Information Warfare: The Art of Operational Planning

Capt Gabrielle M. Nesburg

Air University Advanced Research – Next Generation ISR

17 October 2021

Abstract

Described as, “The employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior,” Information Warfare presents an area in which the United States Air Force must invest to win future conflicts and dominate strategic competition (“16th Air Force and Convergence for the Information War” 2020). Critical to this success is the idea that to effectively generate outcomes utilizing the full spectrum of IW capabilities, convergence, defined as the integration of capabilities that leverage access to data across separate functions in a way that both improves the effectiveness of each functional capability and creates new information warfare outcomes, must be a predominant aspect of the operational planning processes (“16th Air Force and Convergence for the Information War” 2020). The USAF must generate a planning process that creates specific and definitive objectives to enable the convergence of Cyberspace, Intelligence, Surveillance, Reconnaissance, Electromagnetic Warfare, and Information Operations, alongside traditional kinetic elements, to maintain a competitive advantage over adversaries in the information environment.

Described as, “The employment of military capabilities in and through the Information Environment (IE) to deliberately affect adversary human and system behavior,” Information Warfare (IW), and the convergence of those capabilities, presents a space in which the United States Air Force (USAF) must invest to win future conflicts and continue to compete alongside key adversaries (“16th Air Force and Convergence for the Information War” 2020). In order to effectively do so, the USAF must begin to posture itself to focus on planning processes that create definitive objectives to ensure that Cyberspace, Intelligence, Surveillance, Reconnaissance (ISR), Electromagnetic Warfare (EW), and Information Operations (IO) are postured with traditional kinetic elements to maintain a competitive advantage over adversaries in the IE.

Released in December of 2020, Air Force Chief of Staff Gen. Charles Q. Brown, Jr. published a series of documents entitled *CSAF Action Orders to Accelerate Change Across the Air Force*. Particularly applicable to the IW landscape is Action Order C: Competition, which outlines the fact that the United States is engaged in long-term strategic competitions with the People’s Republic of China (PRC) and the Russian Federation (RF), and must take immediate action to compete more effectively with these two actors (“CSAF Action Orders” 2020). Gen. Brown also calls out the fact that we must understand the competition’s ambitions and understand how they may conduct future warfare as effectiveness in deterring or prevailing in high-end conflict depends upon actions taken in peacetime competition (“CSAF Action Orders” 2020). Though it may go by different names, it has long been acknowledged that adversaries such as the RF and the PRC view the art of IW as a critical component in their strategic warfare approaches, particular as a means to continuously operate below the threshold of armed conflict.

The RF defines information war (informatsionnaya voyna) as a broad concept that covers a wide range of activities from utilizing information as a tool, target, or entire domain of operations (“Handbook of Russian Information Warfare” 2016). Also key to the RF view is the idea that information was encompasses computer network operations alongside disciplines such as psychological operations (PsyOps), strategic communications, Influence, intelligence, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, and destruction of enemy computer capabilities in order to form a whole of systems, methods, and tasks capability in order

to influence the perception and behavior of the enemy, population, and international community on all levels (“Handbook of Russian Information Warfare” 2016).

The key to the RF outlook on information war is the fact that they view this subset of warfare as a capability and activity that is not limited to purely wartime, nor something that is only limited to the initial phase of hostility before armed conflict occurs, but rather an ongoing activity regardless of the state of relations with the opponent (“Handbook of Russian Information Warfare” 2016). The U.S. on the other hand, operates in an environment where there is a clear distinction between war and peace and restricts methods and capabilities accordingly (“Russia’s Information Warfare” 2019). This distinction on viewpoint is so clear that the definition of information warfare in the RF’s Military Academy of the General Staff draws a stark comparison between the fact that the RF views this as broad capability, and not limited to wartime, vice the Western definition of IW, which it sees as limited, tactical information operations carried out during hostilities (“Handbook of Russian Information Warfare” 2016).

