Information Warfare Rising (Part II):

Conceptualizing Information Firepower

by

Capt Thomas Jun Hong

Air University Advanced Research

16 December 2020

"Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University, the United States Air Force, the Department of Defense, or any other US government agency.

Virtual In-Residence Squadron Officer School

Maxwell AFB, Alabama

ABSTRACT

Information is one of the key essential elements to win in a future all-domain battlespace. Nevertheless, the discourse on Joint All Domain Operations (JADO) has been limited to identifying the importance of information and offering salient solutions to alleviate a few select symptoms. There is no consolidated framework with which to *evaluate* the Joint Force's information advantage or to *design* its future. This paper proposes the concept of information firepower as such framework and will demonstrate how the concept supports the requirements in doctrine and RAND study findings.

The service components have focused on developing the art and science of Joint All-Domain Operations (JADO).[1] One of the key aspects of JADO that echoes in multiple documents from RAND Corporation studies to Air Force doctrine is the importance of information in JADO. After the Joint Force captures the battlespace in joint information preparation of environment, the Joint Force needs to rapidly converge the effects across multiple domains to operate inside an adversary's decision-making cycle in order to dominate the future battlespace.[2] In order to achieve this end state, the Joint Force needs to effectively leverage its information resources across all domains to achieve information advantage over the adversary, enabling the Joint Force "to quickly acquire, process, and present contextually relevant information from all domains".[3] A framework with which to *evaluate* the Joint Force's information advantage or to *design* its future, however, is not yet evident in the discourse on JADO or information warfare. This paper proposes the concept of information firepower – the comprehensive ability to direct and concentrate information resources to acquire, process, distribute, and employ information against a specific target to directly degrade or enable other capabilities to degrade the target's warfighting capacity – as such framework. Information firepower concept comprises five competencies that constantly interact with one another: extraction, delivery, boresight, attack, and protection. This paper will demonstrate how information firepower concept helps the Joint Force understand and seize information advantage by explaining each competency and examining how five competencies would come together through a hypothetical vignette.

Before delving into the subject matter, one might ask why the Joint Force would need a framework for information advantage. Theoretical framework serves as a blueprint to

[1] Department of the Air Force, *DAF Role in JADO*, 2-3.
[2] Ibid., 2.
[3] Ibid., 11-13.

provide the structural baseline of concepts and principles so the conceptual architects could design and plan on how to bring the vision to life.[4] Without a framework, the objectives remain vague, and planning efforts have huge seams – overlaps or gaps in efforts – as planners do not have a clear idea how their efforts fit together and translate to the vision. Lack of framework on information advantage and its effects are exhibited in RAND studies on JADO. A RAND study on command and control (C2) and situational awareness (SA) in the information environment (IE) points out lack of concepts to visualize the IE and argues that the Joint Force lacks the framing of operational needs in the IE, which leads to commanders' lack of awareness and understanding of the IE.[5] Another RAND study on joint all-domain C2 (JADC2) states that "…an overarching vision or strategy for automating or leveraging [artificial intelligence] is elusive", which contributes to lack of a consolidated plan to incorporate artificial intelligence (AI) and machine learning (ML) into data management.[6] This shows how lack of an overall framework challenges efforts to improve the Joint Force's ability to plan for JADO.

This trend of confusion about what to do with information is also mirrored at the senior level of military leadership. Gen John Hyten, chair of Joint Requirements Oversight Council (JROC) in charge of developing information advantage concept, acknowledged the difficulty of defining what information advantage should entail.[7] Lt Gen Haugh's article on convergence of effects identifies "tight synchronization of [intelligence, surveillance, reconnaissance capabilities], Cyber, [electronic warfare], and [information operations]" as the critical requirement for effective information warfare operations in the future battlespace but

[4] Grant and Osanloo, *Understanding, Selecting, and Integrating a Theoretical Framework*, 13-14.
[5] Paul et al., *Improving C2 and SA for Operations in and Through the IE*, 34, 48.
[6] Lingel et al., *JADC2 for Modern Warfare*, 16.
[7] Hitchens, "JROC Struggles To Build 'Information Advantage' Requirement", *Breaking Defense*, September 17, 2020, https://breakingdefense.com/2020/09/jroc-struggles-to-build-information-advantage-requirement/.

