Information Use and Early Warning Effectiveness: Perspectives and Prospects

Chun Wei Choo
*Faculty of Information, University of Toronto, 140 St. George Street, Toronto, Ontario,
Canada M5S 3G6. E-mail: cw.choo@utoronto.ca*

This introductory article explores how the use of information affects the effectiveness of early warning systems. By effectiveness, we refer to the capacity of the system to detect and decide on the existence of a threat. There are two aspects to effectiveness: (a) being able to see the evidence that is indicative of a threat and (b) making the decision, based on the weight of the evidence, to warn that the threat exists. In early warning, information use is encumbered by cues that are fallible and equivocal. Cues that are true indicators of a threat are obscured in a cloud of events generated by chance. Moreover, policy makers face the difficult decision of whether to issue a warning based on the information received. Because the information is rarely complete or conclusive, such decisions have to consider the consequences of failing to warn or giving a false warning. We draw on sociocognitive theories of perception and judgment to analyze these two aspects of early warning: *detection accuracy* (How well does perception correspond to reality?) and *decision sensitivity* (How much evidence is needed to activate warning?) Using cognitive continuum theory, we examine how detection accuracy depends on the fit between the *information needs profile* of the threat and the *information use environment* of the warning system. Applying signal detection theory, we investigate how decision sensitivity depends on the assessment and balancing of the *risks of misses and false alarms* inherent in all early warning decision making.

Early Warning Systems

With growing populations and expanding infrastructures, our exposure to natural and man-made hazards has increased dramatically. Although disasters often appear to happen suddenly with little or no prior warning, in fact, most disasters incubate over long gestation periods during which warning events accumulate. While these warning signals become painfully clear in hindsight, why is it so hard to detect, recognize, and act on these precursor conditions before they tailspin into tragedy? This introductory article explores two possible reasons. First, in early warning, it is difficult to discern signals about a real threat from random noise. Second, even when signals are detected, policy makers have to weigh the costs and consequences of possible false alarms and misses in deciding whether to activate warning. We contextualize these issues in a broader discussion of the social construction of risk and its consequences on policy and risk management.

Matveeva (2006) traced the origin of "early warning systems" to disaster preparedness, where the systematic collection of information was expected to shed light on the causes of natural disasters, and to the gathering of military intelligence. In the 1950s, a link was made between efforts to forecast environmental disasters and attempts to foresee political crises. The 1960s to 1970s saw investments in information technology and statistical analysis as governments funded projects that coded and analyzed event data, and constructed conceptual models of political conflicts. Throughout the 1990s, local and international practitioner organizations became interested in using early warning information and analysis to guide their planning and programming. The warning systems that were developed initially relied on information from open sources (e.g., news reports, statistical sources), but later sought to understand the complexities of local situations and histories to connect early warning to specific preventive measures for target groups. In December 2004, the Pacific tsunami focused international attention on questions of early warning and preparedness, and led to a call by the United Nations (UN) Secretary General for a global warning system that would cover all hazards with no country left out. This was followed by an international survey of early warning systems that identified gaps and opportunities, and served as a basis for developing global capacities (UN ISDR, 2006).

Early warning systems today monitor a broad spectrum of hazards. A typology created at the UN divides hazards into natural or man-made (Peduzzi, 2004). Natural hazards are classified as climatic (e.g., cyclones, droughts, floods) and tectonic (e.g., earthquakes, tsunamis, volcanic eruptions). Man-made hazard categories include agriculture and unsustainable resource management (e.g., deforestation,

Received November 14, 2008; revised December 29, 2008; accepted December 31, 2008

© 2009 ASIS&T • Published online 9 February 2009 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/asi.21038

TABLE 1. Early warning systems: Examples.

Early warning system	Coordinating organization
ProMED-mail Program for Monitoring Emerging Diseases	International Society for Infectious Diseases
GPHIN Global Public Health Intelligence Network	Public Health Agency Canada
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)
Conflict Prevention Centre	Organization for Security and Co-operation in Europe
FAST International (1998–2008) (Fruhanalyse von Spannungen und Tatsachenermittlung)	International development agencies Swisspeace
International Flood Initiative	International Center for Water Hazard and Risk Management World Meteorological Organization, UNESCO
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/Scenario Planning groups Shell International
RAHS Risk Assessment & Horizon Scanning Singapore	National Security Coordination Centre Government of Singapore

overfishing, pest invasion), energy production (e.g., nuclear accidents), industry (e.g., chemical release, industrial waste), transport (e.g., oil spills), and war. In addition, there are major early warning systems directed at financial crises (e.g., the work by the International Monetary Fund on detecting currency crises); political conflict and humanitarian disasters (e.g., the Forum on Early Warning and Early Response in Africa, Eurasia); public health and epidemic-prone diseases [e.g., Epidemic and Pandemic Alert and Response program of the World Health Organization (WHO)]. Table 1 lists examples of early warning systems.

In 2000, the UN created the International Strategy for Disaster Reduction (ISDR) secretariat as the focal point and information clearinghouse for disaster reduction activities in the UN system (Basher, 2006). Within the ISDR, the Platform for the Promotion of Early Warning (PPEW), the unit that advocates for better early warning systems and disseminates best practices, identified four key elements of early warning systems (see Table 2).

Effective early warning systems need to forge strong information and coordination linkages across all four elements, and this almost always requires the participation of many individuals and groups. Thus, PPEW recognized eight main actors in creating and implementing effective early warning systems: communities, local governments, national governments, regional institutions and organizations, international bodies, nongovernmental organizations, the private sector, and the science and academic community. Matveeva (2006) emphasized the role and contribution of civil society and nongovernmental organizations in both early warning and early response when they, for example, mobilize international support or design local interventions. The UN's efforts in early warning are mainly concerned with systems that enable individuals and communities threatened by natural hazards to act in time to avoid or reduce harm and injury. The UN ISDR (2006) definition of early warning reflects this priority: "the provision of timely and effective information, through identified institutions, that allows individuals exposed to a hazard to take action to avoid or reduce their risk and prepare for effective response" (p. 2).

