POLICY AND TECHNICAL ISSUES IN SYSTEMS OF EMERGENCY ALERTING

Many countries around the world leverage the Common Alerting Protocol (CAP) standard [1] to improve the effectiveness and efficiency of warning systems, especially in the context of public alerting. At all scales (city, province, country, region, global), such warning systems typically leverage CAP alert message sources as key inputs into the "situational awareness" processes that are crucial to emergency management, including when and where to issue warnings.

Although some information sources are local, some very important sources are external, including many of the most-trusted international sources. This is especially the case for large-scale hazards such as earthquakes, tsunami, tropical storms, "space weather", etc. In these cases, essential alert information and data is often available as CAP alert news feeds. Also, warning systems in many places worldwide leverage CAP to enhance dissemination of warning messages across all manner of communication media. Use of CAP helps an alerting authority reach people not only through Internet-based communications (e-mail, web sites, social media) but through: cellular and land-line telephones; radio and television broadcast and cable; satellites; digital highway signage; etc. It is also notable that CAP is embraced by commercial and NGO actors as well as governments, given that effective public warning often depends on public-private collaboration.

For these reasons, CAP is broadly recognized as the key standard for achieving the goal of multi-hazard, all-media public alerting. The World Meteorological Organization (WMO) endorses the CAP standard and encourages the 185 WMO Member states to adopt CAP in their national alerting systems. The International Federation of Red Cross and Red Crescent Societies (IFRC), the International Telecommunications Union (ITU), the International Association of Emergency Managers, among many others, also promote the CAP standard.

The primary target audience of this document is any set of officials and other actors who have a role in emergency alerting. In government, the set typically includes an emergency management and/or disaster agency, a telecommunications regulatory agency, a meteorological and/or hydrological service, public safety and other civic authority agencies, among many others. The set also includes non-government and commercial organizations such as Red Cross/Red Crescent National Societies, telecommunications companies, and intermediaries such as news and weather media and online social media.

TABLE OF CONTENTS

[1] The Common Alerting Protocol standard is formally designated as International Telecommunications Union (ITU) Recommendation X.1303. Specifications of CAP are available in two versions, 1.1 and 1.2, available from the CAP standard maintenance organization, OASIS, at http://docs.oasis-open.org/emergency/cap/

STRATEGIC AND POLICY ISSUES

PRINCIPLES AND SCOPE

Basic Principle of Alerting - Emergency alerting is widely accepted as a core responsibility of civilized societies across all cultures in the world today. In any particular national context, the emergency alerting responsibility may be rooted in various moral, ethical, constitutional, or legal principles. [2]

Equitable Access to Alerting - In the context of a system of emergency alerting within a particular society, government needs to be clear whether the system will try to alert all people affected, and whether that also includes people who are not legal citizens. Government must enlist a range of media for alerting because some media (e.g., sirens, SMS messages) can only get a person's attention while other media can more fully instruct. Also, depending on a person's activities at the moment, quite different media are needed to communicate an alert to him/her. Government should be very clear about the degree to which attempts will be made to alert people with special needs (e.g., people who are blind, deaf, cognitively impaired, or illiterate), and people who do not understand the official language(s) of the area.

Multi-hazard, All-Media - This document focuses specifically on meeting the public alerting responsibility by means of a system of emergency alerting that helps to communicate alerts to people whose lives may be in danger. Because lives can be threatened by all manner of hazards and all communications media are potentially useful in alerting, such emergency alerting should be "multi-hazard" and "all-media" by design.

Digital Telecommunication Networks as a Backbone - Many different means are needed to accomplish effective communications for public emergency alerting, depending on the particulars of the threat and the people who need to be alerted. At the end point, the alert may be communicated by a siren, an official with a megaphone, a person-to-person conversation, an e-mail, an emergency alerting app, and many other means. This document focuses on using digital telecommunication networks as a backbone infrastructure, of which the prime example today is the Internet. The Internet is now, and will likely remain, essential to the public emergency alerting function for the great majority of hazard threats affecting groups of people in modern societies. Other networks, such as radio and television broadcast, cellular telephone services, landline telephones, and digital signage, are end-delivery mechanisms from the alert distribution perspective.