falls short of describing how the Joint Force could achieve that tight synchronization.[8] These anecdotes depict how lack of framework has left the Joint Force designers and thinktank experts with no clear, singular scheme to focus its efforts against the prioritized long-term objectives. Hence, the Joint Force needs a framework that enables its designers and planners to: 1) evaluate and assess the joint and coalition information advantage and adversary's, 2) envision the joint and coalition future dominance in the IE, and 3) design the Joint Force's future force based on the assessment and the vision.

With the need for a framework rationalized, one must ask: what are the requirements should the framework address? The discourse on the IE and JADO generally resonate along the following themes: 1) the need to shape the IE and influence an adversary's decision-making while preserving friendly force's and 2) the need to conduct all informational dynamics[9] rapidly in order to influence an adversary's decision-making. Joint Concept of Operating in the Information Environment (JCOIE) argues that information is not only an enabler but an instrument of military power[10] and that the Joint Force must leverage information to capture the new high ground of perceptions while preserving friendly mission-essential information.[11] Air Force doctrine echoes this view by advocating for presenting an adversary with "dilemmas at an operational tempo complicating or negating adversary responses and enabling the Joint Force to operate inside the adversary's decision-making

[8] Haugh, Hall, and Fan, *16th Air Force and Convergence for the Information War*, 36.
[9] Based on Joint Concept of Operating in Information Environment and Luciano Floridi's "What is the philosophy of information", one could break down informational dynamics in the following functions: Occurring (includes designing, authoring), Acquiring (incl. discovering, collecting), Processing (incl. validating, modifying, organizing, indexing, classifying, filtering, updating, sorting), Managing (incl. storing, networking, distributing, retrieving, transmitting), and Acting on the information (incl. monitoring, modelling, analyzing, explaining, planning, forecasting, decision making, instructing, educating, learning). See Joint Staff, *Joint Concept for Operating in the IE*, 12 and Floridi, *What is the Philosophy of Information?*, 138.
[10] This view is also represented in UK Ministry of Defence Joint Concept Note (JCN) 2/18 on Information Advantage. See UK MOD, *Information Advantage*, 1.
[11] Joint Staff, *Joint Concept for Operating in the IE*, 11.

cycle."[12] Air Force goes a step further by proposing convergence of capabilities and effects across all domains geared toward functions such as Sensing Grid, C2, and targeting to successfully conduct JADO.[13][14] Air Force's characterization of information, however, is primarily focused on information's utility as an enabler. It focuses on informing the decision-makers and operators to support traditional mission sets – maintaining SA and connecting the sensor to the shooter – and comparatively does not go in depth about how the Air Force actually plans to influence an adversary's decision-making.

RAND studies on the IE and JADC2 express similar views and present realistic solutions to help materialize the aforementioned vision. RAND study "Improving C2 and Situational Awareness for Operations in and Through the Information Environment" underlines the need to shape the IE by arguing that 1) effects in and through the IE can influence actors and behaviors outside the IE, and vice versa; 2) all military activities are inherently informational as they "influence the perceptions and opinions of populations that witness them"; 3) military actions seek to accomplish political goals, and politics increasingly takes place in the IE; and 4) defeat is a cognitive decision and process that takes place in the IE.[15] The study also characterizes the competition in the IE as a race for decision advantage – preserving and facilitating one's own decision-making while influencing, disrupting, or degrading an adversary's.[16] This race's highlight is which side can access, utilize, and project required information faster and with greater accuracy and clarity.[17] In addition, the study brings up an important insight regarding the IE: the IE is way too vast and volatile to comprehensively know and understand.[18] This leads to another requirement for the

[12] Department of the Air Force, *DAF Role in JADO*, 2.
[13] Ibid., 8-9, 13.
[14] Haugh, Hall, and Fan, *16th Air Force and Convergence for the Information War*, 34-35, 38.
[15] Paul et al., *Improving C2 and SA for Operations in and Through the IE*, 16-18.
[16] Ibid., 56.
[17] Ibid.
[18] Ibid., 17

framework in addition to the two above: the Joint Force needs to be able to concentrate its information resources against a target of interest for a specified period of time and then dynamically shift the weight of effort to another target as necessary.

