MEETING OF GOVERNMENTAL EXPERTS
ON EARLY WARNING AND CONFLICT PREVENTION
KEMPTON PARK, SOUTH AFRICA
17 – 19 DECEMBER 2006

PSD/EW/EXP/7(I)
Rev.1

MEETING THE CHALLENGE OF CONFLICT PREVENTION IN AFRICA – TOWARDS THE OPERATIONALIZATION OF THE CONTINENTAL EARLY WARNING SYSTEM

BACKGROUND PAPER NO. 2

DEVELOPMENT OF THE INFORMATION TECHNOLOGY SOFTWARE FOR THE CONTINENTAL EARLY WARNING SYSTEM

This document does not necessarily reflect the views of the African Union
1. **INTRODUCTION**

1.1. **Purpose:** The purpose of this background paper is to present Information and Communications Technologies (ICT) software requirements and specifications for the African Union’s (AU) Continental Early Warning System (CEWS). The specifications are framed by the recommendations made in the CEWS “Roadmap” document drafted in July 2005 that emphasized that the objective of the CEWS is the provision of timely advice on potential conflicts and threats to peace and security, to enable the development of appropriate strategies to prevent or limit the destructive effects of violent conflicts.

1.2. **Objectives:** The specific objectives of this background paper involve an explication of the ICT requirements for the establishment of the CEWS, including the linkage between the AU and the Regional Mechanisms for Conflict Prevention, Management and Resolution, as outlined in the July 2002 Protocol Relating to the Establishment of the Peace and Security Council (PSC). This paper also makes recommendations on the specifications for the ICT software applications that would be used for data collection and analysis. Finally, this paper makes recommendations on the requirements for the Situation Room to play its role as outlined in the PSC Protocol.

1.3. **Guidelines:** Four guidelines emerged from an October 2003 workshop that brought together the Regional Mechanisms and other relevant international organizations and institutions, to look into the modalities for the establishment of the CEWS. These guidelines serve to prioritize certain aspects of the recommendations as follows:

   a) begin with significant threats of violence and loss of life;
   b) build a measurable, verifiable and standard database that is simple, user friendly, based on multi-leveled and field-based sources;
   c) develop an analytic capacity and expertise within the AU on early warning, conflict prevention and conflict management; and
   d) establish diagnostic linkages between analysis and desired outcomes, so as to provide the AU with regular reports on conflict situations.

1.4. **Approach:** In addition to the guidelines outlined above, this paper is informed by a data-driven analysis approach to early warning. In other words, CEWS is to be draw upon timely, systematic monitoring of social, economic, political and environmental conditions, activities and events, assess their trends prior to escalation to instability or violence, and formulate response options that seek peaceful, sustainable resolutions to conflicts. Such a data driven analysis approach can produce the baselines required for effective early warning.
This approach seeks to support and leverage human analysts as they observe and record more systematically their assessments of evolving situations. It is important to note that the structure and automation recommended herein does not seek to replace the human element in the assessment of conflict situations; rather by leveraging analysts’ limited time and resources, CEWS can allow them to focus more on interpretation and action rather than gathering, filtering and finding information.

Specifically, the CEWS recommendations herein are designed to produce baseline measures, which are critical for tracking the escalation and de-escalation of volatile situations. This approach supports the kind of systematic measurement of precursors to violence, humanitarian crises and situations of instability required of any early warning and response system. Without empirically driven baselines, early warning alerts and measures of success are too often idiosyncratic and a matter of contention as they are typically based on impressions rather than systematic observation and analysis.

When field report baselines are developed and updated regularly they can be used to monitor a range of indicators as they move toward crossing empirical thresholds generated from the specific context in question. As these baselines are developed over time, thresholds can be specified and the relevant analyst or unit can be automatically notified and presented with a menu of pre-defined response options based on prior contingency planning.

This data driven approach to early warning thus can provide the AU’s Conflict Management Division (CMD) with baselines for political, economic, social, military and humanitarian indicators specific to the African Union. For example, if a series of situation reports reveal migration within a particular country above a certain threshold, it may signal that this movement is likely to escalate into violent conflict. The CMD can thus focus on this issue, analyze its circumstances, and make appropriate recommendations.

No phenomenon evolves in a vacuum. Indicators chosen to track dynamic events need to be considered in the unique social, political, economic and environmental contexts in which they were monitored. For example, a baseline of internal migration over a year might suggest a recurring pattern. This pattern may very well be explained by regular variations in the environment that is the proximate cause for what amount to seasonal cycles. One way to validate (support or refute) this interpretation would be to examine the trend of internal migration against an overlay of rainfall or temperature or some other aspect of seasonal variation. This kind of contextualization of the dynamic data contributes not only to the interpretation of the results, but it also enhances their communication.