We focus on early warning as the process of gathering, sharing, and analyzing information to identify a threat or hazard sufficiently in advance for preventive action to be initiated. An early warning *system* is then a network of actors, practices, resources, and technologies that has the common goal of detecting and warning about an imminent threat so that preventive measures can be taken to control the threat or mitigate its harmful effects. The underlying assumption is that threats develop over incubation periods during which warning signals may be discerned, tracked, and assessed (Choo, 2005, 2008). Because many threats can have a global impact, early warning systems today tend to be distributed, multilevel, and collaborative, and may be supported by a coordinating agency or a central clearinghouse.

The objectives of this article are to examine how the seeking and use of information affects an early warning system's

DOI: 10.1002/asi

TABLE 2. Four elements of early warning systems (adapted from Basher 2006, figure 2, p. 2170).

Risk knowledge	Knowledge of the relevant hazards, and of the vulnerabilities of people and society to hazards
Monitoring and warning service	A technical capacity to monitor hazard precursors, to forecast the hazard evolution, and to issue warnings
Dissemination and communication	The dissemination of understandable warnings, and prior preparedness information, to those at risk
Response capability	Knowledge, plans, and capacities for timely and appropriate action by authorities and those at risk

ability to (a) form an accurate perception of a possible threat and (b) decide to issue warning based on a perception of possible threat. With reference to the four elements of warning systems in Table 2, we will be looking primarily at the monitoring and warning function that lies at the core of all early warning systems. We begin with a discussion of the research literature. The next section conceptualizes threat detection as a perceptual process by applying the Brunswik Lens Model and Cognitive Continuum Theory (Goldstein, 2004; Hammond, 1996). We then conceptualize detection decisions in early warning using signal detection theory (Green & Swets, 1966; Swets, 2000). The final section summarizes and expands discussion of detection accuracy and decision sensitivity in the early warning context.

Research in Early Warning

The research literature on early warning is dispersed over many disciplinary areas including accounting, agricultural research, banking and finance, climate change, clinical medicine, critical care medicine, clinical psychology, education, engineering, environmental health, food safety and hygiene, geophysics, hospital administration, humanitarian disasters, nursing, natural disaster research, political conflict, seismology, strategic planning, and water safety. In these areas, research clusters around recurrent themes such as the conceptual modeling of threats or hazards in specific domains; identification and evaluation of indicators; measurement and scoring systems; and the description of systems that are in operation or being implemented. The expansive literature precludes a comprehensive review; instead, we consider early warning research that is directed at political conflict and public health hazards.

George and Holl (1997) and Alker, Gurr, and Rupesinghe (2001) highlighted the receptivity to warning of emerging threats as a major problem. They suggested that studies in the perception of audio or visual stimuli could provide useful analogies to approach this problem. These studies have shown that the detection of a signal is not simply a function of its signal-to-noise ratio but also the expectations of the observer as well as the costs and benefits associated with recognizing the signal. Observers may require information that counters existing expectations and policies to meet higher standards of evidence and admissibility. Policy makers may reduce their receptivity to warning to avoid making unpopular decisions.

Schmeidl and Adelman (1998) identified a dilemma in the use of information for early warning. While "information and intelligent analysis" must provide the basis for reasonable intervention, the abundance of information available today raises the questions of how to manage data overload, how to know which sources to trust, and how to triage between "the multitude of crises and multiplicity of analyses and solutions" in decentralized systems. In a similar vein, van Walraven (1998) concluded that the key issue in conflict early warning is not the signal, per se, as there are usually numerous indicators of impending conflict. Rather, the difficulties lie in the perception of information by different observers who bring their own frames and interests to bear on the interpretation of signals.

Davies and Gurr (1998) identified six information sources for conflict early warning: in-country situation studies; screening and analytical coding of public news sources; field reports and analyses from governmental, intergovernmental, and nongovernmental institutions; coded assessments by country experts of current situations and trends; country or group profiles, or databases of structural indicators that provide the basis for long-term risk assessment; and episodic databases profiling past crises. Lundin (2004) contrasted two current approaches to gathering events data for early warning, one using global newsfeeds and the other by surveying experts. Using a global newsfeed requires categorizing and classifying each event according to a coding system and then counting the number of events in a time period for a given country and event class. While this approach can provide a cost-efficient way to obtain near real-time coverage of world-wide events, news-monitoring services may display a cultural bias on what is important and may vary reportage depending on current news trends, making it difficult to compare data over time. When using a survey approach, regional experts answer a constant set of questions at regular intervals. The main advantage here is continuity since the same questions are used regardless of current media trends; however, it may be expensive to retain a network of experts and difficult to compare countries objectively since each expert's judgment is subjective.

Heymann, Rodier, and the WHO Operational Support Team, GOARN (2001) believed that infectious disease intelligence, gleaned through surveillance, would be the best defense against the threat. They described the development of the Global Outbreak Alert and Response Network at the WHO as an initiative that increased early awareness and preparedness, and noted that new information technologies were reducing the traditional reluctance of countries to report outbreaks. Wagner et al. (2001) introduced "extreme timeliness" of disease detection as a new requirement of public health. Using signal detection theory and decision theory, they identified information strategies to achieve more timely detection. These included improving the quality of existing signals through more complete reporting, adding new signals to augment existing data, improving detection algorithms, and tuning the detection system for improved timeliness at the expense of specificity or sensitivity. Woodall (2001), Madoff (2004), and Madoff and Woodall (2005) discussed the Program for Monitoring Emerging Diseases (ProMED-mail), a major Web-based service that disseminates information on emerging infectious diseases collected from media sources, official reports, local observers, and subscriber postings. Knowledgeable moderators screen reports, provide commentary, and add references. The ProMED-mail experience shows that public, interactive reporting of outbreaks can be faster than that of official channels, yet be reliable and responsive to the needs of healthcare providers.