On the other hand, RAND study "Joint All-Domain Command and Control for Modern Warfare" points out operational and tactical obstacles to JADO. The study reaffirms the need to conduct operations with high velocity and agility to present multiple dilemmas for an adversary and identifies the following challenges in current operations: 1) slow planning speed and imbalance of planning effort toward deliberate planning in the current Air Operations Center (AOC) structure, 2) siloed databases and disjointed AOC architecture that prevents integration, 3) consequent over-reliance on human liaisons, 4) lack of survivability and robustness of AOC facility and systems, and 5) different approval authorities for capabilities in different domains that further hampers integration across multiple domains.[19] The study calls for looking into alternative C2 construct, instituting and maintaining a reliable data ecosystem suitable for AI/ML to develop, and developing AI algorithms to truly realize multi-domain operations at scale in a short amount of time.[20] Of note, the study also emphasizes the need for an "enterprisewide strategy-to-tasks approach to get enabling capabilities down the same path" and the need to incorporate various external stakeholders.[21]

In summary, this brief literature review identifies three broad requirements for the Joint Force. The Joint Force needs to influence, degrade, or disrupt an adversary's decision-making while preserving its own. Secondly, in order to influence an adversary, the Joint Force needs to conduct all of its operations in and through the IE rapidly so the adversary would not have a chance to respond or attempt to preemptively disrupt the Joint Force's

[19] Lingel et al., *JADC2 for Modern Warfare*, 1-8.
[20] Ibid., 50-57.
[21] Ibid., 58.

cognitive process. Lastly, the Joint Force needs to employ its information resources flexibly, deliberately tailoring and concentrating its capacity against the desired target based on the commander's priority and the expected effectiveness, and promptly shifting its focus when a new, higher priority target emerges. JCOIE discusses *informational power* as the instrument to influence the relevant actors, protect the Joint Force's decision-making, and provide relevant data to enhance combat power.[22] This only addresses the first requirement but does not discuss two other requirements. This is where information firepower comes to the fore.

Information firepower is the comprehensive ability to *direct* and *concentrate* information resources to acquire, process, distribute, and employ information against a specific target to *directly degrade* or *enable* other capabilities to degrade the target's warfighting capacity. The information resources are not limited to traditional information related capabilities (IRCs) as all military activities have informational influence as they travel in and through the IE.[23] Information resources include influence values in various military activities, dataflow capacity and speed of the communication network, redundant communication nodes, sensors, information breadth and depth covered by the sensors, and visual displays of information to name a few. This paper intentionally chooses to label this concept as 'firepower' to highlight how information resources, just as traditional fires, need to be coordinated/synchronized, directed, and concentrated against a target to create desired effects in pursuit of the commander's objectives and intent.[24]

Information firepower has unique characteristics. Information firepower is ubiquitous. Since every military activity either creates information, changes information, or affects cognitive and/or physical dimension of the audience that witnesses the activity[25],

[22] Joint Staff, *Joint Concept for Operating in the IE*, 15.
[23] Paul et al., *Improving C2 and SA for Operations in and Through the IE*, 17.
[24] For synchronization and coordination of fires in general, see Joint Staff, *JOINT FIRE SUPPORT*, I-1-I-3
[25] Paul et al., *Improving C2 and SA for Operations in and Through the IE*, 17.

information firepower resides in every single Joint Force action in varying degrees. As the action travels through the IE, the information firepower interacts with discrete elements in the IE regardless of the Joint Force's original intention. An example of this characteristic was observed in the Philippines in October 2016. At the time, President of the Philippines, Rodrigo Duterte, had publicly demanded U.S. military forces in Mindanao, Philippines to leave after having blamed the United States for inflaming local insurgencies.[26] Shortly afterwards, the Philippine media reported that the U.S. unit deployed to Mindanao had begun pulling out after a U.S. transport aircraft was sighted loading troops and equipment and subsequently taking off.[27] In fact, this was a part of routine rotation of troops and equipment that had been planned for weeks.[28][29] Nonetheless, the simple action of deploying/redeploying troops, fused with the local political dynamic, mutated into an unintended message that impacted U.S.-Philippines relations. This demonstrates the duality of information firepower; the ubiquitous nature of information firepower allows it to grow and spread as it travels through the IE but also causes unintentional impacts.

