

5.0 Offensive Information Warfare in the 21st Century²⁰

Lt Gen Lincoln D. Faurer, USAF (Ret.)

There is no disagreement that information infrastructures are emerging as centers of gravity for (trans-) national power, and that as they grow in strategic importance a new, and thought by many, revolutionary aspect of warfare—information warfare—is taking shape. It is in the “taking shape” that disagreements arise.

Information Warfare (IW) - A Significant New Consideration

Within services and between services there are advocates for several interpretations of Information Warfare. Questions which need resolution, and hopefully common approaches across the services, are such as: Is IW something new or just an aspect of warfare that has been with us since the Trojan Horse? What is the demarcation between IW and C²W? Is it the latter only that is the domain of DoD? Since conduct of IW embraces more than the “warfighter”, where in our government is the responsibility for incorporating IW into the waging of war? Should IW stand alone and have its own advocate for competing within services for budget allocations and attention? Is it information or cyberspace that is a realm like air, land, sea and space? Should the argument between those who would isolate IW as a specific mission and those who would integrate it into doctrine be finessed by definitional fractionation to include Information Operations, Technical Operations, C² Attack, Offensive Counterinformation, etc. all being subsets of Offensive Information Warfare?

Such questions frame the challenge of incorporating IW meaningfully into our national security posture and validating it against more conventional weapons in our force structure. Our exploration of IW will be predicated on the belief that “the information dimension of modern war can be utilized knowingly and proactively in support of national policies, goals, and interests.” This follows logically from the fact that technology advancements have created an information abundant world environment increasingly reliant on timely, accurate flow of information for the conduct of business, the functioning of government, the operation of the national economy, and the conduct of war. This situation has introduced a new and substantial vulnerability into national conflicts. It is a vulnerability that cuts two ways and requires protective actions in parallel with preparations for offensive actions. This paper concentrates its analysis on the Air Force role if development and readiness for national employment of IW offensive capabilities is to be assured. In the course of this analysis the many questions surrounding IW will receive attention.

Cyberspace, “that consensually imagined universe where information reigns supreme,” presents the world with a unique set of problems. National borders cannot be projected into it and ownership of virtual reality is infeasible. Its properties are quite different from those of land, sea, air and space, but it most certainly is a realm in which national security must be contested.

When confronted with potential conflict, a national strategy employing offensive IW would be very advantageous. It would permit us to shape the *battle space* of conflict rather than react to a *battlefield* of the enemy’s choosing. It would provide options which minimize the fatalities

20. See also accompanying classified monograph on “Technical Information Operations.”

of traditional combat. Likely, the long term cost of its preparation would be less than that of hard kill weapons. Finally, its use would effectively complement a declining force structure and offer alternatives to overly stretching forces when confronted with multiple crises.

Offensive IW - What is it all about?

The objective of offensive warfare has always been to deny, destroy, disrupt or deceive the enemy either in his employment of forces or in retaining support of his constituency. The advent of the Information Age simply introduces a major new target consideration. The opportunities it brings us to improve upon our more traditional weapon systems and their management in the conduct of war brings commensurate vulnerabilities. Winning the battle of information dominance requires that we achieve an edge in offensive exploitation of the enemy's vulnerabilities over his ability against our protective measures. Given the global application of commercial progress in the information realm, and the extent to which modernization/upgrading will be pertinent to all countries, one man's "protect" need will be another man's offensive "target". Furthermore, even setting aside the specific, technical actions discussed in the IW Protect portion of this study, an important element of protection is to be able to "attack the attacker" so as to deter or to respond in kind. Couple all of this with a realization that the U.S. is probably the most dependent of nations on both its own and the global information infrastructure, the U.S. must accomplish a deliberate integration and balance of its Protect and Offensive knowledge and investment. Our historic predilection to emphasize the latter must be tempered by the severity of risk in doing so in an Information context, as well as the illogic of not recognizing the inextricable meshing of technology applications to protect and attack.

Although the objective of Offensive IW remains the classical "to deny, destroy, disrupt, or deceive", its most different feature is the extent to which the effect of an act will ripple beyond the immediate target. We learned with the advent of nuclear weapons the critical importance of considering collateral damage. We have extended that learning to all weapons of mass destruction as we factor into our decision process such matters as effects on: enemy civilians, our forces, coalition forces and public attitude. Offensive IW, operating in the virtual reality of cyberspace, exacerbates the above considerations. Operations, often civilian in nature, far from the battlefield are caught up in the affected battlespace. Often this worry is in conjunction with an opportunity for leverage of the greatest value, e.g., termination of conflict before war breaks out into killing, or nearly non-lethal attack options after the onset of hostilities. If the U.S. is to fully prepare an Offensive IW capability, a number of actions must occur.