Mazur (2004) searched for information traits that would serve as “hallmarks” to help differentiate true warnings from false alarms. Based on a statistical analysis of a database of public warnings from 1948 to 1971 on products and processes that were thought to pose serious health hazards, Mazur found that true warnings were more likely when the news source was a report of normal scientific research produced at a recognized scientific institution than when the source was a government agent or citizen advocacy group. Warnings from unbiased sources (i.e., sources with no known biases against the producer of the alleged hazard) were more often true than warnings from identifiably prejudicial sources. Warnings that were derived from or linked to popular social issues also were more often false than those that were not.

Mykhalovskiy and Weir (2006) reflected on the Global Public Health Intelligence Network (GPHIN) created by Canada and suggested that

> GPHIN has created an important shift in the relationship of public health and news information. By exiting the pyramid of official reporting, GPHIN has created a new monitoring technique that has disrupted national boundaries of outbreak notification, while creating new possibilities for global outbreak response. (p. 42)

Morse (2007) concluded that although concerns about the spread of infectious diseases have intensified the need for early warning, many gaps remain in the effectiveness of current systems. Even as the adoption of technology is improving information access and dissemination, it also is increasing the need to better understand how information can be managed and utilized to improve the performance of early warning systems.

Threat Detection: Brunswik Lens Model and Cognitive Continuum Theory

The detection of threats is fundamentally a process of indirect perception: An external phenomenon of interest is being perceived indirectly through the recognition of cues and indicators. To conceptualize threat detection, we draw on the cognitive psychology of perception, specifically the *Lens Model* of Brunswik (1952) and its subsequent extension as a theory of social judgment (Hammond, 1996, 2000). These models explain how a person or system uses information in cues that are imperfect and dispersed indicators of a distal, external object to construct a perception of that object (A cue is a feature of something perceived that is used in the interpretation of the perception.) The models are of particular interest because they concentrate on the value of information in cues: To what extent are cues valid indicators of the external object, and to what extent are valid cues utilized in making judgments about the object?

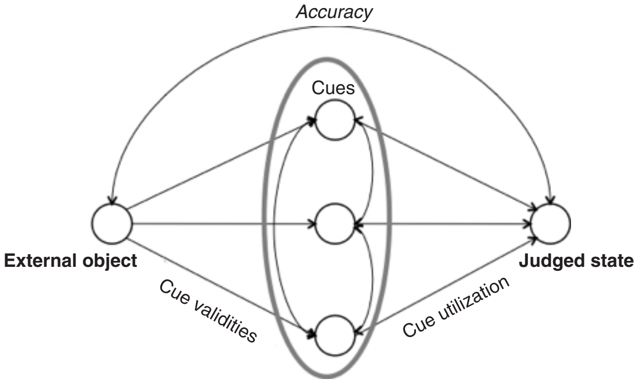

FIG. 1. Brunswik lens model.

Brunswik (1952) viewed perception as an inferential process, where objects in the environment only can be perceived indirectly through available information that has been sensed by the individual. A person 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. In Figure 1, the left side of the model depicts the environment, with its multiple cues (only three are shown) that have varying *cue validity* in indicating the object. The right side represents how these overlapping, fallible cues are weighted and combined by the observer to make a judgment about the object (*cue utilization*). Thus, people infer a percept from a set of cues that are imperfect and unreliable indicators of an external object of interest. The measure of system performance is its *accuracy*, defined as how well the observer’s judgments correspond to the true state of the external object. The model represents an ecological view of information processing where accuracy is the criterion of performance and adaptation.

In the Lens Model, external cues are only probabilistically related to the object of interest. Moreover, cues are also interrelated, as shown by the curved arcs in Figure 1. Varying sets of cues would be available under different environmental conditions: The same cues could indicate different events, and the same event could generate different cues. The environment thus presents cues as entangled and redundant with respect to each other and to the information each gives about the external object (Cooksey, 1996). Systems that have adapted successfully to their environments are sensitive to and can exploit the overlap and redundancy inherent in the multiplicity of cues. For example, observers in the system might make trade-offs between cues when drawing inferences about an external object: High values on some cues could offset, or compensate for, low values on other cues.

TABLE 3. Cognitive continuum of information processing modes (adapted from Cooksey, 1996, p. 15; Hammond, 2000).

Intuitive mode	Quasi-rational mode	Analytical mode
Rapid information processing	Involves aspects of both poles of the continuum. Quasi-rationality 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

The Lens Model refers to this exploitation of cue multiplicity and redundancy to perceive the environment as *vicarious functioning*.

The system perceives cues and combines them into judgments about the external object. There are many methods of combining information in cues. Rules may be used to aggregate, average, or weight cues to predict the external object. When rules are unavailable, people look for patterns in the data or for events that fit a narrative framework derived from past experience. These integrative rules and pattern-matching mechanisms act as *organizing principles* that make sense of the available information. The strategies of vicarious functioning and organizing principles work together to allow an early warning system to combine indicators of varying validity to arrive at a veridical threat assessment.

Cognitive continuum theory (CCT), developed by Hammond (1996, 2000), is an extension of the Lens Model that relates modes of cognition or information processing to the information requirements of the tasks that are to be accomplished. CCT presents a framework in which different modes of information processing and different types of tasks can be profiled and evaluated in terms of their effect on task performance.

In CCT, the ways people make judgments fall on a continuum between two poles: intuitive mode and analytical mode. Most judgments are made with a combination of strategies from these two modes. Hammond (1996) stressed that intuition and analysis are aspects of a repertoire of modes of cognition which may be selectively utilized according to the circumstances. Intuition and analysis are not isolated modes of cognition that exclude each other ("Intuition is not simply the absence of analysis.") but are poles that define the extremities of a range of information processing possibilities. Hammond (1996) proposed a cognitive continuum of properties that characterize the information-processing modes of Intuition, Analysis, and a middle ground, Quasi-rationality (Table 3). Quasi-rationality involves aspects of both intuition and analysis, and may be more or less intuitive or analytical depending upon the relative mix of intuitive and analytical characteristics demanded by the information environment. In complex decision-making and policy-formation tasks involving multiple interdependent cues, quasi-rational thinking may be the only feasible way to manage the situation (Cooksey, 1996). Hammond, Hamm, Grassia, and Pearson (1996) constructed a Cognitive Continuum Index (CCI) that quantitatively represents a person's position on the continuum when working in a particular task environment. The CCI is an equally weighted aggregate of four rescaled measures of cognitive properties derived from the Lens Model of judgment performance: cognitive control, organizing principle, error distribution, and differential confidence in process versus outcomes.

