Common Alerting Protocol for Health Alerting in Sri Lanka and India[1]

Prepared for WMO Common Alerting Protocol (CAP) Implementation Workshop. Geneva, April 6-7, 2011

Gordon A. Gow
Associate Professor
Graduate Program in Communication and Technology,
University of Alberta, Edmonton, Canada
gordon.gow@ualberta.ca

Nuwan Waidyanatha
Senior Researcher, LIRNE*asia*
12 Balcombe Place, Colombo 08, Sri Lanka
nuwan@lirneasia.net

Abstract

This paper describes the approach taken to develop a Common Alerting Protocol (CAP) Profile for a health alerting initiative in Sri Lanka and India. The health alerting system formed part of a research study under LIRNEasia's Real-Time Biosurveillance Pilot Program (RTBP). The CAP Profile developed for the RTBP implementation is an adaptation based on pioneering work done by the US Centres for Disease Control-Public Health Information Network (CDC-PHIN) and released in 2008 under its PCA Guidelines. The aim here is to describe an instantiation of CAP as derived from the PCA Guidelines, highlighting a number of specific issues and considerations associated with a CAP-based health alerting system in a developing country.

1. Introduction

The Real-Time Biosurveillance Program (RTBP) was a multi-partner research initiative to study the potential for new Information and Communication Technologies (ICTs) to improve early detection and notification of disease outbreaks in Sri Lanka and India. The project ran from 2008-2010 under the auspices of LIRNEasia, with funding from Canada's International Development Research Centre (IDRC).

The primary research objective of the Real-time Biosurveillance Program (RTBP) was to produce evidence to indicate in what ways and to what extent the introduction of new ICTs might achieve efficiency gains when integrated with existing disease surveillance and detection systems. The RTBP research design included the development of a testbed using Common Alerting Protocol (CAP) to support health alerting and data interchange.

---

[1] For an expanded version of this paper see: Gow, G. and N. Waidyanatha (2010). "Using Common Alerting Protocol to Support a Real-Time Biosurveillance Program in Sri Lanka and India," in T. Kass-Hout and X. Zhang (Eds.) Biosurveillance: Methods and Case Studies. Chapman and Hall. P. 267-290.

In the following sections, we describe the steps taken toward an implementation of Common Alerting Protocol for the Real-Time Biosurveillance Program (RTBP) initiative. The RTBP implementation is an adaptation based on pioneering work done by the US Centers for Disease Control Public Health Information Network (CDC-PHIN) and contained in August 2008 in its PHIN Communication and Alerting Guide (hereinafter referred to as "PHIN-PCA Guide"). The aim here is to demonstrate an instantiation of CAP as derived from the PHIN-PCA Guide, highlighting a number of specific issues and considerations associated with health alerting for a biosurveillance project in a developing country.

1.1 What is a CAP profile document?

Whereas the CAP standard establishes the basic architecture of an alerting message through its prescribed elements and sub-elements, many of the actual values and usage conventions must be user-defined. As such, any implementation of CAP requires some further specification in terms of how various sub-elements (e.g., message ID) will be populated by an alerting system during message creation. Such specification may lead to the creation of a CAP Profile document. (See, for example, (*Common Alerting Protocol Canadian Profile (v1.1)* 2008)).

The CAP profile document is defined as a set of additional requirements within the scope of and conforming to the basic CAP specification. These constraints establish rules and conventions to ensure that local requirements and alerting policies, as well as particular data requirements, are translated into a fully valid CAP message format. A CAP profile therefore defines a specific instantiation while ensuring that messages created and distributed by that instantiation remain CAP compliant and will "make at least basic sense to recipients that are unaware of the profile restrictions" (CAP Cookbook 2009). This last point is especially important to facilitate sharing of information and growth of a biosurveillance alerting system across organizational and jurisdictional boundaries (Wagner, 2006).

2. Methodology for creating the CAP-RTBP profile

The method used to develop the CAP-RTBP profile involved a three-step process. The RTBP initiative adapted a model based on CDC PHIN PCA Guidelines (United States Centers for Disease Control and Prevention 2008), identifying a set of standardized message attributes for health alerting. These attributes provide a framework for shared vocabulary, predictable system response, and more broadly for identifying policy and procedural issues of interest for the research project.