The opportunities and the challenges of Offensive IW and the investment needed to convert a "possibility" into a national policy and strategy must be understood and accepted at several key decision nodes of our government. These must include the NCA, SecDef, CJCS, Service Chiefs and CINCs in the direct force structure chain, and such other national security principals as the National Security Advisor, and Secretary State. The maturing of an Offensive IW national strategy will also require expansion of involvement to embrace such as Treasury, Commerce, Economic Advisor and several other government and private sector specialist functions hinged by vulnerability and expertise to the global information infrastructure. After understanding and acceptance have been achieved there must be commitment to investment.

Investment in information technology analysis and adaptation must parallel the development of operational concepts. Projects must be as carefully tailored as they are for weapon systems. Information warriors, specially trained and with new attitudes, must be molded from people drawn from the fields of Intelligence, Communications and Operations. Exercising and simulation during concept refinement should feature the problems of complex, Joint integrated planning, execution and over-sight. A linchpin to successful Offensive IW will be preparation, sustainment and easy utilization of a detailed, responsive, massive, integrated data base. Commercial technologies permit implementation of such a data base arrangement, but legacy systems (hardware and software) and resource limitations stand athwart an essential database revamping.

A National Strategy of Offensive IW Needs Leadership and Focus

Information Warfare is receiving attention throughout DoD—in OSD (DISA, ARPA, ASD/C3I), the JCS, and the Services. The efforts appear specialized and non-complementary. There appears to be an absence of over-arching focus that is necessary for creation of a national policy and its implementing wherewithal comparable to the post World War II complementary policies of Containment and Nuclear Deterrence. Yet the potential of Information Warfare is as dramatic and basic to our national security posture as were those policies of 50 years ago.

After World War II, with respect to airpower, we recognized the need for dedicated attention to necessary R&D investment and to development of operational concepts. We stood up an Air Force and gave it focused responsibility to concentrate on air power, even though air arms continued in the other services. The need for similar concentrated focus in cyberspace is every bit as great today, and the breadth of the challenge is every bit as broad. “The playing field of IW is the full dimension of information itself, and embraces any element which supports, feeds, or interacts with the dimension of information. The playing field is practically infinite, delimited for each operation by the weapons chosen, the methods of engagement utilized, the strategy and metric for success.” The players extend well beyond the so called fighting forces of DoD and mirror the targets of IW, which include physical entities, data, decision processes of national leaders and the popular will of the citizenship. As the nation goes about the task of “right-sizing” our national security posture and weighing its costs against other needs, investment in new and not thoroughly understood “info weapons” will come under great scrutiny. It is time once again to take an action that will assure undivided focused attention to a new and critical realm of conflict.

The focused responsibility for “info power” should not be misconstrued as arguing for a mission grab by one service. Ultimately, the conduct of IW will be pertinent to all services and will need be employed tactically and strategically within each service doctrine. Such employment, however, will need be prefaced and supported by development of a common understanding of objectives, buttressed by adequate research and development of implementing technologies. Since IW has a dimension that impacts well beyond the traditional bounds of DoD and embraces decisions throughout our government, focused responsibility is necessary to ensure preparation of a nationally acceptable program. It is logical that the focused responsibility be resident within that department, the DoD, that has as its mission the conduct of war for the nation, even though employment of this new IW “weapon” will involve the remainder of government and could impact the private sector. Whether the target is within the private sector or not, the result, if not

the objective, is inimical to our national security. In fact, the range of harmful results may be the equal of any war we have fought. Therefore, while there are roles for many elements of our government and portions of the private sector, the logical residence for leadership regards to national security is the DoD. Finally, if it should seem practical to choose amongst the existing services for assignment of focused responsibility, rather than some other organizational solution, the Air Force is arguably the most suitable.

