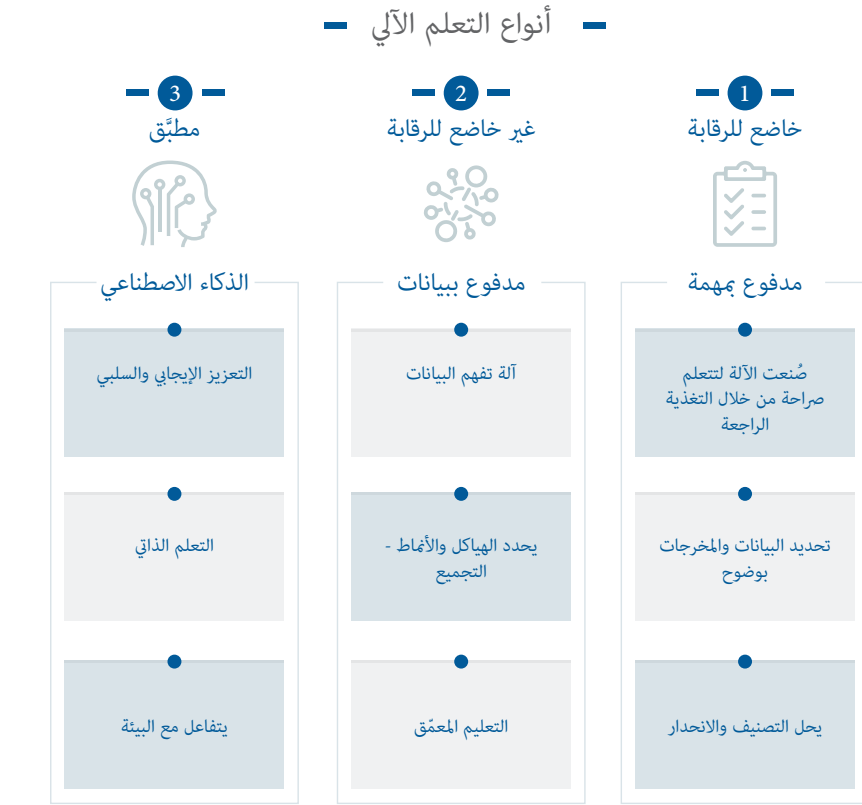
نظرًا لعدم وجود تطبيق مباشر لأنظمة الذكاء الاصطناعي/ التعلم الآلي التجارية والأكاديمية على المهام العسكرية، ستحتاج التقنيات إلى الانتقال إلى بيئة عسكرية قبل أن تتمكن من توفير ميزة تشغيلية. لتحديد تقنيات الذكاء الاصطناعي التي يجب متابعتها، يجب على الجيش أولاً فهم المتطلبات التشغيلية التي ستحتاج التقنيات إلى دعمها (على سبيل المثال التفوق الجوي، والدفاع الجوي، ودعم الناقلات، وما إلى ذلك). ستحدد المتطلبات التشغيلية بعد ذلك عمليات القيادة والتحكم (على سبيل المثال إدراك الواقع الميداني، وعدم تضارب المجال الجوي وما إلى ذلك) اللازمة لتمكين المهام التشغيلية. سيكون فهم قيود تقنيات الذكاء الاصطناعي/ تعلم الآلي، ولا سيما الصعوبة التي يواجهونها في التفكير في ظل ظروف عدم اليقين، مهمًا بنفس القدر. خلاف ذلك، قد لا ترقى التقنيات إلى مستوى التوقعات.

ومع ذلك ، فإن الأنظمة القديمة والبنية التحتية الحالية للتخطيط والجدولة وتنفيذ المهام العسكرية لا تتماشى مع العالم الحديث الشامل الذي يجب أن تتنافس فيه الجيوش. نظرًا للتعقيد المتزايد لتخطيط العمليات متعددة المجالات (MDO)، والنطاقات الزمنية المنخفضة، ومتطلبات البيانات الأكبر، سيحتاج المخططون العسكريون إلى أدوات جديدة، بما في ذلك تلك القائمة على الذكاء الاصطناعي/ التعلم الآلي. يتطلب تحديد الأولويات المناسبة للاستثمار في هذه الأدوات فهمًا لقدراتها، وحواجزها، والوفاء المحتمل باحتياجات القيادة والتحكم الناشئة من العمليات متعددة المجالات (MDO).



الحاجة إلى القيادة والتحكم المشترك لجميع المجالات (JADC2) لدعم العمليات متعددة المجالات (MDO)

توسعت الحرب الحديثة إلى ما وراء المجالات التقليدية للأرض والجو والبحر، الأمر الذي يتطلب من القادة العسكريين وموظفيهم التخطيط والقيادة والسيطرة على القوات ليس في هذه المجالات التقليدية فحسب بل في مجالات الفضاء والإنترنت وعبر الطيف الكهرومغناطيسي أيضًا. ولتعقيد الأمور أكثر، توسعت الأنشطة في جميع هذه المجالات إلى ما بعد الحرب التقليدية لتشكيل البيئة التنافسية التي تعيش فيها معظم الدول اليوم - قبل الأعمال العدائية المفتوحة. يجب أن يكون الجيش قادرًا على الاندماج عبر هذه المجالات ليس في الحرب فحسب، بل في المنافسة أيضًا. تتطلب العمليات العسكرية اليوم بالفعل وسائل مرنة وآمنة للاتصال ومشاركة البيانات عبر المستويات والمجالات والمؤسسات والمناطق الجغرافية. ستضع الحرب والمنافسة في جميع المجالات في الغد علاوات أعلى على نطاق وسرعة الوصول إلى المعلومات، على فهم تلك المعلومات، وعلى اتخاذ القرار السريع، وهي العناصر الرئيسية لقدرة القيادة والتحكم المشترك لجميع المجالات(JADC2) الفعالة.



3 تطوير مفهوم عمليات للقيادة والتحكم المشترك في جميع المجالات مع دور مُدمَج لتطبيقات الذكاء الاصطناعي

شيريل لينجيل

مهندس أعلى، شركة راند

قبل أن يتمكن المرء من الاستفادة من الذكاء الاصطناعي (AI) والتعلم الآلي (ML) للعمليات متعددة المجالات (MDOs)كجزء من القيادة والتحكم المشترك لجميع المجالات (JADC2) ، يتعين عليه القيام بالعمل الشاق المتمثل في إرساء "أساس المعلومات". يتطلب وضع هذا الأساس- الذي يتم فيه تمييز البيانات، وتخزينها ونقلها بشكل آمن، والوصول إليها بسهولة - العمل البسيط والمستمر لتنظيم وحماية جميع المعلومات التي يحتاجها الجيش للقيادة والتحكم عبر المجالات والخدمات والمستويات. ستكون نفس مجموعة المعلومات هي المدخلات لخوارزميات الذكاء الاصطناعي والتعلم الآلي. في غياب مثل هذا الأساس المعلوماتي، لا يمكن إحراز سوى تقدم ضئيل.

فعلى الرغم من أن النجاحات الأخيرة على مستوى الذكاء الاصطناعي/ التعلم الآلي كانت مشجعة في مجال الألعاب، فإن استخدام تقنيات مماثلة لبعض وظائف القيادة والتحكم سيظل يمثل تحديًا نظرًا للعوائق الواقعية المتمثلة في المعلومات غير المكتملة، وضعف جودة البيانات، والإجراءات المعادية. ستكون تقنيات الذكاء الاصطناعي/ التعلم الآلي الأخرى، مثل تلك الخاصة بالتنبؤ بحالة الطائرات في المسرح، أكثر قابلية للتطبيق.

وسيعتمد الوصول إلى أهداف القيادة والتحكم المشترك لجميع المجالات (JADC2) على تحديد احتياجات القياة والتحكم لمجموعات المهام العسكرية الأساسية ووضع خطط لتطوير البرامج التي يمكن تحقيقها على المدى القريب والمدى البعيد.

ويصف الجزء المتبقي من هذا المقال الحاجة إلى القيادة والتحكم المشترك لجميع المجالات (JADC2) بالإضافة إلى الذكاء الاصطناعي/ التعلم الآلي المدمج، ويقدم ملاحظة تحذيرية حول عامل الجذب الذي يشكله الذكاء الاصطناعي/ التعلم الآلي، ويحدد حواجز هذا الأخير للتغلب عليها، ويقترح مسارًا للمضي قدمًا. بشكل عام، ستكون هناك حاجة إلى استثمارات في الأفراد والموارد لتجاوز نموذج القيادة والتحكم القائم على القوة البشرية اليوم. يعد تحسين عمليات التخطيط الحالية باستخدام الأتمتة وبعض الذكاء الاصطناعي/ التعلم الآلي هدفًا واقعيًا يستحق العمل لتحقيقه.

تعمل القوات الجوية الأمريكية على تطوير مفهوم داعم للعمليات لعقيدتها الجديدة المعروفة باسم التوظيف القتالي السريع (ACE) . إنّ هذا الأخير هو عبارة عن مفهوم يوزع القوات والأصول على عدة مواقع منفصلة في غضون مهلة قصيرة لتعقيد تخطيط الخصم. يمكن تعريض أهداف العدو للخطر من العديد من المواقع التي يمكن الدفاع عنها والمستدامة والقابلة لإعادة التموضع باستخدام نظام القيادة والتحكم المناسب. إنّ تفاصيل تطبيق المفهوم فريدة اعتمادًا على مسرح الاستخدام، ولكن الفكرة في الأساس هي نفسها ، وقدرات القيادة والتحكم أساسية لنجاح المفهوم.