Another characteristic of information firepower is that it is constantly changing. The IE is constantly in flux as new actors emerge and introduce new information with more ease than ever due to remarkable development in information and communications technology.[30] The traditional processes of coordinating and updating information collection and targeting, such as Joint Collection Management Board (JCMB)[31] and Joint Targeting Coordination Board (JTCB)[32], are insufficient. Instead, the commander needs to establish and

[26] Pareno, "US military pulls out equipment in Zambo", *philstar GLOBAL*, October 9, 2016, https://www.philstar.com/headlines/2016/10/09/1631805/us-military-pulls-out-equipment-zambo.
[27] Ibid.
[28] This anecdote is also based on author's personal recollection from his deployment to the Philippines.
[29] Alipala, "New batch of US troops already in Mindanao – military", *INQUIRER.NET*, October 25, 2016, https://globalnation.inquirer.net/147847/new-batch-of-us-troops-already-in-mindanao-military.
[30] Paul et al., *Improving C2 and SA for Operations in and Through the IE*, 27-28.
[31] Joint Staff, *JP 2-0 JOINT INTELLIGENCE*, I-14.
[32] Joint Staff, *JP 3-60 JOINT TARGETING*, II-19.

communicate clear objectives and priorities that his/her staff constantly updates according to changes in the IE. The commander also needs to exercise mission command by delegating the authorities for information firepower to the lowest level possible to let the operators constantly coordinate and focus information resources to emerging targets as long as the effort is in pursuit of the commander's intent. The joint mission control (JMC) concept, which empowers tactical-level mission controllers to leverage all domain capabilities flexibly and expeditiously[33], may provide a viable option to effectively employ information firepower.

The ubiquity and the dynamic nature of information firepower requires the Joint Force to deliberately plan, coordinate, and employ information firepower in accordance with the commander's intent. In order to plan, coordinate, and employ information firepower, the Joint Force must understand what constitutes information firepower. Information firepower comprises five competencies that constantly interact with one another: extraction, delivery, boresight, attack, and protection. Various information resources support one or multiple of these competencies. By analyzing and assessing the capacity in each competency, the Joint Force will be able to assess its own and an adversary's information firepower and plan to either exploit the consequent information advantage or mitigate the disadvantage.

Extraction competency deals with acquisition of information from the desired target. Information resources in this competency extract as much raw data as possible to serve as the primer to any process that utilizes information by providing the Joint Force with the data about the target. The information gained also informs the Joint Force on how best to posture its forces to influence adversaries and what the Joint Force needs to protect its decision-making from. The extraction information resources encompass the traditional intelligence,

[33] Chapman and Dalman, *Joint Mission Control*, 50, 53-54.

surveillance, and reconnaissance (ISR) sensors, other Sensing Grid platforms, and ISR techniques, tactics, procedures (TTPs). The Joint Force needs to consistently strive to expand the breadth and depth of information it extracts from targets by investing in new sensor development and recruiting the existing non-traditional ISR sensors onto the Sensing Grid construct. While this competency primarily focuses on the role of information as an enabler[34], extraction can also influence. Perception of being watched, which can materialize as an airborne ISR platform operating along an adversary's border, can very well affect the adversary's decision-making.