The PLA views IW as a key tenant in waging asymmetric warfare, which is critical as this type of warfare can alter traditional power structures and allow a weaker state to overcome a stronger enemy (“Asymmetric War? Implications for China’s Information Warfare Strategies” 2002). Specifically, IW is directed at “the enemy’s information detection sources, information channels, and information-processing and decision-making systems” (“The Chinese People’s Liberation Army and Information Warfare” 2014). Similar to RF IW doctrine, the PLA also specifically calls out the fact that IW is all encompassing, including the offensive and defensive nature of peacetime, crisis, and war operations, as well as national, strategic, and tactical levels of operations during times of war vice just a wartime action (“Asymmetric War? Implications for China’s Information Warfare Strategies” 2002). The overarching fusion of various IW capabilities from both and offensive and defensive perspective are key in the PLA’s strategy to counter US strengths as it allows them the capability to target certain "pockets of excellence," rather than attempting match the US’s overall comprehensive power operations (“Asymmetric War? Implications for China’s Information Warfare Strategies” 2002).

Alongside Gen. Brown's call to develop an understanding of both the RF's and PLA's intent and capability, he also calls for an understanding and identification of areas in which we must improve USAF capabilities ("CSAF Action Orders" 2020). An essential element and key to success is the both RF and PLA IW doctrine is the ability to plan for operations that encompass a broad range of capabilities and objectives, rather than just employing traditional military capabilities to reach an end state. With that in mind, it is vital that USAF begins to look at how it plans to converge capabilities from a planning perspective in order to accomplish objectives below the threshold of armed conflict. In October of 2019, the USAF took a huge leap forward in modernizing its approach to warfare through the standup of 16th Air Force. This new and first of its kind Numbered Air Force (NAF) looks to posture forces to synchronize planning and effects across four main components: Cyberspace, ISR, EW, and IO in order to generate insights, compete now, and prepare for escalation across the competition continuum.

In order to generate outcomes utilizing the full spectrum of IW capabilities, convergence, defined as the integration of capabilities that leverage access to data across separate functions in a way that both improves the effectiveness of each functional capability and creates new information warfare outcomes, is an essential element of success ("16th Air Force and Convergence for the Information War" 2020). That convergence hinges on the ability of focused and defined planning efforts at the strategic, operational, and tactical levels of warfare ("16th Air Force and Convergence for the Information War" 2020). However, current USAF planning doctrine hinges on concepts that do not favor full-spectrum IW convergence.

As defined in *Air Force Doctrine Publication 3-0 - Operations and Planning*, the USAF currently employs an Effects-Based Operational Approach (EBOA). This framework is defined as "an approach in which operations are planned, executed, assessed, and adapted to influence or change systems or capabilities in order to achieve desired outcomes" ("Air Force Doctrine Publication 3-0 - Operations and Planning" 2016). While not a planning methodology specifically, EBOA constitutes the USAF's way of thinking about operations that provides guidance for design, planning, execution, and assessment as an integral whole ("Air Force Doctrine Publication 3-0 - Operations and Planning" 2016). At its core, EBOA

starts with desired outcomes, not particular capabilities or resources, in order to yield certain insights and enhance comprehension of many general planning concepts ("Air Force Doctrine Publication 3-0 - Operations and Planning" 2016).

While on the surface, EBOA seems to facilitate the idea of convergence through IW planning alongside traditional military power employment plans, the joint community has called into question this framework for operational design. In 2008, then commander of US Joint Forces Command, Gen. James Mattis published a powerful pushback against the concept of Effects-Based Operations (EBO) as a whole, stating the command would no longer "no longer use, sponsor, or export the terms and concepts related to EBO" ("USJFCOM Commander's Guidance for Effects-based Operations" 2008). While Gen. Mattis specifically called out the fact that EBO can potentially be beneficial in targeting scenarios against traditional and well-defined targets such as road networks, or railway infrastructure, at its root, future operations will require a balance of regular and irregular competencies due to an incredibly adaptive enemy, which makes predicting effects, rather than planning to achieve objectives, fundamentally at odds with the nature of war ("USJFCOM Commander's Guidance for Effects-based Operations" 2008).