Alerting Here is Messaging Only - Any communication of alerts to people begins with the means to perceive a potential or actual hazard threat. However, those aspects are not the subject of this document. For the purpose of this document, alert communication starts when a message sender decides to warn people of a hazard threat by means of a system of emergency alerting. The alert communication ends when people receive the alert message. Actions taken subsequent to receipt of the alert message are also not in scope of this document.

CROSS-SECTOR COLLABORATION IS ESSENTIAL

Collaboration among Government, Commerce, and NGO's - For a modern society to implement effectively and efficiently the digital telecommunication networks component of public emergency alerting, it is necessary to have collaboration across the three major sectors: government, commerce, and non-government organizations (NGO's). In the government sector, major actors are typically government agencies with a specific hazard threat mandate and other agencies with a civil protection mandate. In the commerce sector, major actors include telecommunications companies, news organizations, and various other actors that may help with emergency alerting for a variety of reasons. NGOs include a range of emergency preparedness and response actors, including some with a trusted and essential presence at the local community level.

Distinguishing Official Sources of Alerts - The system of emergency alerting needs to distinguish official sources from other sources of alerts. This applies both in labeling its own alerts as official and in making use of alerts that originate elsewhere. An important resource for these purposes is the international Register of

[2] The Universal Declaration of Human Rights, Article 3, states: "Everyone has the right to life, liberty and security of person" (see http://www.un.org/en/universal-declaration-human-rights/) Article 3 of the Declaration of Human Duties and Responsibilities asserts that States "shall take positive and effective measures to protect and enforce the right to life" and that "Individuals and non-State actors [...] have a duty to take reasonable steps to help others whose lives are threatened." (see http://globalization.icaap.org/content/v2.2/declare.html)

Alerting Authorities [3], maintained by WMO. Because WMO is a treaty-level organization, each national assertion that a source is official has the force of law for the country making that assertion in this Register. About 500 official sources, including all of the Red Cross and Red Crescent National Societies, are currently listed as alerting authorities in this international Register. For alerting sources not known to be authoritative, government might need to consider if it should, or could, restrict media and online access by such alert sources, internal to or external to the country. An additional consideration is to establish clear policy regarding the practice of re-originating alerts (i.e., receiving an official or unofficial alert and sending out a modified version of the alert, either officially or unofficially).

Private and Public Alerting - Although public alerting is a primary theme of this document, most systems of emergency alerting include some private messaging about hazard threats as well. Alerting authorities in different jurisdictions may send alerts privately so that the appropriate authority can send public alerts if they so decide. The initial report of an emergency situation is often a private message to the local emergency call center. Private messaging is also common as experts or security personnel communicate with emergency managers about a given hazard among themselves as a threat is being evaluated. Also, there are certainly private messages about suspicious activity before any public alert concerning terrorism. It is a choice to what degree any particular system of emergency alerting includes some of this private messaging, but there are obvious efficiencies when relevant private alerting is designed to be interoperable with public alerting.

KEY ROLES MAY BE VOLUNTARY

Voluntary Collaboration Policies - It seems certain that at least some of the actors playing a crucial role in the operational system of emergency alerting will be executing their role on a voluntary basis. For example, amateur radio is often a voluntary adjunct to official telecommunications facilities. Also, in the event that cellular telephone services are not compelled to disseminate official, high-priority alerts, public demand as a market force may motivate a cell service provider to voluntarily deliver life-critical alerts via "cell broadcast". The cell broadcast technology is understood to be especially crucial for "sudden-onset" threats, where seconds can mean the difference between effective warnings and warnings that arrive too late. Regardless of which technologies are involved, an effective system design must take voluntary participation into account, just as it must take into account that a severe and widespread emergency might compromise crucial components of the system of emergency alerting, including some official systems that were mandated to remain operational.