Judgment tasks (including threat-detection tasks) also can be ordered along a continuum according to the type or mode of cognition (information processing) they are likely to induce. Such tasks present different combinations of intuition-inducing and analysis-inducing elements. Hammond (1996) grouped task characteristics into three categories: complexity of task structure; ambiguity of task content, and form of task presentation (e.g., types of cues, whether data-driven or memory-driven). These characteristics create a task continuum of task traits: Inducing Intuition/Inducing Analysis/Inducing Quasi-rationality (Table 4). Tasks that induce quasi-rationality will show a mixture of intuition-inducing and analysis-inducing elements. The relative balance of task traits in the mixture will predict the pole towards which cognition would move. Hammond et al. (1996) operationally defined a Task Continuum Index (TCI) that parallels the CCI introduced earlier. The TCI is an equally weighted aggregate of eight rescaled measures of task characteristics: number of cues, extent of cue redundancy, reliability of cues, extent of task decomposition, availability of organizing principle, nonlinearity in the organizing principle, degree of predictability in the task system, and extent of equal cue weighting.

Applying CCT to early warning systems, the theory predicts that *detection accuracy* increases when there is *congruence* between (a) the information-processing modes or strategies employed to detect the threat and (b) the task traits that characterize the information needs of the threat-detection

TABLE 4. Task continuum of task traits (adapted from Cooksey, 1996, p. 20; Hammond, 2000).

Inducing intuition	Inducing quasi-rationality	Inducing analysis
Task structure complexity: Large number of simultaneous cues High redundancy among cues	Tasks which induce quasi-rationality will show a mixture of intuition-inducing as well as analysis-inducing elements. Relative balance in the mixture will predict the pole towards 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

task. Imagine two contrasting detection scenarios. When a scientific or quantitative model of the threat is available, then that model can provide the organizing principles to analyze information in cues to form a judgment about threat existence. On the other hand, when little is known about the threat and how it might be manifested, then information processing relies more on pattern recognition and discovery, and on exploring the overlap between multiple cues; in other words, it relies more on intuition than on analysis to form an interpretation of what is going on. Most threat-detection scenarios fall between these two polar conditions. The TCI of the CCT offers a systematic way to determine the balance of "analysis-inducing" elements and "intuition-inducing" elements that the detection task entails. The resultant set of task properties thus define the *Threat Information Environment*.

While the TCI assesses the information-processing requirements presented by the nature of the threat and the environment, the other component of CCT, the CCI, may be used to indicate the balance of analytical and intuitive information-processing strategies that are being employed by a system to make judgments about the threat. The resultant set of information-processing characteristics then define the *Information Use Environment* of the system. Taylor (1986, 1991) introduced the term *Information Use Environment* earlier, but uses it more broadly to describe four variables that affect the flow and evaluation of information: sets of people, problem classes and dimensions, organizational settings, and problem resolution and information use. The variables of problem dimensions and information use relate most closely to our discussion here.

CCT predicts that achievement (accuracy) in the threat-detection task would depend on the degree of congruence between task properties and information-processing strategies. Thus, analysis is not always the preferred mode of information processing for all types of threat-detection tasks. The optimal mode depends on the task's position on the task continuum, where "intuitive" elements of the task are best dealt with using intuition and interpretation, and "analytical" elements of the task are best dealt with using logical reasoning.

Based on the aforementioned discussion, we develop three propositions for further research. The propositions explore how Threat Information Environment and Information Use Environment relate to detection accuracy.

> **P1 (threat information environment):** The extent of knowledge and information about the threat determines 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.
>
> **P2 (information use environment):** An early warning system employs 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.
>
> **P3 (congruence and detection accuracy):** 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. More concisely, the better the fit between the threat information environment and the information use environment, the better the performance of the early warning system.

Early Warning Decisions: Signal Detection Theory and Diagnostic Decision Making

The role of early warning systems is not only to monitor conditions that can indicate a hazard or threat but also to decide, using the information available, if the threat exists and warning is to be activated. This decision is made difficult because the information available is always ambiguous, where cues that are true indicators of a threat being present (signal) are intermingled with cues that are generated by chance (noise). Because of irreducible uncertainty in the evidence, there is always the probability of making two kinds of detection decision errors: (a) saying that a threat exists when it does not and (b) failing to see a threat that does exist. For these situations, an extension of signal detection theory to diagnostic decision making introduced by Swets, Dawes, and Monahan (2000) and Swets (2000) provides a framework to analyze detection/decision outcomes. While signal detection theory (Green & Swets, 1966) is most widely applied in psychophysics (the study of the relationship

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

FIG. 2. Warning detection outcome matrix.

between a physical stimulus and its psychological effect), the theory has implications about how any type of decision under uncertainty is made, and is regarded as one of the most successful quantitative models of human performance (Wickens, 2002, p. 3).

The diagnostic decision approach of Swets et al. (2000) considers situations in which a decision must be made whether some condition is present or some event will occur, based on ambiguous information. Because information is uncertain, we must decide how much evidence is needed to warrant a positive decision. Thus, a *decision threshold* has to be set above which we will conclude that the signal or condition is present. Evaluating "how much evidence is needed" is not limited to quantity of information but also can refer to the strength, quality, or probability of the evidence.

In early warning situations, we can discern two detection states—issue warning or issue no warning—and two conditions—threat is real or no threat. Four outcomes are then possible (Figure 2):

- No warning given, and no threat exists: true negative or "all clear."
- No warning given, but threat exists: false negative or "miss,"
- Warning given, but there is no threat: false positive or "false alarm."
- Warning given, and threat exists: true positive or "hit."