Following the PHIN PCA approach, 'Alert Attributes' are semantic descriptors that are associated with specific functional elements and defined precisely using Common Alerting Protocol (CAP) and the Emergency Data Exchange Language (EDXL) Distribution Element. The following list sets out the framework of Alert Attributes adopted for the RTBP initiative:

1. Identity of the agency that issued the alert {*agencyIdentifier*}
2. Message identifier for tracking purposes {*alertIdentifier*}
3. Time and date that the message was sent from the issuing agency {*sendTime*}

4. Indication of whether it is an actual alert, exercise, or test {*status*}
5. Indication of whether it is an original alert, update, or cancellation of a previous alert {*msgType*}
6. Indication of the scope of distribution for the alert (i.e., public, restricted, private) {*scope*}
7. The priority of the message (i.e., urgent, high, low) {*priority*}
8. Indication of the event or incident type {*event*}
9. Contents of the alert message {*message*}

Each of the CDC-PHIN alert attributes was then mapped to a corresponding CAP element or sub-element. At the second stage, additional specifications with regard to conforming to the CAP v1.1 standard were examined for each attribute. Finally, a provisional set of rules and conventions were derived to prescribe how alerts were to be generated for the RTBP initiative using the Sahana alerting broker (Sahana, 2008). See figure 1.

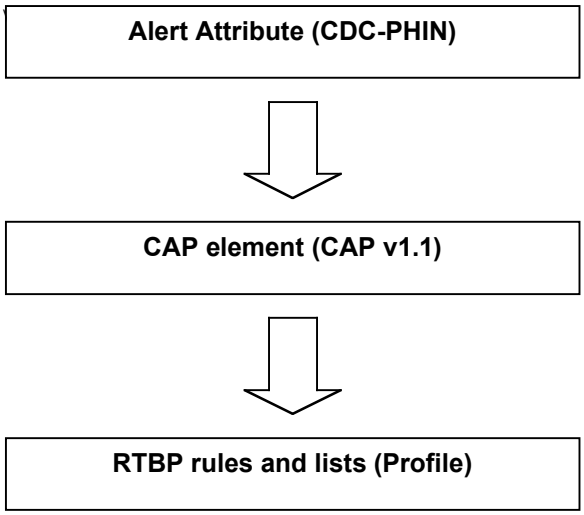

Figure 1: steps taken to create RTBP CAP Profile from CDC-PHIN PCA Guidelines

2.1 Alert attribute {*agencyIdentifier*}

Each message must include a unique identifier for the agency that issued the alert. PHIN PCA Guide v1.0 refers to an "Object Identifer (OID)" of the originating agency and the future creation of an OID and ebXML registry for PHIN.

CAP v1.1 specifies this attribute as a required sub-element within the alert block as <*alert.sender*>. CAP v1.1 further specifies that it must identify "the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name" and "MUST NOT include spaces, commas or restricted characters (< and &)."

CAP profile considerations for RTBP project:

Based on CAP v1.1 requirements, the research team recommended that every person, organization, and agency authorized to issue alerts within the RTBP project be

assigned a unique "object identifier" (OID) based on a valid and appropriate Internet domain name (e.g., RTBP@lirneasia.org). In some cases, discussion was needed to ensure that each organization was willing and able to meet this requirement.

In addition, the research team also identified a need to establish and maintain a registry of object identifiers associated with persons, organizations, and agencies that are authorized to issue alerts for the RTBP project. In the case of RTBP initiative, the number of authorized issuers consists of a relatively small number of authorized users but as the project grows in size and possibly extends across jurisdictions, it is expected that identifying ways to effectively manage this registry will become increasingly important.

2.2 Alert attribute {*alertIdentifier*}

Each message must be assigned a unique identifier.

The CDC-PHIN PCA Guide v1.0 does not specify an encoding requirement for this attribute; however, it notes that "every alerting program must have a unique namespace and its own protocol for generating unique alert identifiers."

CAP v1.1 specifies this as a required sub-element within the alert element as <*alert.identifer*>. CAP v1.1 further specifies that it must be "a number or string uniquely identifying this message, assigned by the sender" and "MUST NOT include spaces, commas or restricted characters (< and &)."