ROLES AND RESPONSIBILITIES MUST BE CLEAR

Alerting at Local to National Levels and Beyond - The system of emergency alerting will certainly involve many actors at different levels: local community, municipality, state, national, and international. It is important to define clearly what are the respective roles and responsibilities of these actors within and across these levels. These definitions of roles will have an effect on the allocation of resources and certain details of the system design, especially the degree to which the operational system will be centralized. Here it should be noted that hazard events are far more common at the local community and municipality level. However, even if alerting for local situations is accomplished without higher-level involvement, higher-level organizations could have awareness of these local situations simply by monitoring the local CAP news feeds that are part of the system of emergency alerting. This capability is important in those cases where a particular local situation evolves to the point of needing involvement by broader-scale organizations. Also, because alerts often span jurisdictions, trans-border coordination of alert messaging is necessary to minimize confusion.

Describing a Hazard Threat as Distinct from Alerting the Public - It is important to clearly define at each level if there is a distinction among the roles of alerting authorities. For example, it is typical that the role of a scientific agency is to *characterize* a particular hazard threat, as distinct from the role of a civic authority to actually *instruct* people in how to deal with the particular hazard threat. In the context of CAP-enabled alerting, it is common in this situation that two separate CAP alerts are issued. The CAP alert issued by the scientific agency would have relatively technical text in the CAP "description" element and might include CAP "parameter" elements with detailed data (e.g., earthquake depth). But in the CAP "instruction" element, that CAP alert would have general text saying something like "Monitor local media for specific instructions from civic authorities". At the same time, a CAP alert issued by the civic authority would have a CAP "description"

[3] The international Register of Alerting Authorities is at http://www.wmo.int/alertingorg An alerting authority can include in its records within the Register the URL of an alert news feed. For example, the record for the U.S. National Weather Service record lists this feed: https://alerts.weather.gov/cap/us.php?x=0

element citing in general terms the message of the scientific agency. But in the CAP "instruction" element, that civic authority CAP alert would provide specific details such as recommended evacuation routes.

Roles of Alerting Collaborators Beyond Government - The system of emergency alerting needs to be clear as to what roles are appropriate for non-government actors in emergency warning, including commercial or public news media and the National Red Cross/Red Crescent Society [4], among others. Some alerting services may be offered to people by entities based outside of the country, such as AccuWeather, Samsung [5], and Google [6], among others. We can also expect: that radio and television could deliver alerts as Public Service Announcements, that cellular telephone services could deliver alerts through their cell broadcast capability [7], that online advertisers could disseminate public warnings through the overlay of online ads, and that billboard companies could display alerts through their digital signage resources [8], among other possibilities.

Intellectual Property Rights and Attribution of Alerting Content - Clarity is needed as to the legal rules for intellectual property rights and attribution on the contents of alerts and alert services, and the manner by which rights and attribution are expressed. [9] Here consideration might be given to classifying alerts as a kind of news story, thereby allowing the system of emergency alerting to inherit the body of existing ethical codes, laws and precedents applicable to the journalism profession and news industry.

Commerciality Issues in Public Alerting - It is important to consider if there is a need for specific rules applicable to the range of non-government, public alerting services. This may also require a further distinction for those entities offering emergency alerting services on a for-profit basis. For instance, there may be equitable treatment issues if companies are allowed to market alerting services on a "tiered scale" where subscribers can buy enhanced alerting or evacuation advice capabilities for a fee.

Privacy Issues in Public Alerting - To target alerts to people who are in the alerting area, components of the system of emergency alerting will need to exploit geo-location information, such as which subscribers are in range of particular cell towers. When geo-location is very precise, personal privacy can become an issue. In this regard, the system of emergency alerting may need a blanket prohibition against the collection of personally identifiable information, including a limit to the precision of geo-location. [10]

Sustaining Public Trust in Emergency Alerting - Especially in an intense emergency, it is crucial that the public has a high degree of trust in the alerting authorities who send out alerts. Obviously, trust is eroded when official authorities fail to alert or accidentally issue a test alert as though it were an actual alert. Yet, trust can be eroded also by inadvertent "over-warning" for hazard threats that are diffuse in area and/or less than urgent, severe or certain. Trust can also be compromised if people in a given alerting area receive conflicting alerts for a given hazard threat because distinct alerting authorities characterize the threat differently or provide different instructions. Even the inadvertent issuance of duplicate alerts can cause people to wonder if their alerting authorities are collaborating as they should. In the event of a high-priority alert, people usually appreciate when alerting authorities issue an "all clear" message after the high-priority threat is over. The system of emergency alerting should have processes to be informed when trust issues arise and policies to take corrective actions such as education, outreach, testing and exercises.