A critical decision of an early warning system is determining whether to warn of a possible threat. It decides how much evidence is needed for it to conclude that a threat is real and imminent: It sets a threshold at which warning will be issued. The probabilities of the four outcomes in Figure 2 will vary as the *decision threshold* is varied. In practice, we need to look at two of the outcomes since the other two are their complements. The relationship between the probability of hits (true positives) and the probability of false alarms (false positives) as the decision threshold is varied can be shown graphically as *receiver operating characteristics* (curved lines in Figure 3). Operating characteristics may be constructed experimentally and mathematically, and their shape is well-established. A number of curves can be plotted to represent different levels of accuracy, depending on the state of knowledge and information about the threat. In Figure 3, the straight, diagonal line corresponds to chance accuracy, where there is equal probability of a hit or a false alarm. The more convex the curve is towards the northwest corner, the greater its accuracy. The most important point made by the curves is that true and false positives go up or down together. In other words, if we want more hits with a given system, we also will have to accept more false alarms. Setting the decision threshold is equivalent to selecting a point on the operating characteristic curve; that is, selecting a trade-off between hits and false alarms.

Figure 3 also shows a lax and a strict decision threshold. Setting a lax or cautious threshold—"weak evidence sufficient to say yes"—increases the probability of hits, but also increases the probability of false alarms. Conversely, a strict threshold—"strong evidence needed to say yes"—reduces the probability of false alarms, but also reduces the probability of hits. Setting a lax threshold is appropriate in certain situations. For example, when predicting a serious storm, we would be prepared to accept a false alarm rather than fail to warn about the storm. On the other hand, setting a strict threshold is appropriate when detecting a nuclear attack since the cost and consequences of incorrectly launching a counterattack could be grave and irreversible. In an important sense, the operating characteristic describes the *sensitivity* of a system to a set of cues and information. Thus, the performance of a detection system would depend not only on its accuracy but also on its receptivity or sensitivity to the evidence available.

While for most early warning systems we would not be able to experimentally construct a set of operating characteristics, the shape of the curves shows the trade-off between hits and false alarms that has to be made when setting decision thresholds. The challenge is to find "a decision threshold that constitutes a reasonable, rational, desirable balance between those two kinds of outcomes." (Swets, 2000, p. 69)

According to Swets et al. (2000), the "rational" decision threshold should be determined using two sets of information: (a) the base rate of the threat, or its probability of occurrence, and (b) an analysis of the benefits and costs, respectively, of hits and false alarms. They showed a general formula to calculate an optimal decision threshold that is expressed as the product of (a) the ratio of prior probabilities of threat and no-threat conditions and (b) a ratio of benefits and costs associated with hits and false alarms (Swets et al., 2000, p. 9). The principle here is that when the base rate is high and the benefit of a hit is high (e.g., predicting and warning of a serious storm), the system should set a lax threshold (i.e., say yes often). Conversely, when the base rate is low and the cost of a false alarm is high (e.g., launching a counteroffensive against a misread military attack), the system should select a strict threshold (i.e., say yes rarely, requiring strong evidence). Both base rates and cost–benefit analysis should be considered relative to the population that is at risk (i.e., its vulnerability, preparedness, exposure).

Although it is theoretically possible to select a "rational" decision threshold based on threat probability and

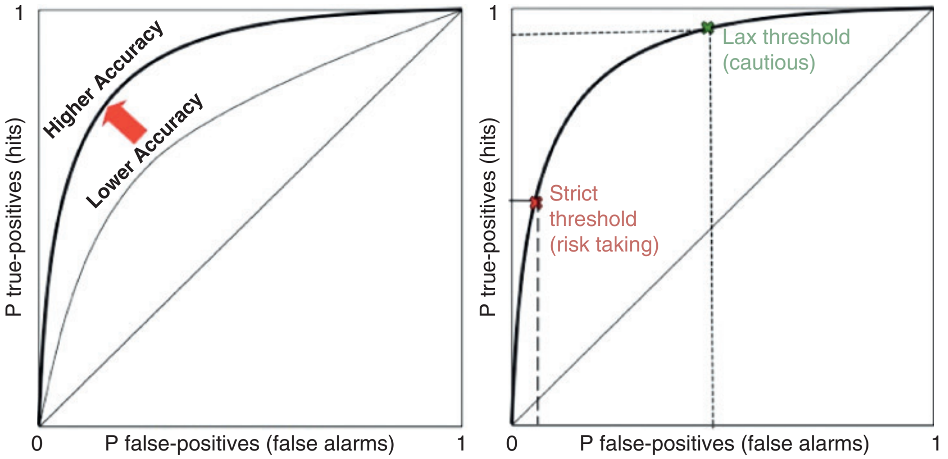

FIG. 3. Signal detection theory in diagnostic decisions: receiver operating characteristics.

cost–benefit analysis, in practice, the adoption of a decision threshold is determined by the complex interplay of interests and interventions among many groups and stakeholders. More often than not, the discussion of early warning and appropriate response is subject to an array of economic, political, and social factors that alter the perception and the evaluation of threat risks. Kasperson, Kasperson, Pidgeon, and Slovic (2003) described the social amplification of risk in which signals about risk events go through "information processes, institutional structures, social-group behavior, and individual responses [that] shape the social experience of risk, thereby contributing to risk consequences" (p. 15). Thus, risk events are portrayed by the media, commented on by experts and opinion leaders, and shaped by risk-related behavior of interested groups, businesses, and public agencies. Economic and political factors such as the cost of litigation, the loss of revenue, and the opposition of communities may weigh heavily in the analysis. Groups concerned with certain threats may attempt to influence the interpretation of risks in support of their beliefs, values, and interests. In some cases, the risks of hazards that experts judge as relatively low in risk (e.g., nuclear plant accidents) may become amplified as a particular locus of concern and sociopolitical activity. Other risks that experts judge more serious (e.g., automobile accidents) may become attenuated, receiving comparatively less attention from society (Pidgeon, Kasperson, & Slovic, 2003).

