BOOK REVIEW

CYBERSPACE AND THE USE OF FORCE

W. GARY SHARP, SR., AEGIS RESEARCH CORPORATION (FALLS CHURCH, VIRGINIA). 1999. 234 PP.

JAMES P. TERRY*

The explosion of information related to national security, which can now be computer-directed or computer-downloaded, has evoked serious discussion by concerned leaders in the United States, Europe, and Asia. In the past, the question of law surrounding this issue has been largely ignored. Now, however, the active and urgent response of most developed nations to the requirements of information security, threat analysis and characterization, and effective countermeasures requires consideration of the legal parameter.

In *Cyberspace and the Use of Force*, Gary Sharp, the editor of the highly regarded *UN Peace Operations*,[1] provides an important contribution in the discussion of information security. This treatise on the application of law to new technology first delineates those peacetime state activities falling within the information highway that constitute an unlawful threat or use of force. The treatise then examines the circumstances under which states have the right to use force in response to such a threat or use of force.

In this comprehensive volume, Sharp claims that information technology is both redefining national security and the use of force by states. The author begins his examination with a review of the international legal process, and then looks at how international law has traditionally been applied to new technologies. He posits that computer espionage, computer network attacks, as well as the subversion

---

* James Terry served as Legal Counsel to the Chairman of the Joint Chiefs of Staff from 1992-1995. He currently serves as a senior official in another Government agency. The reviewer is widely published in the areas of coercion control and national security law.

1. UNITED NATIONS PEACE OPERATIONS: A COLLECTION OF PRIMARY DOCUMENTS AND READINGS GOVERNING THE CONDUCT OF MULTILATERAL PEACE OPERATIONS (Walter Gary Sharp, Sr. ed., 1995).

of political, economic, and/or non-military information bearing on a nation's capabilities and vulnerabilities may well constitute an unlawful use of force in cyberspace under traditional international law principles. For example, he urges that few would dispute that the United States has the right under existing international law to respond with military force if a state destroyed or significantly damaged the New York Stock Exchange.

The primary focus of this volume, therefore, is to examine the two following threshold issues: (1) identifying those peacetime interstate activities falling within the telecommunications highway that constitute a threat or use of force under the international law of conflict management, and (2) identifying when such a threat or use of force warrants a concomitant right to use force in self-defense. Accordingly, this analysis details the effect of the law of conflict management on the use of force between states in cyberspace.

As a predicate, the author addresses the military applications of information technology. First, he explains that the Internet was originally a network of computers linked by telecommunications infrastructure and managed by the Department of Defense (DoD) in the 1970s. He reiterates the process by which the internal computer networks of universities and private research facilities were merged via the development of hypertext, which was created in 1989 as the primary platform of the Internet and translated diverse computer protocols into standard format.

This process, while extremely beneficial to both the military and civilian sectors, has created vulnerabilities for the United States. Sharp reviews how the World Wide Web, at once the heart of the Defense Reform Initiative and key to the reengineering and streamlining of U.S. business practices, can provide for adversaries with a potent instrument to obtain, correlate, and evaluate an unprecedented volume of aggregated information regarding DoD capabilities. For example, he notes that the DoD web site contains detailed information on the DoD total force anthrax immunization program as well as Operation Desert Fox in Iraq.

The strength of the text lies in its discussion of the two threshold issues described above. In reviewing state activities affecting information that constitute a threat or use of force, Sharp focuses on the threat posed by states and non-state actors who anonymously pry into another state's public, sensitive, and classified computers to collect a wide range of government and business information, to manipulate data, to deceive decisionmakers, to influence public opinion,

and to even cause physical destruction from remote locations abroad. The author warns that information technology used for these purposes adds a new meaning to over-the-horizon warfare.

The second issue—when is a response in self-defense justified and appropriate—is more delicate. Sharp begins with a review of the existing legal regime available to deter such destructive actions, including the U.N. Charter system, the Geneva Conventions, and customary international law in the context of state activities conducted through information technology. Sharp concludes that a new definitional structure, which would embrace every use of force that might constitute an armed attack in cyberspace and thus justify a response in self-defense, may never be drafted. Nevertheless, he describes a series of sobering instances where information technology has already been used to threaten U.S. interests by unlawful intrusions into and/or critical alterations of information transmissions of both a military and civil nature.

Sharp urges, however, that the best way to accurately predict what may be considered a use of force constituting an armed attack under the Charter is by studying state practice. He states that in addition to traditional, universally accepted examples such as the 1990 Iraqi invasion of Kuwait, an armed attack may occur "when a use of force or an activity not traditionally considered an armed attack is used in such a way that it becomes tantamount in effect to an armed attack."

One area that may not constitute an armed attack is espionage conducted through unauthorized computer access into government networks. The author explains that when a state intrudes, without authority, into another state's computer systems, it is very likely engaging in acts that are unlawful under the domestic law of the territorial state. However, under international law, the intruding state may be conducting lawful acts of espionage that may be not be considered a use of force in violation of Article 2(4) of the Charter. The author carefully explains that espionage conducted by the nonconsensual penetration of another state's computer systems is lawful under existing international law when it does not violate systems so vital that their incapacity or destruction would have a critical destabilizing effect on the national security of a state. Executive Order 13010 lists eight commercial and non-commercial infrastructures that fall within this critical category for the United States.

Part IV of the volume provides important core principles that must be understood by every international law practitioner con-

cerned with information technology. Central to this discussion is the thesis that what constitutes a prohibited threat or use of force in cyberspace and elsewhere is a question of fact, which must be subjectively analyzed in each and every case in the context of all relevant law and precedent. The discussion of these core precepts includes a very thorough and reflective compilation of Charter and customary principles in the context of information technology.

This volume leaves for another day the juxtaposition of rights of international satellite contractors and states whose vital national interests may be affected by their ability or lack of ability to control information flow through these satellite links. This is critically important to military planners because nearly all communications between national leaders and their forces in the field are transmitted through these or similar satellite nodes. Nevertheless, the principled discussion within this volume concerning how to determine whether, and when, a vital national interest has been breached through information technology has significantly advanced the debate in this critical area. This volume is a welcome addition to the literature and will be considered a valued resource of every serious international practitioner.