After the acquisition, the Joint Force needs to rapidly process the information, deliver it to the right customer, and share it with appropriate external stakeholders. Delivery competency hinges on how fast the network can transmit the relevant pieces of information and whether the network can sustain that rate of transmission. For this, the Joint Force not only needs a resilient, high-capacity, and high-speed communication infrastructure but also an automated data management scheme that can automatically process the raw data into concise, intuitive information for the operators as raw data flow in. This necessitates extensive data standardization and algorithm development to facilitate effective data management, as JADC2 proposal calls for.[35] All incoming pieces of data need to be tagged at the point of extraction; as they are delivered, the network needs to automatically filter, reform pieces into information, classify, and distribute the appropriate information at different classification levels. The data management scheme also needs to ensure that information is versatile; that is, the information needs to be modularized so it can conform to standards of multiple organizations and coalition partners to facilitate sharing with zero human involvement. The operator needs to access this processed information in a form of

[34] Information's enabler role highlights information in terms of acquiring quality information, exploiting it, and delivering it to the customer. See UK MOD, *Information Advantage*, 19.
[35] Lingel et al., *JADC2 for Modern Warfare*, 43.

intuitive visual display instead of textual reports in chatrooms as cognition from reading may take more time compared to cognition from pictorial icons. Over-redundancy is another key requirement for this competency; the communication infrastructure needs to resemble a web instead of a hub-and-spoke model where a single communication path presents a critical information vulnerability. The Joint Force should be ready to carry on with minimal interruption on delivery of information even if an adversary degrades or destroys a communication node. It is important to over-invest in the infrastructure even though it may seem wasteful. As Air Force doctrine states, "effectiveness must be prioritized over efficiency to generate adaptive capability"[36], and centralized communication hubs, while they may be cost-effective, present a high value target for an adversary.

Information resources need to be flexible so an entity like a JMC team can direct, concentrate, and dynamically shift the information weight of effort to the desired targets. As aforementioned, it is impossible to know and understand everything about the IE because the IE is constantly changing. The Joint Force thus needs to concentrate the limited information resources against high priority targets and sustain the concentration until the information resources achieve the desired effects. This is the information boresight competency – the ability to focus and sustain the Joint Force's information resources against the desired targets. The boresight can be used to extract or project information. In addition, due to ever-changing nature of the IE, the information boresight requires constant targeting support to determine which target deserves the brunt of the Joint Force's information firepower. The Joint Force should also be able to dynamically shift the boresight to other targets, which is another critical competency element. The mission controllers under the JMC concept could control the boresight by refocusing, monitoring the information flow, evaluating the quality of the

[36] This quote is in reference to logistics in the document, but it is also valid for communication infrastructure. See Department of the Air Force, *DAF Role in JADO*, 24.

information being received or projected through the boresight, and refining the boresight further to achieve effects more efficiently.

As the boresight tightens around the target, the Joint Force may choose to attack the target with its information resources. Attack competency in information firepower illustrates the ability to offensively employ information resources, kinetic or non-kinetic, against the desired target through the boresight to directly and/or indirectly degrade the target's warfighting capacity through influence. Key elements are weaponeering, the process of matching the right weapon to the target to create the desire effects[37], and collateral damage estimation (CDE). The targeteers need to understand the information resource's influence and the target characteristics in order to choose the right option to achieve the desired effect. CDE for information attack is far more difficult than for kinetic strikes as it is difficult to predict what second or third order impacts the action will bring about, as demonstrated in the Philippines example. Simple action could cause a myriad of unintended effects from unintended audiences. Leveraging AI/ML to analyze the historical trend data of the target and the environment could help the targeteers and operators to make the best decision.

Lastly, the Joint Force needs to protect its decision-making from unwanted external influences. Protection competency includes operational security (OPSEC), military deception (MILDEC), emission security (EMSEC), personnel security (PERSEC), and other security measures. The Joint Force may leverage information firepower's ubiquity. By utilizing information resources everywhere with no central hubs, the Joint Force denies an adversary high value targets to prosecute. The key question is striking the balance between the accessibility and security. Security policies have often prioritized the protection of information at the expense of accessibility and integration.[38] The Joint Force needs to

[37] Joint Staff, *JP 3-60 JOINT TARGETING*, II-15.
[38] Lingel et al., *JADC2 for Modern Warfare*, 43.

continue to invest in creative ways to make information accessible to friendly forces anywhere but inaccessible to adversaries.

