: Can surveillance data mislead decision-makers?

by Daniel J. Power

Editor, DSSResources.com

Data from electronic surveillance devices may be falsified or inaccurate. The presumption can be that it is accurate, but the data should be examined for anomalies and implausible values. Gaps, time-stamping problems, and "white noise" should be examined closely. Surveillance refers to close observation and data gathering relevant to the behavior of a person or group. Various methods can be used to obtain data and information, to establish connections among people, and to establish a person's location. Surveillance involves monitoring activities of people, places, or objects. Video cameras, mobile phones, and microphones can be used for covert surveillance. Also, these electronic surveillance devices can capture and then store huge quantities of data. All surveillance data is not necessarily accurate and some data might actually be misleading.

Counter-surveillance devices can help one recognize that surveillance is occurring and also help develop suitable countermeasures. The use of electronic counter-measures can add noise and erroneous data to both passive and active data capture and hence data analysis becomes more complex. For example, a handheld radio spectrum analyzer helps detect electronic surveillance devices. Awareness of surveillance helps one deploy and use simple and complex counter-measures to limit or distort data gathering. Surveillance can be either active or passive. Active surveillance is especially prone to manipulation and intentional distortion.

Machine-generated surveillance data from sensors, video, audio, etc. seem inherently factual, but the possibility of tampering should not be ignored. Technologists should always ask "how can one improve a surveillance system?" The security of the data must be assured and managers must realize that a visual assessment can be misleading. A visual assessment is a direct evaluation of an event, a physical object, or an animate being like a person. Also, sometimes systematic distortional bias occurs in visual assessment and data analysis. Pre-decisional information distortion can create a form of self-fulfilling prophecy in which a decision-maker is prone to choose or see what was initially preferred or perceived without evidence.

On TV shows like Leverage, the "good guys" and the "bad guys" hack surveillance cameras and alter what is recorded. Since 2000, many movies have had surveillance as a major or minor part of the story. Castiglione et al. (2011) assert visual data can be "maliciously manipulated in order to either hide and/or introduce fake evidence (p. 246)." Photos are altered. Videos are edited. So we can't believe everything we see even when it appears to be real-time action.

: Can surveillance data mislead decision-makers?

Data may be altered or deleted both intentionally and unintentionally. The reality is that it may be difficult to know how, when, and by whom the data alteration occurred. Altered or missing data can have a major impact on the "facts". Electronic surveillance data can mislead analysts. Too often the presumption is that surveillance data is accurate and unbiased. Check the data source and check the reasonableness of the data. Check to ensure the data is 1) complete, 2) accurate and error-free, and 3) consistent.

Any source for data can be tampered with and mislead decision-makers. The distributed, remote nature of surveillance data makes such data especially susceptible to tampering. Managers should be skeptical of all data sources, but especially those that are hard to secure and monitor. Source security is an ongoing problem, cf., Xavier (2018).

Data integrity is essential. The goal of a data integrity process should be the maintenance and assurance of data accuracy and consistency over the entire data life-cycle. Procedures and software to maintain data integrity ensures the "raw" data is recoverable and searchable. Keeping logs ensures traceability of storage transfers and data transformations and changes. Protecting the validity and accuracy of data is important.

Surveillance refers to any ongoing, systematic collection, analysis, interpretation, and dissemination of data for control, diagnostic, or decision making purposes. Finding facts for decision making requires both high-quality data and meaningful analyses. We seek facts to make better predictions and hence to enhance decision making quality and timeliness.

References and Resources

Bhanot, P., "The Three Key Requirements to Achieve Data Integrity," Blazent, April 27, 2017 at URL https://www.blazent.com/three-key-requirements-achieve-data-integrity/

Castiglione, A., A. De Santis, and F. Palmieri, "Ensuring Privacy and Confidentiality in Digital Video Surveillance Systems," in G. O.M. Yee **Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards: Aspects and Standards," (Chapter 10) IGI Global, 2011.**

HEAT (Hostile Environment Awareness Training) at URL https://www.ultimate-survival-training.com/counter-surveillance-and-anti-surveillance/

Miller, C., "The False Promise of the Surveillance State," The American Interest, March 30, 2020 at URL https://www.the-american-interest.com/2020/03/30/the-false-promise-of-the-surveillance-state/

RF Explorer — Handheld RF Spectrum Analyzer at URL http://rfexplorer.com/models/

Xavier, K., "3 Ways to Hack CCTV Cameras (and How to Prevent It from Happening to You)," Verkada, Nov. 09, 2018 at URL https://www.verkada.com/blog/3-ways-to-hack-a-cctv-camera/

Author: Daniel Power
Last update: 2020-06-16 02:42