A Global Forum for Naval Historical Scholarship

International Journal of Naval History

Volume 2 Number 3 December 2003

Wayne Michael Hall, **Stray Voltage: War in the Information Age** (Annapolis: Naval Institute Press, 2003). ISBN 1-59114-350-0. Notes. Index. Pp. xvii + 219, $36.95.

Reviewed by Timothy Wolters,
National Air & Space Museum, Smithsonian Institution

Stray Voltage is a timely book for a nation engaging in a global war on terrorism. Unlike most of the monographs reviewed in this journal, it does not explore the past, but rather offers a vision for the future. Written by retired brigadier general Wayne Michael Hall, the central premise of *Stray Voltage* is that the United States has entered into a "Hundred Years' War" against cunning, ruthless adversaries who hate America and the American way of life. Because these enemies have no chance of competing with conventional U.S. military forces, Hall concludes that they will have no choice but to employ asymmetric strategies, tactics, and tools to achieve their ends. Foremost of these will be "knowledge war" and "information operations."

Hall posits that knowledge war – which he defines as "a struggle between adversaries over accessing and using valuable information and knowledge to gain advantages in decision making" (p. 14) – will serve as the underlying foundation of all future conflict, and that information operations – which he identifies as "activities in physical settings and in cyberspace purposefully designed to influence or directly affect the decisions of an adversary and the processes that support it" (p. 98) – will become the primary method of combat employed by America's enemies in the twenty-first century. According to Hall, today's U.S. military is ill-prepared to engage in knowledge war against an asymmetric foe skilled in information operations.

A Global Forum for Naval Historical Scholarship

International Journal of Naval History

Volume 2 Number 3 December 2003

Hall sees several root causes underlying the American defense establishment's inability to fight a successful knowledge war. Chief among these is the failure of military leaders to recognize that two new domains of conflict – cyberspace and the cerebral world – soon will eclipse in significance the traditional domains of air, land, sea, and space. When this happens, "knowledge workers" will become more important than the tanks, ships, and aircraft traditionally associated with industrial-age war. According to Hall, neither the civilian nor the military educational system in the United States currently is structured to produce the knowledge workers or "cyberwarriors" needed for information-age warfare. As such, he encourages educational reforms that will teach people how to analyze and synthesize information more efficiently. Finally, Hall lambastes the U.S. government's propensity for hoarding information, a tendency that precludes the collaborative efforts required to solve the complex problems of national defense in the twenty-first century.

Like any good officer, Hall not only identifies what he sees as a series of problems, he also provides suggestions on how to fix them. Specifically, he outlines four interrelated reforms for improving the United States' capacity to cope with knowledge war assaults from determined adversaries. First, Hall advocates the creation of national, regional, state, and local Knowledge Advantage Centers (KACs), which he describes as locations where "people and machines collaborate to integrate data, information, and knowledge" (p. 160). In these KACs, knowledge workers will convert information into knowledge, thereby enabling leaders to make quicker and more effective decisions. Second, Hall argues for immediate development of a joint asymmetric opposing force "to help friendly security forces prepare for combating a multitude of terrorist attacks against key people, physical landmarks, and symbols, and, of course, to conduct operations in cyberspace" (p. 169). For maximum effectiveness, this asymmetric opposing force must use the tools of the modern knowledge warrior, employ foreign languages in all its operations, and strive ardently to avoid the trap of mirror-imaging. Third, Hall

International Journal of Naval History

Volume 2 Number 3 December 2003

recommends establishing a "Joint Information Operations Proving Ground" where U.S. forces can test and evaluate the effects of digital conflict on people, organizations, and materiel. Lastly, Hall proposes the creation of an internet replicator to simulate cyberspace and the internet. Scientists and engineers would use this simulator to develop "cyberbots" – sophisticated software programs that learn with experience and perform complex tasks such as surveillance, intelligence collection, deception, communications, and computer network attacks.

At first glance, all of these recommendations appear reasonable, perhaps even prudent. Yet *Stray Voltage* fails to address adequately several significant issues. To begin, from where is the money for these reforms going to come? Hall suggests that resources will have to be diverted from the traditional kinetic weapons of force-on-force conflict, but provides no further guidance. Exactly which industrial-age systems should the United States eliminate to pay for a Joint Information Operations Proving Ground or an internet simulator? The book also says nothing about the complex legal and Constitutional issues that would surround the creation of Knowledge Advantage Centers. Would these centers be allowed to track the physical movements, spending patterns, and religious affiliations of U.S. citizens? If so, would this constitute an appropriate mission for the American military? Finally, all of these reforms are premised on the ability of knowledge workers to freely and openly exchange information. Yet even as Hall recommends fusing "all classifications of information" (p. 166), he acknowledges that "much of the nation's infrastructure lies in the control of people loath to share relevant information, thereby rendering the notion of a holistic, sharing, knowledge-oriented networked defense system moot" (p. 183). Hall may well be right – many now believe the tragedies of 11 September 2001 could have been prevented if government agencies had been more willing to share critical information – but he offers no suggestions on how to eliminate the stovepipes in which so much national security information now resides.

A Global Forum for Naval Historical Scholarship

International Journal of Naval History

Volume 2 Number 3 December 2003

For the reader interested in a lucid explanation of the buzzwords often uttered by defense intellectuals – knowledge war, asymmetric warfare, information superiority, information operations, knowledge management – this book has much to offer. Indeed, this reviewer would not be surprised to see one or more of America's war colleges adopt *Stray Voltage* as a standard text. On the other hand, Hall's reluctance to address many of the complex issues surrounding his recommendations makes the reforms he suggests seem like so much pie in the sky. After all, a viable national security strategy for the twenty-first century requires not only good ideas, but a game plan as well.