It is not intended that “focused responsibility” be interpreted as usurpation of assigned roles and missions elsewhere in our government structure. It is not intended to generate conflict between “law enforcement” and “military”. What is intended is responsibility for “end to end” consideration and subsequent guidance relative to ensuring information dominance (protection and exploitation) with respect to any hostile (trans) national entity—country, group, or person. One might liken the task facing us in the information realm to that confronting us after World War I and the inheritance of an “interesting capability”—the airplane. Even as the military was groping its way to a proper role, the private sector was expanding its applications. The envelope of capability needed to be pushed and a supporting structure of aids, regulations and controls needed to be developed. It fell to the Army Air Corps to lead the way. The “focused responsibility” for cyberspace, or the information realm, or information warfare should be viewed in much the same context as our experiences with airplanes and air power after WWI and WWII respectively. It is meant to be leadership not sole authority.

The Air Force, whether or not designated the lead service for IW, should embrace with enthusiasm and invest significantly and immediately in preparing capability. The Air Force’s Global Reach—Global Power (Global Presence) mission logically embraces the standoff offensive potential of Information Warfare. The exploitation of information infrastructure vulnerabilities is a natural extension of Air Force strategic targeting, an area in which visionary debate to clarify roles within our government structure regarding the conduct of IW in a time continuum of peace into declared war, and of C²W vs. IW within DoD, is of great importance.

Although tactical applications are obvious, it is in the strategic dimension that offensive IW most likely will have its greatest impact. It has the potential for application prior to the “shooting” phase of conflict. Early application should permit shaping of the “battlefield” (more properly, battlespace) to our advantage such that engagement of forces may be avoidable, or in the event of engagement, bloodshed can be minimized. The dominant strategic considerations make U.S. mastery of offensive IW critical to the Air Force. Such mastery requires priority investment of people and money and an intellectual commitment to the development and acquisition of technical understanding and capabilities. If we fail to do so, we’ll be caught short in an increasingly dangerous realm whose risks and opportunities we have contemplated but not yet adequately studied. Furthermore, we will be missing the opportunity to properly judge reduced investment and reinvestment in “killing” weapon systems as tradeoff to offensive IW investment.

We offer a final consideration in the assignment of a “leadership” role for either the protection of our national interests regards an information infrastructure or the development of an offensive IW capability. To separate the two would be a mistake. The synergy between the efforts are too pervasive to ignore. They are more than two sides of the same coin—each is, on occasion, the other in technology and process. Whatever organizational decision is made in designating focused responsibility and leadership for IW, it should embrace both aspects of

Information Warfare, much as NSA has both SIGINT and Information Security, so that cross fertilization of technical talent and operational experience can be achieved.

Summary

With information infrastructures emerging as centers of gravity for (trans) national power, the U.S. is faced with critical risk and critical opportunity. We can confront them as one by establishing as a national objective the achievement of information dominance. Pursuit of that objective demands that some hard decisions be made soon. Soon, because the U.S. is probably the most dependent of nations upon Information and Information Infrastructure—currently the cost of access to our information systems is extraordinarily low. Soon, because of the rate at which computer and communications technologies are compounding the volume and complexity of the global structures we must protect and attack.

The overarching decision that must be made is how best to bring cohesion to the many disparate Information Warfare efforts underway in DoD, elsewhere in our government, and even to some extent in the private sector. The following two observations are offered :

- A national objective of the significance and potential impact of information dominance requires top down establishment of a national strategy and governing policies. In effect, it must have focused leadership—an assigned responsibility for end-to-end consideration of all the needed and integrated components of a most complex national scheme.
- Although protect and attack actions will involve and impact the private sector, a national security rather than private/commercial sector perspective must dominate strategy and policy formulation.

Logically, it follows from these observations that the SecDef and DoD be Executive Branch designee for paramount responsibility within the government for IW. Whether this responsibility is delegated within DoD to one of the existing services (arguably the Air Force would be a good choice) or organized in some different fashion (perhaps a joint service NORAD), a prompt decision is needed. We must have such if we are to have timely planning, cohesive investment, and a reasonable chance of meeting the objective.

A third observation is that the contributions of protect and attack actions to the objective of information dominance are mutually supporting and technically commingled. Thus it can be argued that the protect and attack dimensions of IW should be addressed as two integrated features of a single strategy. Aside from technical cross fertilization, operational performance of each will strengthen the other. Together they constitute the challenge of ensuring information dominance.

In planning an IW strategy, whether as an Air Force or a national plan, it should be recognized that target information systems will change fundamentally in the near future, and that the following actions should be featured:

- Robust attack technologies capable of on-demand use against a range of target technologies/systems

- Leveraging of intelligence community parallel technologies to access and process targets
- Pursue long term expert based study on improved techniques for computer attack which increase on-demand effectiveness with reduced manpower investment
- Pursuit of intelligent agents for attack mission