A Feasibility Study
January 2011

Contents

1. Feasibility Study

This document summarises a Feasibility Study into the idea of launching PAX – a digital system to provide early warning of violent conflicts, wars and genocides.

The study looks at the sources for information about emerging conflicts, how the digital system might work, case studies, existing systems, a proposed operational structure, and next steps.

The study, and a project website, have been helped by funding from Google.

The website, www.pax2011.org, has a description of the PAX proposal, and asks for feedback and comments.

Homepage of the PAX 2011 project website

2. Introduction by Brian Lapping

Mobiles, satellites and the web dazzle mankind with a constant flow of new possibilities. Some attempts have been made to use these tools to prevent wars or genocides. Can those efforts be enhanced and applied worldwide?

In the years 2007-10, thousands in conflict zones uploaded pictures of violence being perpetrated. They knew they were exposing themselves to grave risk when they, in effect, said to the world, "My village/people/priests are being attacked. Here's evidence. Please help."

In response, PAX proposes to develop a digital system that would enable it to gather such uploads (and other on-the-spot reports); to evaluate the information; and, when satisfied that the data justifies it, to issue 'Alarms'.

To ensure that its Alarms make the necessary impact on those in a position to calm down the incipient violence, PAX would need to establish a unique level of both authority and independence.

Its authority would derive from demonstrating unequalled commitment to getting the facts right. To conduct the evaluation needed to exclude dishonest reports, PAX would, once it was considering declaring an Alarm, hire journalists and academics who have proved outstanding at achieving accuracy and who know the area in question.

PAX's independence would derive from two rules. Its governing body and those working for it would be drawn from all races, religions (and non-religions) and continents. And no government, international body, sponsor or funder would be allowed to editorially influence a PAX report.

To guarantee its independence further, PAX would restrict its role to gathering, checking and disseminating information. In short, PAX would be a specialised public service communicator.

PAX needs to counter several challenges. Here is one. "It is not lack of knowledge that explains the failure to prevent wars or genocides. It is lack of will. More knowledge will make no difference."

In 1995, in the week of the Srebrenica massacre, a documentary producer put a courteous question to Slobodan Milosevic, then President of Serbia. The question concerned acts by Serbs against other communities in Yugoslavia. Milosevic replied: "What? Us? Ridiculous."

Today a foreign minister or non-governmental peace-maker, visiting the leader of a dangerous aggression, would be able to show him uploads of events in his area recorded that very day. These would make a Milosevic-type denial easier to handle. That is one reason why the new technologies offer peace-makers a useful tool.

That tool would not have been of much use in 1995, when Milosevic and his allies were in full murderous mode – and had crushed counter-attacks galore. The moment when the data provided by the new technologies might help prevent war/genocide comes much earlier: when aggression is building up, but the rival parties are still capable of being swayed.

In the case of the Serb wars, that moment began in April 1987, when Milosevic declared, "Serbs, you will not be beaten again" to a crowd of Kosovo Serbs. His words were played and replayed on television. They inspired a coup in which Milosevic defeated communism as the dominant force in his country and replaced it with Serb nationalism.

Many, both in and outside Serbia, saw the danger of rampant nationalism. Could they have used PAX-type data, during the months following his speech, to stop Milosevic and his allies in their tracks?

Serbia's ruler at that time, Milosevic's boss Ivan Stambolic, was dedicated to keeping the area's rival nationalisms at peace. He was appalled by Milosevic's provocation of war. Serbia's most powerful ally, Moscow, was on Stambolic's side. Might PAX data, used both by Moscow and by Serbia's fellow Yugoslav republics, have helped the moderate Stambolic to stay in power? (Russia's suggested role here is not unrealistic. In 1999, 12 years later, who persuaded Milosevic to back down? Russia's ex-Prime Minister, Viktor Chernomyrdin).

Thus, had PAX existed in 1987, Europe's worst series of wars and genocides since 1939-45 might have been averted.

Brian Lapping
January 2011

3. Proposal Summary

Aims

PAX is an independent organisation that plans to launch a global digital system to give early warning of conflicts, wars, genocide, or mass atrocity crimes.

The PAX digital platform would collect and analyse information from mobile phones, the internet and satellites, and then publish information about emerging conflicts. The aim is to help prevent these conflicts escalating.

The PAX Global Digital System

PAX would be based on the following workflow:

1) PAX would use crowdsourcing, through an automated computer system.

2) The sources could include:

   - Keyword searches of public websites, blogs, and social networks
   - Uploads of words indicating aggression in the language of potential conflict areas
   - SMS texts and photos sent from mobile phones
   - Emails and other uploads from computers
   - Information from other alert websites and organisations
   - Pre-arranged feeds from other international networks.

3) The information would go through an automated PAX algorithm – which would analyse reports of incidents, and trends in hate, violent and other relevant 'danger' words, via keyword searches.

4) Registered volunteer evaluators would then assess PAX's data. The evaluators would need to be able to write in one of the UN's six languages.

5) The computer system would automatically gather the information and evaluation to produce a graphics-based early warning barometer for emerging conflicts. It would give each conflict a level: 'Early Warning', 'Tension', 'Crisis'.

6) Once a conflict reached the 'Tension' point, the evidence about it would be sent to paid Specialist Evaluators – selected from a PAX Experts' Database.

7) The final stage is for the PAX editorial team to collate reports - and decide whether to email a PAX Alarm to non-governmental organisations/policy groups/journalists in states with relevant influence and to people in the conflict zone.

The main sections of the PAX website would be in the six UN languages: Arabic, Chinese, English, French, Russian and Spanish. It would be a cross-platform website – carrying information about conflict areas, easy-to-use upload features, and interactive panels for the registered volunteer evaluators.

A full description of the process is in *Section 5: Digital System,* and *Appendix 3: Technical Details on the PAX Algorithm*

The PAX Approach

PAX should be authoritative, global, multi-cultural, independent, impartial, and open.

- It would put intensive efforts into getting the facts right.
- It would ensure that its staff were drawn from a range of races, creeds and continents.
- It would be independent of governments or other international bodies.
- It would report conflicts factually in any part of the world.
- It would embody openness through information-sharing and partnership.
- It would build a global community of people willing to help prevent wars and genocides.

Governance, Management, Phasing and Budgets

We propose that PAX would have the following organisational structure:

1) The PAX Trust and Executive Board – to monitor PAX's performance, protect its independence, and help ensure that PAX Alarms get to those with influence.

2) A Management and Editorial Team – to manage the PAX digital system, maintain the databases, supply information to the evaluators, and issue the PAX Alarms.

We propose a 5-phase approach: (1) Feasibility Study (completed January 2011), (2) Development, (3) Pilot, (4) Launch and (5) Ongoing Service.

PAX would be non-profit-making

Key Issues

During the study, the PAX project team has identified the following major challenges:

- How to process large amounts of data in a way that delivers accurate and timely warnings.
- How to weed out deliberate misinformation.
- How to protect the website from cyber-attacks.
- How to deal with the world's many languages.
- How to protect those who upload information.
- How to make sure that data showing a war is imminent gets into the hands of those who can influence the rival parties to stop it.
- How to get funding.
- How to ensure that the technology will work.

These topics are examined in *Section 5: Digital System* and *Section 7: Governance, Operations and Budgets*.

4. Sources

Overview

PAX would mine and receive data from a wide variety of sources, including mobile phone and internet uploads, open source material on the web and social sites, news from diaspora networks, feeds from agencies, and information from satellites.

This section of the feasibility study is based on desk research, email interviews, and face-to-face meetings. A full list of people interviewed and literature reviewed is in *Appendix 2: Acknowledgments*.

Mobile Phone Uploads

Mobile phones have become mankind's most accessible form of communication, with over five billion users at the end of 2010. In many parts of the developing world, the mobile phone has leapfrogged fixed line phones and is also now on track to become the most popular method of accessing the internet.

