Sensemaking and knowledge creation in early warning detection

Detection and decision in early warning

Chun Wei Choo
Faculty of Information
University of Toronto

1

Early warning

We define early warning as the process of gathering, sharing, and analyzing information in order to identify a threat or hazard sufficiently in advance for preventive action to be initiated.

An early warning *system* is a network of actors, resources, technologies, practices, and organizational structures that monitors the environment for the purpose of detecting and controlling threats.

2

EARLY WARNING SYSTEMS - EXAMPLES	
ProMED-mail Program for Monitoring Emerging Diseases	International Society for Infectious Diseases
GOARN Global Outbreak and Alert Response Network	World Health Organization Epidemic and Pandemic Alert and Response
GIEWS Global Information and Early Warning System	Food and Agriculture Organization of the UN
HEWS Humanitarian Early Warning Service	Inter-Agency Standing Committee World Food Programme, UNICEF
ReliefWeb	UN Office for the Coordination of Humanitarian Affairs (OCHA)
FEWER Forum on Early Warning and Early Response	Non Governmental Organization FEWER-Africa, -Eurasia, -Russia
Pacific Tsunami Warning System	Intergovernmental Oceanographic Commission, UNESCO
EWS Models of Financial Crises	International Monetary Fund, World Bank
Strategic Intelligence Strategic Early Warning	Competitive Intelligence team, Scenario Planning group Shell International
RAHS Risk Assessment & Horizon Scanning Singapore	National Security Coordination Centre Singapore

All early warning systems share the basic goal of detecting and warning about an imminent threat so that the warning can be acted on in time by responsible agencies.

We introduce a theoretical analysis of how the seeking and use of information may affect:

1. **DETECTION ACCURACY**
   an early warning system's ability to form an accurate perception of a possible threat;

2. **DECISION SENSITIVITY**
   the system's decision to recognize and act on a perception of possible threat.

4

Agenda

- Lens Model (Brunswik) and its extensions to social judgment – Cognitive Continuum Theory (Hammond 1996)
- Signal Detection Theory (Swets 2000)

5

Brunswik Lens Model

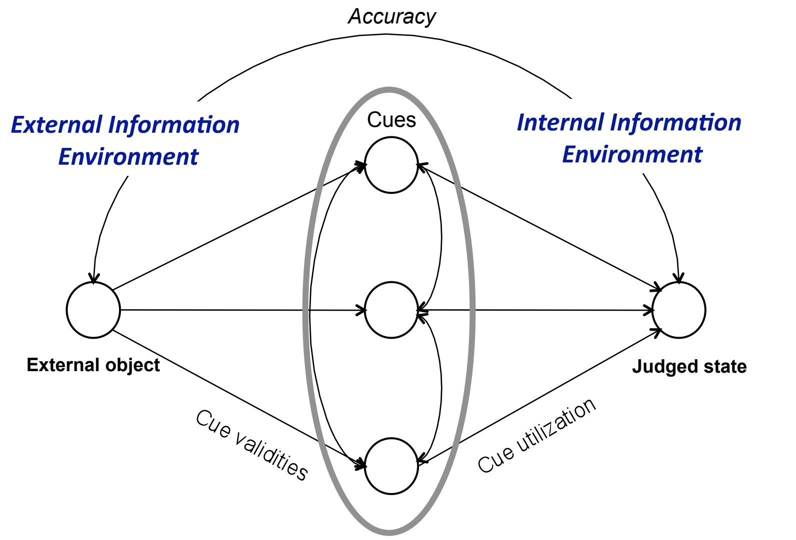
Brunswik (1903-1955) viewed perception as an inferential process.

Objects in the environment can only be perceived indirectly through available information that has been sensed by the individual.

An organism or system is represented as a lens that collects information from the many cues generated and scattered by an external object, and refocuses them like rays of light on to a perception or judgment of the object.

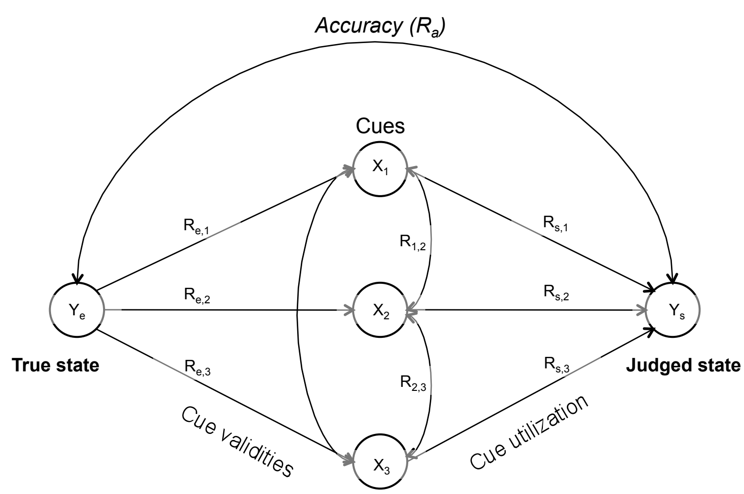
6

Brunswik Lens Model



7

Brunswik Lens Model



$$r_a = GR_e R_s + C\sqrt{1-R_e^2}\sqrt{1-R_s^2}$$

8

Cognitive Continuum Theory

developed by Hammond (1996, 2000) as an extension of the Lens Model

CCT examines the modes of **cognition** or information processing as they relate to the information requirements of the **tasks** that are to be accomplished.