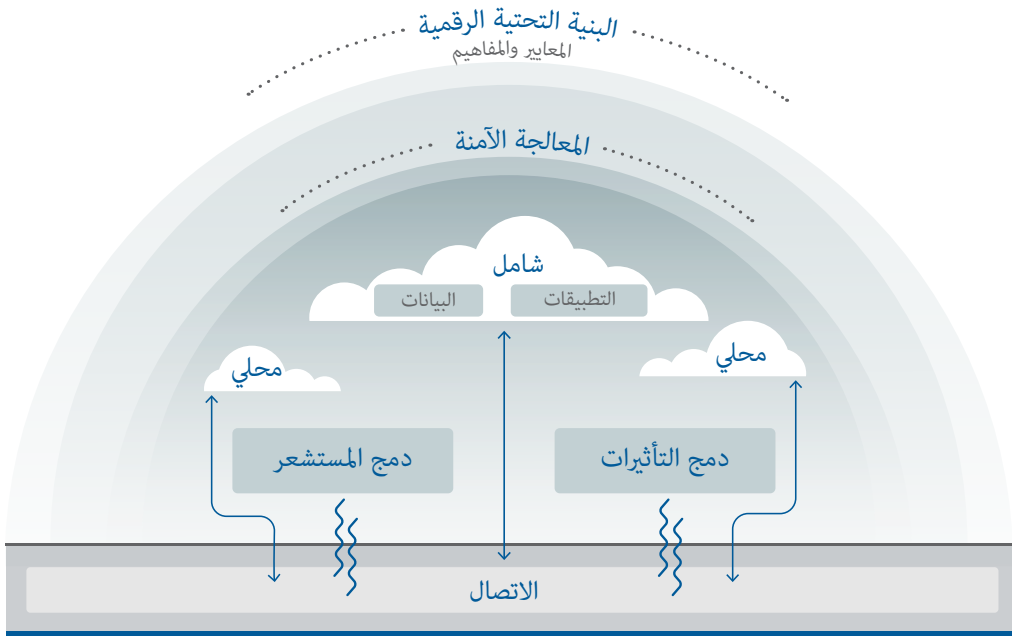
في حين أن مركز العمليات العسكرية المشتركة (CAOC) سيظل وسيلة قابلة للتطبيق لإجراء عمليات القيادة والتحكم خلال فترات صراع إقليمي أقل من رئيسية، لتحقيق أهداف شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2، سيتعين علينا تقديم المعلومات إلى المقاتلين على خطوط ساحة المعركة دون الحاجة إلى الاعتماد على نموذج مركز العمليات العسكرية المشتركة التقليدي والذي يضم مئات الأشخاص المنظمين في فرق متداخلة حول مناطق مهمة منفصلة. وعليه، فإننا نحتاج إلى التطور سريعًا إلى ما وراء الهياكل المركزية الكبيرة التي تعتمد على مركز العمليات العسكرية المشتركة المعتمدة اليوم إلى مجموعة من العمليات وبنى القيادة والتحكم أكثر مرونة وقابلية للتشتت. في الوقت نفسه، يجب أن تكون هذه البنية الجديدة قابلة للتكيف مع تطورات النظام المتقدم لإدارة المعركة (ABMS). وشبكة القيادة والتحكم المشترك في جميع المجالات (JADC2). ومع ذلك ، نظرًا للتطور البطيء لهذه البرامج ، لا يمكننا الانتظار لبدء تغيير بنية القيادة والتحكم لقوى الفضاء.

إنّ الخيارات لهذه البنية الجديدة عديدة منها بناء مراكز عمليات عسكرية مشتركة صلبة وإبعاد الوظائف عن الوحدات المخصصة وتوزيع وظائف التخطيط المدمجة حاليًا في المراكز بين مواقع متعددة وشبكة الخطط الناتجة وإنشاء العمليات والإجراءات التي يتعين تنفيذها على أساس درجة تدهور الاتصال بين الوحدات القتالية وعناصر القيادة الخاصة بكل منها عن طريق تحويل سلطة التنفيذ المقابلة لمستويات الاتصال وغيرها. بغض النظر عن الخيار أو الخيارات المحددة للتطوير، فإنّه ثمة شيء واحد مؤكد وهو أننا يجب أن نبذل جهدًا حازمًا لتوزيع وظائف القيادة والتحكم اللازمة لضمان الاستخدام الفعال لقوى الفضاء في بيئة متنازع عليها، وهذا الجهد يجب أن يبدأ الآن.

سلس عبر ساحة المعركة بطريقة آمنة وموثوقة وقوية لكل من شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) ونظام إدارة المعركة المتقدم (ABMS) سيستغرق سنوات عديدة. نظرًا للتطور السريع للتهديدات الكبيرة وضعف منشآت القيادة والتحكم الحالية فإنّه يجب تعديل بنيتها الحالية لقوات الفضاء الجوي الآن.

ترتكز شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) على دفع المعلومات دقيقة والتي ترتقيإلى جودة القرار، نحو أدنى عقدة معلومات لتحقيق التأثير المطلوب، بغض النظر عن الخدمة أو المجال أو النظام الأساسي.

نظام إدارة القتال المتطور



ما نحتاجه هو بنية جديدة لدعم مفهوم التشغيل الذي يحقق نموذج القيادة والتحكم الذي تم تضمينه مؤخرًا في عقيدة القيادة المركزية للقوات الجوية الأمريكية والسيطرة الموزعة والتنفيذ اللامركزي. ليست هناك حاجة إلى اختراقات في التكنولوجيا لتأسيس بنية قيادة معركة جديدة حيث أن التكنولوجيا موجودة بالفعل للتعامل مع التحدي الفوري المتمثل في توزيع وظائف القيادة والتحكم بحيث لا يمكن القضاء عليها ببضع ضربات على عدد قليل من عقد القيادة والتحكم الحساسة.

الجماعية. إنّ العمليات المرتكزة على الشبكة والمترابطة والمتكاملة وظيفيا هي مفاتيح النجاح العسكري في المستقبل.

سرعة المعلومات

تنشأ تطوّرات كبيرة على مستوى الاتصالات وأجهزة الاستشعار وتخزين البيانات وقوة المعالجة كل يوم. ونتيجة لذلك فقد تطوّرت دورة الاستهداف من أسابيع إلى أيام إلى دقائق، ومن طائرات متعددة ومتخصصة ومنفصلة إلى القدرة على "البحث والإصلاح والإنهاء" من طائرة واحدة في دقائق. تتطلب إمكانية الوصول المتزايدة إلى المعلومات إعادة هيكلة التسلسل الهرمي للقيادة والتحكم لتسهيل الاشتباك السريع للأهداف القابلة للتلف والاستفادة من قدرتنا التكنولوجية. يجب نقل السلطة المسؤولة عن توليف المعلومات والتنفيذ إلى أدنى المستويات الممكنة بينما يجب على كبار القادة والأركان ضبط أنفسهم للبقاء على المستوى المناسب للحرب.

إنّ الانتقال إلى ما وراء مرافق القيادة والتحكم الكبيرة والمركزية والثابتة نحو تلك المتنقلة والموزعة، باستخدام القدرة على التعامل مع نفس مستوى الحجم والتنوع من المعلومات الخاصة بـمركز إقليمي مشترك للعمليات الجوية والفضائية (CAOC) اليوم، سيتطلب إعادة تقييم لكيفية تعاملنا مع تدفق المعلومات. سيتمحور أهم جانبين لهذه القدرة المستقبلية حول تحول "القيادة" الذي سيكون ممكنًا من خلال قدرات "السيطرة" المتزامنة التي ستوفرها. سيتحول "فن القيادة" لتحقيق قيم شبكة قانون ميتكالف، والذي ينص على أن قيمة شبكة الاتصالات تتناسب مع مربع عدد المستخدمين المتصلين بالنظام. في حين أن "علم التحكم" سيستمر في تطبيق قانون مور لتوسيع التكنولوجيا لرفع مستوى القدرات البشرية. تم العثور على مسار النمو الأمثل لكليهما من خلال التركيز على اكتساب ميزة دورة القرار والحفاظ عليها كدليل المسار الحرج.

الحاجة إلى بنية جديدة لقدرات القيادة والتحكم الفضائية – بسرعة

نحن الآن في منعطف تتطلب فيه التهديدات والتكنولوجيا وسرعة المعلومات تغييرًا في البنى المعتمدة لقيادة قوات الفضاء والسيطرة عليها. لقد أدركت جميع الخدمات العسكرية الأمريكية ذلك وشرعت في اتخاذ الإجراءات المناسبة لتطوير مفاهيم جديدة للعملية في المجالات الخاصة بها. سيتركز التحدي حول كيفية ضمان تكامل كل من مفاهيم الخدمة الفردية للعملية في بنية قيادة وسيطرة مشتركة موحّدة لكل مجال. لقد تم تطوير هذه "السحابة القتالية" باستخدام فكرة إنشاء مركّب الاستخبارات والمراقبة والاستطلاع (ISR) والهجوم والمناورة والاستدامة التي تستخدم تقنيات عصر المعلومات لإجراء عمليات مترابطة وموزعة للغاية، وستؤدي إلى بنية مختلفة تمامًا لإدارة الحرب. ترتكز شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) على دفع المعلومات دقيقة والتي ترتقي الى جودة القرار، نحو أدنى عقدة معلومات لتحقيق التأثير المطلوب، بغض النظر عن الخدمة أو المجال أو النظام الأساسي. يستند نهج القوات الجوية الأمريكية لتحقيق هذا الهدف على جهودهم لتصميم وتطوير نظام متقدم لإدارة المعركة (ABMS). ومع ذلك، في حين تم تحديد عناصر هذا النظام، لم يتم تطويرها بعد إلى بنية القيادة والتحكم القابلة للتنفيذ. بهدف بلوغ الحالة النهائية المطلوبة لمشاركة المعلومات في كل مكان وبشكل

تهدد قدرات منع الولوج والمناطق المحرمة A2/AD قدرتنا على القيادة والتحكم بالعمليات الجوية والفضائية بثلاث طرق. يمكن للأعداء القريبين استخدام الأسلحة الحركية وغير الحركية لحرماننا من الاتصالات والاستخبارات والمراقبة والاستطلاع (ISR) بواسطة أصولنا الفضائية، وبالتالي عزل قواتنا وإغفال رؤيتنا. لقد أصبحت الهجمات الإلكترونية أكثر تعقيدًا ويمكن أن تعطل العمليات في مراكز العمليات الجوية والفضائية المتينة لدينا، وأصبحت الصواريخ الباليستية والبعيدة المدى الدقيقة تهدد الآن هذه المنشآت الكبيرة والثابتة والضعيفة. وعليه فقد تحوّل مركز العمليات الجوية المشتركة إلى هدف مربح للغاية لكونه مصنع لوضع الإستراتيجيات والخطط وإصدار أوامر المهام للقوات الجوية والفضائية.

التكنولوجيا

تتيح التقنيات الجديدة إمكانات جديدة لتحسين آليات القيادة والتحكم بهدف تسهيل تحقيق التأثيرات المرغوبة. نحن بحاجة إلى التفكير في ما وراء القيود التي تفرضها الثقافة التقليدية على التكنولوجيا الجديدة. على سبيل المثال، قد لا تزال طائرات الجيل التالي مصنّفة في التسميات التقليدية مثل المقاتلات والقاذفات والرافعات الجوية وما إلى ذلك، ولكن من الناحية التكنولوجية فإنّ لديها القدرة على أداء مهام متعددة بسبب تصغير المستشعرات وقوة المعالجة والأسلحة وإنتاج الطاقة وغيرها من القدرات. إنهم في الواقع "مستجيبات حساسة" طائرة يمكنها أن تشكّل الأساس لشبكات عالية المرونة من العقد الزائدة عن الحاجة ومسارات قتل متعددة. إنّ الهدف من ذلك هو تقليل قيمة النظام الحرجة لعقد القيادة والتحكم الحالية الشديدة المركزية والمحدودة، مثل المراكز الإقليمية المشتركة للعمليات الجوية والفضائية (CAOC) والتي يمكن للعدو استهدافها بسهولة.