CAP profile considerations for RTBP project:

Based on these considerations, the research team recommended that RTBP establish a convention for generating and assigning the attribute {*alertIdentifier*}. This must conform to CAP v1.1. Participants and authorized issuers should be encouraged to adopt that convention when issuing alerts over the system.

2.3 Alert attribute {*sendTime*}

Each message must include the time and date that it was first issued. PHIN-PCA Guide v1.0 specifies that this attribute is to be encoded using ISO 8601 format, which corresponds with CAP v1.1 requirement (see below).

CAP v1.1 specifies this as a required sub-element within the alert element as <*alert.sent*>. CAP v1.1 further specifies that it must be "represented in [dateTime] format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT)" and that "Alphabetic timezone indicators such as 'Z' MUST NOT be used. The timezone indicator for UTC MUST be represented as '-00:00' or '+00:00."

CAP profile considerations for RTBP project:

The research team recommended that RTBP adopt the ISO 8601 dateTime standard format, taking into account any other considerations related to the W3C form for

XML dateTime. Furthermore, it was recommended that the ISO 8601 format be embedded in the message creation sub-system software to eliminate need for individuals to enter this data themselves.

It was also recommended that assignment of the {*sendTime*} attribute should be done automatically by the message creation sub-system only at the moment the message is sent to the distribution sub-system. The {*sendTime*} attribute should NOT be assigned at the time the message is drafted in order to avoid confusion in situations where a message is created and then stored as a standby template.

Looking ahead to potential expansion of a region-wide biosurveillance program, there is a need to examine potential issues with time zone coordination and to identify a reliable, common source for the dateTime data feed.

2.4 Alert attribute {*status*}

Each message must indicate whether it is an actual alert, exercise, or test.

PHIN PCA specifies enumeration values of "Actual" (referring to a live event), "Exercise" (indicates that designated recipients must respond to the alert as part of an exercise), "Test" (indicates that the message is related to a technical system test and should be disregarded by recipients).

CAP v1.1 specifies this as a required sub-element within the alert element as <*alert.status*>. CAP v1.1 further specifies that is be represented as one of five designated code values, each with specific meaning and intent:

"Actual"—actionable by all targeted recipients
"Exercise"—actionable only by designated exercise participants
"System"—for messages that support alert network internal functions
"Test"—technical testing only, all recipients disregard
"Draft"—a preliminary template or draft, not actionable in its current form

CAP v1.1 recommends that <*alert.note*> sub-element be used to provide an exercise identifier when message is assigned "Exercise" status.

CAP profile considerations for RTBP project:

The research team recommended that RTBP adopt the full CAP v1.1 code values and definitions for the {status} attribute to provide maximum flexibility in terms of accommodating future requirements of the biosurveillance program.

It was also recommended that message creation software provide a menu choice "Draft" in addition to the other status values to enable the creation of preliminary templates that can be saved for use when needed. Importantly, however, the research team recommended that message creation software be designed to prevent messages with "Draft" status from being sent to the distribution sub-system. This would help to reduce incidents of accidental alerts sent when drafting templates.

Other considerations identified by the research team included the need to consider establishing unique identifiers for messages that refer to exercises and simulations as distinct from those that refer to actual alerts. This would provide users and system administrators with an additional degree of redundancy in the event that the {status} attribute failed to be displayed on an end-user device.

Furthermore, there is a need to establish clear specifications and rules for using the values "System" and "Test" within the scope of the RTBP project to ensure that issuers and recipients are aware of when and how these are to be assigned.

2.5 Alert attribute {*msgType*}

Each message must indicate whether it is an original alert, update, or cancellation of a previous alert.

PHIN PCA specifies enumeration values "Alert" (to indicate an original alert), "Update" (to indicate that a prior alert has been update and superseded), "Cancel" (to indicate that a prior alert has been cancelled), "Error" (to indicate that a prior alert has been retracted).

If {*msgType*} is "Update", "Cancel" or "Error" then the message attribute {*reference*} must be included in the message to provide a unique identifier of the message being updated, cancelled, or issued in error.