CCT is a framework in which different types of information processing and different types of task can be profiled and evaluated in terms of their effect on task performance.

9

CCT: Cognitive Continuum (Hammond, Cooksey 1996)

Intuitive mode	***Quasi-rational mode***	***Analytical mode***
Rapid information processing	Involves aspects of both poles of the continuum. QR may be more or less intuitive or analytical depending on the relative mix of intuitive and analytical characteristics demanded by the information environment.	Slow information processing
Simultaneous cue use		Sequential cue use
Formal rules unavailable		Formal rules available and used
Reliance on nonverbal cues		Reliance on quantitative cues
Raw data stored in memory		Complex organizing principles stored in memory
Cues evaluated perceptually		Cues evaluated at measurement level
Vicarious functioning (exploit cue redundancy)		Vicarious functioning unnecessary due to use of organizing principle
Organizing principles of pattern recognition, averaging		Task specific organizing principles

10

CCT: Task Continuum (Hammond, Cooksey 1996)

Inducing Intuition	***Inducing Quasi-rationality***	***Inducing Analysis***
Task structure complexity: Large number of simultaneous cues; High redundancy among cues	Tasks which induce QR will show a mixture of intuition-inducing as well as analysis-inducing elements. Relative balance in the mixture will predict the pole toward which cognition will move.	***Task structure complexity:*** Small number of sequential cues; Low redundancy among cues
Task content ambiguity: Organizing principle unavailable; Unfamiliar task content; High accuracy unlikely		***Task content ambiguity:*** Organizing principle readily available; Highly familiar task content; High accuracy likely
Task presentation: A posteriori task and cognitive decomposition; Nonverbal, perceptual cues		***Task presentation:*** A priori task and cognitive decomposition; Quantitative, measured cues

11

P1 (threat information environment)

The extent of knowledge and information available about the threat determine the structure, complexity, and information needs of the detection task. These properties together define the threat information environment (TIE).

Different threat information environments require different modes of information processing.

12

P2 (information use environment)

Early warning systems employ a range of information processing strategies to detect threats. Different strategies emphasize analytical, intuitive, or quasi-rational modes of information processing.

The mix of information processing approaches characterize the information use environment (IUE) of the early warning system.

13

P3 (congruence)

The greater the congruence between the balance of requirements presented by the threat information environment and the balance of information processing strategies utilized in the early warning system, the greater the accuracy of the threat detection task.

14

Signal Detection Theory

- A model for analyzing the performance of a system that has to separate signal accurately from background noise
- Measures the ‘discrimination performance’ of a system judging whether or not a piece of information is evidence of a ‘signal’ or merely ‘noise’
- SDT separates the analysis of judgment policies into an information-knowledge component (accuracy) and a value component (decision criteria)

Green and Swets 1966. Swets, Dawes, Monahan 2000.

15

Signal Detection Theory

Signal detection in EW is difficult because the information available is always ambiguous:
cues that are true indicators of a threat (signal) are intermingled with cues that are generated by chance (noise).

2 kinds of decision errors:
saying that a threat exists when it does not, and
failing to see a threat that does exist.

SDT can help us analyze the detection/decision process in early warning systems.

Green and Swets 1966. Swets, Dawes, Monahan 2000.

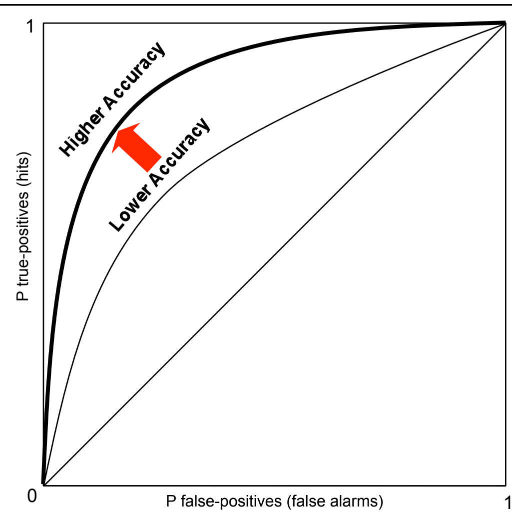
16

	No Threat	*Threat*
Warning	**False positive** (false alarm)	**True Positive** (hit)
No Warning	**True Negative** (all clear)	**False Negative** (miss)

↑ **Decision threshold**: How much evidence is needed? ↓

17

Signal Detection Theory



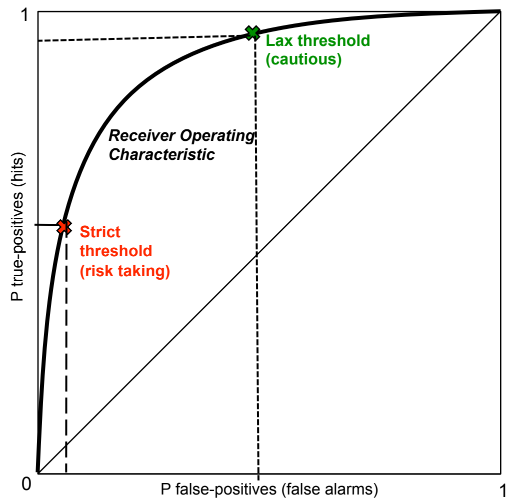
Swets (2000)

Performance curve depends on our state of knowledge and information about the threat.