> ستتطلب شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) الكثير من الوقت للهندسة لأنها تتضمن تحويلًا ضخمًا للمفاهيم والقدرات ووجهات نظر الخدمة الحالية. ومع ذلك، يمكن تسريع هذه المساعي من خلال التطوّر السريع لنماذج القيادة والتحكم الحالية.

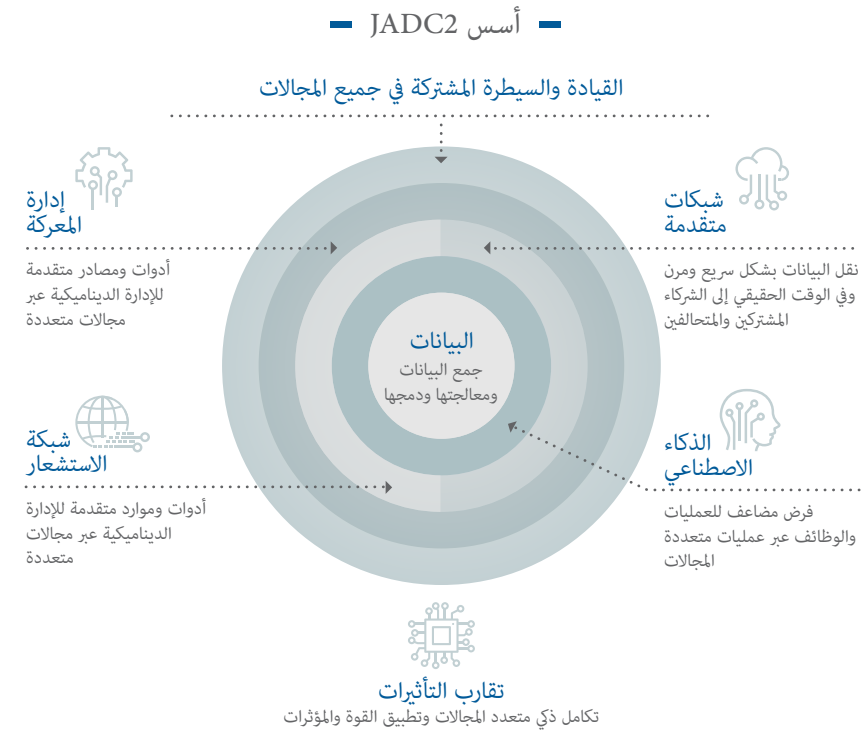
ستتطلب هذه العملية إمكانات شبكات متطورة واتصالات مضمونة ومقاربات مختلفة لإيجاد حل لتحديات عرض النطاق الترددي للبيانات. على سبيل المثال، بهدف إيجاد حل للزيادة الكبيرة على مستوى نمو البيانات من أجهزة الاستشعار المتقدمة، وبدلاً من بناء أنابيب أكبر لنقل جميع البيانات التي تم جمعها، فإن رفع مستوى قوة المعالجة الآن تتيح معالجة البيانات على متن الطائرة وخارجها فقط لما هو مهم بالنسبة للمستخدمين. يعكس هذا النهج الطريقة التي نقوم بها بمعالجة الاستخبارات والمراقبة والاستطلاع (ISR) اليوم. يعد التبادل السريع للمعلومات مهمًا بشكل خاص في خطوط القتال الأمامية، لأن قيمة البيانات الفعلية غالبًا ما تكون عابرة وتتضاءل مع مرور الوقت والظروف. إن تطوير نهج تقني لمشاركة المعلومات تلقائيًا وبسرعة بين مستخدمين متنوّعين وعبر تصنيفات متعددة ودول حليفة سيكون مفتاحًا لإنشاء القوة المستقبلية.

لم يعد القول القديم "السرعة هي الحياة" يتمحور حول الطيران فحسب بل أصبح يشير أيضًا إلى برمجيات سريعة التطور مُعتمدة للقتال وتحقيق الفوز. علينا أن نفكر خارج الهياكل التنظيمية التي حفرها التاريخ في نفسيتنا

التهديدات المستقبلية وبيئة العمليات

التهديدات

إنّ تهديدات الأقران اليوم تجعل الوسائل الحالية للقيادة والتحكم معرَّضة لخطر غير مقبول عند محاولة العمل داخل بيئة منع الولوج والمناطق المحرمة A2/AD. لأكثر من 30 عامًا، كنا في الأساس في إجازة في ما يتعلق بالقيادة والتحكم، كما كنا نتمتع برفاهية عدم التنافس في مجالات الطيران. لقد ولت تلك الأيام. فالمنافسون العسكريون قد تمكنوا من تحقيق هذا التحديث على نطاق غير مسبوق. وقد قاموا بسرعة بسد الفجوة مع الولايات المتحدة والحلفاء والجيوش الصديقة عبر مجموعة واسعة من القدرات بما في ذلك الطائرات والمركبات الفضائية والصواريخ والأسلحة والأنظمة السيبرانية وأنظمة القيادة والتحكم وأجهزة التشويش والحرب الإلكترونية وروابط البيانات وغيرها. لقد درس الخصوم المحتملون أيضًا الطريقة الأمريكية للحرب وقرروا أنه من الأفضل إبعادنا عن جيرانهم بدلاً من مواجهة قوتنا القتالية. لقد تبنوا وينشرون قدرات منع الولوج والمناطق المحرمة A2/AD المصممة لحرمان الولايات المتحدة وحلفائها من حرية التصرف. يفرض التخفيف من قدرات منع الولوج والمناطق المحرمة A2/AD تحديات كبيرة تدفعنا إلى العمل ضمن مخاطر أكبر وبعيدًا عن مناطق الصراع المحتملة.



والتحكم المشترك في جميع المجالات (JADC2) والتي يمكن تغييرها الآن لمواجهة تحديات التهديدات التي نواجهها اليوم.

تمتلك كل من مكوّنات القوات والقيادات المقاتلة قيادة تشغيلية ومفاهيم تحكم راسخة ومرافق وإجراءات أثبتت أنها قابلة للتطبيق في صراعات الماضي. ومع ذلك، فإن كل مجموعة متنوّعة من هيكليات القيادة والتحكم الموجودة حاليًا سوف تتطلب تعديلات واسعة النطاق من أجل البقاء، ناهيك عن العمل ضد نوع التهديدات الحديثة التي ظهرت الآن.

> تتطلب إمكانية الوصول المتزايدة إلى المعلومات إعادة هيكلة التسلسل الهرمي للقيادة والتحكم لتسهيل الاشتباك السريع للأهداف القابلة للتلف والاستفادة من قدرتنا التكنولوجية. يجب نقل السلطة المسؤولة عن توليف المعلومات والتنفيذ إلى أدنى المستويات الممكنة بينما يجب على كبار القادة والأركان ضبط أنفسهم للبقاء على المستوى المناسب للحرب.

يتمحورالشرط الأساسي للعمليات الناجحة في جميع المجالات حول التحكم في بيئة الفضاء الجوي. ، فإنّ هذه البيئة، وبمجرد إنشائها، تسهّل حرية العمل والحركة لجميع القوات المشتركة والمُدمجة، وبدونها لن يكون من الممكن القيام بعمليات مشتركة و/أو ملتئمة فعالة. وبناءً على ذلك، فإن القيادة والسيطرة الفعالة لعمليات الفضاء الجوي هي وظائف حاسمة يجب أن تكون ذات أولوية.

تتأثر قدرتنا في مجال القيادة والسيطرة على القوات الجوية والفضائية بثلاثة عناصر رئيسية: التهديدات والتكنولوجيا وسرعة المعلومات. لقد كانت التغييرات في هذه المجالات الثلاثة منذ تصميم وإنشاء وتشغيل مركز العمليات الجوية والفضائية التابع للقوات الجوية الأمريكية، إي إن/ يو اس كيو- 163 فالكونر -(AN/USQ 163 Falconer) دراماتيكية ويستمر هذا الوضع في التسارع. لذلك، فقد حان الوقت لتحديد ما إذا كان بإمكاننا تحقيق النجاح في العمليات المستقبلية من خلال تطوير مفاهيمنا الحالية للعمليات والمنظمات وعمليات الاستحواذ من أجل التحديث، أو أننا يجب أن نسعى إلى تغيير جذري لكل عنصر من هذه العناصر التي تؤثر على نظام التحكم الجوي والفضائي الحالي. قبل الإجابة على هذه الأسئلة، لنلقِ نظرة سريعة على كل من الاتجاهات التي تؤثر في قدرتنا على قيادة عمليات الطيران والتحكم بها بشكل فعّال.

على وزارة الدفاع الأمريكية (DOD) أن تكون جادة في تحويل النظرية إلى واقع. إنّ هذا يعني اتخاذ خطوات إضافية وملموسة نحو تحقيق أهداف شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2)، وليس انتظار حلّ كامل قبل التنفيذ. ستتطلب شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) الكثير من الوقت للهندسة لأنها تتضمن تحويلًا ضخمًا للمفاهيم والقدرات ووجهات نظر الخدمة الحالية. ومع ذلك، يمكن تسريع هذه المساعي من خلال التطوّر السريع لنماذج القيادة والتحكم الحالية. على وجه التحديد، حان الوقت للانتقال إلى ما بعد مرافق القيادة والتحكم الكبيرة والمركزية والثابتة نحو تلك المتنقلة والموزَّعة، مع الحفاظ على القدرة على التعامل مع نفس حجم المعلومات وتنوّعها من مركز إقليمي مشترك للعمليات الجوية والفضائية (CAOC).

بالنظر إلى كون هذا النظام يسعى إلى تحقيق التآزر في جميع المجالات، واحتضان التوظيف الإضافي للقدرات من مجالات مختلفة، فإنّ هدف شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) يتمحور حول البحث عن الاعتماد المتبادل الذي يعزز الفعالية، ويعوّض عن نقاط الضعف الفردية لكل مجال من المجالات. سوف تنشأ التأثيرات العسكرية المرغوبة بشكل متزايد من خلال تفاعل الأنظمة التي تتشارك المعلومات وتمكّن بعضها البعض. تركّز رؤية شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) على هذه الأصول مجموعةً باستخدام "غراء" رقمي ضام لتصبح "نظام سلاح" لإجراء عمليات مفصّلة وموزّعة على منطقة تشغيلية بأكملها، بدلاً من اعتماد مجموعة من الأنظمة القتالية المنفصلة والمركّزة بشكل فردي في كل مجال من المجالات. سيتطلب هذا الأمر التعامل مع كل منصة على أنها جهاز استشعار بالإضافة إلى "مستجيب". سيتطلب الأمر بنية جديدة لقيادة المعركة ونموذج قيادة وتحكم يتيح الربط التلقائي، كما هو حال تقنية الهاتف الخلوي اليوم. سيحتاج أيضًا إلى نقل البيانات بشكل آمن وموثوق وسلس دون الحاجة إلى تفاعل بشري.