Our research confirms that mobile phones could form a primary source of information from people affected by conflict. Via local telephone numbers, publicised by NGO and other partners, a system could be opened up for people to send PAX both pictures and messages. PAX could also receive voice calls which could be translated into searchable online text through phonecasting technology, such as Ipadio.

Two key issues for PAX are (1) access to mobile phone technology in places at risk of conflict and (2) how to help mobile phone users who upload sensitive material to do so as safely as possible.

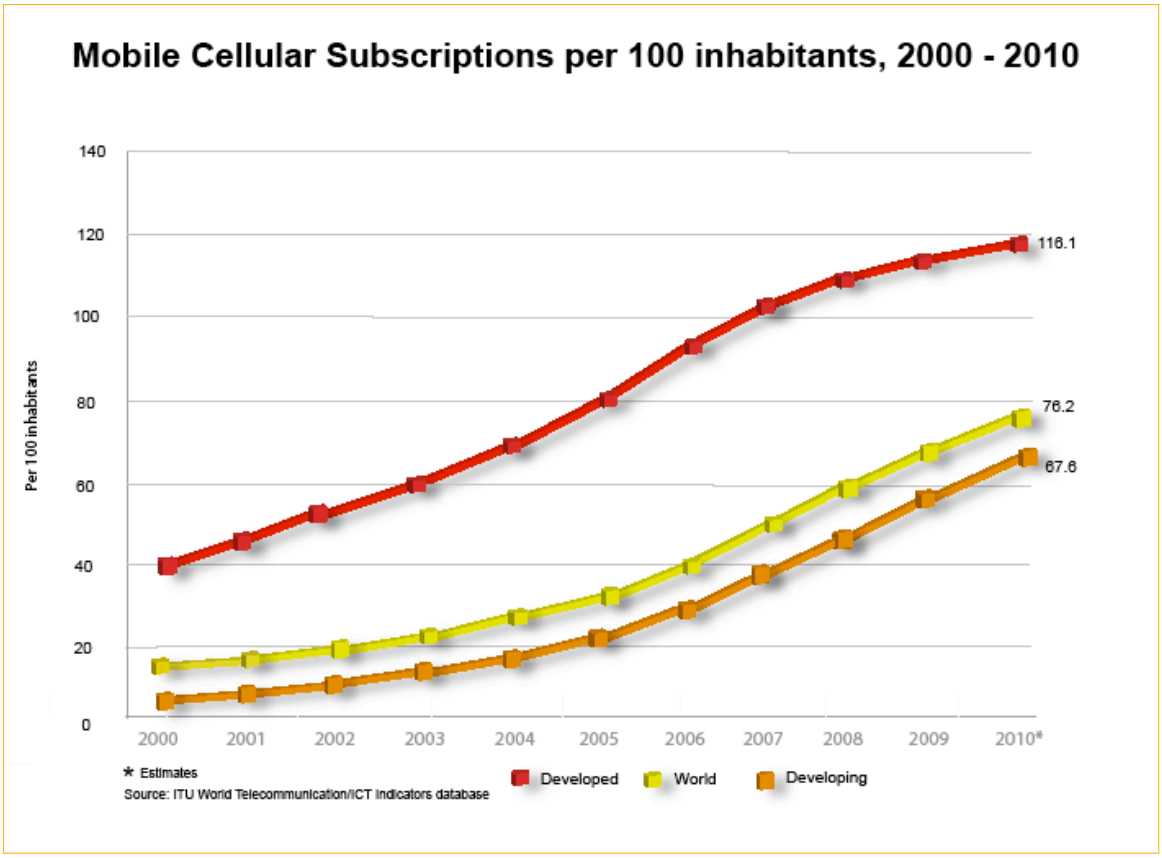
1) Access

The rate of growth of 3G, smartphone and basic handsets is so rapid that PAX's aims are realistic, even in countries with currently low levels of access.

For example, across Africa, mobile phone penetration rates were expected to reach 41% of the population by the end of 2010, and the developing world continues to experience double-digit growth year on year.

Indeed, growth in developed countries has only tailed off as it reaches saturation point with more than 100% subscription penetration (accounted for by users with more than one mobile).

The following chart shows the growth in mobile phone subscriptions, reaching some 68% of the developing world's population by 2010.



The figures show strong growth in recent years in all regions bar Europe and North America, with penetration figures more than doubling in Latin America and almost tripling in Africa, the Middle East and Asia Pacific.

2) Safety and Anonymity

It would not be possible for PAX to guarantee to keep the identities of those who upload information to its website safe. But one of its highest priorities would be to keep constantly abreast of the latest developments in user security and keep uploaders informed of ways to protect their identity.

Mobile network companies are subject to licensing laws in the countries in which they operate – and all states require the right to monitor telephone calls, text messages and increasingly require registration of SIM card users.

A person who sends a text message to PAX describing a military attack by government forces therefore risks persecution or arrest – or worse.

Government monitoring systems are becoming increasingly sophisticated, although the level differs between states because of the high cost of examining data traffic.

Recent disputes between RIM (the company behind BlackBerry) and India and Saudi Arabia over encrypted emails show the growing determination of governments to monitor communications.

Ways to anonymise mobile phone communications include:

a) Anonymous cash purchases – In many states it is possible to purchase SIM cards with cash and without providing identification. This is particularly popular where access to credit and bank accounts is limited.

   However, many countries, including Zimbabwe, Kenya, Sudan, Bahrain, and Fiji, are introducing legislation banning the sale of unregistered SIMs. Whether this will prevent anonymous communication remains to be seen.

b) Anonymising and Circumvention software – These hi-tech approaches are becoming increasingly effective and available on smartphones.

   The TOR project's routing system, for instance, bounces online communications around a network of relays run by volunteers across the world, so that a user's online activities are difficult (but not impossible) to trace.

   Circumvention technologies, including Alkasir, Psiphon, Freegate, Hotspotshield and Ultrasurf, enable an internet user to access websites which are blocked in certain countries. The technologies aim to mask the user's online movements from in-country ISP monitors – and they provide a reasonable (but not complete) level of anonymisation.

c) Mobile handset optimisation methods – Some commercial systems have been developed to optimise basic handset services. These translate SMS data into internet and online chat via offshore servers, using randomised secondary routing systems. While these services are designed to increase access to the internet on basic 2G handsets, they also make communications harder to trace.

d) Mobile banking securitisation methods – Systems developed for mobile phone banking and financial transactions may increasingly help to deliver a higher level of securitised communication between uploaders and PAX.