CAP v1.1 specifies this as a required sub-element within the alert element as <*alert.msgType*>. CAP v1.1 further specifies that is be represented as one of five designated code values, each with specific meaning and intent:

> "Alert"—initial information requiring attention by targeted recipients
> "Update"—updates and supersedes the earlier message(s) identified in <references>
> "Cancel"—cancels the earlier message(s) identified in <references>
> "Ack"—acknowledges receipt and acceptance of the message(s) identified in <references>
> "Error"—indicates rejection of the message(s) identified in <references>

CAP v1.1 requires that <alert.references> sub-element be used to provide an unique message identifier when message type is "Update", "Cancel", "Ack", or "Error".

CAP v1.1 suggests that <alert.note> sub-element be used to provide an explanation when message type is "Error".

CAP profile considerations for RTBP project:

It was recommended that RTBP adopt the CAP v1.1 code values and definitions for <alert.msgType> within the CAP envelope. The research team also suggested that RTBP adopt EDXL Distribution Element v1.0 code values and definitions for message distribution, mapped appropriately to the CAP v1.1 values for the EDXL envelope (e.g., "Alert" is equivalent to "Report"; "Update is equivalent to "Update).

It was suggested that it is not necessary for RTBP to implement the code values "Request", "Response" and "Dispatch" at this time, as these do not apply to the aims or activities of the biosurveillance program.

The research team also identified the need to establish a procedure and associated rules for issuing various message types, with particular guidelines for updates, cancellations, and errors.

There is a need to establish a method for generating and assigning <alert.reference> when required.

2.6 Alert attribute {*scope*}

Each message must indicate the scope of distribution for the alert (i.e., public, restricted, private).

PHIN PCA Guide v1.0 specifies that "PHIN alerting systems should always use the value 'Restricted', meaning 'for dissemination only to users with a known operational requirement.'" This is not a required attribute in PHIN-PCA Guide v1.0 but it is acknowledged that the attribute must be included to produce valid XML messages conforming to CAP.

CAP v1.1 specifies this as a required sub-element within the alert element as <alert.scope>. CAP v1.1 further specifies that is be represented as one of three designated code values, each with specific meaning and intent:

> "Public"—for general dissemination to unrestricted audiences
> "Restricted"—for dissemination only to users with a known operational requirement
> "Private"—for dissemination only to specific addresses

CAP v1.1 requires that sub-element <alert.restriction> be used when the scope value is "Restricted." The <alert.restriction> sub-element is therefore conditional and contains "text describing the rule for limiting distribution of the restricted alert message."

CAP v1.1 requires that sub-element <alert.addresses> be used when the scope value is "Private." The <alert.addresses> element is therefore conditional and contains "the group listing of intended recipients of the private alert message." CAP v1.1 specifies certain rules for this sub-element: "each recipient SHALL be identified by an identifier or address", "multiple space-delimited addresses MAY be included. Addresses including whitespace MUST be enclosed in double-quotes."

CAP profile considerations for the RTBP project:

It was recommended that RTBP adopt the CAP v1.1 code values and definitions for <alert.scope> within the CAP envelope.

However, it was noted by the research team that since the RTBP was a testbed project that it adopt a rule whereby all messages issued within the scope of the project be designated as “Restricted” or “Private”. This would ensure that CAP messages that might be distributed beyond the confines of the system would not inadvertently be sent to members of the public or those not authorized by the RTBP.

In terms of message creation, it was recommended that the RTBP software interface provide menu options only for “Restricted” or “Private” messages, but with future provision for “Public” messages should this become an option at some point in time.

The use of restricted or private messages introduces a number of administrative duties to ensure appropriate and effective distribution of alert messages. For example, when using the “Restricted” value, system designers must assign text to describe the rule for limiting distribution of those messages, ensuring that it conforms to CAP v1.1 sub-element <alert.restricted>.

When assigning messages the “Private” value, there is also a need to establish a registry of addresses for specific recipients that are designated to receive such messages. This registry must be capable of expressing the designated recipients in a format that conforms to requirements defined in CAP v1.1 sub-element <alert.addressess>.

2.7 Alert attribute {*priority*}

Each message must indicate the priority level of the alert.

PHIN PCA Guide v1.0 does not specify an equivalent message attribute {*priority*} but includes three related message attributes: *severity*, *urgency*, *certainty*. Of these, *severity* is the only required attribute. Code values for these attributes are to follow CAP v1.1 enumeration values for corresponding CAP sub-elements.

CAP v1.1 establishes message priority with the info element using three required sub-elements: <info.urgency>, <info.severity>, <info.certainty>. All three elements must be included to produce a valid CAP-XML document.