التحوّل المتصوَّر

في الواقع، سيتطلب الهدف الشامل المتمثل في إنجاز شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) باعتماد درجة التكامل المطلوبة لتحقيق مجمع التشكل والشفاء الذاتيين جهدًا كبيرًا ولن يكون سهلاً. ستشارك في هذه العملية كل قوّة من القوات العسكرية بالإضافة إلى كل قيادة مقاتلة. سيتطلب تحقيق ذلك التغلب على العديد من العقبات الرئيسية على مستوى التنظيم و الثقافة والتمرين والاستحواذ والسياسة. كما سيتطلب أيضا الاتصال واتخاذ القرار والاستجابة بسرعة، وسيكون ثمة حاجة لشبكات مرنة ودرجة من المشاركة بين مكوّنات الخدمة والحلفاء لم يتم تحقيقها بعد.

إنّ هذه التحديات العديدة والمتعددة الأوجه تتم معالجتها عبر قيادات جيوشنا وقواتنا ومقاتلينا. ومع ذلك، وبالنظر إلى تعقيدها، سيستغرق الأمر سنوات عديدة، إن لم يكن عقودًا، قبل أن تصبح الرؤية النهائية للعمليات المشتركة والمؤتلَفة المتكاملة والمترابطة والذاتية التشكيل والشفاء في جميع المجالات حقيقة واقعة. ومع ذلك، فإن التهديدات التي تواجهنا تتزايد وتتطلب حلولًا اليوم. وعليه، فقد حان الوقت للانتقال إلى تلك العناصر من شبكة القيادة

2 هندسة قيادة معركة جديدة للعمليات في جميع المجالات التي يقودها سلاح الجو

ديفيد أ. ديبتولا، فريق (متقاعد)، القوات الجوية الأمريكية

عميد، معهد ميتشيل لدراسات الفضاء

مقدمة

تحدّث رئيس هيئة الأركان المشتركة الأمريكية مؤخرًا أمام الكونجرس عن مفهوم القتال المشترك (JWC) الجديد للجيش الأمريكي وأهمية دور شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) في تحقيق ذلك. وقد جاء تصريحه تحديدًا أمام مجلس النواب الأمريكي في 23 يونيو 2021 على الشكل الآتي:

يُشكّل مفهوم القتال المشترك (JWC) نتيجة جهد تم بذله على مرّ سنوات عدّة لتطوير نهج شامل للعمليات المشتركة ضد التهديدات المستقبلية، ولتوفير دليل لتصميم وتطوير القوة في المستقبل. توضح المفاهيم الداعمة لمفهوم القتال المشترك (JWC) وظائف القتال الرئيسية. إنّ هذه الأخيرة هي الحرائق واللوجستيات والقيادة والتحكم وميزة المعلومات. تتيح شبكة القيادة والتحكم المشترك في جميع المجالات (JADC2) تحقيق التطوير الشامل بالإضافة إلى مفهوم القتال المشترك (JWC) والمفاهيم الداعمة.

تتمحور الركيزة الأساسية لمفهوم القتال المشترك (JWC) حول فكرة العمليات في جميع المجالات. هذا هو التطور التالي في رحلة الجيش الأمريكي لتحسين تآزر التأثيرات التي تنشأ من العمل بطريقة متكاملة عبر جميع المجالات، في الجو والفضاء والبحر والأرض وعلى مستوى الطيف الكهرومغناطيسي. لقد بدأت الرحلة بتمرير قانون غولدووتر – نيكولاس (1986) الذي يهدف إلى تحسين قدرة القوات المسلحة الأمريكية على تنفيذ عمليات مشتركة ومُدمجة أو متحالفة في ما بين القوات. في حال تم تطوير مفهوم القتال المشترك (JWC) وتنفيذه بشكل صحيح، فإنّه ستتأتى عنه مجموعة من النتائج القتالية الأكثر حسماً وقوةً من العمليات "المشتركة" الحالية والتي في كثير من الحالات تتضمن ببساطة عدم تضارب مكوّن الخدمة بدلًا من التكامل. وبهدف تحقيق ذلك، يتعيّن

روس، ايه. 2010. في الابتكار العسكري: نحو إطار تحليلي. موجز سياسة 1 .IGCC ، ص 14-17. متوافر على: https://escholarship.org/uc/item/3d0795p8

ستانلي ولوكمان. زي. 2021(ايه). منظمة العفو الدولية العسكرية المسؤولة والأخلاقية: الحلفاء ووجهات نظر الحلفاء. موجز إصدار مركز الأمن والتكنولوجيا الناشئة. 25 أغسطس. متوافر على: https://cset.georgetown.edu/publication/responsible-and-ethical-military-ai/

ستانلي ولوكمان. زي. 2021(ايه). مجموعة أدوات التعاون العسكري للذكاء الاصطناعي: تحديث شراكات علوم وتكنولوجيا الدفاع للعصر الرقمي. موجز إصدار مركز الأمن والتكنولوجيا الناشئة. 25 أغسطس. متوافر على: https://cset.georgetown.edu/publication/military-ai-cooperation-toolbox/

https://www.technologyreview.com/2019/10/21/132277/military-artificial-intelligence-can-be-easily-and-dangerously-fooled/

لي ، سي ام 2016. خطوط الصدع في آسيا الصاعدة. واشنطن العاصمة: مؤسسة كارنيغي للسلام الدولي ، ص 119 - 175. متوافر على: https://carnegieendowment.org/2016/04/20/fault-lines-in-rising-asia-pub-63365

لينجل، اس. وال. 2020. القيادة والسيطرة المشتركة في جميع المجالات للحرب الحديثة - إطار تحليلي لتحديد وتطوير تطبيقات الذكاء الاصطناعي. تقرير مشروع مؤسسة راند للقوات الجوية. متوافر على: https://www.rand.org/pubs/research_reports/RR4408z1.html

ماهنكن، تي (محرر). 2012. الاستراتيجيات التنافسية للقرن الحادي والعشرين: النظرية والتاريخ والممارسة. ستانفورد: مطبعة جامعة ستانفورد ، ص 3-12.

راسكا، ام. 2016. الابتكار العسكري في الدول الصغيرة: خلق عدم تناسق عكسي. نيويورك: روتليدج. متوافر على: https://www.routledge.com/Military-Innovation-in-Small-States-Creating-a-Reverse-Asymmetry/Raska/p/book/9780367668617

راسكا، ام. 2020. المنافسة الاستراتيجية للتقنيات العسكرية الناشئة: مسارات وأنماط مقارنة. المنشور - مجلة العمليات المعقدة. 8 (3) ، ص 64 - 81. متوافر على: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Raska_64-81.pdf

راسكا، ام. 2021. الموجة السادسة لثورة الشؤون العسكرية: اضطراب في الشؤون العسكرية؟ مجلة الدراسات الاستراتيجية. 44 (4) ، ص 456-479.

راينولدز، كاي. 2006. التحول الدفاعي: إلى ماذا؟ لماذا؟ كارلايل: معهد الدراسات الاستراتيجية.

روبنسون، تي. 2021. القوة الجوية لعام 2040 - مدربة صناعياً ، مرتبطة بالشبكات السحابية ، ممكّنة في الفضاء و NetZero؟ الجمعية الملكية للطيران ، 10 أغسطس. متوافر على: https://www.aerosociety.com/news/the-air-force-of-2040-synthetically-trained-cloud-networked-space-enabled-and-netzero/

فوكس، ج. ومنزل، لم. 2018. الدور المستقبلي للذكاء الاصطناعي - الفرص والتحديات العسكرية. مجلة JAPCC، 7727-70.pp . متوافر على: https://www.japcc.org/wp-content/uploads/JAPCC_J27_screen.pdf

فريدمان ، ل. 2006. تحول الشؤون الإستراتيجية. لندن: المعهد الدولي للدراسات الاستراتيجية.

فريتاس، اس. سيلفا، اتش.، الميدا، ج. وسيلفا، اي. 2018. التصوير فائق الطيفية لكشف الهدف البحري لمركبة جوية بدون طيار في الوقت الحقيقي. مجلة الأنظمة الذكية والروبوتية. 90 ، ص 551-570.

جولدمان ، إي. 1999. المهمة ممكنة: التعلم التنظيمي في زمن السلم. في تروبويتز، ب.، جولدمان، اي.، ورودس، اي. سياسة التعديل الاستراتيجي: الأفكار والمؤسسات والمصالح. نيويورك: مطبعة جامعة كولومبيا ، ص 233 - 266.

جراي ، سي 2006. الاستراتيجية والتاريخ: مقالات عن النظرية والتطبيق. لندن: روتليدج ، ص 113 - 120.

هاميس ، ت. 2016. تتقارب التقنيات وتنتشر القوة: تطور أسلحة صغيرة وذكية ورخيصة. معهد CATO لتحليل السياسات. 786 ، 27 يناير. متوافر على: https://www.cato.org/policy-analysis/technologies-converge-power-diffuses-evolution-small-smart-cheap-weapons

هورويتز ، إم. 2018. وعد وخطر التطبيقات العسكرية للذكاء الاصطناعي. نشرة علماء الذرة. 23 أبريل. متوافر على: https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/

المعهد الدولي للدراسات الاستراتيجية. 2019. الحوسبة الكمومية والدفاع. في .IISS :التوازن العسكري. لندن: روتليدج ، ص 18 - 20.

جنسن، بي. وباشكيويتز، جي. 2019. حرب الفسيفساء: الصغيرة والقابلة للتطوير جميلة. الحرب على الصخور. 23 ديسمبر.متوافر على: https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/

نايت، دبليو. 2019. يمكن خداع الذكاء الاصطناعي العسكري بسهولة وخطورة. استعراض تكنولوجيا معهد ماساتشوستس للتكنولوجيا. 21 أكتوبر. متوافر على:

المراجع:

بارساد، آي وهورويتز، إم 2018. الذكاء الاصطناعي وراء القوى العظمى. نشرة علماء الذرة. 16 أغسطس. متوافر على: https://thebulletin.org/2018/08/the-ai-arms-race-and-the-rest-of-the-world/

بورنيت ، إم. وآل. 2018. المواد المتقدمة والتصنيع - الآثار المترتبة على الدفاع حتى عام 2040. تقرير مجموعة علوم وتكنولوجيا الدفاع. وزارة الدفاع الاسترالية. متوافر على: https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-GD-1022.pdf

تشونغ، ت. 2021. إطار مفاهيمي للابتكار الدفاعي. مجلة الدراسات الاستراتيجية ، / DOI: 10.1080 01402390.2021.1939689.