LEVERAGING THE COMMON ALERTING PROTOCOL (CAP) STANDARD

The CAP Standard is Essential - In many emergency alerting systems already or soon-to-be implemented in societies worldwide, the CAP standard is regarded as essential to building a "multi-hazard" and "all-media" alerting system that leverages existing digital telecommunication networks within the country and internationally. Moreover, deploying a CAP-enabled alerting system leverages a vast array of already available

[4] The CAP-enabled Red Cross Hazards App is described at http://preparecenter.org/content/hazard-app
[5] Samsung Geo News is described at http://www.samsung.com/ie/support/skp/faq/1061356
[6] Google Public Alerts is described at https://support.google.com/publicalerts/
[7] Cell broadcast is described at http://www.eena.org/ressource/static/files/2011_11_17_one2many.pdf CAP-based cell broadcast in the United States is known as the Wireless Emergency Alerts system.
[8] An example of emergency alerts being displayed via highway digital signage is described at http://www.lamar.com/About/givingback/Community/EmergencyAlertSystem
[9] Creative Commons licenses are a popular mechanism for rights and attribution of electronic resources. Creative Commons licenses are described at https://creativecommons.org/
[10] A privacy issue arises when geo-location information is precise enough to identify an individual. Here It may be of interest that the Network Advertising Initiative Code of Conduct asserts "Use of Precise Geo- location Data for Interest-Based Advertising shall require a user's Opt-In Consent." (see http://www.networkadvertising.org/2013_Principles.pdf)

and relevant alerts provided by neighboring countries and international institutions such as the WMO, the World Health Organization, and the IFRC, among others.

CAP Provides the Content Definition for Alert Messaging - In its essence, a CAP alert can be seen as a kind of standard business form. Like any other business form, a CAP alert defines various value selections, fill-in boxes, and check boxes that together provide key details of a specific emergency, such as the type of event, the alerting area, the headline, the sender, and so on. That set of information, the CAP-compliant content, is then communicated in the form of an Extensible Markup Language (XML) file as a CAP alert message. This communication is typically accomplished by the sender putting the CAP alert file on a publicly accessible Internet host and updating a news feed that links to that CAP alert file. Subscribers to that news feed then retrieve the CAP alert file as they would retrieve any other news item.

CAP Messaging in the system of emergency alerting - At a functional level, an essential success factor of the system of emergency alerting is that it facilitates CAP alerts being sent reliably and securely through digital telecommunication networks and other means, in time to warn people in the alerting area for the particular hazard threat. Already, CAP alerts can be of immediate use for alerting across virtually all sectors: civil protection, firefighting, health, safety, law enforcement, schools/universities, transportation, hotels, embassies, intelligence, etc. Local siren control systems may be already equipped to handle CAP alerts automatically. [11] Local broadcast television and radio stations may have already installed equipment that automatically interrupts programming to insert the CAP alert as a television "crawl text" or audio message. [12] Perhaps the most common technical interface for such automated alerting devices today is the interface specified for the Emergency Alert System (EAS) in the United States. Eventually, the applications for CAP-enabled alerting will expand dramatically as CAP alerts are increasingly generated by devices and used by devices. An example of this trend is seen in the upgrading of home smoke alarms to become all-hazard alarms simply by adding an inexpensive cell broadcast receiver. However, we should not expect legacy alerting systems to disappear quickly. CAP-enabled systems will co-exist with legacy alerting systems for the next decade or more in many communities.

Standardized Alert Messages Facilitate Analysis - Having a set of alert messages in the standard CAP format greatly facilitates analysis of the degree to which dissemination has been effective. This analysis can be conducted after the event, resulting is a document typically known as an "after-action report". Depending on the dissemination methods, this analysis can also be done in real-time during the event, giving a kind of "heat map" showing areas where dissemination is being less effective than desired.