Other examples of structural contexts that need to be considered in the present data driven approach to early warning include demographics, religion, politics and the economy. Differences in these and other structural attributes of a country differentially affect the risk propensiy or vulnerability of a given area even in the face of similar events. Structural indicators are used in risk assessments to better determine the likelihood of some form of violence or instability within a particular setting.
Another feature of the present data-driven approach is its inclusion of positive/cooperative indicators as well as negative/conflictual indicators. Monitoring positive incidents can help inform appropriate response strategies for building local capacities and sustaining peace as well as preventing conflict. Also, the inclusion of gender-specific and age-related dynamic indicators may be useful in illuminating costs of conflict that might otherwise be overlooked. A solid orientation, explicit understandings and quality control are all required if gender and age issues are to be “seen” in the data.

1.5. Assumptions: Several key assumptions undergird the paper’s recommendations. Perhaps the single most important consideration is that the ICT system, as central as it is to supporting the early warning objective, it is not the essential component. Rather the analytic capacity of the staff is explicitly recognized as the locus of the early warning process. Thus capacity building to secure and sustain these analytic skills is emphasized. A sustainable solution is also sought. Likewise, customized, cost-effective technologies, tailored to the institutional requirements and suitable for the conditions are therefore explicitly invoked.

Two additional assumptions are operative herein. The first is that the indicators and information to be monitored are to come from a variety of open sources. Since the quality of the data and analyses are critical to their value for generating early warnings, a provision for independent academic assessments has been invoked. This approach is not just consistent with the open source transparent system stipulated by the PSC Protocol, but it is also critical to assuring that the ongoing data collection and analysis remain rigorous, systematic and credible.

The other assumption emphasized herein is the explicit recognition of the integral role that Regional Mechanisms, including their civil society counterparts, are to play in the overall security architecture of the African Union. Thus the tasks of harmonizing, coordinating and working closely with Regional Mechanisms and their civil society partners are considered central to CEWS, and in particular, these tasks are to be integrated into the core information collection and analysis activities of the Situation Room.

Two final comments are in order in this discussion of operative assumptions. We assume that at any given time the substantive content of the system (i.e. the indicators, parameters and their respective scaling) can be improved. Thus the objective is to seek an extensible system in terms of the refinement of the contents, but also in terms of software functionality extensions and upgrades. It is also assumed that at any moment, the software system may fail, if only briefly. The early warning operation must continue, however, so we urge that all electronic procedures have “paper” alternatives. At the very least, all automated procedures must be transparent and well documented so the Situation Room as well as the field staff can function in the case of intermittent outages.

2. Overall Description

2.1. Usage of Key Terms: The term system as applied to software is sometimes used to refer to the software per se, that is the software application. However, since the
term “system” is part of the acronym applied to the Continental Early Warning System, its meaning here refers more broadly to the units within the AU responsible for early warning, their governmental and nongovernmental partners, the information they collect, their communications and exchanges, the analyses they conduct, and their formulation of timely advice on potential conflicts and threats to peace and security.

From this expansive perspective on the Continental Early Warning System, the operational anchor of CEWS is the Situation Room due primarily to its central role in information collection. In other words, the Situation Room may be considered usefully as the hub of CEWS software, and the focus of discussion with respect to software applications’ requirements and specifications. To set CEWS, and particularly its Situation Room, in its ICT context, this paper next describes the nodes of information within the system, the types of information to be collected and/or monitored, its management and analysis, and the communication of the results.

2.2. Nodes of the System: The primary information nodes for CEWS are identified in the draft Roadmap document. Specifically, the Situation Room plays a central role in the collection of information for the system. This central role is bound organizationally to the early warning unit within the Conflict Management Division.

The relationship between the Situation Room as an information provider and the Early Warning Unit as the focus for analyzing that information is interactive and iterative. Actually, the distinction between these two nodes is more functional than organizational. They work together as a single organizational unit to define, compile, analyze and manage the strategic assessment process. The Situation Room is also linked to reporting channels for incoming information such as from AU field offices, Missions and Regional Mechanisms and to the output presented to the Peace and Security Department.

The Situation Room information links extend externally from the AU, to engage the UN and other international organizations, academic institutions and research centers, nongovernmental organizations (NGOs) and the media. With the explicit inclusion of NGOs and the media, it is arguable that civil society in general is to be engaged by CEWS, at least through these representative organizations.