The better our knowledge, the more convex the curve, the greater our accuracy and sensitivity.

18

Signal Detection Theory



Swets (2000)

Curve describes performance of our system. True-positives and false-positives vary together: if we want more hits we have to accept more false alarms.

Organization sets a **decision threshold** that may be lax, strict, or moderate.
At Lax Threshold, we say yes often – we would not require very strong evidence to say yes.

At Strict Threshold, we say yes rarely – we demand strong evidence.

19

P4 (system sensitivity)

Different early warning systems are characterized by their sensitivities or receptiveness to evidence. Sensitivity depends on the decision threshold that is explicitly or implicitly adopted by the system to weigh the strength of evidence needed to recognize a threat.

20

P5 (decision outcomes)

Setting a decision threshold in an EWS always requires a compromise between increasing the probability of a true-positive (hit) and increasing the probability of a false-positive (false alarm).

Thus setting a lax, cautious threshold increases hits but also increases false alarms;
setting a strict, risky threshold reduces false alarms but also reduces hits.

21

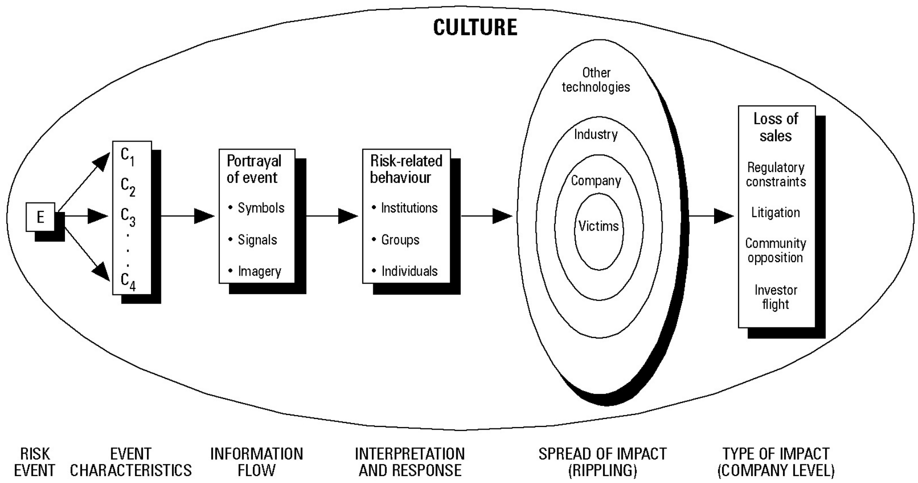
P6 (decision threshold)
The decision threshold is influenced by many complex factors, including:

•The public's perception of the risk posed by the threat

•Policy makers' cost-benefit analysis associated with misses and false alarms

22

Social Amplification of Risk



Source: After Kasperson *et al.* (1988)

23

Precautionary Principle

"When an activity raises threats of harm to the environment or human health, precautionary measures should be taken even if some cause and effect relationships are not established scientifically."

(The Lancet, 2000)

24

Summary (1)

In Lens Model/CCT, we focused on **perceptual accuracy**.

Accuracy is improved when there is congruence between the threat information environment and the information use environment of the system monitoring the threat.

Both environments may be analyzed as a blend of factors that induce or involve cognitive (rule-based) and intuitive (pattern-based) information processing.

Summary (2)

In SDT, we focused on **detection sensitivity**.

Sensitivity or receptivity depends on the decision threshold that is adopted regarding the amount and strength of evidence that is needed in order to conclude that there is a threat.

For a given EWS, the setting of the decision threshold always involves a trade-off between the error of failing to raise the alarm and the error of raising a false alarm.

Performance of an early warning system =
f {perceptual accuracy + decision sensitivity}

P1-P3: Perceptual Accuracy

Develop threat information profiles of a number of hazards in different domains.

Identify major early warning systems that target each type of hazard.

Identify information gathering and information processing strategies adopted by each system.

Compare the balance of threat information attributes with the balance of information strategies. Assess the overall "congruence" as predicted by theory. Relate to the historical/reputational accuracy of each warning system.

P4-P6: Decision Sensitivity

Study a number of EWS and identify the warning or decision threshold adopted. Determine if decision thresholds vary significantly between systems.

Examine the rationales (both the espoused theory and the in-use theory) used to justify decision thresholds.

Examine how the risks and costs of false alarms or misses are analyzed and talked about in each system.

Analyze how the social perception and social discourse of the risk of a hazard influence the decision threshold.