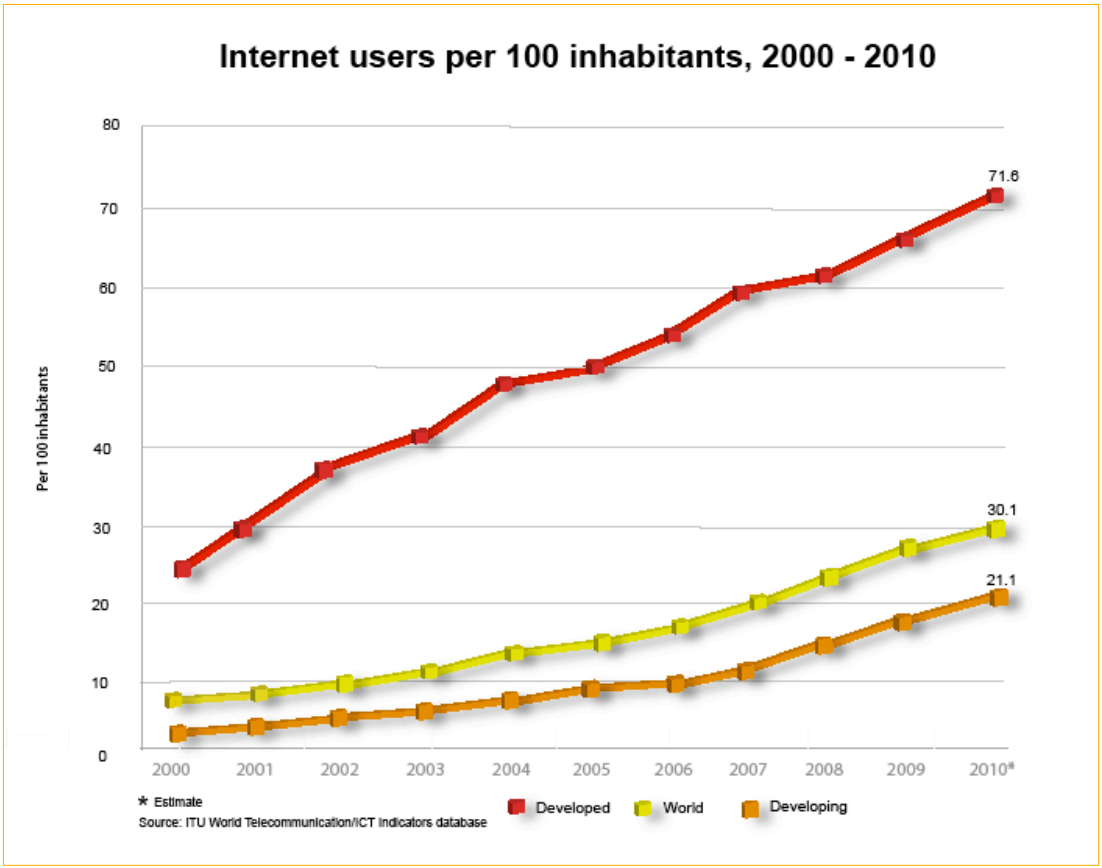
e) Passing information via phone to contacts in other countries – Links between relatives, friends or colleagues in different countries are frequently strong, and the content of private phone calls may be uploaded by contacts with access to the required technology.

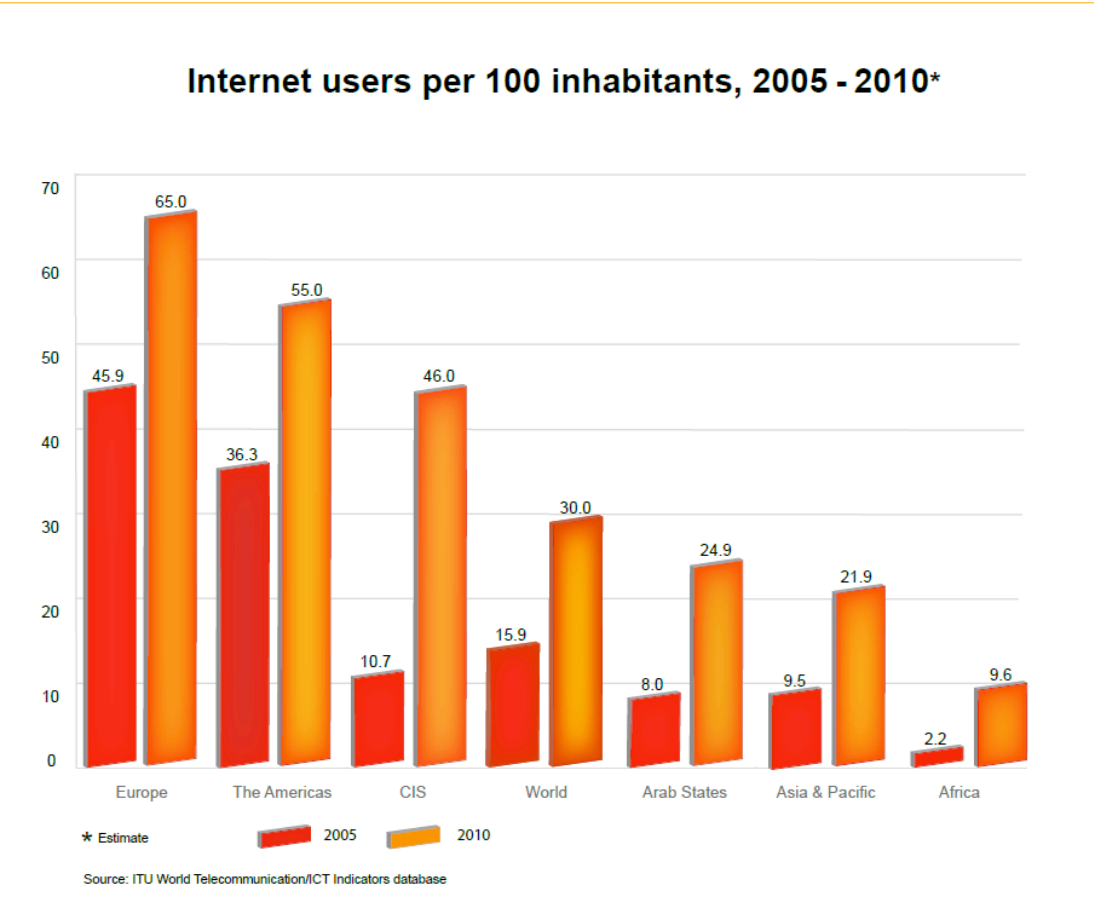
Internet Uploads

PAX would also receive uploads via the internet, including emails containing text or pictures. Internet access is less widespread than mobile phone access – there are 2.1 billion internet users compared to 5.3 billion mobile phone users worldwide, and in many parts of the world the divide is even wider (9.6% as opposed to 41% of the people of Africa for example).

Rates of growth, however, are high with mobile broadband overtaking fixed line as the method of choice for connection.

The charts on the following page spell out the growth of internet access.


Internet users per 100 inhabitants, 2000 - 2010
Per 100 inhabitants
80
70
60
50
40
30
20
10
0
71.6
30.1
21.1
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010*
* Estimate
Source: ITU World Telecommunication/ICT Indicators database
Developed
World
Developing


Internet users per 100 inhabitants, 2005 - 2010*
70
60
50
40
30
20
10
0
45.9
65.0
36.3
55.0
10.7
46.0
15.9
30.0
8.0
24.9
9.5
21.9
2.2
9.6
Europe
The Americas
CIS
World
Arab States
Asia & Pacific
Africa
* Estimate
2005
2010
Source: ITU World Telecommunication/ICT Indicators database

The same challenges of access to technology and how to protect the anonymity and safety of uploaders apply to internet uploads.

As with mobile phone networks, internet service providers must comply with interception requirements laid down by the countries where they operate, so anonymity cannot be guaranteed. Many states are tightening up these requirements.

WikiLeaks has examined anonymity issues carefully. The site offers a secure electronic drop-box, which prevents even WikiLeaks staff from tracing information about the sender. It also recommends the use of the TOR anonymising and Psiphon circumvention tools.

PAX would encourage internet uploaders to take similar precautions when sending data. And an online form on the PAX website, similar to the WikiLeaks' electronic drop-box, could be developed to provide maximum anonymity for the uploader.

Keyword searches of websites and social media

In addition to information sent directly to PAX, the proposed algorithm would also mine data from news websites and social media, using sophisticated keyword searches and tagging.

Adopting the latest search engine technology, the PAX algorithm would search through online news and community media for keywords of places at risk. The algorithm would also comprise social media listening tools to examine information from online forums, blogs, Twitter, Facebook updates and other accessible social media.

Geotagging pictures and tweets would help PAX to show the location of an event and improve its ability to verify information.

People affected by conflict have sent information to public micro-blogging sites such as Twitter. They have published reports on blogs (as seen during the Saffron Revolution protests in Burma in 2007, and the post-election demonstrations in Iran in 2009). And they have posted pictures to sites like flickr and tumblr, videos to sites like YouTube and Vimeo, and updates to social network sites such as Facebook.

The rush to send information out from Burma in 2007 led the Burmese junta to switch the internet off altogether. But the economic impact of a shutdown becomes increasingly damaging, even for the most authoritarian governments.

Direct feeds from specialist information-gathering and alert websites

PAX could receive direct feeds from information-gathering specialists and websites within the conflict prevention community.