CAP PROFILE POLICY

Policy on CAP Usage Guidelines - Any special requirements or preferred practices applicable to the sending or receiving of CAP messages should be communicated to all actors that process CAP messages. This typically includes the content of specific CAP elements for which the system of emergency alerting needs to specify a required or preferred usage. Such CAP-specific requirements are sometimes conveyed through a "CAP Profile" or "Best Practice Recommendations". Whenever a CAP Profile is specified, there must be a clear policy on how to handle a CAP message that is not compliant with that CAP Profile. For example, the policy might state that such a message must be ignored as invalid. Yet, such a policy would seem harsh in the case of a life-critical alert, and that policy might be impossible to enforce worldwide. A better alternative might be that the policy asserts that the message can be disseminated but the alert source will receive a follow-up directive to fix the non-conforming content. This alternative policy would also address the common situation wherein some alert dissemination actors do not regard themselves as compelled to check CAP Profile conformance. The second section of this document provides notes on various issues that might be addressed in a CAP Guidelines document.

[11] In 2015 an "Outdoor Warning Sirens Market Survey Report" was published and is available at https://www.dhs.gov/sites/default/files/publications/Outdoor-Sirens-MSR_0315-508.pdf.

[12] For example, the CAP-enabled radio interrupt equipment in Dominica is an "Emergency Alert Encoder/Decoder" made by Digital Alert Systems of New York. Its interface specifies that the CAP alerts are accessed via an ATOM or RSS news feed.

NOTES ON TOPICS FOR A CAP GUIDELINES DOCUMENT

CAP ALERT NEWS FEEDS

Preference of CAP Alert News Feed Format - CAP alert feeds published on the Internet could use either of two standard XML formats for news feeds: Really Simple Syndication (RSS) or Atom. The system of emergency alerting should specify whether there is no preference between these two formats, a preference for RSS, or a preference for Atom. It is noted here that: RSS is the more common format, RSS is adequate for the purpose of a CAP news feed, and RSS will not change over time. The OASIS Emergency Management Technical Committee (OASIS EM TC), maintainer of the CAP specification, published a guide titled "Example Practices: CAP Feeds". [13]

Mapping of Element Values between CAP Alerts and RSS Items - If RSS is the preferred or required Internet news feed format, it would be useful to suggest how the values in an RSS item can be populated using values of the CAP alert elements, plus the CAP file URL. Here is an example mapping:

RSS channel/item/title	CAP alert/info/headline
RSS channel/item/link	CAP file URL
RSS channel/item/description	CAP alert/info/description
RSS channel/item/author	CAP alert/sender
RSS channel/item/category	CAP alert/info/category
RSS channel/item/guid	CAP alert/identifier
RSS channel/item/pubDate	CAP alert/sent

VALIDITY, ENCRYPTION, AND AUTHENTICATION OF CAP ALERTS

Validating CAP Alerts - As mentioned earlier in this document, a CAP alert must be packaged as a file of type XML. The XML content of the file must be valid according to the currently adopted CAP schema version. The system of emergency alerting should specify which version of CAP (1.1 or 1.2, as of this writing) is preferred or required, which may change over time. [14] It is noted that CAP version 1.2 is widely supported and is only slightly different than version 1.1.

Encrypting CAP Alerts - It is likely that many, perhaps most, CAP alert messages communicated through the system of emergency alerting will not be intended for public dissemination. To protect against unintentional disclosure of alert message content, encryption on communications links should be applied. For messaging over the Internet, such encryption is accomplished using HTTPS.

Authentication of CAP Alerts - Emergency alerting should be regarded as a likely target for malicious attacks, which can include attempts to send deceptive CAP alerts. The system of emergency alerting should state if a digital signature is required to provide assurance that the content of the CAP alert as received is identical to the content of the CAP alert as sent.

