Chapter 10
Surveillance Communities of Practice:
Supporting Aspects of Information Assurance for Safeguards and Compliance Monitoring

Peter Goldschmidt
The University of Western Australia, Australia

ABSTRACT

This discussion focuses primarily on supporting communities of practice tasked with compliance monitoring in complex environments. Here, the decision makers, as members of the surveillance community of practice, may be confronted with rapidly changing information, and the solution or solutions may be required rapidly at a low cost. In these cases, fully automated monitoring or surveillance systems are limited in their utility because of dynamic contexts and temporal and spatial variations. Managing these limitations typically requires human judgement to assess the results of these monitoring systems. Other reasons for requiring human judgement include a need for the surveillance results to be verified and assured with substantiating evidence, and the delegation of control and responsibility when actioning remedial responses to generated alerts and alarms. Surveillance Information Systems performance depends on reducing the decision time for remedial action by verifying alarms and generating actionable indicators, in context. This chapter discusses support and assurance of surveillance monitoring and compliance verification knowledge management of surveillance results. The aim is to support information assurance real time alarm identification and verification, assurance and management decision making by tracking the parameters monitored by the existing information assurance monitoring infrastructure and operating work systems, and using that data/knowledge to create useful and actionable information. The goal is to reduce the (information assurance remedial action) time to decision to enable accurate and rapid operational execution.

DOI: 10.4018/978-1-4666-0197-0.ch010

INTRODUCTION

Work systems (Alter 2006) supporting communities of practice tasked with assessing the results of surveillance operations typically use a matching process by which some predetermined conditions are compared with observed events or event related information. If an unacceptable variance is detected this is usually followed by the generation of an alert or alarm highlighting the variance. The alarm is presented to an evaluating agent in order to determine the alarm context and validity and to recommend one or more remedial actions to reduce the variance. For surveillance in complex environment such as defence, the financial markets, national security, medical and public health monitoring and critical industrial processes, the evaluating agent need to be human. The goal is to be, as practically as possible, informed as to what is happening as opposed to knowing what has happened.

BACKGROUND

Typical monitoring operations align with (Boyd 1976) the Observe, Orient, Decide, Act (OODA) construct. The primary monitoring process, the matching component, fulfils the Observe function and in some cases may also include the Orient function, whereby the context in which the variance occurred is also taken into account. If not, then the human agent fulfils this function when assessing the variance. There may also be a temporal issue when assessing the context, as this may change over time for any given variance. Based on this assessment, a Decision is then made to Act in order to remedy the observed variance. The aim of a surveillance operations decision support work system is to reduce the time between the Decide and Act components, with assurance that the underlying evidence supporting the variance is sound.

Broadly, five problem areas drive this necessity to assure and verify the alarm:

1. The quality of the data/information being monitored and the quality of the primary monitoring process;
2. The potential biases inherent in the evaluating agent's analysis of the variance and the supporting or refuting evidence;
3. The combination of the alarm and contextual or environmental evidence;
4. The accountability and transparency of the verification and assurance process, and
5. The accuracy and efficacy of the remedial action.

Current Issues Relating to Surveillance Monitoring

Ubiquitous intelligence and pervasive computing (combined with the new management paradigm described by Gabriel (2003), where the old iron cage of management command and control has now been replaced by a flexible glass cage of transparency, accountability, flexibility and the continuous monitoring of human activities, often in real-time) calls for a need to further research electronic data monitoring and practice, including monitoring of societies. These may be the workplace society, the society in general or the surveillance communities of practice who are tasked with this activity. These societies are generally interlinked and cannot readily be seen as mutually exclusive as they may all, at some point, be monitored, assessed and be subject to remedial actions. Gabriel points out that this glass cage work environment has led to a degree of employee alienation and distrust of the accompanying monitoring. Combined with Bohn's et al. (2004), observations that the "new monitoring techniques extend far beyond credit-card checks, call-logs and postings. Not only will the spatial scope of such monitoring activities be significantly extended in ambient-intelligence landscapes, but