Puranam, Powell, and Singh (2006) suggested that the costs of false alarms or misses are rarely symmetrical in early warning situations. An alarm that initiates action which is disruptive and unpopular (e.g., closure of offices, schools, transportation) may be perceived as having high economic and social costs. When the costs of false alarms are expected to be prohibitive, decision makers may be more concerned about the probability of false alarms when setting the threshold. For example, during the Asian tsunami of 2004, the Thai Meteorological Department did not issue warnings based on information it had about the earthquake near Sumatra that had set the tsunami in motion. It was a matter of government policy that such a warning would harm tourism and damage the Thai economy if it proved to be a false alarm (Gerstein & Ellsberg, 2008).

In a classic study, Slovic (1987) found that risk perception by the public differs from risk judgment by experts. Public risk perception is affected by three factors: (a) "dread risk," defined as risk that is high in perceived lack of control, dread, catastrophic potential, fatal consequences, and inequitable distribution of risks; (b) "unknown risk," defined as risk perceived to be unobservable, unknown, new, and delayed in the manifestation of harm; and (c) "number of people" exposed to the risk. For laypeople, the most important factor is "dread risk." The higher the dread factor, the higher the perceived risk, the more people want to see the threat reduced, and the more they want to see strict regulation enacted to attain this. Dread risk may thus generate public pressure to lower the decision threshold of warning systems, increasing the probability of false alarms.

Based on the previous discussion, we introduce three more propositions for further research. The propositions explore how setting the decision threshold determines the sensitivity of the early warning system, and how the social construction of risk has a major influence on the decision threshold adopted by policy makers.

P4 (decision sensitivity): Different early warning systems are characterized by their sensitivities or receptiveness to evidence. Decision 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.

P5 (decision outcomes): Setting a decision threshold in an early warning system 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 whereas setting a strict, risky threshold reduces false alarms, but also reduces hits.

P6 (decision thresholds): In theory, a rational decision threshold should be set based on threat probability and a cost–benefit analysis of false alarms and hits. In practice, the

> decision threshold is influenced by many economic, political, and social forces, as well as by individuals, groups, and institutions that act according to their beliefs, values, and interests.

Discussion

Our discussion touches on two conceptual dilemmas that underlie the informational aspects of early warning. The first is often referred to in the early warning literature as the bind of quantitative and qualitative data, or what we have alluded to as the tension between analysis and intuition/interpretation. The quantitative-analytical approach typically employs technology and formal schemes to collect, categorize, and process large amounts of data on streams of events that can indicate emerging threats. Such an approach promises efficiency, wide coverage, and timely reporting. At the same time, the huge volume of data generated and the diversity of conditions in which events are observed create serious difficulties in making sense of the data available. Intuition, rooted in local knowledge and experience, is often the key to seeing patterns in the data, interpreting their significance, and imagining scenarios that connect the events. The qualitative approach is not without its own problems, as interpretations are subjective and subject to personal and institutional biases. Our discussion in this article asks: To what extent is this dichotomy between analysis and intuition real and relevant to early warning detection? How important would it be for warning systems to combine analytical and intuitive/interpretive approaches according to the information exigencies of the threat or hazard?

The second dilemma is contained in the observation that "we live in a risk society," both in terms of the degree and distribution of risk to which we are exposed and in our heightened sensitivity towards the ramifications of risk. Our attitudes have changed with regard to how society and its institutions should respond to or regulate situations where risk is significant, but knowledge about the hazard is incomplete. A general shift towards precaution and the need to create a margin of safety may be accounted for by three factors: (a) the affective and cognitive grip of recent disasters, (b) the amplification of risk through the media and the active engagement of interest groups, and (c) the adoption by policy makers of the precautionary principle as a guide for risk management and regulation.

When we consider threats such as terrorist attacks, infectious disease outbreaks, natural calamities, and humanitarian disasters, the terror and tragedy of recent events are cognitively available and emotionally salient, and they elevate our feelings of anxiety and our appetite for caution. Some have suggested, perhaps exaggeratedly, that we are living in an epidemic of fear (Siegel, 2005). At the same time, the ramification of risk is being socially constructed and amplified as interest groups, communities, and stakeholders press their concerns through an expanding arena of media channels and public forums that cater to expert as well as citizen commentary.

The Precautionary Principle has become a staple of regulatory policy making, and is now inscribed in many international treaties and agreements. There are many formulations of the principle, one familiar version is the Wingspread Statement (Wingspread Conference, 1998):

> When an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not fully established scientifically. In this context the proponent of the activity, rather than the public, should bear the burden of proof.

A well-known discussion of precaution by Talbot Page (1978) illustrates the logic underlying the principle. Page noted that since the expected damage of risky technologies may well exceed the expected harm or forgone benefits of not adopting these technologies, precautionary decisions are justified on three grounds: (a) avoiding the risks of uncertain, but highly harmful, outcomes; (b) not making irreversible commitments that foreclose future courses of action; and (c) not imposing risks on future generations.

The net result of risk dread, risk amplification, and precautionary decision making is an increased pressure on early warning systems to adopt a cautious posture that diminishes the costs of false alarm and increases the penalty of failing to warn. A corollary is that warning systems lower decision thresholds, increasing the probability of false alarms. After the attacks of 9/11, warning systems have tended to set low thresholds on the possibility of another terrorist attack. For example, both Siegel (2005) and Sunstein (2005) suggested that the 2001 anthrax scare in the United States was largely a false alarm induced by a cautious decision threshold.