HIGH PRIORITY ALERTS MUST BE EASILY DISTINGUISHED

Need to Distinguish High-Priority Alerts - The term "high priority" refers to alerting situations in which people should be alerted in a "broadcast intrusive" manner, such as sounding a siren, inserting a television "crawl text", sending a cell broadcast message, etc. This is usually reserved for situations in which people need to act: immediately or within the next hour, in response to an extraordinary or significant threat, that is already observed or is likely to occur. (These correspond to the top two values of Urgency, Severity, and Certainty in a CAP message.) Although high priority alerts are less than one percent of the alert messages typically accessible to the public, such messages are especially crucial to enable people to preserve life and protect property. [15] Also, given the intense nature of a high-priority alert, alerting authorities should issue an "all clear" message after the high-priority threat is over.

---

[13] The OASIS EM TC guide named "Example Practices: CAP Feeds" is at http://docs.oasis-open.org/emergency-adopt/cap-feeds/v1.0/cap-feeds-v1.0.html

[14] The XML schema for CAP alerts is found in the specifications, versions 1.1 and 1.2, at http://docs.oasis-open.org/emergency/cap/

[15] The IFRC Global Disaster Preparedness Center "Guide for Identifying High Priority Public Warnings" is at http://preparecenter.org/resources/universal-app-identifying-high-priority-public-warnings

Criteria to Distinguish High-Priority Alerts - The designation "high priority" should be defined as any valid CAP alert that satisfies these six criteria for specific CAP element values:

alert/status = Actual	(not = Exercise, System, Test, nor Draft)
alert/msgType = Alert or Update	(not = Cancel, Ack, nor Error)
alert/scope = Public	(not = Restricted nor Private)
alert/info/urgency = Immediate or Expected	(not = Future, Past, nor Unknown)
alert/info/severity = Extreme or Severe	(not = Moderate, Minor, nor Unknown)
alert/info/certainty = Observed or Likely	(not = Possible, Unlikely, nor Unknown)

ALERTING OF SUDDEN ONSET SITUATIONS

Special Handling Needed for Sudden Onset Hazards - The term "sudden onset" refers to alerting situations in which the hazard might occur so quickly that people need to be alerted in seconds. Typical examples of such hazards include earthquakes, tsunami, tornadoes, dam failure, flash floods, landslides, avalanches, toxic chemical spills, active shooter incidents, terrorist attacks, etc. One implication of this situation is that time may not allow for a "human in the loop". That is to say, detection of the situation by sensors or other means may be directly and automatically tied to issuance of a CAP alert. The subsequent dissemination must then be as fast as possible. If carefully designed, an alerting system should be able to limit delays to only a second or two from the posting of a CAP alert to having that alert trigger sirens and cell phones in the alerting area.

SUGGESTIONS FOR VALUES IN SPECIFIC CAP ALERT ELEMENTS

Example Practices for CAP Elements - The OASIS EM TC published a useful guide named "Example Practices: CAP Elements". [16] This guide contains notes on these topics pertinent to CAP alerts: Optimize alert areas, Include useful descriptions and instructions; Take care with XML encoding; Customize urgency, severity, certainty to event; Provide rich content by linking to resources; Prepare CAP Usage Documentation; Public Alert Aggregators Should Ignore CAP Messages with a Restriction Element; Alerts that span jurisdiction boundaries; Alert updates; and, Alert information expiration.

Usage of Particular CAP elements - In addition to the OASIS EM TC suggestions, the system of emergency alerting could consider providing guidance on the usage of particular CAP elements such as those described here following.

CAP element - alert/identifier: Many countries are using CAP Object Identifiers (OIDs) that are tied to the international Register of Alerting Authorities. This identifier scheme assures that each CAP alert has a globally unique identifier that is also traceable to the particular official alerting authority which sent the alert. [17]

CAP element - alert/sender: It is considered good practice that the sender value contains an e-mail address leading to an inquiry function that can respond when necessary.

CAP elements - alert/status, alert/msgType, and alert/scope: The system of emergency alerting could define more precisely what is regarded as appropriate use of the allowed values of the status element (Actual, Exercise, System, Test, and Draft), the msgType element (Alert, Update, Cancel, Error) and the scope element (Public, Restricted, Private). However, it is very important to understand that the value of "Cancel" in the CAP msgType element means the referenced alert was a mistake; it does not mean that the hazard threat has resolved. To indicate a hazard threat has resolved, one would issue a CAP alert with msgType value of "Update" and a responseType value of "AllClear".

