Information Warfare:
Same wine, different bottle?

by

Lt Kurt Konopatzke, USAF

Information warfare (IW) is a highly contentious subject that has spawned widespread debate on a variety of issues, ranging from arguments over what to call this new phenomenon (cyberwar, netwar, or C2W), to how we should incorporate IW concepts and principles into AF doctrine. The debate is fueled in large part by disagreements over how we should define information warfare, and whether it has anything really new to offer the warfighter. Many will argue that information warfare is a fundamentally new and different concept that may completely change the way we fight wars of the future, while others will tell you that information war is merely a new label for things we have done for a long time (EW, PSYOP, deception, physical destruction, etc.). Regardless of what you believe to be true about information warfare, the fact remains that IW is a subject that merits serious study and consideration. To help in that regard, I'd like to offer a few observations about some the complex issues and arguments that are currently under debate.

Of all the issues that have arisen out of the IW controversy, two in particular deserve special mention--not because they are any more important than all the rest, but because they seem to appear in nearly every discussion on information warfare.

The first issue, whether or not we should establish a separate information "corps", has already generated a lot of controversy in both the Air Force and in our sister services as well. In the future, policy makers will have to choose between integrating information warfare capabilities into all Air Force, Army, Navy, and Marine Corps missions, or creating a separate information "corps" to more effectively utilize the new weapons that information age technologies promise to bring to the fray. While there good arguments for both sides, it appears that the senior Air Force leadership has already dismissed the possibility of creating a separate info corps. Having said that, while I am not advocating one position or another, this rather short-sighted view should set off alarm bells in all of us. After all, it was this kind of thinking that almost prevented the creation of the U.S. Air Force during the 1930's and 1940's. Again, the establishment of a of sixth service may or may not be the right approach, but we as an institution need to carefully consider all the options before choosing a course of action.

The second issue is actually an argument frequently advanced by naysayers who claim that information age weapons (e.g., computers, networks, and telecommunications equipment) only work against high-tech adversaries like ourselves. In other words, information warfare cannot be waged against an adversary like Rwanda, where there are probably less than two dozen computers in the whole country.

While there are many nation-states in the world today that are clearly not as technologically advanced as the United States, we must keep in mind two points when examining the implications of information war. The first point is that powerful information-age weapons (like modem-equipped computers, for instance) can be purchased in the commercial market for several hundred dollars. The technology is no longer limited or controlled by a select number of businesses or nation-states, and nearly everyone has access to a formidable IW capability.

The second point to consider is that the United States has become extremely dependent on computers, computer-based networks, and telecommunications equipment to manipulate and process a wide variety of information--financial data, medical data- bases, defense-related information, etc. Much of this information still travels on unprotected electronic networks that are subject to manipulation by anyone with the right equipment and a modicum of technical knowledge.

Take these two points together and you can see why our dependence on information and information systems has exposed us to a number of organizations (both big and small) that possess the tools to exploit vulnerabilities we have yet to protect. In many cases, protecting ourselves may involve using DoD computers to conduct our own counter-information attacks against a wide variety of potential foes, from the lone hacker operating out of his room, to highly organized, well-financed crime syndicates. The point is, the capability to wage information warfare is not limited to advanced nation-states. Formidable IW weapons can already be purchased in the commercial market for a few hundred dollars, which gives lots of people and organizations the capability to attack us. Now that they have that capability, all they need now is the motivation.

These are but a few of the many contentious issues that have surfaced in the debates on information warfare. There is little doubt in anyone's mind that other issues will be hotly contested in the months and years to come as we struggle to understand and cope with the implications of the information age. Like it or not, information warfare is here to stay, and we in the Air Force cannot afford to ignore the possibilities and the vulnerabilities that IW brings to the table.

Disclaimer

The conclusions and opinions expressed in this document are those of the author cultivated in the freedom of expression, academic environment of Air University. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force or the Air University.

This article has undergone security and policy content review and has been approved for public release IAW AFI 35-101.