These feeds would be amalgamated into the data sources for the PAX algorithm, to be analysed alongside other open source data and information sent directly to PAX.

For example, news analysis tools have been developed by the European Joint Research Centre to amalgamate information from online news sources. Their output can be received as a data feed. These tools also incorporate a level of analysis to monitor spikes in news stories and can be focused selectively on conflicts.

Other specialist subscription feeds that PAX could potentially incorporate into its analysis include: Reuters, Jane's, LexisNexis' Global Business Information Research Database, BBC Monitoring, and the Open Source Center at World News Connection. These would require funding and licence agreements.

PAX could also seek to work with organisations like International Crisis Group's Crisiswatch, Channel 16, UN Reliefweb and Reuters AlertNet.

Diaspora Networks

An important source of information would be diaspora networks. When groups are attacked, some flee. In the cases of Burma/Myanmar, Iran and Kyrgyzstan, those who have fled have been key recipients of information from their people, which they have helped distribute.

Satellite Imagery

The American Association for the Advancement of Science (AAAS), in collaboration with Amnesty International and Human Rights Watch, has carried out several studies on the role satellite imagery can play in the prevention of conflicts.

For instance, images of villages burned in Janjaweed militia attacks in Darfur, were put to the Sudanese government; and the burning of villages subsequently went down – although we cannot prove that the two events were linked and other forms of violence continued.

The latest project to take advantage of satellite imagery for monitoring conflict is the Satellite Sentinel project, a partnership between George Clooney's Not On Our Watch human rights organisation, the anti-genocide Enough project, UNOSAT, Google, the Sudan Vote Monitor Ushahidi deployment, and the Harvard Humanitarian Initiative (HHI).

The project raised funds for the purchase of high resolution imagery of the border area of North and South Sudan. They set out to speed up the processing time to 36 hours and combine it with rapid analysis by experts at UNOSAT and HHI. In addition, Google Earth has updated its imagery of the area.

Satellite Technology

Satellite images can now be captured of any location in the globe, bar extreme poles and places with cloud cover. Six high resolution imagery satellites are currently in orbit – and within the next two years US satellite GeoEye-2, the French Pleiades pair of satellites and India's IRS-3 are also due to launch.

These satellites can provide imagery of less than one metre Ground Sample Distance (GSD). This level of resolution allows for the observation of troop and vehicle movements, damage to homes, and shelling or digging patterns in the earth.

The primary challenge for PAX would be acquiring satellite imagery rapidly, without paying the standard, high costs of direct procurement. Directly tasked and procured rush images now cost in the region of $2,500 to $10,000, depending on how many other people are in the queue for imagery of a particular area.

The UN's satellite research body, UNOSAT, potentially offers a lower cost option. It puts satellite imagery on its website, alongside expert analysis – and PAX may be able to access these feeds to assist with verification of reports.

Use of Satellite Imagery

At present, we believe that satellite imagery would most effectively be used by specialist evaluators for verification purposes at the 'Tension' point (see page 6, point 5). As computerised analysis of satellite imagery develops, though, it will be possible to feed this data automatically into the PAX algorithm to help assess reports on impacts of violent conflict – such as fires, shelling damage, or mass burials.
Research projects in this area are examining the relationship between conflict and active fires and smoke, which can be tracked through meteorological satellites. Lars Bromley at UNOSAT is working on research into developing algorithms to analyse unusual fire patterns which may be linked to conflict.

The Center for Civil Crisis Information and Georisks at the German Aerospace Center is also conducting research into the correlations between remote-sensing data – such as radar, optical, and thermal data - and risk indicators for conflict.

As satellite imagery becomes more widely and rapidly available, it may be possible for geo-referenced images to be laid onto maps in real-time, with visual documentation of troop movements, build-up to conflict, and resulting damage alongside witness reports – raising the alarm as never before.

Sources: Summary

Key points:

1) Mobile phone and internet use will continue to grow in areas affected by conflict.

2) Where a hostile government is likely to monitor who is sending uploads, PAX would need to warn uploaders about the risks and advise on ways to either attempt to anonymise communications or to use other channels.

3) Potential methods of anonymising mobile communications include cash payments where registration is not required, anonymising and circumvention technologies, mobile optimisation, and mobile banking securitisation tools.

4) Existing information already available through the web and social media, and feeds from specialist data-gathering organisations, would form an important part of the information to be analysed by the PAX algorithm and specialist evaluators.

5) Currently, satellite imagery could be used by PAX's paid experts to verify evidence. In future, as automated systems for analysing high-resolution satellite imagery improve, this material could form part of the raw data in the PAX algorithm.

5. The Digital System

The Digital System

As explained in Section 3, we propose that PAX would collect and analyse information about emerging conflicts from mobile phones, the internet and satellites.

Summary of the PAX Workflow

1) PAX would gather and mine information from the digital 'crowd' (ie crowdsourcing), through an automated computer system. Digital crowdsourcing technologies are developing at a rapid pace – and have the potential to be a powerful method of evaluating information about events and trends.

2) The information sources could include:

   - Automated keyword searches of community, news and other public websites, blogs and social networks.
   - A study of words indicating aggression in the languages of Early Warning zones.
   - SMS texts and photos from mobile phones – sent to PAX or to other public websites/networks.
   - Emails, forms, and photos sent to PAX from computers and mobile phones.
   - User generated audio and video.
   - Information from other alert websites and organisations, such as Reuters AlertNet and the International Crisis Group's Crisiswatch.
   - Filtered information from global information-gatherers, such as BBC Monitoring, LexisNexis etc.
   - Pre-arranged information feeds from other international networks, such as embassies, multi-national companies etc.

3) The information would go through an automated PAX algorithm – a computer analysis system built for PAX by a third party software development company.

   The algorithm would look out for trends in violent and other relevant words, via keyword searches.

The computer system would also organise, prioritise and categorise other evidence from the information flow (such as photos, videos or satellite images), which could then be seen and analysed during the PAX evaluation process.

Sources which had proved accurate would be given more weight, through a system of credibility filtering. The PAX algorithm would track sources, and those that proved accurate would be identified, and be given extra 'value' in the future.

4) Volunteer evaluators would be able to assess and rank PAX's data and information – in a designated section of the website. They would have to show that they can write in one of the UN's six languages, and would need to complete a registration form outlining their background and experience. They would use a range of interactive tools to carry out the evaluation – including ranking systems, online forms, and comment panels. We would investigate ways of giving them the option of contributing anonymously.

5) The crowdsourcing of information and the website volunteer evaluation and analysis would produce an online graphics-based early warning barometer for emerging conflicts, with conflicts moving up and down the scale according to the latest developments. The levels in the digital barometer would be 'Early Warning', 'Tension', and 'Crisis'. The barometer system would provide a top level summary for each conflict, and would then link through to more detailed evidence pages.

6) If conflicts reach the 'Tension' point, the evidence about them would be sent to paid Specialist Evaluators – selected from a PAX Experts' Database.

   These experts would include journalists and academics, who had knowledge of the conflict area, and who were demonstrably objective and independent. We propose that a committee of the PAX Trust would oversee their selection.

7) The final stage is for the PAX team to collate reports, and to decide whether to email them and a PAX Alarm to non-governmental organisations, policy groups, journalists, and to people in the conflict zone.

   PAX would set up an Alarm Advisory Committee to work with NGOs that were in a position to put PAX data before key members of the governments with influence over the parties to the conflict.

The Alarms would be posted onto the PAX website – and would also be emailed to the global PAX community of paid Specialist Evaluators, volunteer evaluators, and other site users who sign up to receive the Alarms (including those in the Alarm zone area itself).

The main sections of the PAX website would be in the six UN languages: Arabic, Chinese, English, French, Russian, and Spanish. In addition, we propose that the section dealing with each Tension, Crisis and Alarm zone, would be in that zone's local languages.