A simplified outline below presents the major information nodes in CEWS that are addressed in this paper. They are selected because they each have a distinctive set of requirements for software applications to be coordinated by the Situation Room.

<table>
<thead>
<tr>
<th>Early Warning Unit</th>
<th>Other Governmental Bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU Missions</td>
<td>Nongovernmental Organizations</td>
</tr>
<tr>
<td>Situation Room</td>
<td>Academic Institutions</td>
</tr>
<tr>
<td></td>
<td>News Media</td>
</tr>
<tr>
<td>Regional Mechanisms</td>
<td></td>
</tr>
</tbody>
</table>

2.3. Types of Information: Information relevant to early warning may be characterized as knowledge about things, activities and conditions. The things most important to early warning include actors (such as individuals, groups, organizations...
and countries) and resources (oil, for example or other key commodity). This information about things represents attributes of the actors and are typically presented as profiles. Activities significant for early warning include cooperation and conflict as well as actions and environmental events that are not associated with either of these two poles on the human interaction continuum. Finally, the conditions or context in which activities take place is important in that it may constrain the actors in their choice of actions or present opportunities that would otherwise not be available. For example, environmental degradation in general and drought in particular is a context that can exacerbate competition for resources, contribute to instability and even spark conflict.

To suggest that such a wide range of knowledge about things, activities and conditions is important is not to say that omniscience is a requirement for early warning. The identification of key actors, relevant activities and exacerbating/mitigating conditions is a challenge to be sure. Thus the concern here is on specifying a system that can manage the collection and analysis of these basic types of information without regard to the labels being used to describe them. Specifically, the information types discussed here are presented generically. Other papers may use more specific terms, which while consistent with, are not identical to the generic labels used herein.

For the sake of clarity, the focus is on country profiles and resource inventories for things, and on conflict and cooperation for the activities. With respect to collecting information on activities and assessing conditions, a distinction is made between incident reports and situation reports. Incident reports detail the journalistic parameters of who did what to/with whom, when, where why and how of a given activity, interaction or event. Situation reports, on the other hand, present a systematic and regular assessment of the conditions within a country or as related to a given Mission as they evolve over time. Situation reports may also be used to track a localized region or “hot spot” and even the status of issue-defined phenomena such as small arms transfers or refugees.

In sum, the following types of information for use in the CEWS:

- **Actor Attributes (things)**
  - Individual, Group, Organization and Country Profiles
  - Resource and Infrastructure Inventories

- **Events Data (activities)**
  - Incident Reports
  - News Reports

- **Situation Assessments (conditions)**
  - Country Situation Reports
  - Hot Spots Situation Reports
  - Mission Situation Reports

Across all of these types of information, the objective is also to track lessons learned. These lessons may be found in formal case studies as well as in informal annotations, comments or reactions attached to a field report. In all cases, it is important to retain this information and make it accessible to analysts in an attempt to learn from past mistakes and failures.
Finally, it is important to note that all of these types of information include both qualitative and quantitative data. The analysts in the Early Warning Unit clearly need both, and there is little if any purpose served in making such a distinction between them at this generic level of discussion.

2.3. Management and Analysis: The locus of information management within CEWS is in the Situation Room. The Situation Room’s primary responsibility for information collection is rivaled only by the necessity for it to manage the information in real time. This management task includes collecting, classifying, collating, distributing and archiving data from disparate sources. In addition, the Situation Room must provide technical support for requested analyses of the data as well as generating and communicating automated alerts when called for by anomalies or inflections in the analysis routines. The Situation Room thus functions as a 24/7 operations center supporting the CMD’s early warning activities.

Several software modules are required to support this information management activity in the Situation Room. These modules may be viewed as linking the various nodes and types of information outlined above. The starting point is a base module to facilitate the Situation Room’s management of actor attributes information. These attributes data consist of individual, group, organization and country profiles and inventories of resources and infrastructures. These profiles provide information about specific actors, but they also illuminate the context and to some extent the conditions in which activities take place. This base module is most simply a database, and more specifically, an enterprise level relational database, fully indexed and searchable across a number of different “cuts” of the data, and with a secure web interface to allow for both in-house and remote access.

In addition to serving as the actor attributes database, this module will also serve as the repository for the events data and situation assessments. In other words, this module serves to integrate and link the various types of information to be collected in a coherent archive of historical as well as current data. This relational database base module therefore is usefully considered the backbone of the Situation Room’s information management tools. This base module may be run with a standard enterprise level database such as Microsoft’s SQL Server.