CAP v1.1 specifies the following code values for the sub-element <info.urgency>:

> “Immediate”—responsive action should be taken immediately
> “Expected”—responsive action should be taken soon (within next hour)
> “Future”—responsive action should be taken in the near future
> “Past”—responsive action is no longer required
> “Unknown”—urgency not known

CAP v1.1 specifies the following code values for the sub-element <info.severity>:

> “Extreme”—extraordinary threat to life or property
> “Severe”—significant threat to life or property
> “Moderate”—possible threat to life or property
> “Minor”—minimal threat to life or property

"Unknown"—severity unknown

CAP v1.1 specifies the following code values for the sub-element <info.certainty>:

"Observed"—determined to have occurred or to be ongoing
"Likely"—likely (p > ~50%)
"Possible"—possible but not likely (p <= ~50%)
"Unlikely"—not expected to occur (p ~ 0)
"Unknown"—certainty unknown

A potential drawback to the CAP v1.1 approach to message prioritization is complexity. While the three sub-elements of urgency, severity, and certainty permits a high degree of precision in defining the nature of an alert, it also makes if more difficult to establish consensus as to how any particular incident should be defined according to the three variables. As a result, both issuers and recipients may find it difficult quick ascertain the nature of an alert and the action required.

To address this problem of potential ambiguity, previous efforts adapting CAP v1.1 for a hazard alerting project in Sri Lanka resulted in a simplified message prioritization scheme by adopting a bundled approach (Gow 2007). This approach uses pre-assigned code values for each of the CAP sub-elements noted above. The issuer selects from a menu one of three priority levels—low, high, urgent—and the software interface automatically populates the CAP sub-elements with preset values mapped to an optional CAP sub-element <info.value>, designated as "Priority." This sub-element is then further specified by the sub-element <info.valueName> "Urgent," "High," or "Low" depending on the combination of urgency, severity, certainty sub-elements. Required actions are based on the assigned priority level: low priority (information only); high priority (prepare to take action; standby); urgent priority (take action immediately).

CAP Profile considerations for the RTBP project:

The research team recommended that RTBP adapt the simplified message prioritization scheme and ensure that message creation software provide users with a limited menu of choices based on this message prioritization scheme to enhance reliability and simplicity.

It was also noted by the research team that issuers and recipients would benefit from a clear understanding of conditions by which priority levels are to be assigned to alert messages, as well as corresponding actions.

2.8 Alert attribute {*event*}

Each message must indicate the event or incident type.

PHIN PCA Guide v1.0 does not specify a message attribute {event} but includes two related message attributes: *alertProgram* and *category*. Of these, only *alertProgram* is a required message attribute and is specified using CAP v1.1 required sub-element <info.event>. Enumeration values for this attribute refer to specific PHIN alerting

programs (e.g., HAN, Epi-X). The attribute *category* is specified using the CAP v1.1 required sub-element <info.category> and is always enumerated as "Health."

CAP v1.1 specifies that all messages contain sub-elements <info.category> and <info.event>. Sub-element <info.category> denotes the general category of the subject event of the alert message and must correspond to a range code values specified in CAP v1.1 standard. For the RTBP project, the code value "Health" is appropriate.

The code value for sub-element <info.event> is to provide "the text denoting the type of the subject event of the alert message" and is intended to be more specific than the <info.category> sub-element. CAP v1.1 does not provide specific code values.

CAP Profile considerations for the RTBP project:

Given the limited scope of the project to biosurveillance, was recommended that CAP v1.1 sub-element <info.category> be specified as "Health" for all RTBP alert messages. As such, message creation software developed for the project should automatically assign all RTBP alerts as "Health" messages using CAP v1.1 <info.category>.
It was also recommended, in contrast to the PHIN PCA Guide, that CAP v1.1 sub-element <info.event> be included in all RTBP alert messages to ensure CAP-XML compliance going forward.

With this consideration, the team recommended that RTBP message creation software provide a list of one or more RTBP-designated events corresponding to the foreseeable subject events of potential alert messages. There is a corresponding need to develop an event list and registry suited to the needs of a biosurveillance project.

2.9 Alert attribute {*message*}

Each message must include a description of the alert.