كامينغز ، م. 2017. الذكاء الاصطناعي ومستقبل الحرب. ورقة بحث تشاثام. 26 يناير. متوافر على: https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf

كامينغز ، م. 2021. إعادة التفكير في نضج الذكاء الاصطناعي في البيئات الحرجة للسلامة. مجلة منظمة العفو الدولية ، 42 (1) ، ص 6-15. متوافر على: https://ojs.aaai.org/index.php/aimagazine/article/view/7394

دانكس، د. 2020. كيف يمكن للهجمات العدائية أن تزعزع استقرار أنظمة الذكاء الاصطناعي العسكرية. IEEE Spectrum 26 فبراير. متوافر على https://spectrum.ieee.org/adversarial-attacks-and-ai-systems

ديفيس ، م. 2021. "المقعد الخلفي" للذكاء الاصطناعي في القتال الجوي في المستقبل. إستراتيجي ASPI، 5 فبراير. متوافر على: https://www.aspistrategist.org.au/the-artificial-intelligence-backseater-in-future-air-combat/

افرستين، ب. 2020. يو-2 تطير بذكاء اصطناعي كطيار مساعد لها. مجلة القوات الجوية ، 16 ديسمبر. متوافر على: https://www.airforcemag.com/u-2-flies-with-artificial-intelligence-as-its-co-pilot/

التعلم الآلي المختارة قد تخفف من بعض التحديات ، فإن الأنظمة نفسها تخلق مجموعة أخرى من المشاكل الجديدة المتعلقة بضمان الذكاء الاصطناعي الموثوق به. وعليه، قد يجادل المرء بأن اتجاه مسارات الذكاء الاصطناعي وطبيعتها لدى القوة الجوية المستقبلية سيعتمدان على المرونة الاستراتيجية والتنظيمية والتشغيلية المقابلة، لا سيما كيفية تفاعل هذه التقنيات مع الهياكل التشغيلية الحالية والناشئة وهياكل القوة.

وفي هذا السياق، فإن مستوى المشاركة البشرية في مستقبل الحرب، والحاجة إلى تغيير هياكل القوة التقليدية وأنماط التجنيد وفي المجالات التي ستستخدم فيها القوة، هي جميعها أمور تواجه تحديات من قبل التقنيات الجديدة. تعمل القوات الجوية على تطوير حلول خاصة بها وغالبًا ما تكون متنوعة لهذه القضايا. كما في الماضي، ستعتمد فعاليتها على العديد من العوامل المرتبطة بالمبادئ الثابتة للاستراتيجية - الغايات والطرق والوسائل "لتحويل" الموارد الدفاعية المتاحة إلى قدرات عسكرية جديدة، وإنشاء القوات الجوية ذات الكفاءات التشغيلية وتحقيق استدامتها من خلال القيام بذلك للتعامل مع مجموعة واسعة من حالات الطوارئ. لن تكون العوامل الرئيسية للتنفيذ الناجح هي الابتكارات التكنولوجية في حد ذاتها، ولكن التأثير المشترك للتمويل المستدام والخبرة التنظيمية (أي قواعد البحث والتطوير الكبيرة والفعالة ، العسكرية والتجارية على حد سواء) والمرونة المؤسسية لتنفيذ الابتكار الدفاعي (تشيونغ، 2021). بالنسبة لمستقبل القوة الجوية، يعني هذا امتلاك الأشخاص والعمليات والأنظمة القادرة على تقديم حلول مبتكرة مع الحفاظ على القدرات الأساسية الحالية التي من شأنها توفير خيارات سياسية قابلة للتطبيق في بيئة استراتيجية متزايدة التعقيد.

الاصطناعي ستكون قادرة بشكل متزايد على تبسيط القيادة والتحكم وعمليات صنع القرار في كل خطوة من حلقة نموذج راقب، وجّه، قرّر، تصرّف (OODA) التابع لجون بويد: جمع البيانات ومعالجتها وترجمتها إلى وجهة نظر موحدة لإدراك بالحالة، مع توفير خيارات لمسار الإجراءات الموصى به، وفي النهاية، مساعدة البشر على التصرف (فوكس ومنزل، 2018).

ومع ذلك ، فإن دمج أنظمة الذكاء الاصطناعي في منصات القوة الجوية والأنظمة والمؤسسات لتحويل أجهزة الكمبيوتر من أدوات إلى آلات "تفكير" لحل المشكلات سيستمر في تقديم مجموعة من التحديات التكنولوجية والتنظيمية والتشغيلية المعقدة (راسكا وال.، 2021). قد يشمل ذلك تطوير خوارزميات تمكّن هذه الأنظمة من التكيّف بشكل أفضل مع التغييرات في بيئتها، والتعلم من التكتيكات غير المتوقعة وتطبيقها في ساحة المعركة. كما سيتطلب أيضًا تصميم قوانين أخلاقية وضمانات لآلات التفكير هذه. أما التحدي الآخر فيتمحور حول أنّ التقدم التكنولوجي، وخاصة في الأنظمة العسكرية، هو عملية مستمرة وديناميكية. فالخروقات تحدث دائمًا، وقد يكون تأثيرها على الفعالية العسكرية والميزة النسبية كبيرًا ويصعب التنبؤ به في مراحله الأولى.

لكن الأهم من ذلك يبقى أن السؤال المهم هو إلى أي مدى يمكننا الوثوق بأنظمة الذكاء الاصطناعي لا سيما في مجالات أنظمة السلامة الحساسة؟ كما يحذر ميسي كامينغز فإنّ "التاريخ مليء بأمثلة عن كيفية انتهاء الوعود المماثلة للاستعداد التشغيلي بإخفاقات مكلفة على مستوى النظام ويجب أن تكون هذه الحالات بمثابة قصة تحذيرية" (كامينغز، 2021). علاوة على ذلك، يركز مجال بحثي متنامٍ على كيفية خداع أنظمة الذكاء الاصطناعي لتقديم تنبؤات خاطئة عن طريق توليد بيانات خاطئة. قد تستخدم كل من الجهات الفاعلة الحكومية وغير الحكومية ما يسمى بالتعلم الآلي العدائي لخداع الأطراف المتعارضة باستخدام بيانات غير صحيحة لتوليد استنتاجات خاطئة، فيتم بذلك تغيير عمليات صنع القرار. قد يكون التأثير الاستراتيجي العام للتعلم الآلي العدائي أكثر اضطرابًا من التكنولوجيا نفسها (ناي، 2019- دانكس، 2020).

> عند القيام بذلك، يتم وضع السحب القتالية المدعومة بالذكاء الاصطناعي لتحديد الأهداف وتخصيصها بالنسبة إلى "الرماة" الأكثر صلة في أي مجال، سواء كانت محمولة جواً أو فوق سطح الماء أو تحت الماء - والتي تصوّرها بعض القوات الجوية على أنها مشتركة للقيادة والتحكم في جميع المجالات (JADC2).

فمن منظور تكتيكي وتشغيلي، تحتاج العديد من أنظمة الذكاء الاصطناعي المعقدة هذه أيضًا إلى الارتباط معًا - ليس من الناحية التكنولوجية فحسب بل على المستوى التنظيمي والتشغيلي أيضًا. بالنسبة للعديد من القوات الجوية، يعد هذا تحديًا مستمرًا، حيث يجب أن يكونوا قادرين بشكل فعال (في الوقت الفعلي) على دمج حلقات الاستشعار إلى مطلق النار المدعومة بالذكاء الاصطناعي وتدفق البيانات بين الخدمات والأنظمة الأساسية المختلفة. وهذا يعني الربط الفعال بين إدارة المعارك المتنوعة للقوات الجوية والجيش والقوات البحرية والسيبرانية ؛ والقيادة والتحكم، والاتصالات والشبكات والاستخبارات و فالمراقبة والاستطلاع (ISR) والحرب الإلكترونية وتحديد المواقع والملاحة والتوقيت باستخدام ذخائر دقيقة. في حين أن أنظمة الذكاء الاصطناعي/

ووفقًا لدراسة حديثة أجرتها مؤسسة راند (RAND) (لينجل وال.، 2020)، ثمة حاليًا على وجه التحديد ست فئات من البحث والتطوير التطبيقي للذكاء الاصطناعي/ التعلم الآلي التي لها آثار على الحرب المستقبلية، بما في ذلك القوة الجوية:

(1) رؤية الكمبيوتر- التعرف على الصور- اكتشاف الأشياء في العالم المرئي التي يمكن استخدامها لمعالجة الذكاء متعدد المصادر ودمج البيانات وتصنيفها ؛

(2) معالجة اللغة الطبيعية (NLP) - القدرة على فهم أنماط التعرف على الكلام والنص البشري بنجاح، بما في ذلك الترجمة، التي يمكن استخدامها لاستخراج الاستخبارات من الكلام والنص، ولكن أيضًا مراقبة الاتصالات الودية والمعلومات المباشرة ذات الصلة لتنبيه الأفراد أو الوحدات التي هي بحاجة؛

(3) الأنظمة الخبيرة أو الأنظمة المستندة إلى القواعد- جمع كميات كبيرة من البيانات للتوصية بإجراءات معينة لتحقيق الأهداف التشغيلية والتكتيكية؛

(4) أنظمة التخطيط- استخدام البيانات لحل مشاكل الجدولة وتخصيص الموارد، والتي يمكن أن تنسق مجموعة مختارة من الأصول الجوية والفضائية والإلكترونية مقابل الأهداف وأصدار إجراءات مرحلية زمنية موصى بها؛

(5) أنظمة التعلم الآلي- اكتساب المعرفة من تفاعلات البيانات مع البيئة، والتي يمكن استخدامها بالاقتران مع فئات أخرى من الذكاء الاصطناعي، أي لتمكين أنظمة القيادة والتحكم من تعلم كيفية أداء المهام عندما لا تتوفر معرفة الخبراء أو عندما تكون التكتيكات والتقنيات والإجراءات (TTPs) المثلى غير معروفة؛

(6) الروبوتات والأنظمة المستقلة- الجمع بين أساليب الذكاء الاصطناعي/ التعلم الآلي من جميع الفئات السابقة أو بعضها والتي من شأنها تمكين تفاعل الأنظمة غير المأهولة مع بيئتها؛

إنّ هذه الفئات المتعلقة بالذكاء الاصطناعي قابلة للتطبيق في كل جانب من جوانب القوة الجوية تقريبًا، الأمر الذي من المحتمل أن يطرح أشكالًا جديدة من الحرب الآلية: بدءًا بدعم قرار القيادة والتحكم والتخطيط، حيث يمكن للذكاء الاصطناعي/ التعلم الآلي تقديم الخيارات أو المقترحات الموصى بها في الأوقات الصعبة بشكل متزايد؛ ودعم قدرات الاستخبارات والمراقبة والاستطلاع (ISR) من خلال قدرات التنقيب عن البيانات؛ والخدمات اللوجستية والصيانة التنبؤية لضمان سلامة القوات وتوافر المنصات والوحدات؛ والتدريب والمحاكاة؛ وعمليات الفضاء الإلكتروني لاكتشاف الهجمات الإلكترونية المتقدمة ومكافحتها؛ والروبوتات والأنظمة المستقلة مثل الطائرات دون طيار التي يتم استخدامها عبر مهام مختلفة بدءًا بالاستخبارات والمراقبة والاستطلاع (ISR) ووصولًا إلى المهام القصوى مثل قمع الدفاعات الجوية للعدو والقتال التعاوني الذي يدمج مختلف المنصات المأهولة وغير المأهولة في عمليات الضربات الجوية والبرية. بعبارة أخرى، فإنّ الحجة هنا هي أن أنظمة الذكاء