More specifically, EBO starts by determining an objective, and moving immediately to outlining effects that could accomplish those objectives, with the last step being to actually determine the tasks that will actually generate the actions or effects ("Effects-Based Operations: A Critique" 2006). There is an active attempt to quantify the end state of warfare, which can be exceedingly difficult due to the fact that effects themselves are effects are far less specific than objectives and tasks, causing issues to utilize them as the basis for military planning and execution ("Effects-Based Operations: A Critique" 2006). This is counter to traditional joint planning methodologies where the objective is identified, capabilities and tasks are assigned to the meet the objective, and the second and third order effects are outlined after the initial plan of execution has been outlined ("Effects-Based Operations: A Critique" 2006).

While this approach can be successful at a very tactical level of planning, at the strategic and operational levels of warfare, this planning approach proves incredibly difficult as there are a large number of intangible factors that can influence an effect that may not be initially identified ("Effects-Based

Operations: A Critique" 2006). Especially in the IW realm where the speed of the environment can cause drastic changes in the blink of an eye, it is essential that the USAF employs a planning methodology at the strategic and operational levels that not only clearly identifies and employs capabilities to accomplished a very specific and targeted objective, but also allows for considerable flexibility given potential shifts in the operational environment.

From a joint perspective, the idea of irregular warfare planning fits this concept. Much like IW, irregular warfare has an abundance of recognized definitions, however it is often known as a form of warfare that has as its objective the credibility and/ or legitimacy of the relevant political authority with the goal of undermining or supporting that authority ("Assessing Irregular Warfare: A Framework for Intelligence Analysis" 2008). Key to this type of warfare is the idea that while campaign planning as a whole is similar to military operations in general, there is a significant distinction: the military instrument of national power is usually, if not always, a supporting effort to the other instruments of national power ("Irregular Warfare Joint Operating Concept" 2007). The main challenge to overcome becomes the idea that that the military plan must integrate with and support the other instruments of national power to attain national strategic objectives, thus an irregular warfare campaign must begin with an incredibly strong understanding of the political purpose and strategic objectives ("Irregular Warfare Joint Operating Concept" 2007).

Taking the scope of irregular warfare planning a step further, a significant amount of scholarly work already exists on the idea that cyberspace operations are heavily aligned to irregular warfare and special operations doctrine and planning concepts. Many similarities exist between cyberwarfare and irregular warfare. In a domain where a preponderance of leadership does not always focus on the objectives that cyber capabilities can achieve, the similarities between irregular warfare and cyberwarfare can help to establish a foundation concept for employing the capabilities. Unlike conventional warfare means, both cyber and irregular warfare operations are global elements that, as specialized forces, can prepare to execute in a relatively short period of time ("Applying Irregular Warfare Principles to Cyber Warfare" 2019). The operate in grey space with unclear ROEs, where attribution can be incredibly difficult to find out ("Applying Irregular Warfare Principles to Cyber Warfare" 2019). The dynamic nature of both the irregular warfare

and cyberspace environments is a clear example that in order to accomplish effective planning in a holistic IW domain. While little has been explored comparing irregular warfare to IW as a whole, the concept of the IE even more directly aligns than the comparison to the cyber sub-component. The USAF must be focused on specific objectives, rather than a broad nature effects approach to ensure effective utilization of wide-ranging capabilities within its arsenal.

