10-17-2003

Trends. Non-Physical Approaches to Physical Security

IBPP Editor
bloomr@erau.edu

Follow this and additional works at: https://commons.erau.edu/ibpp

Part of the Defense and Security Studies Commons, Other Political Science Commons, Other Psychology Commons, Peace and Conflict Studies Commons, and the Terrorism Studies Commons

Recommended Citation
Available at: https://commons.erau.edu/ibpp/vol15/iss7/5

This Trends is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in International Bulletin of Political Psychology by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.
Abstract: This Trends article discusses the vulnerabilities of protecting physical assets with purely physical means, as well as the potential benefits of non-physical approaches.

The most common response to protecting physical assets is to set up static physical protection. Most often this entails the construction of a physical system that might include fences that vary in thickness, constituent material, permeability, height, depth below ground, flexibility, mobility, and distance from what truly needs to be protected. Added to fences may be technology-based remote sensors, proximal and distal trenches, stone and cement blocks, and yet other barriers. In a figurative sense, human protectors also may be considered as static physical protection.

One problem with a physical protection approach is running the risk of developing a Maginot Line that can be flown over or that can remain vulnerable to mortars, missiles and the like that also would fly over physical protection. Physical protection also can be destroyed via explosives and ammunition as well as cut into or pierced with yet other physical tools.

In contrast, a non-physical approach alone or in conjunction with a physical approach presents an interesting alternative or adjunct. A prototype could be modeled on a neighborhood watch program. Employees and other individuals authorized to be proximal to an area deemed worthy of protection would be trained and appropriately motivated to recognize, report, and effect yet other rules of engagement concerning anomalies. These anomalies could include unknown people in or proximal to the area, known people engaged in unwarranted activity, unauthorized equipment and other materiel in or proximal to the area, and anything else deemed to pose a potentially significant threat.

Certainly it’s the case that human constituents of the neighborhood watch can be subverted, can be covert adversarial operatives, or can be murdered, injured, or threatened. However, human resource management activities, counterintelligence programs, and other security programs can help minimize such vulnerabilities. Moreover, immediately after on-the-job murder and intentional injury, the element of surprise becomes attenuated as the neighborhood watch system is activated. And, in addition, it’s much more difficult to deconstruct or destroy a social psychological phenomenon such as a neighborhood watch system than merely some of the people constituting it.