Information collected and analysed by the PAX algorithm would be of use to those in conflict zones. It would also encourage local people to report incidents. PAX would form working relationships with established local groups and NGOs to encourage both.

During our Feasibility Study we have consulted local groups in Nepal, Pakistan, Zimbabwe and Burundi with the help of Peace Direct, an organisation dedicated to supporting local peacebuilding efforts. They have given positive feedback on the potential value of PAX. These consultations would need to be expanded in PAX's next development stage.

Alarms

When the data from its website justified declaring an Alarm, what would PAX do?

Other organisations have spent years building up the contacts and insider knowledge necessary to open the doors of the top people in each appropriate government/NGO. So, during an Alarm, PAX would serve as their data-provider.

The procedure at an Alarm moment would, unavoidably, be many-staged:

1) PAX's Alarm Advisory Committee calls partner organisations and works out with them the best way to make those with influence look at the data and appreciate its importance.
2) Partner organisation persuades minister/NGO with influence (over the leader of one side in the conflict) to use it.
3) Minister/NGO rep visits conflict leader (and allies).
4) Minister/NGO rep. uses today's PAX data to clinch his/her argument.

Thus PAX and its partner organisation would equip the minister/NGO rep to tell the conflict-leader: "These uploads show what acts your people are suffering/committing at this moment. If you don't call a halt now, the consequences can be predicted by looking at these further uploads of weapons-build-ups/deserted villages/training camps/ destroyed buildings etc. You must prevent this turning into a war."

To ensure that its data was used effectively at an Alarm moment, PAX would need to have established strong, on-going relations with the organisations that have access to the appropriate minister/NGO (see *Section 7: Governance*).

PAX Alarms would also be sent to as many organisations in the conflict zone and as many people affected there as possible, via mobile phone or internet, to help them conduct local mediation, get out of harm's way, dispel dangerous rumours, and in other ways try to prevent the worst happening.

The PAX Approach

We believe that PAX would bring together the best of Google-style ranking, Wikipedia-style community involvement, and Linux-style expert input. It would be a step towards realising the ideal of open source intelligence working for conflict prevention.

Examples of how the PAX system could work are analysed in *Section 6: Conflict Summary and PAX Case Studies .*

The PAX workflow is illustrated in the chart on the following page.


PAX Workflow
Sources
Keyword Searches
SMS Texts
Emails
Photos/ Videos
Alert Agencies
Global Information Networks
PAX Algorithm
Crowd Analysis by Registered Evaluators
PAX Barometer
Verification by Specialist Evaluators
PAX Alarm
Credibility Filtering

The PAX Website

The public face of PAX would be its website – which would be available across platforms (computers, IPTV and mobile networks).

We propose that the site would have the following six main sections:

- PAX Alarms (current and recent)
- Upload
- Evaluation
- Barometer
- Archive
- About

1) The latest PAX Alarm would be summarised on the homepage, with more details in the Latest PAX Alarm section, which would include evidence, contested data, and background information – categorised by relevant filters, and searchable.

   Users would be able to download or share key PDF evidence – such as a copy of the PAX report compiled as part of the Alarm process.

2) The Upload section would allow users to upload photos, written information, audio or videos.

   The Upload system would be easy-to-use, with a step-by-step navigation process.

   The latest UGC uploading systems would be used.

3) The Evaluation section would include a registration area, an interactive evaluation area, where volunteer evaluators would rate and comment on evidence coming out of the automated process, and community features, such as forum pages.

   For registration, potential evaluators would have to complete an online form outlining their knowledge and experience, and which language they would use.

4) The Barometer section would show a graphics based summary of all conflicts currently on the Barometer scale – in the Early Warning, Tension or Crisis levels. Each conflict would link through to relevant information and evidence.

5) The Archive section would have historical information and evidence drawn from the PAX process – searchable by date, topic, location and conflict. In time, this could become a valuable resource for students and researchers.

6) The About section would explain the background to PAX, the role of the PAX Trust, and how to get involved in or work with the organisation.

The website would also have the following functionality:

- Translation

  All main text on the site (headings, PAX Alarms, PAX reports etc) would be translated into the UN's six languages – by a team of translators. An automated translation tool, such as Google Translate, would be attached to each page for uploads, evaluation comments etc.

  In addition to both expert and automated translation, PAX would seek to build a community of volunteer translators – people around the world interested in helping to work towards conflict prevention. Some recent projects which have developed teams of volunteers to translate data include Ushahidi-Haiti and Mission 4636, translating messages from Haitians affected by the 2010 earthquake, and the Global Voices blogging community, which uses volunteer translators to bring blogs from around the world to a global readership.

- Search

  Search would be an important feature of the site given the volume of data coming into the PAX system. The search process would need to be via keywords, categories, filters, and maps.

- Share

  Sharing features would be built into every level of the site, allowing users to share, bookmark or download content.

The site would be built on open-source frameworks, and be hosted on a secure global Content Distribution Network, which would have servers around the world, with deep and broad levels of resilience and back-up, and robust security measures. And it would need to be developed by people who have experience in discourse analysis as well as those who know about causes of conflict.

One option for PAX may be to work with existing data mining and analysis tools, such as the SwiftRiver platform. This would require testing and adapting to meet PAX's aims. SwiftRiver is a free, open source platform which enables the filtering and verification of real-time data, sorted for authority and accuracy, combining natural language processing/artificial intelligence process and verification algorithms (www.swiftly.org).

Considerable work needs to be done during the Development, Pilot, Launch and Ongoing phases to ensure that the latest anti-spamming, anti-hacktivists, and anti-cyber-attack technologies were used on the site.

The development of the site would follow best-practice systems:

- A full Technical Specification with detailed wireframes would be drawn up, for approval and sign off.
- Usability Testing, with Scenario User Journeys, would be put in place at key stages of the development.
- A full technical testing process would ensure that the site worked across all browsers, operating systems and platforms; that it had the necessary SEO and accessibility features; that it linked cleanly to the relevant external sites and social networks; and that its navigation and layout was intuitive and clearly sign-posted.

The following page has a mock-up, for illustrative purposes only, of the proposed PAX homepage – showing the menu tabs, the Latest PAX Alarm, and Call to Action, Translate, Search, and About panels.