One crucial opportunity that permeates through all the above competencies is AI/ML. AI/ML will be the key to difference between information overload and timely decision based on relevant information. AI/ML will be especially critical in the delivery competency to sort and filter incoming pieces of raw data, restructure them into relevant information, and send it to the right customers. AI/ML can also help the operators across all competencies to make better informed decisions more quickly by identifying appropriate resources for the desired effects and assisting planning efforts.

Information firepower concept builds upon the *informational power* concept in JCOIE and integrates the three requirements identified in the literature review. Information firepower concept provides a framework for designers and planners to better conceptualize the Joint Force's information resources to answer all three requirements by addressing influence, resiliency, timeliness, flexibility, and scalability with the five competencies. Next section will present a hypothetical vignette to showcase how one could apply information firepower framework in real-world.

VIGNETTE: CHINA'S 'GRAY-ZONE' ASSAULT ON TAIWAN[39]

This vignette hypothesizes that the People's Republic of China's (PRC) has intensified its efforts to coerce Taiwan to reunify. It is an amalgamation of a scenario posited by Krepinevich's "7 Deadly Scenarios" and a Reuters report on the PRC's real-world 'Gray-Zone' assault on Taiwan that has been ongoing since September 2020. Krepinevich posits potential reasons for the PRC to embark on an aggressive reunification campaign as: 1)

[39] Lee, Lague, and Blanchard, "China launches 'gray-zone' warfare to subdue Taiwan", *REUTERS INVESTIGATES*, December 10, 2020, https://www.reuters.com/investigates/special-report/hongkong-taiwan-military/.

prospect of the PRC's economic growth slowing down; 2) growing imbalances in the PRC demography that increase instability in its society; and 3) shortage of critical resources such as clear water.[40] These factors together challenge the PRC leadership's legitimacy, which is based on a rapidly growing economy.[41] Another factor is, having forcibly suppressed opposition in Hong Kong, Tibet, and Xinjiang, that the Chinese Communist Party (CCP) may view democratic Taiwan as the "last outpost of resistance" to realizing the dream of unified and rejuvenated China.[42] An in-depth analysis of the PLA's rationale is outside of this vignette's scope. Nevertheless, studying and understanding PRC leadership's decision-making will be critical in planning and directing the appropriate information firepower at the right target.

While Krepinevich hypothesizes a physical de-facto blockade of Taiwan by PLA forces[43], the real-world PLA forces have been conducting less obvious efforts against Taiwan. Since mid-September, PLA fighters, bombers, and support aircraft have crossed into Taiwan's Air Defense Identification Zone (ADIZ) almost every day.[44] The direct impact on Taiwan's military is taxing; in October, the Taiwanese air force scrambled 2,972 times against PLA aircraft in a nearly 550% increase from the previous monthly average up to October.[45] Naval intercept of PLA vessels also increased by 300%.[46] This relentless operation tempo does not only degrade Taiwan's physical readiness; as an information campaign, it also slowly degrades Taiwanese military's confidence and decision-making. This would increase chances of mistakes and accidents that the PLA could exploit.

[40] Krepinevich, *7 Deadly Scenarios*, 172-185.
[41] Ibid., 173.
[42] Lee, Lague, and Blanchard, "China launches 'gray-zone' warfare to subdue Taiwan".
[43] Krepinevich, *7 Deadly Scenarios*, 169-209.
[44] Lee, Lague, and Blanchard, "China launches 'gray-zone' warfare to subdue Taiwan".
[45] Ibid.
[46] Ibid.

What if the PRC decides to go one step further to bully Taiwan to induce capitulation? The PLA could conduct cyber/information attacks against U.S. and Taiwanese institutions to cause instability and erode Taiwanese public's trust in the coalition. On the physical dimension, the PLA could leverage military/law enforcement actions such as large joint amphibious forced entry exercise or 'escorting' commercial shipping through South China Sea, boarding and delaying Taiwan-bound vessels under cover of inspection. These actions would put significant pressure on the coalition public and decision-makers by grinding down their resolve and confidence.