Cost–benefit analysis is another tool for the assessment and management of social risks, and is sometimes seen as an alternative to the precautionary principle. The approach is often supported on the basis of economic efficiency, as it allows regulators to choose the policy that maximizes net benefits over costs. Sunstein (2000) did not endorse this economic view, and instead makes a *cognitive* case for cost–benefit analysis:

> I have suggested that cost-benefit analysis, often defended on economic grounds, can be urged less contentiously on cognitive grounds. Cost-benefit analysis, taken as an inquiry into the consequences of varying approaches to regulation, is a sensible response not only to interest-group power but also to limited information and to predictable problems in the public demand for regulation. These problems include the use of the availability heuristic; social amplification of that heuristic via cascade effects; a failure to see the benefits that accompany certain risks; a misunderstanding of systemic effects, which can lead to unanticipated bad (and good) consequences; and certain emotional reactions to risks. In all of these areas, an effort to identify costs and benefits can properly inform analysis. (p. 1096)

Posner (2000) drew a helpful distinction between three uses of cost–benefit analysis: (a) as an input into decision making; (b) as a decision rule; and (c) as a method of pure evaluation, without regard to possible use of its results in a

TABLE 5. Research propositions and methods.

Propositions	Example research methods
P1 (threat information environment): The extent of knowledge and information about the threat determines 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. 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. P3 (congruence and detection accuracy): 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.	Develop threat information profiles of a number of hazards in different domains (e.g., natural disasters, political conflict, public health, financial crises). [P1] Identify major early warning systems that target each type of hazard. Identify information gathering and processing strategies of each system (e.g., newsfeeds, indicators, scenarios, expert panels, statistical analysis). [P2] Compare the balance of threat information attributes with the balance of information processing strategies. Assess the overall “congruence” as predicted by theory. Relate congruence to the accuracy of each warning system using historical record, perceived capability, internal evaluation, other criteria. [P3]

P4 (decision sensitivity):
Different early warning systems are characterized by their sensitivities or receptiveness to evidence. Decision 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.
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 while setting a strict, risky threshold reduces false alarms, but also reduces hits.
P6 (decision thresholds):
In theory, a rational decision threshold should be set based on threat probability and a cost–benefit analysis of false alarms and hits. In practice, the decision threshold is influenced by many economic, political, and social forces; and by individuals, groups, and institutions that act according to their beliefs, values, and interests.
	Examine information procedures and systems; indicators, events, and reports monitored by each system which could trigger warning.
	Determine inductively decision thresholds adopted: How much and what type of evidence is needed to activate warning? Analyze the rationales used to justify decision thresholds. [P4]
	Analyze how threat probabilities, threat risks, and costs–benefits are assessed and talked about by analysts, decision makers, experts, stakeholders. [P5]
	Compare adopted decision threshold with that prescribed by theory (based on threat probability and costs–benefits).
	Analyze how the action of concerned stakeholders influences the decision threshold. [P6]

decision. We view cost–benefit analysis as providing decision input. While there has been much discussion on cost–benefit analysis for policy making, there is much less research on its use in early warning to assess the benefits of hits relative to the costs of false alarms.

Summary

This introductory article explored the relationship between information use and early warning effectiveness. By effectiveness, we refer to the capacity of the system to detect and decide on the existence of a threat or hazard. There are two aspects to effectiveness: (a) being able to see the evidence that is indicative of a threat and (b) making the decision, based on the weight of the evidence, to warn that the threat exists (As noted earlier, this article focuses on the monitoring and warning function of early warning systems. Other functions such as dissemination and communication, and response capability, are outside our scope.) In early warning, information use is encumbered by cues and messages that are fallible, dispersed, and equivocal. Cues that are true indicators of a threat are invariably obscured in a cloud of events generated by chance. Apart from being able to see the threat, policy makers also face the difficult decision of whether to issue a warning based on the information received. Because the information is rarely complete or conclusive, such decisions have to assess the consequences of failing to warn or giving a false warning.

We conceptualized early warning as perceptual inference and as signal detection. In applying the Lens Model and CCT, we focused on detection 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 balance of factors that induce cognitive (rule-based), intuitive (pattern-based), or quasi-rational (hybrid) information processing. Different types of threats and hazards (e.g., financial crises vs. terrorist attacks) vary significantly in the amount and kind of information and knowledge that can be brought to bear in detecting their presence. It would be interesting to see if informationally distinct threats are matched by early warning systems that deploy systematically different information-gathering and information-processing strategies.

In applying Signal Detection Theory as extended to diagnostic decision making, we focused on decision sensitivity. Sensitivity or receptivity depends on the decision threshold that is adopted regarding the amount and strength of evidence that is needed to conclude that there is a threat. The threshold may be inferred by analyzing the warning indicators, trigger events, and hazard scenarios monitored by the system. Setting 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. Although theory suggests that the decision threshold should be based on threat probability and the benefits and costs of hits and false alarms, respectively, this is complicated in practice by the actions of interested groups, stakeholders, and experts as they shape the perception and evaluation of threat risks.

Our analysis led to six research propositions that link the concepts of threat information environment, information use environment, detection accuracy, decision sensitivity, and early warning effectiveness. In the hope of stimulating interest, we conclude with a sketch of research strategies that might be used to investigate these propositions (Table 5).

References

Alker, H.R., Gurr, T.R., & Rupesinghe, K. (Eds.). (2001). Journeys through conflict: Narratives and lessons. Lanham, MD: Rowman & Littlefield.

Basher, R. (2006). Global early warning systems for natural hazards: Systematic and people-centred. Philosophical Transactions of the Royal Society A-Mathematical Physical and Engineering Sciences, 364(1845), 2167–2180.

Brunswik, E. (1952). The conceptual framework of psychology. Chicago: University of Chicago Press.

Choo, C.W. (2005). Information failures and organizational disasters. Sloan Management Review, 46(3), 8–10.

Choo, C.W. (2008). Organizational disasters: Why they happen and how they may be prevented. Management Decision, 46(1), 32–46.

Cooksey, R.W. (1996). Judgment analysis: Theory, models, and applications. San Diego, CA: Academic Press.

Davies, J.L., & Gurr, T.R. (Eds.). (1998). Preventive measures: Building risk assessment and crisis early warning systems. Lanham, MD: Rowman & Littlefield.

George, A.L., & Holl, J.E. (1997). The warning-response problem and missed opportunities in preventive diplomacy: A report to the Carnegie Commission on preventing deadly conflict. New York: Carnegie Corporation.

