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

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 reconceptualization 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.

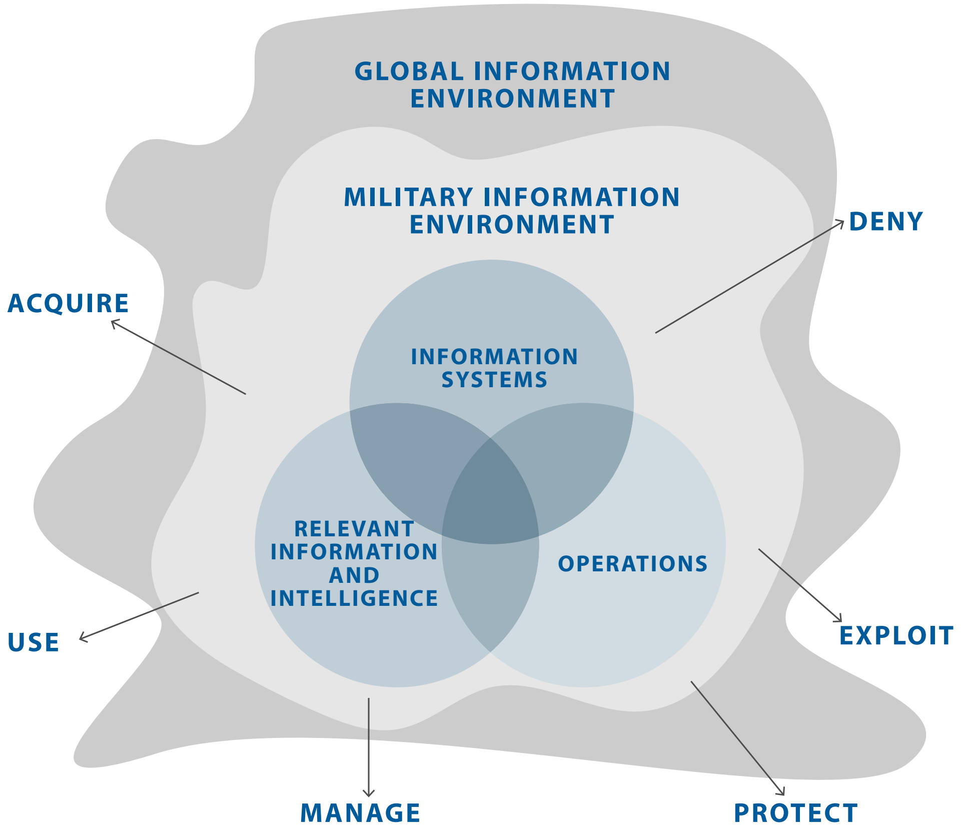
This is especially true as most Joint Force operations are anticipated take place in highly contested and distributed environments where IW will be an inherent feature of the competition space. Yet, with constraining budgets, threats on the rise, and more actors present in these same very spaces, Joint 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

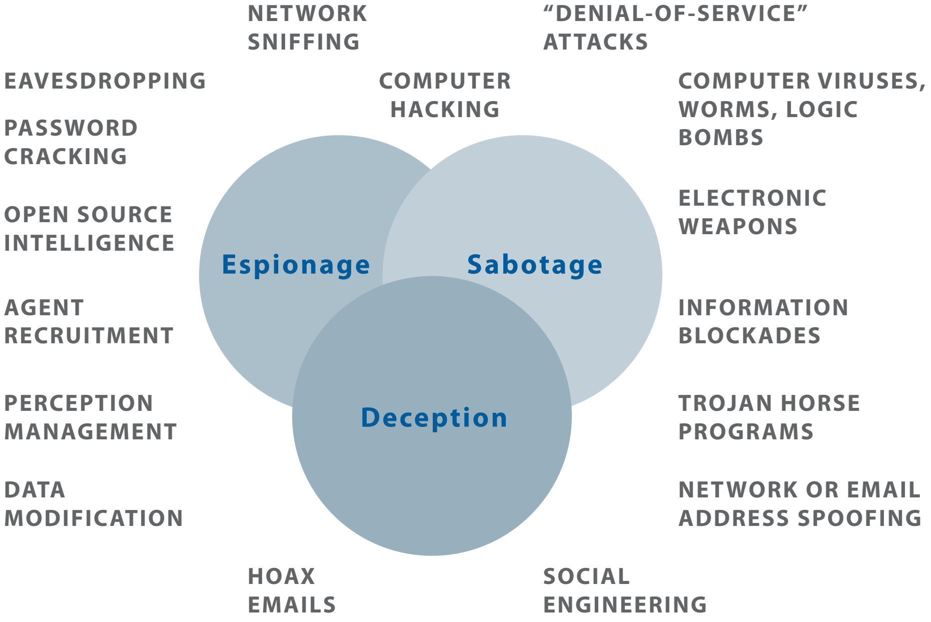
It will be vital for the Joint Force to address the question of whether its focus ought to be more on offensive or defensive IW. Many would agree that the Joint Force should develop and maintain a balance of offensive and defensive IW capabilities however there are more limitations to the former. Ultimately, 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


GLOBAL INFORMATION ENVIRONMENT
MILITARY INFORMATION ENVIRONMENT
INFORMATION SYSTEMS
RELEVANT INFORMATION AND INTELLIGENCE
OPERATIONS
ACQUIRE
DENY
USE
EXPLOIT
MANAGE
PROTECT

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.

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.