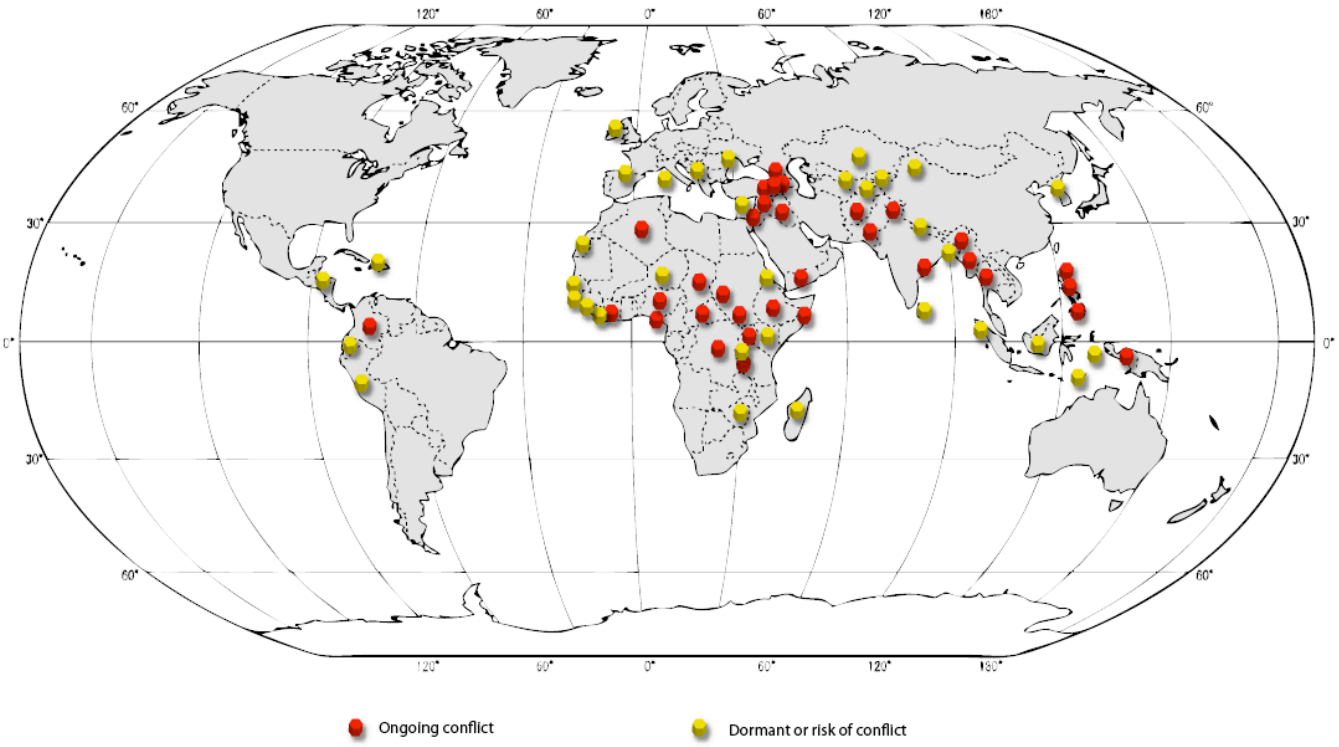
Mockup of PAX Homepage *© PAX 2011 Ltd*

6. Conflict Summary and PAX Case Studies

At the end of 2010, throughout the world, 42 armed conflicts were active. The map below highlights the main ongoing conflicts (in red), and dormant or at risk of conflict (in yellow).

The information for the map and the Conflict List was provided by the International Institute for Strategic Studies.

World Conflict Map



The IISS Conflict List (December 2010)

High Intensity
Afghanistan
Democratic Republic of Congo
Iraq
Pakistan (FATA & K-P/NWFP)
Somalia

Medium Intensity
Algeria (AQ Islamic Maghreb)
Colombia
Ethiopia (ONLF/ONLA and OLF/OLA)
India-Pakistan (Kashmir)
International Terrorism/Al-Qaeda
Israel (Intifada)
Korea – North and South
Myanmar
Pakistan (Balochistan)
Pakistan (TJP/SMP SSP/LeJ)
Philippines (ASG)
Philippines (NPA)
Russia (North Caucasus)
Sudan (Darfur)
Sudan (Southern)
Thailand
Turkey (PKK)
Yemen (Houthis/AQAP/SMM)

Low Intensity
Burundi (Palipehutu-FNL)
Central African Republic
Chad
Côte d'Ivoire
Georgia (Abkhazia)
Georgia (South Ossetia)
India (Assam)
India (Manipur)
India (Nagaland)
India (Naxalites)
India (Tripura)
Indonesia (Papua)
Lebanon-Hizbullah-Syria
Nagorno-Karabakh
Nigeria (Delta region)
Nigeria (Ethno-religious violence)
Philippines (MILF)
Southeast Asian Islamist terrorism
Uganda (LRA)

Dormant or Risk of Conflict:
Bangladesh
China (Xinjiang)
Cyprus
Ecuador
Eritrea-Ethiopia
France (Corsica)
Guinea
Guinea-Bissau
Haiti
Honduras
Indonesia (Aceh)
Indonesia (Kalimantan)
Indonesia (Maluku)
Kazakhstan
Kenya
Kosovo
Kyrgyzstan
Liberia
Madagascar
Moldova (Transnistria)
Morocco (Polisario Front)
Nepal
Niger
Peru
Rwanda
Sierra Leone
Spain (ETA)
Sri Lanka
Tajikistan
Timor-Leste (East Timor)
United Kingdom (Northern Ireland)
Uzbekistan
Zimbabwe

Case Study 1: Georgia 2008

Could PAX, by circulating information, have helped prevent the Georgia-Russia conflict of 2008 from turning into a war?

Months before war broke out, top insiders in Washington saw satellite pictures of Russian forces deployed beyond the Roki tunnel. As a result, Condoleezza Rice and her officials urged Georgia's government to act with caution. Rice herself visited Tbilisi on July 9 and, according to US officials, told President Saakashvili that if his government used force in South Ossetia, Russia would hit back hard - and Georgia would suffer.

The fact that Washington gave such warnings suggests that PAX is not needed, that lack of information is not the problem.

But that is not the whole story.

Soon after Rice's visit, the summer holidays began. President George W Bush flew to Beijing for the Olympics (where he met Prime Minister Vladimir Putin). The State Department was confident that its boss's advice, delivered less than a month ago, had been accepted. So it eased off the pressure. Then, on 7 August, Saakashvili launched the attack on the South Ossetian capital, Tskhinvali, which led Russia's army to sweep through Georgia.

In the four weeks since Rice's visit, citizens' uploads could have made the crucial difference, if mobile phones had been widely used in South Ossetia. But in 2008 they weren't - yet.

So Washington was not flooded with pictures and descriptions, including:

- Two improvised devices (IEDs) explode near Tskhinvali, killing one (25 July).
- A delegation from Georgia's defence ministry tours the South Ossetian conflict zone, planting a Georgian flag on the Sarabuki Heights (28 July).
- A Georgian military post on the Sarabuki Heights comes under fire (29 July)
- A bomb hits a Georgian police vehicle wounding five (1 August).
- A shoot-out between Georgian and South Ossetian forces leaves six dead and dozens injured. Tbilisi and Tskhinvali each blame the other (2 August).

Those incidents all occurred in just one week. No doubt US diplomats reported them to Washington. But they failed to make the State Department revive its pressure. Had South Ossetians been uploading pictures and reports to Twitter, Facebook, the websites of their local newspapers and TV channels, Amnesty International etc, PAX would almost certainly have categorised South Ossetia as an Alarm zone.

Consequently it would have commissioned fast, high level evaluations of the data and it would have passed selected extracts to its key NGO and other allies in Washington. These allies would have been, or had easy access to, beltway insiders – who knew the way to get through to the President, the Secretary of State, top officials, Senators, and Congressmen. And people who could organise big public meetings fast. And those able to get well-briefed celebrities onto television.

Their purpose would have been to persuade them that late July 2008 was not the moment to stop trying to calm Saakashvili.

If its allies had thus succeeded in persuading Rice to fly back to Tbilisi, PAX would have moved onto the next stage in its task. It would have asked what current data could best help her prove to Saakashvili that failure to halt the slide towards war would do his country major damage. PAX and its allies would then have made the latest uploads available to Rice, live, to be ordered and shown to Saakashvili in his office.

Thus PAX might have helped Washington prevent the 2008 war.

What if a similar crisis were to arise again? Saakashvili would probably be weaker, others throughout Georgia and South Ossetia stronger. So the efforts of NGOs and peacemakers on the ground would be more significant. It would be vital for PAX to equip those dedicated to calming rival war-mongers with the latest data. Then they could each show today's uploads to the leaders they were seeking to deflect from violence.

In the cities and villages of Georgia/South Ossetia, the latest citizen-reporting, made available by PAX, would thus increase the chance of making angry young men put their AK47s back under the bed.

Case Study 2: Kyrgyzstan 2010

In June 2010, fighting in the cities of Osh and Jalalabad resulted in the destruction of homes in Uzbek neighbourhoods, up to 400 deaths of mainly Uzbek residents, and 400,000 fleeing in fear of the violence. In the months before June, a number of incidents would have resulted in the region being designated a PAX Alarm zone.

Most important in provoking the PAX system would have been the uprising on April 7th in the capital Bishkek, in which 85 people were killed and President Kurmanbek Bakiyev was ousted from power. In the weeks before the uprising in Bishkek, many internet sites were blocked by the Kyrgyz government.

