PRACTITIONER

What warning indicators would you expect leading up to the scenario?

What are the sources of that type of information?
Would you expect to receive information from these sources notwithstanding that you know from experience they are likely to have information you might be able to use? If not, why not?

What level of details would you want from the sources of data or the alerts?

a) Do you need routine access to steady state information along with alerts of anomalies?
b) Is the response to "a)" above dependent on which agency you are to receive the info from? If yes, why? (lack of trust as to ability to provide 'good' info?)

Are the organizations that monitor alerts providing appropriate information (details, timeliness, etc.) on threat/attack activity?

How do you evaluate the warning indicators you have given the diversity of threats?
Would your answer differ if you had better or different technical capabilities vs human interaction/intervention?

How do these indicators differ across attack types?
In the NY Times Square scenario, could technology (e.g., could CCTV cameras be built with algorithms that could have detected the anomoly spotted by the sidewalk vendor?), or, can technology replace an individual's 'gut feel'?

How do you separate the nuisance attacks for the serious threats?
How do you firstly determine if something is a 'nuisance' vs a serious threat in today's "I must examine everything' world?

What additional information do you need that you don't have today?

What potential other new indicators are there?

What new sensors are needed in cyberspace to trigger alerts?
And if those sensors existed would they too become 'white noise' indistinguishable from what we have today?

Are the visualization tools of activity and alerts adequate for human understanding of network activity?

Is pre-defined computer processing of routine attacks without a human in the loop acceptable?

What routine cyber event analysis is performed by humans that could be done automatically by a computer?

Do you have confidence in the threat models?
Is the term 'threat model' outmoded, overused, underused, or used inappropriately? Is there a better term?

Do the threat models provide you enough information or do you need more details, i.e. actual data, detailed logic for each decision, etc.?

What access do you need for historic data, i.e. 1 hour, 1 day, 1 week, etc.?
Does the answer to this question depend on the kind of threat? And whether it is immediate or pre/post event?

Is it essential that people who design tools for your use have current or prior experience as a practitioner?
(Consider the analogy of a Warrant Officer in the Army who was prior enlisted - and usually receive much more respect from the 'troops' than an officer right out of a Military Academy.)