ذاتية التشغيل سيتحدى المبادئ القانونية الدولية أو سيعززها. في إطار مواجهة الآثار القانونية والأخلاقية المتضاربة لتطبيقات الذكاء الاصطناعي العسكرية، تدرك المؤسسات العسكرية بشكل متزايد الحاجة إلى معالجة الأسئلة المتعلقة بالسلامة والأخلاق والحوكمة والتي تعد ضرورية لبناء الثقة في القدرات الجديدة، وإدارة تصعيد المخاطر، وتنشيط السيطرة على الأسلحة. ومع ذلك فإنّه لا يزال هناك توتر بين مدى تركيز وزارات الدفاع والجيش لجهودهم الأخلاقية بشكل ضيق على أنظمة الأسلحة الفتاكة ذاتية التشغيل أو على نطاق أوسع على سلسلة الأنظمة التي تدعم الذكاء الاصطناعي. ومن ثم فإن الجيوش، بما في ذلك القوات الجوية، بحاجة إلى تتبع وجهات النظر المتطورة حول الذكاء الاصطناعي والاستقلالية والمناقشات حول الآثار المترتبة على البيئة الاستراتيجية والتشغيلية في العقد الأول من القرن الحادي والعشرين وما بعده (ستانلي لوكمان، 2021 ب).

> ويتم النظر على نطاق واسع إلى تقارب التقنيات الناشئة مثل الروبوتات والذكاء الاصطناعي وآلات التعلم والمنصات المعيارية مع تقنيات الاستشعار المتقدمة والمواد الجديدة وأنظمة الحماية والدفاعات والتقنيات السيبرانية التي تطمس الخطوط الفاصلة بين المجالات المادية والسيبرانية والبيولوجية على أنّ لها آثار عميقة على طبيعة الحرب في المستقبل.

الآثار المترتبة على القوة الجوية

على المستوى التشغيلي، تهدف القوات الجوية إلى تسريع تكامل الأنظمة والتقنيات المختلفة المتعلقة بالذكاء الاصطناعي مثل أنظمة السحابة القتالية متعددة المجالات والتي تجمع البيانات الضخمة من مجموعة متنوعة من المصادر بهدف خلق صورة تشغيلية في الوقت الفعلي، وبشكل أساسي أتمتة عمليات القيادة والتحكم وتسريعها (روبنسون، 2021). عند القيام بذلك، يتم وضع السحب القتالية المدعومة بالذكاء الاصطناعي لتحديد الأهداف وتخصيصها بالنسبة إلى "الرماة" الأكثر صلة في أي مجال، سواء كانت محمولة جواً أو فوق سطح الماء أو تحت الماء - والتي تصوّرها بعض القوات الجوية على أنها مشتركة للقيادة والتحكم في جميع المجالات (JADC2). تقوم القوات الجوية المختارة أيضًا بتجربة خوارزميات الذكاء الاصطناعي باعتبارها "مقاعد خلفية افتراضية"، والتي تتحكم بشكل فعال في أجهزة الاستشعار التابعة للطائرة وبالملاحة وبالعثور على أهداف معادية، ومن خلال القيام بذلك، تقليل عبء العمل على طاقم الطائرة (ايفيرستين، 2020). في هذا السياق، تتمحور الحجة الرئيسية حول أنّ التطورات على مستوى أنظمة الذكاء الاصطناعي، أو على نطاق واسع البرامج التي يمكن أن تستشعر وتسبب وتتصرف وتتكيف، بما في ذلك أنظمة التعلم الآلي (ML) والخوارزميات التي يتحسن أداؤها مع زيادة تفاعلات البيانات بمرور الوقت، والتعلم العميق (DL)، التي تتعلم فيها الشبكات العصبية متعددة الطبقات من كميات هائلة من البيانات - تتمتع بالقدرة على "تحويل عمليات القتال الجوي والطريقة التي يتم بها تصور واستخدام القوة الجوية" (دايفيس، 2021).

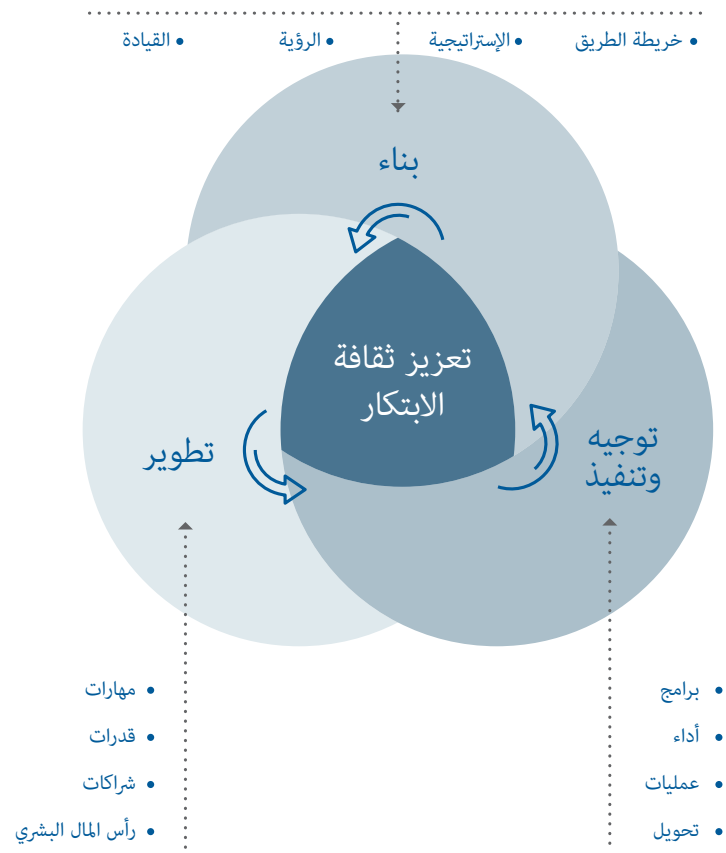
ثانيًا، على عكس العقود السابقة التي تم خلالها باعتراف الجميع استعمال بعض التقنيات ذات الاستخدام المزدوج لتطوير منصات وأنظمة أسلحة رئيسية، تختلف الموجة الحالية المدعومة بالذكاء الاصطناعي من حيث حجم الابتكار التكنولوجي التجاري كمصدر للابتكار العسكري وتأثيره (راسكا، 2020). لم تعد الأعداد الأولية الصناعية العسكرية هي المحرك الوحيد للابتكار التكنولوجي؛ لا بل يتم بدلاً من ذلك تطوير التقنيات المتقدمة ذات الاستخدام المزدوج في القطاعات التجارية ثم يتم "نسجها" للتطبيقات العسكرية. في هذا السياق، فإنّ انتشار التقنيات الناشئة، بما في ذلك التصنيع الإضافي (الطباعة ثلاثية الأبعاد) وتكنولوجيا النانو والقدرات الفضائية والشبيهة بالفضاء والذكاء الاصطناعي والطائرات دون طيار لا يقتصر على القوى العظمى فحسب (هاميس، 2016). ينعكس انتشار أجهزة الاستشعار التي تدعم الذكاء الاصطناعي وأنظمة الأسلحة المستقلة أيضًا في المسارات الدفاعية لدول صغيرة متقدمة مختارة وقوى وسطى مثل سنغافورة وكوريا الجنوبية وإسرائيل وغيرها. تمتلك هذه الشركات الآن القدرة على تطوير تقنيات ناشئة متخصصة لتعزيز قدراتها الدفاعية وقدرتها التنافسية الاقتصادية وتأثيرها السياسي ومكانتها على الساحة الدولية (بارساد وهورويتز، 2018).

> أنظمة الذكاء الاصطناعي ستكون قادرة بشكل متزايد على تبسيط القيادة والتحكم وعمليات صنع القرار في كل خطوة من حلقة نموذج راقب، وجّه، قرّر، تصرّف (OODA) التابع لجون بويد

ثالثًا، يتحدى انتشار أنظمة الأسلحة المستقلة وذاتية التشغيل المدعومة بالذكاء الاصطناعي، إلى جانب الهياكل التشغيلية الجديدة وهياكل القوة، اتجاه وطابع المشاركة البشرية في الحروب المستقبلية، حيث قد تشكل الخوارزميات عملية صنع القرار البشري ويتم تصور القتال في المستقبل في استخدام أنظمة الأسلحة الفتاكة ذاتية التشغيل (LAWS). تقوم الجيوش المتقدمة، بما في ذلك القوات الجوية باختبار تقنيات مختلفة تعتمد على تحليلات البيانات والأتمتة في الحرب. تتغلغل هذه التقنيات بشكل متزايد في تجارب الحرب المستقبلية وبرامج تطوير القدرات (جينسين وباشكويتز، 2019). تركز مجالات البحث والتطوير المحددة ذات الأولوية في الولايات المتحدة مثلًا على تطوير أنظمة الذكاء الاصطناعي والأسلحة المستقلة في مختلف أنواع التعاون بين الإنسان والآلة، مثل أنظمة الإنذار المبكر التي تدعم الذكاء الاصطناعي وشبكات القيادة والتحكم وأنظمة الحرب الفضائية والإلكترونية والقدرات السيبرانية وأنظمة الأسلحة الفتاكة المستقلة وغيرها.

إن التقارب بين الدوافع الثلاثة - المنافسة الاستراتيجية والابتكار التكنولوجي الناشئ ثنائي الاستخدام والطابع المتغير للتفاعلات بين الإنسان والآلة في الحرب، يدفع مجموعة جديدة من الشروط التي تحدد موجة ثورة الشؤون العسكرية التي يحركها الذكاء الاصطناعي (AI-RMA). كما يطرح مسار انتشارها بطبيعته تحديات وأسئلة جديدة تتعلق بالاستقرار الاستراتيجي وعلاقات التحالف ومراقبة التسلح والأخلاق والحوكمة، وفي نهاية المطاف، إدارة العمليات القتالية (ستانلي لوكمان ، 2021 أ). إنّ المناقشات المعيارية الدولية حول دور أنظمة الذكاء الاصطناعي في استخدام القوة على سبيل المثال تركز بشكل متزايد على نشر نظم الأسلحة الفتاكة ذاتية التشغيل وقدرة الدول على الامتثال لمبادئ القانون الدولي الإنساني. مع انتقال التقدم التكنولوجي من عالم الخيال العلمي إلى الواقع التقني، فإن للدول أيضًا وجهات نظر مختلفة حول ما إذا كان إدخال أنظمة الأسلحة الفتاكة

التي يحركها الذكاء الاصطناعي (AI-RMA) الخاص بها. وعليه، فإنّ السؤال الرئيسي ليس ما إذا كانت موجة ثورة الشؤون العسكرية التي يحركها الذكاء الاصطناعي (AI-RMA) هي "الموجة" التي ستؤدي إلى انقطاع جوهري في الحرب، وإذا كان الأمر كذلك، فكيف ولماذا؟ بدلاً من ذلك، فإنّ الأمر يتعلّق بما إذا كان يمكن إبطال ثورة الشؤون العسكرية التي يحركها الذكاء الاصطناعي (AI-RMA) الأمريكي، أو على الأقل إضعافه، بواسطة ثورة الشؤون العسكرية التي يحركها الذكاء الاصطناعي (AI-RMA) الصينية أو الروسية المقابلة؟ بعبارة أخرى، تقل هوامش التفوق التكنولوجي بشكل فعال، مما يسرع بشكل فعال أيضا الضرورة الاستراتيجية للتقنيات الجديدة كمصدر للميزة العسكرية.



