SSI STRATEGIC STUDIES INSTITUTE

Executive Summary

Strategic Studies Institute and U.S. Army War College Press

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH—WISDOM

CONFIDENCE-BUILDING IN CYBERSPACE: A COMPARISON OF TERRITORIAL AND WEAPONS-BASED REGIMES

Mary Manjikian

This paper examines two historic examples of the development of confidence-building measures (CBMs) in order to make recommendations regarding the development of CBMs for cyberspace. The first study looks at CBMs aimed at preventing the escalation of conflict in contested territories such as the Indo-Pakistan border. The second study looks at the development of a chemical weapons ban following World War I and the establishment of reporting and monitoring procedures to stem the proliferation of chemical weapons. Both cases offer lessons for cyber-based CBMs: One can borrow from territorial CBMs in order to establish a secure environment, or from weapons-based CBMs in order to shape the development of new cyber technologies and prevent their proliferation.

As this analysis shows, the development of confidence-building measures for the purposes of reducing cyber conflict is challenging. Because technology in the field of cyber warfare is advancing rapidly and in unpredictable ways, it is difficult to predict what sorts of issues might arise in the future or what sorts of measures might ultimately offer the most utility in terms of stemming conflict. However, it is clear that, at the moment, there are certain elements in the field of cyber warfare that are lacking and that need to be created and addressed prior to going forward.

First, the U.S. Government needs to take a leading role in starting a conversation about the ethics of cyber warfare and cyber weapons. Such a conversation needs to include practitioners, ethicists, and academics, as well as military personnel. Practitioners in particular need to be encouraged to think about their own statement of purpose, or what it means to be an individual or a community engaged in the production of new research in this field. Grants could be provided for the writing and production of textbooks in this area, and universities could be encouraged to include conversations about cyber ethics in introductory and graduate-level engineering and computer science courses.

Next, progress will not be made in the development of cyber confidence-building measures without the active and prolonged engagement of practitioners from academic and the private sector, as well as government. The issues are too complex for traditional government administrators ever to master satisfactorily on their own, and progress is advancing too rapidly for anyone but a specialist to keep up.

Finally, the U.S. Government, including the military, needs to decide consciously how committed they are to the principle of transparency and information sharing in this vitally important defense sector. Decisions regarding what information will be shared in the future need to be made with a full awareness of both the costs and benefits of agreeing to transparency.

*****

the following statement: "Reprinted with permission of the Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College."


This Publication


SSI Website


USAWC Website