By April 2010, mobile phone penetration in Kyrgyzstan had reached 85%, at least one phone per household, and 40% of the population were able to access the internet, mainly in public places such as internet cafes, workplaces, and educational institutions. As the state-owned news media in Kyrgyzstan imposed a total blackout on reporting the April uprising, many people in the country are likely to have accessed news on the events through word of mouth, telephone calls and text messaging.

One of the main telephone networks, Megafon, became completely inaccessible on April 7th, and difficulties with buying credit for the network were reported on April 8th. Whether the shutdown of the mobile network resulted from traffic overload or government censorship remains unclear.

The April uprising was followed by a period of unrest during which Bakiyev fled to South Kyrgyzstan, where many of his core supporters are based. Throughout May, incidents between Bakiyev supporters and local Uzbek politicians would have led PAX to shift the area from Early Warning to High Tension.

On 14th May, riots by Kyrgyzstan's residents resulted in the occupation of local government buildings in Osh and Jalalabad, during which one person was killed, and the two provisional governors were removed by force. Then an arson attack on the Bakiyev family compound was followed by the storming of the Uzbek-led university in Jalalabad by Bakiyev's supporters, causing two further fatalities. These incidents were all reported online by news agencies, both local and international, but made little impact on worldwide headlines.

It was clear that the national provisional government, based in Bishkek – which had taken over for an interim period following the April uprising, until elections could be held in October – lacked control in the Southern region.

In addition to online news reports, analyses published by regional specialists throughout May warned both of growing inter-ethnic tension, and of the danger inherent in the provisional government's weakness in the south.

Rumours spread through Osh of rival armed groups of young Uzbeks and Kyrgyz. These rumours were picked up by local news reports and online discussion forums. The posting of hate messages, emphasising ethnic divisions and mutual suspicion, would have automatically increased Southern Kyrgyzstan's prominence in the PAX tension-measuring system.

On May 19th, events appeared to crescendo with an armed protest by residents in Jalalabad against local Uzbek community leader, Kadyrjan Batyrov, whom they blamed for the arson attack at Bakiyev's family compound and for the increase in inter-ethnic tensions. Three people were killed in clashes along ethnic lines and the provisional government responded by declaring a state of emergency. This heightened tension would have led PAX to consider moving the region to Alarm zone status and issuing reports to those who might have brought about action to calm the situation.

While access to mobile phones is widespread throughout Kyrgyzstan, participation in social media such as Twitter's micro-blogging tools is not.

During the April uprising, a Kyrgyz student in the diaspora, Elena Skochilo in Tennessee, became a vital source of real-time information as she published updates that she was receiving from friends and contacts in Osh and Jalalabad on her *Morrire* blog. News via Elena in the US became more instant and informative than news from the state or international media, which had little presence in Osh and Jalalabad.

Kyrgyzstan had been seen by many Western foreign policy-makers as an 'island of democracy' among its more troubled neighbours, and then more recently the US and Russia appeared to lose confidence in the provisional government, stepping back from involvement. Evidence of the threat of violence accelerating in April and May 2010 was insufficient to alter this perspective.

PAX distributing and placing information from ground level would have increased the chance that the message of intensifying danger got through. Governments such as those of Russia, China, and the US (which leases a military airbase in Manas, Kyrgyzstan, to deliver supplies to its forces in Afghanistan) all had an interest in preventing conflict in Kyrgyzstan damaging stability in the region.

Had PAX been monitoring the data coming out in April and May, had it consequently declared Kyrgyzstan an Alarm zone, and had the evidence been pressed on key leaders, the threat of war would surely have received more attention in time to increase the chance of preventing the events of June.

Case Study 3: South Sudan 2011 (written in January 2011)

As Southern Sudan prepared for the announcement in early February of the results of its referendum on independence, many observers predicted violent conflict.

One problem PAX would have faced, had it been seeking to report the risk of war, is the Sudanese government's interception legislation. Khartoum has invested heavily in both monitoring telecommunications and filtering the internet with the use of SmartFilter software.

Since 2008, mobile phone users in Sudan have had to provide registration details to their mobile network operator. In the case of MTN, this resulted in the disconnection and loss of an estimated 1 million customers. So someone who wanted to upload information would find it difficult to buy a mobile anonymously with cash.

Still, access to mobiles in Sudan is growing fast, with subscription penetration currently at 36% of the population. And 10% of Sudan's population are internet users (accessing primarily through public places such as internet cafes).

Sudan's telecoms infrastructure is relatively well-equipped in urban areas, and benefits from investment in 3G networks and connection to the FLAG (Fiber-optic Link Around the Globe) and the EASSY (East Africa Submarine Cable System) networks.

The Comprehensive Peace Agreement of 2005 (signed by the Khartoum government and the Sudanese Peoples Liberation Movement, SPLM) gave the government of Southern Sudan the right to license two mobile network operators, Gemtel and Vivacell. They use the Ugandan international dialling code rather than the Sudanese. Thus South Sudan entered a space for communications outside the reach of Khartoum. The number of Sudanese from both North and South, putting political opinions or reports about the situation online is low, but growing fast.

In the presidential elections in April 2010, a group of young citizens, Girifna (Arabic for 'We are fed up'), was formed in response to the lack of information on election registration. Girifna created a website with the help of Sudanese contacts in New York, and communicates via YouTube and Twitter (which helped alert the world to the arrest of several of its members).

A further push towards opening up communications has come from the US Treasury. It has modified its Sudanese Sanctions Regulations to facilitate social media and other web technology exports to Sudan.

Mobile message optimisers - such as ForgetMeNot Software's eTXT - which enable communications via email and online chat on a basic handset, have uncovered a huge demand from consumers across Africa to access Facebook.

Even in regions where internet, smartphone and computer access are low, most people can borrow or briefly hire a mobile phone to call relatives, partners, friends in the – increasingly numerous and wired - Sudanese diaspora. So in both North and South, connecting with the world outside Sudan is becoming easier.

During 2010, the SPLM reported the build up of tens of thousands of Sudan government troops in the border areas of oil-producing Heglig and Unity, as well as South Kordofan, Abyei, Raja. The SPLM says it raised this issue at three consecutive Ceasefire Monitoring Commission meetings, but was told by the UN that the matter could not be investigated due to lack of access.

Satellite imagery should enable PAX – and other bodies with which it would seek to co-operate - to monitor troop movements and attacks on remote areas, without the restraints that UN-backed bodies sometimes suffer.

In the second half of 2010, a number of border incidents were reported, including a shooting in Abyei by northern Sudan soldiers and fighting between North and South Sudanese armies on the border between Sennar and Upper Nile states. As the referendum began, ten Southern Sudanese returnees were killed in an ambush on the northern side of the South Kordofan state border, allegedly by armed Misseriya militias.

The Satellite Sentinel project was launched to monitor events in the border region through satellite images and reports gathered by the Enough Project and Sudan Vote Monitor. The information obtained includes high resolution imagery of Sudanese government troops deployed along the border. Putting such a spotlight on the region must surely help prevent the escalation of conflict.

7. Governance, Key Allies, Operations and Budgets

Governance

We propose that PAX should be governed by an international trust (the PAX Trust). Among those who might be asked to nominate members would be NGOs, universities, and research institutions that specialise in foreign policy, strategy, and defence.

Trust members should be drawn from Asia, the Islamic world, Africa and Latin America, as well as from Europe and North America.

The PAX Trust should normally meet by video-conference - partly to avoid unnecessary travel, and partly because, when an Alarm occurs, meetings may be needed at short notice.

The Trust would have the following tasks:

- To protect PAX's independence.
- To monitor the performance of the service, and hold its senior executives to account for standards and delivery.
- To deal with serious complaints.
- To help ensure that PAX Alarms get to people and organisations with influence.
- To sign off senior appointments, oversee annual budgets, and discuss and approve strategic development.

Overall, the Trust would be responsible for ensuring that PAX and its management and editorial teams observe the key values of accuracy, multi-culturalism, independence, impartiality, partnership and openness.