How should the Joint Force counter the PLA's aggression? The United States would need to influence so the PRC decision-makers decide that it is not advantageous to continue its aggression against Taiwan. The Joint Force could approach this end state directly via cognitive dimension or indirectly by shaping the physical and informational dimensions. The application of information firepower begins with extraction; the Joint Force needs to integrate with coalition and partner (such as Taiwan, Japan, Australia, Great Britain, India, and Singapore) ISR networks and leverage as many sensors as possible. The extracted information would then be automatically processed and delivered to the customer via a thriving AI/ML ecosystem and resilient, redundant communication web. Partner nations' networks would provide additional resilience and bandwidth. Based on the relevant information, the JMC teams could build information boresights, tighten them, and steer resources to them. In this case, the JMCs could establish boresights on 1) the PLA and PRC decision-making process as a direct influence approach and 2) influential nodes in coalition, partner, and neutral nations as an indirect approach. The boresights would also need to be flexible to warrant dynamic shift of focus.

As teams establish boresights, they need to begin weaponeering by selecting the most effective weapons and assessing collateral damages as part of the attack competency. In case

the direct attack against the PLA's leadership turns out impractical or ineffective, the Joint Force should consider the information campaign to allies, partners, and other nations as the primary option. The goal would be to force the PLA into a cognitive Stalingrad – convincing the PLA leadership that the PLA might be able to isolate Taiwan, but the PRC would have to risk isolating itself from the free world at prohibitive diplomatic and economic costs. To this end, the coalition would need to highlight PLA aggression and the PRC's dishonesty to the members of international community and convince them to reconsider their relations with the PRC. As protective measures, the Joint Force should fully utilize the partner nation capabilities to maximize ubiquity and anonymity of these attacks to deny the PLA any single entity to pinpoint or attribute the activities to. The Joint Force could also conduct combined joint island defense exercise and combined freedom of navigation operations. The island defense exercise should demonstrate the coalition's capability to thwart the PLA's prized regional advantages such as large numbers of ballistic/cruise missiles, attack submarines, and fighters.[47] The Joint Force would need to conduct all explicit military actions with partner nations to reinforce the coalition's stance as guardians of internationally common values such as freedom, democracy, and human rights.

The convergence of effects would alienate the PRC from the free world and suggest to the PRC leadership that the PRC could suffer unsustainable costs, while the U.S.-led coalition would appear capable and willing to defeat the PRC's threats. Real-world planning and execution would undoubtedly involve more complicated factors; however, this vignette demonstrates how information firepower concept helps planners conceptualize and develop capabilities and employ information resources for specific desired effects.

CONCLUSION

[47] Krepinevich, *7 Deadly Scenarios*, 185-190.

This paper has examined RAND studies, Joint, and Air Force doctrines to establish that 1) information advantage is one of critical elements of winning all-domain battles and 2) the Joint Force needs a framework to understand and employ information effectively. Further literature review has diagnosed three requirements that the framework would need to address: the need to influence, degrade, or disrupt the adversary's decision-making cycle while preserving own; the need to conduct all OIE rapidly before adversary could react or threaten friendly forces; and the need to project information capabilities flexibly, tailored to a specific target for desired effects.

These requirements have led to the information firepower concept. By characterizing information firepower in five competencies of extraction, delivery, boresight, attack, and protection, this paper has demonstrated how the concept better postures planners on how to grasp the utility of information in JADO and design the Joint Force's future to achieve information advantage. A deliberate cultivation of the Joint Force leaders in information warfare would also be critical to realizing information firepower superiority.

One caveat of information firepower concept is that it alone will likely not deter, deny, and defeat an adversary. It is not the first time that military theorists have posited that the power of information is critical to future warfare. After Operation Desert Storm, a school of thought even argued that information warfare can subdue an adversary by itself without firing a bullet.[48] Defeat is a cognitive decision, but degrading an adversary's decision-making while leaving its capacity alone will not likely force an adversary to simply give up; information is not a technological silver bullet.[49] Moreover, the employed information could have multiple unintended effects that can ironically put the Joint Force's operation in jeopardy. The Joint Force needs to carefully leverage information firepower in conjunction

[48] Whitehead, *Information as a Weapon*, 17-22, 28-29.
[49] Ibid., 28-30, 33-34

with other capabilities to achieve a true convergence of effects across all domains in order to dominate the battlespace of 2030.