Plugging into this relational database is a module for collecting news reports. Some of these news reports must be purchased by subscription services while others may be “scraped” from open news sites on the Internet. The Situation Room already operates a semi-automated news clipping service for the AU, compiling both subscription and public news reports into a daily narrative summary.

The European Commission’s Joint Research Center in Milan, Italy has developed a fully automated news clipping service along the same lines. It is called the Europe Media Monitor (EMM) News Explorer (http://press.jrc.it/NewsExplorer/home/en/latest.html). Given the state of the art sophistication of the News Explorer, and its likely availability for use by the African Union (based on the preliminary discussions with the News Explorer developers at the Center on Milan), there seems to be little if anything to be gained in searching for a commercial alternative. The current EMM system monitors
1,000 news sites round the clock in 30 languages, processing about 35,000 articles per day. The system can easily be expanded to cover many more African specific sites.

Actually, there are two distinct EMM services, the live monitoring and clustering service that can feed into a natural language processor (discussed below) as well as an EMM NewsBrief that automatically classifies each news story and offers a user customizable alert system. What is proposed here is an Africa-specific version of the EMM NewsBrief that focuses on African issues and reports concerning individual countries.

News clippings, however, are not news events; the former simply yields text-based narratives while the latter offers numeric-based data matrices. The developers of the News Explorer have been experimenting with the natural language parsing of news leads to supplement and enhance the graphical depiction of trends in news reports. The automated clipping service should be enhanced with a news events data module to support the analysis of social, political and economic news events in near real-time. This functionality serves to generate the events data for baseline and trends analysis.

Supplementing news clippings with news events data in this way makes it possible to conduct statistical analysis of events at a very refined level of analysis. Subtle inflections in the incidence of certain events can indicate escalation into a volatile situation. For example, the rise of hate speech may presage future hate crimes; likewise, unmet demands may lead to protest demonstrations or to suppression.

Parallel to the news events data module is a similar module proposed for collecting and assessing incident reports and situation assessments reported directly from the field. At least two Regional Mechanisms (IGAD and ECOWAS) already have operational field reporting and analysis systems that include both incident and situation reporting. Rather than have the AU duplicate these regional efforts, it is recommended that the Situation Room’s use of these tools focus on reports submitted by AU Missions and perhaps Hot Spots on an ad hoc basis.

A separate module (or possibly an automated agent) is also suggested here to facilitate the submission (pulled or pushed) of periodic summaries of field data from the Regional Mechanisms to the Situation Room. This functionality would operate to support field report and other data sharing between the Situation Room and the RECs, including aggregated or summary data. Given the likely differences among the REC’s data collection systems, this module/agent is proposed here to allow a limited (summary data only) sharing of field reports when the sharing of raw reports is not possible.

Finally, a bulletin board module is recommended to provide a means of communicating to and exchanging ideas with the constituencies of the CMD, both internal and external to the AU. The exchange part of this module most likely will have to be moderated, or at least restricted in terms of its users on some issues. Another use of this module could be for qualified academics to access the public news events data and perhaps some field data as well for independent verification and testing.

It is important to note that with the exception of the field summaries module, all of the modules recommended have extensive track records. All have been reduced to practice albeit separately in some cases. The new element in this recommended list of information management modules is their integration.
It is noteworthy that this integration is to take place at the level of institutional cooperation as well as technology. The coordination and harmonization role of the AU with respect to the Regional Mechanisms is explicit in the PSC Protocol. Clearly, securing the cooperation among these sub-regional intergovernmental organizations will be critical to meeting the AU’s early warning mandate.

One example of how this continental-regional cooperation could work is in the maintenance of the country profiles data. It makes little sense for the AU and the relevant Regional Mechanisms to duplicate efforts in the periodic updating of the profiles’ data. The establishment of a common data structure for the profiles by the AU would be useful in providing a comparable standard while the Regional Mechanisms in turn submitted their respective data updates. The kind of reciprocity in which the AU takes a standards setting lead and then facilitates the exchange of data submitted by the Regional mechanisms can help build a cooperative environment that can support the early warning mandate.

Equally important is the role of academic institutions, especially with respect to capacity building, training and independent assessment of the data and analyses. Extensive and ongoing training will be required to deploy and operate these modules in the field. Forging institutional partnerships with academic institutions can help make the operation of these software modules sustainable at the AU by supporting the ongoing training of technical support and analyst staff alike.