Gerstein, M.S., & Ellsberg, M. (2008). Flirting with disaster: Why accidents are rarely accidental. New York: Union Square Press.

Goldstein, W.M. (2004). Social judgment theory: Applying and extending Brunswik's probabilistic functionalism. In D. Koehler & N. Harvey (Eds.), Blackwell handbook of judgment and decision Making (pp. 37–61). Oxford, United Kingdom: Blackwell.

Green, D.M., & Swets, J.A. (1966). Signal detection theory and psychophysics. New York: Wiley.

Hammond, K.R. (1996). Human judgment and social policy: Irreducible uncertainty, inevitable error, unavoidable injustice. New York: Oxford University Press.

Hammond, K.R. (2000). Judgments under stress. New York: Oxford University Press.

Hammond, K.R., Hamm, R.M., Grassia, J., & Pearson, T. (1996). Direct comparison of the efficacy of intuitive and analytical cognition in expert judgment. In W.M. Goldstein & R.M. Hogarth (Eds.), Research on judgment and decision making: Currents, connections, and controversies (pp. 144–180). Cambridge, United Kingdom: Cambridge University Press.

Heymann, D.L., Rodier, G.R., & WHO Operational Support Team, GOARN (2001). Hot spots in a wired world: WHO surveillance of emerging and re-emerging infectious diseases. Lancet Infectious Diseases, 1(5), 345–353.

Kasperson, J.X., Kasperson, R.E., Pidgeon, N., & Slovic, P. (2003). The social amplification of risk: Assessing 15 years of research and theory. In N. Pidgeon, R.E. Kasperson, & P. Slovic (Eds.), The social amplification of risk (pp. 13–46). Cambridge, United Kingdom: Cambridge University Press.

Lundin, H. (2004). Crisis and conflict prevention with an Internet based early warning system. Stockholm: Stockholm International Peach Research Institute.

Madoff, L.C. (2004). ProMED-mail: An early warning system for emerging diseases. Clinical Infectious Diseases, 39, 227–232.

Madoff, L.C., & Woodall, J.P. (2005). The internet and the global monitoring of emerging diseases: Lessons from the first 10 years of ProMED-mail. Archives of Medical Research, 36(6), 724–730.

Matveeva, A. (2006). Early warning and early response: Conceptual and empirical dilemmas. Den Haag, The Netherlands: European Centre for Conflict Prevention/GPPAC.

Mazur, A. (2004). True warnings and false alarms: Evaluating fears about the health risks of technology, 1948–1971. Washington, DC: Resources for the Future.

Morse, S.S. (2007). Global infectious disease surveillance and health intelligence. Health Affairs, 26(4), 1069–1077.

Mykhalovskiy, E., & Weir, L. (2006). The Global Public Health Intelligence Network and early warning outbreak detection: A Canadian contribution to global public health. Canadian Journal of Public Health, 97(1), 42–44.

Page, T. (1978). A generic view of toxic chemicals and similar risks. Ecology Law Quarterly, 7(2), 207–212.

Peduzzi, P. (2004). Typology of hazards. In Environment and Poverty Times No. 3 (p. 67). Arendal, Norway: UN Environment Programme/GRID-Arendal.

Pidgeon, N., Kasperson, R.E., & Slovic, P. (Eds.). (2003). The social amplification of risk. Cambridge, United Kingdom: Cambridge University Press.

Posner, R.A. (2000). Cost-benefit analysis: Definition, justification, and comment on conference papers. Journal of Legal Studies, 29(2), 1153–1157.

Puranam, P., Powell, B.C., & Singh, H. (2006). Due diligence failure as a signal detection problem. Strategic Organization, 4(4), 319.

Schmeidl, S., & Adelman, H. (Eds.). (1998). Early warning and early response. New York: Columbia University Press. Retrieved July 18, 2008 from Columbia International Affairs Online http://www.ciaonet.org/book/schmeidl/intro.html

Siegel, M. (2005). False alarm: The truth about the epidemic of fear. Hoboken, NJ: Wiley.

Slovic, P. (1987). Perception of risk. Science, 236, 280–285.

Sunstein, C.R. (2000). Cognition and cost-benefit analysis. Journal of Legal Studies, 29(2), 1059–1103.

Sunstein, C.R. (2005). Laws of fear: Beyond the precautionary principle. Cambridge, United Kingdom: Cambridge University Press.

Swets, J.A. (2000). Enhancing diagnostic decisions. In T. Connolly, H. R. Arkes, & K.R. Hammond (Eds.), Judgment and decision making: An interdisciplinary reader (2nd ed., pp. 66–81). Cambridge, United Kingdom: Cambridge University Press.

Swets, J.A., Dawes, R.M., & Monahan, J. (2000). Psychological science can improve diagnostic decisions. Psychological Science in the Public Interest, 1(1), 1–26.

Taylor, R.S. (1986). Value-added processes in information systems. Norwood, NJ: Ablex.

Taylor, R.S. (1991). Information use environments. In B. Dervin & M. J. Voigt (Eds.), Progress in communication science (Vol. 10, pp. 217–254). Norwood, NJ: Ablex.

UN ISDR. (2006). Global survey of early warning systems. Geneva: United Nations International Strategy for Disaster Reduction.

van Walraven, K. (Ed.). (1998). Early warning and conflict prevention. The Hague, The Netherlands: Kluwer Law International.

Wagner, M.M., Tsui, F.-C., Espino, J.U., Data, V.M., Sittig, D.F., Caruana, R.A., et al. (2001). The emerging science of very early detection of disease outbreaks. Journal of Public Health Management Practice, 7(6), 51–59.

Wickens, T.D. (2002). Elementary signal detection theory. New York: Oxford University Press.

Wingspread Conference Participants. (1998). Wingspread statement on the precautionary principle. The Science and Environmental Health Network. Retrieved January 30, 2009, from http://www.sehn.org/wing.html

Woodall, J.P. (2001). Global surveillance of emerging diseases: The ProMED-mail perspective. Cad Saude Publica, 17(4), 147–154.