والمتاحة المتعلقة بالميزانية. بالإضافة إلى ذلك، فقد ركزت الابتكارات المفاهيمية والتكنولوجية والتنظيمية والتشغيلية المتنوعة في المقام الأول على دمج تقنيات المعلومات الرقمية في الأنظمة الأساسية والأنظمة التقليدية القائمة (راسكا، 2016).

> قد تستخدم كل من الجهات الفاعلة الحكومية وغير الحكومية ما يسمى بالتعلم الآلي العدائي لخداع الأطراف المتعارضة باستخدام بيانات غير صحيحة لتوليد استنتاجات خاطئة، فيتم بذلك تغيير عمليات صنع القرار.

فعلى سبيل المثال، تضاءلت روايات الابتكار العسكري التخريبي تدريجياً من عام 2005 فصاعدًا في الفكر الاستراتيجي للولايات المتحدة مع التحديات والتجارب العملياتية في الحروب في العراق وأفغانستان. أشارت الأصوات الأكثر انتقادًا إلى وعود لم يتم الوفاء بها بتحولات دفاعية "تخريبية". إن الأساس المنطقي لـ"طريقة جديدة في التفكير وطريقة جديدة للقتال" يبرر فعليًا كل مبادرة أو اقتراح دفاعي، يشير إلى الارتباك بدلاً من استراتيجية واضحة (فريدمان، 2006). لقد حذر المشككون في التحوّل الدفاعي أيضًا من المنطق الخاطئ في حل التحديات الإستراتيجية المعقدة من خلال التكنولوجيا، مع تجاهل القدرة التكيفية للأعداء أو المنافسين المحتملين. باختصار فقد تحولت الروايات التخريبية للتحولات الدفاعية الوشيكة إلى فكرة غامضة مدفوعة بمتطلبات الميزانية ومجموعات القدرات غير الواقعية بدلاً من المنطق الاستراتيجي والتشغيلي الفعلي (رينولدز، 2006).

لماذا تختلف موجات الذكاء الاصطناعي؟

تختلف موجة الابتكار الدفاعي الجديدة "المدعومة بالذكاء الاصطناعي" عن الموجات السابقة التي قادتها تكنولوجيا المعلومات من نواحٍ عديدة. أولاً، يتم نشر الابتكارات العسكرية المدعومة بالذكاء الاصطناعي بوتيرة أسرع بكثير، من خلال أبعاد متعددة، لا سيما من خلال المنافسة الجيوستراتيجية المتسارعة بين القوى العظمى، أي الولايات المتحدة والصين وبدرجة أقل روسيا. إنّ المنافسات الاستراتيجية بين القوى العظمى ليست جديدة، فقد كانت متجذرة بعمق في التاريخ من الاستراتيجيات الأثينية والإسبرطية الكبرى خلال الحرب البيلوبونيسية في القرن الثالث قبل الميلاد، إلى الانقسام ثنائي القطب في الحرب الباردة خلال النصف الثاني من القرن العشرين. ومع ذلك، فإن طبيعة المنافسة الاستراتيجية الناشئة تختلف عن مقارنات المنافسات الاستراتيجية السابقة. لقد أصبحت مسارات وأنماط المنافسة الاستراتيجية في القرن الحادي والعشرين أكثر تعقيدًا وتنوعًا، ما يعكس منافسات متعددة في إطار مجموعات مختلفة أو متداخلة من القواعد التي تتعايش فيها الترابطات الاقتصادية طويلة الأجل مع التحديات الاستراتيجية الأساسية (لي، 2017). ومع ذلك، في التنافس على السيادة المستقبلية، يُصوَّر الابتكار التكنولوجي على أنه مصدر مركزي للتأثير الدولي والقوة الوطنية حيث يولّد القدرة التنافسية الاقتصادية والشرعية السياسية والقوة العسكرية (ماهنكن، 2012). على وجه التحديد ولأول مرة منذ عقود، تواجه الولايات المتحدة منافسًا استراتيجيًا نظيرًا وهو الصين، القدرة على متابعة وتنفيذ ثورة الشؤون العسكرية

> لم تعد الأعداد الأولية الصناعية العسكرية هي المحرك الوحيد للابتكار التكنولوجي؛ لا بل يتم بدلاً من ذلك تطوير التقنيات المتقدمة ذات الاستخدام المزدوج في القطاعات التجارية ثم يتم "نسجها" للتطبيقات العسكرية.

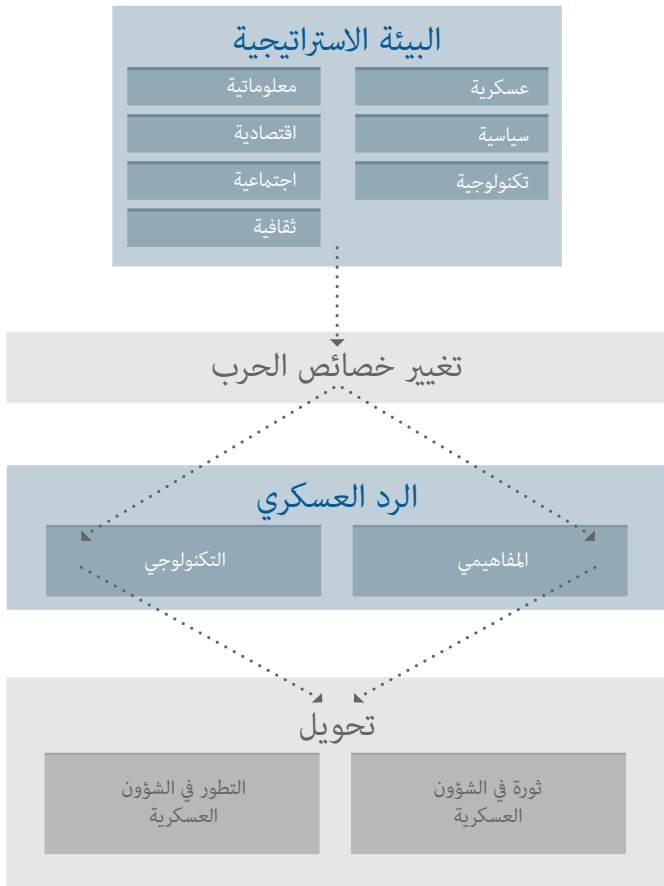
على الرغم من السياقات الإستراتيجية المتغيرة، إلا أن انتشار هذه التقنيات الناشئة يثير أيضًا أسئلة نظرية وتوجيهية للسياسة مماثلة لتلك التي تم طرحها على مدى العقود الأربعة الماضية: هل يشير انتشار التقنيات الناشئة حقًا إلى تحول " تخريبي" في الحرب، أو هل هو مجرد تغيير تطوري؟ إذا كانت التقنيات الناشئة تنص على تغيير تخريبي في الحرب، فما هي ضرورات تخصيص الموارد الدفاعية، بما في ذلك هيكل القوة ومتطلبات شراء الأسلحة؟ كيف يمكن للمنظمات العسكرية، بما في ذلك القوات الجوية، استغلال التقنيات الناشئة لصالحها؟ علاوة على ذلك، ما مدى فعالية التقنيات الناشئة في مواجهة التهديدات والتحديات الأمنية في القرن الحادي والعشرين، والتي تتميز بالتقلب والريبة والتعقيد والغموض؟

أربعة عقود من الروايات التخريبية

مدفوعة إلى حد كبير بالقفزات الكمية في تقنيات المعلومات، تم تحديد مسار روايات وناقشات الابتكار العسكري "التخريبية" في سياق ثورة الشؤون العسكرية التي تحركها تكنولوجيا المعلومات (IT-RMA)، والتي تقدمت عبر خمس مراحل على الأقل: (1) الاكتشاف المفاهيمي الأولي للثورة العسكرية التقنية من قبل المفكرين الاستراتيجيين السوفييت في أوائل الثمانينيات، (2) التكيف المفاهيمي والتعديل والتكامل في الفكر الاستراتيجي الأمريكي خلال أوائل التسعينيات، (3) نقاش ثورة الشؤون العسكرية المحبة للتكنولوجيا خلال منتصف التسعينيات إلى أواخره، (4) الانتقال إلى "التحوّل الدفاعي" الأوسع نطاقًا والتحقيق التجريبي الجزئي في أوائل العقد الأول من القرن الحادي والعشرين، و(5) الانعكاس النقدي الذي يشكك في السرد التخريبي من عام 2005 فصاعدًا (جراي، 2006) . منذ منتصف عام 2010، ومع الانتشار السريع للتقنيات الجديدة مثل الذكاء الاصطناعي والأنظمة المستقلة، يمكن للمرء أن يجادل في ظهور ثورة الشؤون العسكرية التي يحركها الذكاء الاصطناعي (AI-RMA) الجديدة - أو الموجة السادسة من ثورة الشؤون العسكرية (راسكا، 2021).

