SSI
STRATEGIC STUDIES INSTITUTE

Executive Summary

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

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

DETERRING CYBERTRESPASS AND SECURING CYBERSPACE: LESSONS FROM UNITED STATES BORDER CONTROL STRATEGIES

Mary Manjikian

In recent years, analysts have begun discussing strategies for securing entities in cyberspace—including the files and software belonging to corporations, government institutions, and private individuals. Increasingly, analysts have suggested utilizing two types of deterrence strategies: deterrence by denial and deterrence by punishment. In determining how both deterrence strategies might be applied to preventing hostile individuals, states, and nonstate actors from entering cyberspace and inflicting damage there, analysts have borrowed from deterrence strategies that have been framed for a variety of other situations. While the tendency among members of the military community is to look to other military situations—such as nuclear war, or the use of biological or chemical weapons—in which deterrence strategies may have been used, it is my contention that these scenarios are not necessarily the best fit for describing what happens in cyberspace. Rather, my intent in this Letort Paper is to look at other literature that refers to deterrence strategies—namely, criminology literature, which looks at strategies and tactics for deterring illegal immigration.

In the first section of this Letort Paper, three possible strategies for responding to criminal behavior as presented in the criminology literature are described, including: prevention by design; deterrence by denial; and deterrence by punishment. Moreover, this Letort Paper suggests that cyber-deterrent strategies are more properly categorized as prevention by design strategies rather than deterrence by denial strategies, and the difference between the two is explained.

The second section points to existing problems of applying the theories regarding nuclear deterrence to the cyberconflict situation—focusing in particular on the knowledge problem (the problem of attribution) and the temporal problem (the ways in which time functions in cyberspace), both of which are spelled out in greater detail in that section.

The third section explains what can be learned from the criminology example of providing border security. In the border security case, we are able to see how different types of would-be aggressors are approached differently, how targeted strategies are created, and how border security is an issue that needs to be handled in association with related issues, including economic ones. Then, the section examines the ways in which the United States has been able to work with its neighbors in creating border security.

Finally, the concluding section of this Letort Paper draws on the border security example to develop lessons for the provision of cybersecurity.

*****

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute's homepage at *www.StrategicStudiesInstitute.army.mil.*

*****

This Publication

SSI Website

USAWC Website