CAP element - alert/info: The system of emergency alerting should prohibit more than one "info" element in a single CAP alert. Although Canada, for example, uses two info elements in order to carry English and French in a single alert, this practice does not align with common practice of Internet news feeds. A news feed is expected to have one language, so the CAP alerts linked from that news feed should also have just one language. Also, some current EAS technology only processes the first "info block" of a CAP message.

---

[16] The OASIS EM TC guide named "Example Practices: CAP Elements" is available at http://docs.oasis-open.org/emergency-adopt/cap-elements/v1.0/cn01/cap-elements-v1.0-cn01.html

[17] Common questions about OID's are addressed at http://www.oid-info.com/faq.htm For example, OIDs for CAP alert messages from Dominica Meteorological Services start with "urn:oid:2.49.0.1.212.0.", which identifies the country (212 is the ISO 3166 numeric code for Dominica), and an alerting authority in Dominica (0 for Dominica Meteorological Services). OIDs can have any number of periods, but only positive numbers (not zero filled) between the periods.

CAP element - alert/info/language: The system of emergency alerting should specify use of the two-character language code, rather than the five character code for a country variant of the language.

CAP elements - alert/info/urgency, alert/info/severity, and alert/info/certainty: The system of emergency alerting should prohibit use of "Unknown" value in these elements. This is necessary because many deployed CAP systems handle "unknown" incorrectly, treating the respective values as "not urgent", "not severe", and "not certain".

CAP element - alert/info/web: The system of emergency alerting could use this element to link to online information that provides practical guidance for people reacting to the alerts, such as where to find shelter. Such online information is available from the Mexican Red Cross, for example.

CAP element - alert/info/area/geocode: Although the use of geocode values is allowed by the CAP standard and is sometimes useful to distinguish an area very accurately and precisely, it should be understood that some actors in alert dissemination will not have access to the particular gazetteer function necessary to convert the given geocode values to lat/lon polygons. For this reason, the system of emergency alerting should require that the corresponding polygon is also included in each CAP alert.

ALERT CONTENT SHOULD BE EASILY UNDERSTOOD

Templates with Stock Phrases - There appears to be broad consensus that an alert composer should incorporate "stock phrases" in emergency alert messages [18] and such phrases are often part of a "template". For instance, templates for 20 common emergency alert situations were developed as part of the Regional Risk Reduction Initiative in the Caribbean and are feely available. [19] A more comprehensive set of field-verified alert messages is given in the IFRC Public Awareness and Public Education Messages (PAPE). [20] As one instance from the IFRC PAPE set , the message for a Typhoon alert would be:

> 1. Prepare to evacuate, and know when and where to evacuate
> 2. Turn off utilities and gas tanks. Unplug small appliances
> 3. Never try to drive through flood waters. Turn around and go the other way

Predefined Alert Areas - In some situations, the public should be aware of areas that have a well-known risk for a particular hazard. Examples include areas near active volcanoes and the "tsunami-aware communities" that have distinctive signage and other education. In a CAP-enabled alerting system, the official alerts should include polygons matched to these pre-defined areas.

Communicating Uncertainty - An ongoing challenge for alerting authorities is to communicate uncertainty in a way people understand and different techniques have been employed for different kinds of hazard threats. [21] Given that every person is potentially faced with hazards of many different types, the communication of uncertainty ought to be approached from a multi-hazard perspective.

