The Psychology of Intelligent Video Analysis

Editor

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

Part of the Defense and Security Studies Commons, International Relations Commons, Other Computer Sciences Commons, Other Political Science Commons, Other Psychology Commons, Peace and Conflict Studies Commons, Social Psychology Commons, and the Terrorism Studies Commons

Recommended Citation
Available at: https://commons.erau.edu/ibpp/vol15/iss6/5

This Article 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.
Title: The Psychology of Intelligent Video Analysis
Author: Editor
Volume: 15
Issue: 6
Date: 2003-10-03
Keywords: Intelligence Analysis, Security, Software, Terrorism

Abstract: This article examines issues surrounding software-enhanced video analysis in an intelligence context.

One of many products marketed to confront a post-9/11 terrorism challenge—a challenge that has morphed into an attempt to foster a world of security in a world of insecurity—is that of the combination of behavior-recognition software and intelligent video analysis. Most often the combination is hooked into a closed-circuit television system and will identify a putative security threat based on the detection of specific behaviors that are presumed to be indicators of threat.

A common set of behavioral indicators of security threat are an individual running who should be walking, lurking who should not be lurking—perhaps merely going about some business—and seeming erratic who should be no such thing. There are significant problems with such indicators. One is that the indicators are premised on acting in a statistically deviant fashion from people who are in the area. Another is the premise of acting in a statistically deviant fashion from how people should act in the immediate area—even if there are no other people in the area. Still another is the nature of some behaviors—e.g., lurking—that only can be simplistically constrained by another set of definitional behaviors or subjectively intuited. Yet another is that a tried-and-true modus operandi of security violators seeking to act as much as possible like people who are not security violators would seem to immediately invalidate the subjective basis of the objective security technology to be installed and employed.