To execute this planning, there must be a focus on two key components: The Right Teams and The Right Data ("AF A2/6 Strategy & Plans" 2021). In regards to creating the right teams, holistic IW and kinetic planning efforts are not simply about bringing in all of the correct subject matter expertise into the room. The USAF must maintain a focus on building and fostering that specialized expertise. An example of this is heavily apparent in the ISR community. While the Intelligence Officer career field is somewhat allowed to specialize in the application of particular areas such as intelligence integration into cyber, space, or special operations, our core analytic force of enlisted all-source analysts are afforded no such opportunities. To truly build a team that understands the wide-ranging scope of IW, you need a force that has in-depth understanding of how ISR applies to cyber, EW, and IO, rather than a wave-top understanding akin to a jack of all trade's mentality.

In regards to developing the right data, this also directly ties into objective centric planning processes across every component of IW. The USAF must be able to answer a requirements question of in order to achieve an objective, what data do I need, who has those data points, and how do I get that data into the hands of the operators. From an ISR perspective, there are a multitude of longstanding ISR processes that allow for requirements injection into collection management. However, in the age of information warfare, those collection processes are not designed for quick turn support of operations when an adversary shifts intent or capability. To overcome those limitations, until such time as the community is effective at meeting tactical needs on a quick timeline, partnership with industry to obtain additional threat intelligence from an all source perspective becomes critical.

In order to converge a myriad of different capabilities in the large-scale IE, the USAF must maintain a focus on understanding and outlining key objectives. By also ensuring that the USAF has the right teams,

and the right data, it effectively produces the result of a problem centric approach, where Airmen clearly define the problem they are trying to solve, and then identify very specific objectives that will provide joint force commanders with options to achieve the desired end state. What those specific objectives allow for is a calculated planning effort to ensure that the full range of capabilities across the IW spectrum are applied. Instead of capabilities or platforms planning in specific silos to achieve what they interpret as commander's intent, all of those capabilities and platforms have the ability to come together to solve a singular priority objective. Taking this a step further, those IW planning efforts that bring together cyberspace, ISR, EW, and IO must also incorporate the traditional military elements from a kinetic effects piece to truly achieve an all-encompassing desired end state.

References

2006. "Effects-Based Operations: A Critique." *Joint Forces Quarterly*. gttps://apps.dtic.mil/sti/pdfs/ADA521851.pdf.

2020. "16th Air Force and Convergence for the Information War." *Cyber Defense Review*. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Haugh_Hall_Fan_CDR%20V5N2%20Summer%202020.pdf?ver=2020-07-27-053232-357.

2020. "CSAF Action Orders." *USAF*. https://www.af.mil/Portals/1/documents/csaf/CSAF_Action_Orders_Letter_to_the_Force.pdf.

2016. "Handbook of Russian Information Warfare." *NATO Defense College*. https://www.ndc.nato.int/news/news.php?icode=995.

2019. "Russia's Information Warfare." *MCU Journal*. https://www.usmcu.edu/Portals/218/CAOCL/files/RussiasInformationWarfare_MCUJ_Fall2019.pdf?ver=2019-11-19-093543-040.

2002. "Asymmetric War? Implications for China's Information Warfare Strategies." *American Asian Review*. https://web-a-ebscohost-com.aufric.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=1&sid=1e01d639-d0d8-4695-983f-1680c3230403%40sdc-v-sessmgr02.

2014. "The Chinese People's Liberation Army and Information Warfare." *U.S. Army War College Strategic Studies Institute*. https://publications.armywarcollege.edu/pubs/2263.pdf.

2016. "Air Force Doctrine Publication 3-0 - Operations and Planning." *Lemay Center for Doctrine*. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-0/3-0-AFDP-OPERATIONS-PLANNING.pdf.

2008. "USJFCOM Commander's Guidance for Effects-based Operations." *Joint Force Quarterly*. https://www.hsdl.org/?view&did=233314.

2019. "Applying Irregular Warfare Principles to Cyber Warfare." *Joint Force Quarterly*. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

2008. "Assessing Irregular Warfare: A Framework for Intelligence Analysis." *RAND*. https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG668.pdf.

2007. "Irregular Warfare (IW) Joint Operating Concept (JOC)." *Department of Defense*. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v1.pdf?ver=2017-12-28-162020-260.