PHIN PCA Guide v1.0 refers to this as "the main message text" and specifies CAP v1.1 required sub-element <info.description> to convey this information. It is a required attribute in PHIN PCA Guide v1.0.

CAP v1.1 does NOT require messages to include the info sub-element <info.description>. The element is specified as "an extended human readable description of the hazard or event that occasioned this message."

CAP v1.1 also includes an optional info sub-element <info.headline> that provides "a brief human-readable headline … that SHOULD be made as direct and actionable as possible while remaining short. 160 characters MAY be a useful target for headline length."

In addition, CAP v1.1 includes an optional info sub-element <info.instructions> that provides "extended human readable instructions to targeted recipients" that describes "recommended action to be taken by recipients of the alert message." PHIN PCA Guide v1.0 specifies this sub-element for an optional message attribute *dissemination*

intended to provide instructions for sharing message information beyond the initial intended recipient.

CAP profile considerations for the RTBP project:

It was recommended that RTBP adopt CAP v1.1 info sub-element <info.description> to convey a human readable description of the event that occasioned the alert message.

Recognizing the need for a brief description of the alert, especially with respect to the use of small screen devices like mobile phones, it was also recommended that RTBP adopt CAP v1.1 info sub-element <headline> to convey a brief human readable message under 160 characters describing the event that occasioned the alert message.

It was also recommended that RTBP include consideration of CAP v1.1 info sub-element <info.instructions> for future implementation, when issuers might wish to provide recipients with specific directions in terms of responding to an alert message.

There is a need to develop procedures and guidelines for message texts pertaining to various alerts that will be issued during the RTBP project.

There is a need to ensure that message delivery software will correctly and reliably render message contents from <info.description> and <info.headline> sub-elements to correspond with long text, short text, and voice messages.

3. Summary

This paper has described the initial steps taken toward an implementation of CAP v1.1 as an alerting protocol for the Real-Time Biosurveillance Program (RTBP) initiative. The first step in such a process is the creation of a reference document that defines a required set of alert attributes, as well as vocabulary and valid value sets for a local instantiation of CAP. The RTBP implementation is an adaptation based on pioneering work done by the CDC-PHIN and released in 2008 under its PHIN-PCA Guide. The aim here is has been to illustrate an instantiation of CAP as derived from the PHIN-PCA Guide, highlighting a number of specific issues and considerations associated with health alerting for a biosurveillance project in a developing country.

4. References

CAP Cookbook. 2009. *CAP Fact Sheet*, Jan. 14 2009 [cited April 2009]. Available from http://www.incident.com/cookbook/index.php/CAP_Fact_Sheet.

Common Alerting Protocol Canadian Profile (v1.1) 2009. Industry Canada, May 8 2008 [cited April 2009]. Available from http://www.ic.gc.ca/eic/site/et-tdu.nsf/vwapj/CAPCPv1.1_May_8_2008_E.pdf/$FILE/CAPCPv1.1_May_8_2008_E.pdf.

Evaluating Last-Mile Hazard Information Dissemination (HazInfo) 2009. LIRNEasia 2007 [cited April 2009]. Available from http://lirneasia.net/projects/2006-07/evaluating-last-mile-hazard-information-dissemination-hazinfo/.

Gow, Gordon A. 2007. Implementing Common Alerting Protocol for hazard warning in Sri Lanka. *Journal of Emergency Management* 5 (2):50-56.

Organization for the Advancement of Structured Information Standards (OASIS). 2008. *Common Alerting Protocol v1.1 (CAP -V1.1)* 2005 [cited May 2008]. Available from http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf.

Sahana. 2008. *Sahana - Free and Open Source Disaster Management System*. Lanka Software Foundation 2008 [cited November 2008]. Available from http://www.sahana.lk/.

United States Centers for Disease Control and Prevention. 2008. *Public Health Information Network Communication and Alerting Guide (Version 1.0)*. Public Health Information Network (PHIN) - Guides, August 21 2008 [cited Sept. 2008]. Available from http://www.cdc.gov/phin/library/documents/pdf/PCA_Guide_V1.pdf.

Wagner, M. 2006. The Challenge of Biosurveillance: Introduction. In *Handbook of Biosurveillance*, edited by M. Wagner, A. Moore and R. Aryel. London: Elsevier Academic Press.