ومع ذلك ، وبالعودة إلى الوراء ، فإن تنفيذ ثورة الشؤون العسكرية التي تحركها تكنولوجيا المعلومات (IT-RMA)على مدى العقود الأربعة الماضية قد اتبع أيضًا مسارًا ذي مستوى ثوري أو تخريبي أقل بشكل واضح، ويتألف من تحسينات تدريجية وشبه مستمرة في القدرات الحالية (روس ، 2010). في حين أن الابتكارات العسكرية الكبيرة والواسعة النطاق والمتزامنة في تقنيات الدفاع والمؤسسات والعقائد كانت ظاهرة نادرة، فقد تقدمت المنظمات العسكرية إلى حد كبير من خلال مجموعة مستدامة من الابتكارات العسكرية التي تتراوح من الابتكارات الصغيرة إلى الابتكارات واسعة النطاق التي شكلت سلوك الحرب (جولدمان ، 1999). في حين أن العديد من الابتكارات العسكرية خلال هذه الحقبة، مثل مفاهيم الحرب المتمركزة على الشبكة قد نضجت، إلا أن الروايات الطموحة لـ "التحول العسكري التخريبي" الوشيك قد تجاوزت دائمًا الإمكانات التكنولوجية والتنظيمية

ويتم النظر على نطاق واسع إلى تقارب التقنيات الناشئة مثل الروبوتات والذكاء الاصطناعي وآلات التعلم والمنصات المعيارية مع تقنيات الاستشعار المتقدمة والمواد الجديدة وأنظمة الحماية والدفاعات والتقنيات السيبرانية التي تطمس الخطوط الفاصلة بين المجالات المادية والسيبرانية والبيولوجية على أنّ لها آثار عميقة على طبيعة الحرب في المستقبل. ففي سياق القوة الجوية، يعد تطبيق خوارزميات التعلم الآلي الجديدة على مشاكل متنوعة أيضًا بتوفير قدرات غير مسبوقة من حيث سرعة معالجة المعلومات، والأتمتة لمزيج من منصات الأسلحة وأنظمة المراقبة المأهولة/ غير المأهولة، وفي النهاية، القيادة والتحكم (C2) في اتخاذ القرار (هورويتز، 2018؛ كومينغز، 2017).



1

موجة الذكاء الاصطناعي ومستقبل القوة الجوية

د. مايكل راسكا

استاذ مساعد، مدرسة س. راجاراتنام للدراسات الدولية

في العشرينيات من القرن الحالي، تركز نقاشات القوة الجوية بشكل متزايد على تأثير التقنيات الناشئة على الابتكار في مجال الدفاع والطابع المستقبلي للحرب. إنّ تقارب التقنيات الجديدة المتقدمة مثل أنظمة الذكاء الاصطناعي (AI)، والروبوتات، والتصنيع الإضافي (أو الطباعة ثلاثية الأبعاد)، وحوسبة الكم، والطاقة الموجهة، وغيرها من التقنيات "التخريبية"، المحددة تحت المظلة التجارية للثورة الصناعية الرابعة (4IR)، تعِد بفرص جديدة ويحتمل أن تكون مهمة للتطبيقات الدفاعية، وبالتالي لرفع مستوى التفوق العسكري للفرد على المنافسين المحتملين.

يمكن القول إن الكثير من الجدل الحالي يصوّر تقنيات "الحدود التالية" على أنها مرادف للابتكار العسكري "المتقطع" أو "التخريبي" في طبيعة الحرب وسلوكها- من "العصر الصناعي" إلى "حرب عصر المعلومات" و الآن بشكل متزايد نحو "حرب الأتمتة" (راسكا ، 2021). على سبيل المثال، تهدف تقنيات المستشعرات المتقدمة مثل الصور الفائقة الطيفية والتصوير الحسابي وتصميم المستشعرات المدمجة إلى تحسين قدرات اكتشاف الهدف والتعرف عليه وتتبعه والتغلب على تداخل خط البصر التقليدي (فريتاس وال.، 2018). إنّ المواد المتقدمة مثل المركبات والسيراميك والمواد النانوية ذات الخصائص التكيفية ستجعل المعدات العسكرية أخف وزنا ولكن أكثر مقاومة للبيئة (بورنيت وال.، 2018). قد توفر تقنيات الضوئيات الناشئة، بما في ذلك الليزر عالي الطاقة والأجهزة الإلكترونية الضوئية، مستويات جديدة من الاتصالات الآمنة القائمة على الحوسبة الكمية والتشفير الكمي (اي اي اس اس، 2019).

قائمة المحتويات

سيؤدي السعي وراء هيمنة المعلومات إلى رفع مستوى استمرارية المنافسة بطرق جديدة وغير مؤكدة عبر العوالم المادية والكهرومغناطيسية والافتراضية. سيتم تقديم مخاطر ونقاط ضعف ونقاط فشل جديدة مع تطوير القوات الجوية لاعتمادها للسحب القتالية باستخدام أدوات وتطبيقات الذكاء الاصطناعي (AI) المضمنة. توفر مجموعة المقالات والأفكار من كبار المفكرين حول العالم في هذا المنشور وجهات نظر معمَّقة حول بعض أكثر القضايا ذات الصلة لرسم إطار ووضع تصوّر للتكامل متعدد المجالات وتفوّق المعلومات في القوة الجوية. تعكس وجهات النظر والمناقشات الواردة هنا أحدث الأفكار حول مجموعة متنوعة من المستويات الإستراتيجية والقيادية والتشغيلية للاعتبارات التي سيجدها القراء مفيدة لفهمهم الأوسع.

إن وجهات نظر الخبراء المعروضة هنا ليست متفائلة ولا متشائمة في حد ذاتها، وما تم تأكيده، كما نتوقع، هو أن العديد من الفرص الجديدة التي تحقق "قفزة إلى الأمام" والتي تدعمها التكنولوجيا تتشكل في الأفق ولكن استغلالها الفعال سيخلق تحديات جديدة مُعقَّدة ومُخرِّبة. يتم تسليط الضوء على بعض هذه التحديات الرئيسية والحاجة إلى فهمها بشكل أفضل. وكما هو الحال عادة، فإنّه ما من حلول سريعة أو حلول متاحة بسهولة. ومع ذلك، ثمة أسباب مقنعة لافتراض أن نتمكّن اليوم من التغلّب على التحديات العديدة المتوقعة نظريًا وفنيًا، وبعضها الآخر حتى في السنوات القليلة القادمة. إزاء العديد من الشكوك الموجودة حول المستقبل، فإنّ ما يمكن قوله بالتأكيد هو أنّه سيتم إعادة تعريف القوة الجوية بشكل جذري.

صباحت خان *PgCert PgDip BA MA PMP*
مستشار مستقل

مقدمة

تتغير طبيعة الحرب بشكل أساسي ويظهر عمق تشعبات هذه التغيّرات على مستوى القوة الجوية بشكل خاص. يحدد التكامل متعدد المجالات سلسلة من التحولات على مستوى القوة الجوية، وبشكل متزايد، القوة الفضائية على مدى السنوات القادمة والتي لا تتعلق بالتكنولوجيا فحسب بل بالمفاهيم الاستراتيجية والتشغيلية التي تنظمها القوات الجوية وتجري تخطيطها وعملياتها من خلالها.

وبحسب ما يبدو فإنّ الانتقال الوشيك والحتمي نحو العمليات متعددة المجالات يمثل تطوراً منطقياً عالي الأهمية بالنسبة للقوة الجوية لدرجة أنها قد تطرح السؤال التالي: لماذا لم نفكر في مفاهيم التشغيل ونطوّرها بهذه الطرق من قبل؟ بالنهاية، فإن البحث عن التحسين والتآزر التشغيلي واقتصاد القوة مستمر بالنسبة للقوة الجوية. يمكن القول إن القوات الجوية والقوات الشقيقة حاولت في الواقع العمل في سياق متعدد المجالات، بطريقة أو بشكل ما على مر السنين. ومع ذلك، فإن الجهود المبذولة لتوليد التآزر التشغيلي والتأثيرات عبر ساحة معارك متعددة المجالات على مستوى القوة أو حتى على مستوى المسرح الذي اقترحه المفهوم المبكر للعمليات متعددة المجالات (MDO) تُعد في الواقع جهود استثنائية.

تصيغ الإنشاءات المختلفة كالقيادة والتحكم في جميع المجالات المشتركة (JADC2) مستقبل للحرب يوفر قدرات على مستوى السحابة القتالية حيث يتم تضمين قيادة المهمة وإدارة ساحة المعركة بشكل فعال عبر القوة القتالية وحيث تكون حلقة المراقبة والتوجيه واتخاذ القرار (OODA) عامِلًا يزيد من سرعة الحوسبة المتطورة. تحدد شبكات الاستشعار والاتصالات القدرة الوظيفية للقوات الجوية للقيام بالطيف الكامل لمهامها التقليدية تقريباً. ستصبح تدفقات البيانات والبيانات بحد ذاتها أكثر أهمية من الاعتماد التقليدي لسلاح الجو على حرية المناورة، كما ستصبح هي عامل التمكين الاستراتيجي بشكل فعال. وسيتحوّل تركيز القوة الجوية بشكل متزايد على الشبكات بدلاً من المنصات، والبيانات بدلاً من أنظمة الأسلحة.

لطالما كان نجاح المهمة وفشلها يتحدد دائماً بمستوى الوعي الظرفي المتوافر للقادة والمشغلين. في النموذج التشغيلي الناشئ، فإن قدرة القوات الجوية على جمع البيانات ومعالجتها واستغلالها بسرعات قريبة من الوقت الفعلي تجعل البيانات أداة ذات فعالية أكبر وتحوّلها إلى أكثر سلاح مرغوب فيه. يجب أن يتم جمع ومعالجة وتجميع وتحليل ودمج ونشر كميات هائلة من البيانات والمعلومات والمعرفة بنفس مستوى سرعة الأحداث في ساحات المعارك في المستقبل. ستؤدي رقمنة الحرب الجارية الآن إلى اعتماد "البيانات الضخمة" في العمليات التشغيلية على نطاق واسع في السنوات القليلة المقبلة. بالإضافة إلى ذلك فإنّه سيكون للمجال الفضائي دور كبير بشكل موسع في تمكين الاتصالات المستمرة والمضمونة والآمنة على نطاق عالمي، وسيتم استخدامه كوسيلة نقل لذلك، إلى جانب استخدامه الأكثر تقليدية للمراقبة بعيدة المدى.

شكر وتقدير

هذا العمل هو منتج SPPS وقد تم تحضيره بالتعاون مع مؤلفي المقالات الواردة هنا. تود شركة SPPS أن تشكر العديد من المؤلفين الذين استثمروا الوقت الكافي للمساهمة في هذا المنتج في محاولة لعرض هذا الموضوع للمناقشة.

إخلاء مسؤولية

إنّ الآراء والأفكار الواردة في هذا المنشور تمثل آراء المؤلفين فحسب ولا تمثل آراء شركة SPPS أو سياساتها الرسمية أو موقفها أو أي وكالة أو أي حكومة، وهي مصممة لتقديم نظرة عامة مستقلة وتحليل وأفكار جديدة في ما يتعلق بهذا الموضوع. إنّ أمثلة التحليل التي يتم عرضها في هذه المقالة ليست سوى أمثلة وتستند فقط إلى معلومات محدودة ومفتوحة المصدر. الافتراضات الواردة في التحليل لا تعكس موقف أي جهة حكومية أو المنظمات التي يعمل فيها المؤلفون أو يرتبطون بها.

تم نشره وتوزيعه في نوفمبر 2021 بواسطة

شركة SPPS

102 ، مكاتب بوابة ابن بطوطة

دبي، الامارات العربية المتحدة

مجلة القوة الجوية

العمليات متعددة المجالات والذكاء الاصطناعي وسيطرة المعلومات

خريف 2021