BIBLIOGRAPHY

Alipala, Julia. 2016. "New batch of US troops already in Mindanao – military." *INQUIRER.NET.* October 25. Accessed December 15, 2020. https://globalnation.inquirer.net/147847/new-batch-of-us-troops-already-in-mindanao-military.

Chapman, Matthew B, and Gerrith H Dalman. 2019. "Joint Mission Control: From Component to Joint Leadership of All-Domain Missions." *Air & Space Power Journal*, Spring: 50-61. https://www.questia.com/library/journal/1P4-2235154921/joint-mission-control-from-component-to-joint-leadership.

Floridi, L. 2002. "What is the Philosophy of Information?" *Metaphilosophy*, January: 123-145.

Grant, C, and A Osanloo. 2016. "Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for your "House"." *Administrative Issues Journal*, 12-26.

Haugh, Timothy D, Nicholas J Hall, and Eugene H Fan. 2020. "16th Air Force and Convergence for the Information War." *The Cyber Defense Review*, Summer: 29-44.

Hitchens, Theresa. 2020. "JROC Struggles To Build 'Information Advantage' Requirement." *Breaking Defense.* September 17. Accessed December 15, 2020. https://breakingdefense.com/2020/09/jroc-struggles-to-build-information-advantage-requirement/.

Joint Staff. 2018. "Joint Concept for Operating in the Information Environment (JCOIE)." *Joint Chiefs of Staff.* July 25. Accessed December 15, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.

Joint Staff. 2013. "JP 2-0, Joint Intelligence, 22 October 2013." *Joint Publications Intelligence Series.* October 22. Accessed December 15, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf.

Joint Staff. 2019. "JP 3-09, Joint Fire Support, 10 April 2019." *Joint Publications Operations Series.* April 10. Accessed December 15, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf?ver=2019-05-14-081632-887.

Joint Staff. 2013. "JP 3-60, Joint Targeting, 31 January 2013." January 31.

Krepinevich, Andrew F. 2010. *7 Deadly Scenarios: A Military Futurist Explores War in the Twenty-First Century.* New York, NY: Bantam Books.

Lee, Yimou, David Lague, and Ben Blanchard. 2020. "A REUTERS SPECIAL REPORT: China launches 'gray-zone' warfare to subdue Taiwan." *REUTERS INVESTIGATES.* December 10. Accessed December 15, 2020. https://www.reuters.com/investigates/special-report/hongkong-taiwan-military/.

Lingel, Sherrill, Jeff Hagen, Eric Hastings, Mary Lee, Matthew Sargent, Matthew Walsh, Li A Zhang, and David Blancett. 2020. *Joint All-Domain Command and Control for Modern Warfare.* Research Report, Santa Monica, CA: RAND Corporation.

Pareno, Roel. 2016. "US military pulls out equipment in Zambo." *Philstar Global.* October 9. Accessed December 15, 2020. https://www.philstar.com/headlines/2016/10/09/1631805/us-military-pulls-out-equipment-zambo.

Paul, Christopher, Colin P Clarke, Bonnie L Triezenberg, David Manheim, and Bradley Wilson. 2018. *Improving C2 and*

Situational Awareness for Operations in and Through the Information Environment. Research Report, Santa Monica, CA: RAND Corporation.

UK Ministry of Defence. 2018. "Joint Concept Note 2/18: Information Advantage." *Guidance: Information advantage (JCN 2/18).* September 18. Accessed December 15, 2020. https://www.gov.uk/government/publications/information-advantage-jcn-218.

Whitehead, YuLin G. 1999. "Information as a Weapon: Reality Versus Promises." *Air University School of Advanced Airpower Studies.* January 1. Accessed December 15, 2020. https://apps.dtic.mil/sti/citations/ADA360997.