Impact-Based Alerting - A current trend in making alerts more understandable is to focus more on the impact of a hazard on people and what actions they need to take, as distinct from describing the hazard itself. The CAP standard facilitates this trend to some degree because the CAP instruction element is distinct from the CAP description element, in contrast to traditional free text alerts wherein instructions are mixed with descriptions in a narrative crafted in a bulletin or press release style. [22]

Text-to-Voice and Automated Language Translation - Technologies for text-to-voice and for automated language translation have improved dramatically so that now it is often feasible to offer emergency alerts in

---

[18] Janoske M, Brooke L, Sheppard B. Understanding Risk Communication Best Practices: A Guide for Emergency Managers and Communicators. Final Report. College Park, MD, USA. http://www.start.umd.edu/start/publications/UnderstandingRiskCommunicationBestPractices.pdf

[19] Templates for twenty common emergency alert situations (in Dutch, English, French, Spanish, and Papiamento) are feely available at https://docs.google.com/file/d/0B5FiAsl5yGbZUHZkWnE1Y2I5aTg/

[20] The IFRC Public Awareness and Public Education Messages are available at: http://www.ifrc.org/PageFiles/103320/Key-messages-for-Public-awareness-guide-EN.pdf

[21] Gill J. Guidelines on Communicating Forecast Uncertainty (PWS-18). Technical Document. Geneva, Switzerland; World Meteorological Organization, Public Weather Services; 2008. WMO/TD No. 1422. http://www.wmo.int/pages/prog/amp/pwsp/documents/GuidelinesonCommunicatingUncertainty_TD-4122.pdf.

[22] see WMO Guidelines on Multi-hazard Impact-based Forecast and Warning Services / Directrices de la OMM sobre servicios de predicción y aviso multirriesgos que tienen en cuenta los impactos

real time in several languages. That is especially the case with CAP messages because much of the key content is expressed in coded values, and these can have associated text in many languages, pre-packaged for use.

Message Distribution Constraints - Many CAP-enabled systems distribute alert messages with only text and coded values and these messages average only a thousand bytes (characters) or so. But some systems embed extra content, for example an audio file to directly support messaging over radio. Such embedded content can enlarge the CAP message to millions of bytes. It is clear that the larger a message, the less broadly it can be distributed unchanged. Wherever possible, large content should be referenced from the message rather than embedded in the message. Also, it may be of interest that the US Emergency Alert System (EAS) sets an alert text limit of 1800 characters. [23]

GLOSSARY OF TERMS

alerting authority - an organization designated by a nation as authoritative in the context of alerting, typically listed in the international Register of Alerting Authorities

Atom (Atom Syndication Format) - Atom is an XML format used for web feeds, alternative to Really Simple Syndication (RSS)

CAP (Common Alerting Protocol) - an XML-based data format for exchanging public warnings and emergencies between alerting technologies

EAS (Emergency Alert System) - the national public warning system of the United States

HTTPS (Hypertext Transfer Protocol Secure) - the use of Hypertext Transfer Protocol (HTTP) with Secure Socket Layer (SSL)

IFRC (International Federation of Red Cross and Red Crescent Societies) - the world's largest humanitarian organization, with 190 member National Societies

OASIS EM TC - OASIS (Organization for the Advancement of Structured Information Standards), Emergency Management Technical Committee

OID (Object Identifier) - a hierarchically-assigned identifier expressed using the ASN.1 (Abstract Syntax Notation) standard, X.690, defined by the International Telecommunication Union

Red Cross and Red Crescent National Societies – National Societies are the independent members of the IFRC, typically having a formal auxiliary role to their national governments

RSS (Really Simple Syndication) - RSS is an XML format used for web feeds, alternative to Atom

Register of Alerting Authorities - an online facility maintained by the maintained by the World Meteorological Organization and the International Telecommunication Union

URL (Uniform Resource Locator) - an Internet address usually consisting of the access protocol, the host domain name, and optionally the path to a service or resource accessible on that host

SMS (Short Message Service) - a text messaging service component of phone, Web, or mobile communication systems

SSL (Secure Socket Layer) - encrypts data being transmitted so that a third party cannot understand it

WEA (Wireless Emergency Alerts) - emergency messages sent by authorized U.S. government alerting authorities through mobile carriers

Internet news feed - data in the format of either ATOM or RSS, used for providing users with frequently updated content

ITU (International Telecommunications Union)

XML (eXtensible Markup Language) - a set of rules for encoding documents in a format that is both human-readable and machine-readable

[23] From section 3.6: "Constructing Alert Text from CAP V1.2 IPAWS v1.0 Profile for EAS Activations" in the Guide at http://www.eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf