



Book review

Information warfare and security by Dorothy E. Denning (Addison-Wesley Pub. Co., 1998).

The idea that “information societies” conduct “information warfare” is almost inevitable. If, as is argued, such societies present distinct modes of political, economic, and cultural organization, it is only natural to think that they should present equally distinct modes of warfare. Yet, the notion of information warfare seems to suffer from the same conceptual confusion plaguing that of “information society”: What does it exactly encompass? What does it *not* encompass? What precisely is *new* about it, if anything? The topic has thus engendered much debate within national security circles.¹

In *Information Warfare and Security*, Dorothy Denning, a professor of computer science at Georgetown University best known for her work on U.S. encryption policy, offers a balanced view of information warfare that seeks to avoid either denial or hype: there *is* indeed something real and new about this threat, stemming from a general dependence on technology throughout society. Denning notes: “What the new technologies have brought, then, are more options and opportunities for conducting information warfare.” (p. 19) Yet, this does not justify that we fall for the catastrophic fantasies that have become all too abundant on the eve of the new millennium. As she goes on to point out:

“It is easy to postulate scenarios such as ‘Stock market crashes after hacker tampers with Wall Street computers’ or ‘Planes collide after terrorists hack into navigation system and alter routes.’ It is much more difficult to assess whether a scenario is plausible or likely. [...] The big question is this: Can someone launch an attack with catastrophic consequences and, if so, what are the chances of that happening? In truth, nobody knows.” (p. 19)

Rather than offering (premature) assessments and policy statements, Denning aims, above all, to “enhance understanding of threats, defenses, and issues.” (xvii)

Denning sets the stage with an account of the Persian Gulf War as an information war, where both sides exploited, to a degree previously unknown, the new

propaganda and offensive opportunities offered by ubiquitous communication and information technologies. After a brief sketch of the theory of information warfare, defined as consisting of “operations that target or exploit information media in order to win some objective over an adversary” (p. xiii), the larger part of the book is occupied by anecdotal descriptions of “offensive” and “defensive” information warfare. The first includes such diverse destructive practices as copyright infringement, defamation, spam, dumpster diving, eavesdropping, calling card fraud, hacking, email forgery, and computer viruses. The second consists of all methods known to evade corresponding information attacks, including encryption and authentication technologies, firewalls, networking security standards, backup, risk insurance, as well as national security policies.

Denning’s stated goal is “to situate the areas of my greatest expertise, computers and cryptography, within a larger context,” (xvi) and she succeeds well in providing the reader with a view of that larger context, in the form of a compendium of the wide array of informational abuses nowadays possible. Successfully organizing an impressive mass of otherwise seemingly unrelated case stories, from voice mail abuse, to identity theft, to encryption policy, *Information Warfare and Security* will prove a useful resource to anyone wishing for an up-to-date account of information crime. At all times, Denning maintains a balanced attitude towards her topic, underlining the complexity inherent in assessing threats and risks. For those who have come to view encryption as the end-all of security solutions on the Internet, she warns that “[...] the connection between encryption policy and security is not simple and may be vastly overstated. Security demands much more than encryption, and encryption deployment is affected by factors other than government policy. Liberalizing exports controls on encryption would no doubt promote the availability of encryption and boost security, but it would not eliminate the majority of vulnerabilities in critical information infrastructures.” (p. 424) In the networked society, there is no simple “magic bullet”: threats and risks are multiple and distributed, and no single solution is likely to solve all difficulties.

This attention to complexity is, unfortunately, not reflected in Denning's approach to the theory of information warfare, which she implicitly presents as a self-evident and unproblematic category. In contrast, Martin Libicki, a researcher at the Rand Corporation, underlines the difficulties inherent adopting "information" as a core conceptual category: "[a] fundamental difficulty in coming to terms with information warfare [is] deciding on its nature. Is it a new art? The newest version of some time-honored features of warfare? Is it a new medium of conflict that issues from the burgeoning global information infrastructure or one to which information technologies have contributed but which originates in the wetware of the human brain?"² The definition issue is far from trivial: information warfare, in seeking to explain everything, runs the risk of explaining nothing: What is *not* information warfare?, one is tempted to ask throughout Denning's account.³ While Denning does recognize that she may have cast her net wide, she unfortunately fails to acknowledge that the terms of the debate are themselves contentious.

In thinking about the various new kinds of ethical challenges brought about by the insinuation of information technologies into seemingly every aspect of our lives, moral philosophers may wish to consider Denning's book not only as an information resource, but as a theoretical experiment as well. Should ethical issues be similarly approached under the unifying banner of "information"? Does the paradigm of information, as Masahiko Mizutani has recently argued, offer the basis of a new taxonomy of ethical problems?⁴ Is it then productive to think in terms of "information ethics," to gather areas of inquiry as diverse as business, medical, or environmental ethics under a single umbrella? *Information Warfare and Security* is one experiment that suggests both the dangers and promises of such an all-encompassing category.

Notes

1. See, for example: Winn Schwartau, *Information Warfare: Chaos on the electronic super highway*, 2nd ed. (N.Y.: Thunder's Mouth Press, 1996); Alan D. Campen, Douglas H. Dearth and R. Thomas Goodden (eds.) *Cyberwar: Security, Strategy, and Conflict in the Information Age* (Fairfax, VA: AFCEA International Press, 1996); Roger C. Molander (ed.) *Strategic Information Warfare Rising* (Santa Monica: Rand Corporation, 1996); John Arquilla and David F. Ronfeldt (eds.) *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: Rand Corporation, 1998).
2. Martin Libicki, "What is information warfare?," *Strategic Forum* 28, Institute for National Strategic Studies, National Defense University.
3. For example: "John Petersen predicts that information warfare in the future will [...] involve the manipulation of "memes" – big, powerful ideas such as global warming and nuclear war that move people to action [...]. Human history has been shaped by memes, religion being a good example, so Petersen's projection might be viewed as a continuation of age-old methods." (p. 18)
4. Masahiko Mizutani, "Information Ethics in the Age of the Internet: An Overview," keynote address, First International Workshop for the Foundations of Information Ethics (FINE '99), March 15–16, Kyoto, Japan.

Jean-François Blanchette
Department of Science and Technology Studies,
Rensselaer Polytechnic Institute,
Troy, New York,
USA