2.5 Communication of Results: Early warnings not communicated or left unheeded are worthless. An essential component of each of the modules discussed above is the compelling, visual and interactive display of results. This communication can be enhanced with a combination of tabular, graphic and geographic presentations, including drill access as appropriate to the full text of the underlying documents. The ability to readily export results for manipulation independent of the modules is also important.

Communication of results may also be improved with easy to use standardized interfaces and seamless integration across the modules. A simple yet fully featured common console or dashboard across all modules is the ideal, as is a single user log-on across all modules. These criteria for optimizing the communication of results are discussed more fully in the software requirements section below.

A summary listing of the informant management and analysis modules follows:

- **Bulletin Board Module** (non-structured information exchange)
  - Supporting Announcements
  - Supporting Interactive Feedback

- **Events Data Module** (text and numeric news events data tracking)
  - News Clipping Module
  - News Events Data Module
Field Reports Module (text and numeric field events data tracking)
- Incident Reports
- Situation Reports

Field Summaries Module (from the Regional Mechanisms and other organizations)
- Incident Report Tallies
- Situation Report Tallies

Relational Database Base Module (Integrated Archives for all other Modules)
- Country Profiles
- Individual, Group and Organization Profiles
- Resource and Infrastructure Inventories

3. Software Specifications

3.1. Security Model: Each of the modules outlined above should share a common access control list and security model. The security model should include independent, configurable parameters for organizational and regional membership and user roles. In addition certain fields in field reports that contain sensitive information (names of victims and perpetrators, for example) need to be configurable such that they can be masked to users who do not need to know this information.

A multi-level hierarchy of organizational membership structure is recommended, with the CMD set to “trump” all other organizations. That is, users who are members of CMD will have a set of rights commensurate with their security model memberships that will be higher than users with an organizational membership in other organizations.

Similarly, a multi-level regional (geographic) membership is recommended. The hierarchy here would simply follow the smallest geographical unit to the largest. Provision should also be made to associate geo-coordinates (latitude and longitude values) with each of the place names. Given the variety of spellings and alternate names of any given place, normalization of all regional membership values is critical to assure seamless use of the place values in mapping displays.

As for the roles, at least four, and perhaps five, seem to be required. An administrator would have complete access rights to the system and all reports. Editors would be able to submit and modify reports within their respective memberships. Reporters would be able to submit reports within their memberships as well as modify their own reports only. Viewers would be able to see the reports within their membership but not submit or edit them. Finally, an optional guest role would be able to see only the report listings (as opposed to the reports themselves). In all roles the masked fields would be configurable so that only the submitter and, presumably, certain CMD personnel, could see this sensitive information.

In sum, the security model should contain at least the following configurable parameters:
3.2. Required Functions: Overall, the main user requirements are CEWS system are ease of use and seamless integration among the various modules identified above. No single vendor supplies the full range of software applications required by CEWS, so plug and play, modular integration and technical support is critical to deployment, operations and ongoing improvements in the system. As suggested earlier capacity development is the foundation for the system, so a train the trainers approach should be required for all orientations and training.

At least three layers of features should be selectable in all modules, including the main console or dashboard of the system: a top layer for users who consume the information, a middle layer for analysts who work with, transform and organize the information, and a bottom layer for system administrators to manage the information, the users and the system. In addition, all parts of the system should also be multi-language capable, again through a user selection. However, it may be useful to defer the implementation of this multi-language feature in order to deploy and refine the system as a whole more quickly provided that the extensibility is built-in from the beginning.

Another set of system-wide functional requirements deals with the display of data and results. Each of the modules should have a consistent mode of displaying data and results in several forms, including the following: full text (of the originating documents) the header or meta-information associated with those documents, a document listing or tabular presentation of query results, statistics on results, graphical displays of data and geographical displays (maps). The level of granularity of maps may be problematic given the lack of standardized data available, but at least to start, national level data should be available and within a year or so, a goal of provincial level data is realistic. Of course, in certain areas, much more detailed data are already available, so when they are available, the system should be able to handle it.

In addition to generating displays of data and results within the system, the system should be able to export into standard formats with ease; numeric data into spreadsheet formats, for example, and textual data into rich text formats should be supported.

And finally, a note of caution about intellectual property rights is in order here. Certain information, a news subscription service for example, may not allow the display or export of full stories except to those users to whom and end user license has been issued. The ability to restrict the display of certain portions of data should therefore be a part of each module. This limited access feature is covered under the security model’s masked field’s parameter. These restrictions are typically set by the system administrator when adding user profiles.