We also propose that members of the Trust would form an Executive Board **-** which would oversee the more general management issues.

Key Allies

Many organisations work at preventing war. All those PAX has contacted say that the data it proposes to gather could help them in that task. Formalising alliances with them would be crucial for PAX, particularly when it declares an Alarm and urgent action is needed to use the data to try to prevent a war exploding.

The precise character of their relationship with PAX remains to be worked out. Perhaps such organisations should be asked to nominate members to the PAX Trust. Or might such close association with some of them lead particular governments to distrust PAX's data? Could those organisations that see advantage in having access to PAX reports set up an independent committee to keep an eye on its work?

Some of these bodies have ex-presidents, prime ministers and foreign ministers on their boards - the kind of people who can quickly get through to those currently in office.

And members or ex-members of international courts could be asked to keep an eye on PAX's evaluators and, when Pax's reports are challenged, to offer an independent judgement on their quality.

Operations

PAX would be based on the following operational principles:

1) It would be run on a global basis – with staff spread around a number of centres in different continents. The centres would keep in contact via desktop video links, and by working within an integrated and shared online work portal.

   Travel and courier costs would be kept to a minimum. Video conferencing would be built into the daily operation for all staff and centres. All documents would be distributed electronically.

2) Staff would be recruited from different backgrounds, to ensure that the operation was truly multi-cultural.

3) Initial and ongoing training would be given a high priority – to instill the PAX values of accuracy, impartiality and independence into all activities.

Phasing

We propose a 5-phase approach for PAX:

1) Phase One: Feasibility Study

   The current phase – which has included desk research, interviews, meetings, a project website, and this document.

2) Phase Two: Development

   This would cover:

   - Fundraising.
   - Refinement of the proposal in the light of feedback and technical, digital, and diplomatic developments.
   - Compilation and issue of a Technical Specification to third party systems companies – to allow us to compile a more detailed technical proposal, to investigate more fully keyword searches in local languages, and to formulate more accurate cost options.
   - Further investigation of the role that PAX would play after the issuing of PAX alarms.
   - Liaison with stakeholders – and discussion of how PAX could collaborate with other organisations.
   - Negotiation with satellite companies about access to images.
   - Discussions and, if necessary, negotiations with existing alert websites and global organisations about automated news and information feeds.
   - Setting up the corporate and legal framework for the organisation.

3) Phase Three: Pilot

   We believe that it is crucial that we carry out a pilot phase – although the scale and nature of the pilot would depend on funding and further discussions.

   It could focus on one target area, using existing digital networks, or cover some or all of the known conflict zones, with a fully-developed PAX digital system.

4) Phase Four: Launch

The Launch would include:

- Setting up the PAX Trust and senior team
- A global roll-out of the service
- Compilation of the necessary databases
- Appointing and training all staff
- Online marketing and PR activities.

5) Phase Five: Ongoing Service

Budget

As part of this Feasibility Study, we have drawn up an illustrative annual operating budget.

The budget needs more work as the plans continue to develop, as the potential for and level of funding becomes clearer, and as we get a more accurate insight into necessary staffing levels, translation processes, and the cost of building the PAX computer technical system.

The budget is based on the following proposed staff requirements:

- PAX Editor - to lead the editorial and web teams, and be responsible for the editorial output of the digital service.
- Editorial Staff - to compile information for the website, support the online evaluation community (both volunteer and paid evaluators), send information to Specialist Evaluators, and write the reports that would go out with a PAX Alarm.
- Website Editorial Team - to write information for the website, and to input text and images into the PAX Content Management System.
- Translation Producers - to co-ordinate the translation process.
- Translators - to present the main parts of the website in the six UN languages, and those of danger zones.
- Database Researchers - to compile the Specialist Experts' Database, and the database for sending out PAX Alarms.
- Website Designer and Developers - to maintain and develop the website.

- Systems Programmers - to maintain and develop the PAX Digital System.
- Management Staff - to include Executive Director, Head of Technology, Finance Director, Finance Manager, Business Affairs Executive (to oversee contracts and legal issues), Office/HR Executive, and other support staff.
- Public Affairs Staff – including Head of Public Affairs, Head of Stakeholder Relations and Fundraising, and Online Marketing Executive.

Other costs in the budget include:

- Development and maintenance of the Digital Service
- Design and development of the website
- Hosting and streaming
- Office IT and communications
- Desk-top and meeting room video-conference systems
- Office and website software
- Insurance
- Search Engine Marketing (SEM)
- Staff costs
- Limited travel costs
- Accountancy/audit fees/legal fees
- General office costs.

Funding

PAX would be non-profit-making, and it would therefore need to attract funding from people or organisations who wanted to support its aims.

To achieve this, PAX would need to:

1) Set up a professional fundraising operation, led by an experienced fundraising executive, and supported by the necessary documents and promotional material.
2) Agree what kind of people and organisations could fund PAX, and draw up guidelines on how their role would be explained on the website.

Given the economic downturn, fundraising could be difficult. However, we remain confident that PAX is an appropriate target for potential funders and funding organisations.

In the longer term, as the site grows, alternative or supplementary revenue sources could include: appropriate advertising/sponsorship, crowdsourced donations or subscriptions from site users and supporters, or income from access to PAX's information archive.

Profile

PAX would need to put effort into building its profile – ensuring that people around the world knew of its role and how it worked. This would need to include:

- SEO (Search Engine Optimisation) – the website would need to be optimised to perform well in search engines.
- SEM (Search Engine Marketing) – we are proposing in the budget a substantial ongoing campaign.
- PR – the aim would be to get coverage about PAX in newspapers, magazines, online sites, blogs, radio and TV programmes, around the world.
- Stakeholder Relations – it would be important to maintain constructive relations with a wide range of NGOs and other relevant bodies, so that PAX could be promoted through these third party organisations.
- Public Affairs – events and other activities would need organising to raise PAX's profile amongst governments, policy and international organisations, and university departments.

8. Other Early Warning Systems

Overview

The field of conflict early warning expanded during the post-Cold War period, primarily as a result of the genocide in Rwanda and the civil wars in the Balkans in the 1990s, and the failure to prevent violence in both cases.

Worldwide reaction to these events and debate on how they might have been prevented have resulted in advances in early warning research.

This research has taken a variety of approaches – including conflict modelling, military simulation exercises, field monitors reporting directly from areas at risk of conflict, and analysis of online newsfeeds and other data.

For this study, we have spoken with several of the leading voices in this field, including:

- Heinz Krummenacher, Deputy Director of Swisspeace, CEO of the BEFORE project and former Head of the FAST International early warning programme.
- Andrew Stroehlein, Communications Director at International Crisis Group.
- Christoph Meyer, Senior Lecturer, War Studies Department, King's College London University and lead of the FORESIGHT Early Warning and Conflict Prevention research group.
- David Nyheim, Chief Executive of International Conflict and Security (INCAS) Consulting Ltd, former Director of the FEWER early warning programme, author of 'Preventing Violence, War and State Collapse, The Future of Conflict Early Warning and Response' report for OECD (2009).

Other Systems

The evolution of this field has been charted through three phases, which those working in the field call three 'generations'.

1) First generation refers to the systems developed from the mid-1990s onwards by inter- and non-governmental institutions, including, for example, the European Commission conflict indicators, using quantitative and qualitative data analysis.

   This work was mainly carried out within institutional headquarters in the West, looking at conflicts in developing countries.

2) Second generation systems were developed in the early 2000s, with a greater link to affected locations, and were characterised by regional initiatives, and moves towards using designated reporters on the ground.

   These systems introduced qualitative in-country data gathering, and one example was FAST, the Swisspeace early warning programme.

   This phase demonstrated the importance of including local perception of threats and events in the data stream.

3) Third generation early warning systems incorporate micro-level early warning systems, capitalising on developments in technology to enable real-time access and evaluation.

   An example of a third generation system is the Foundation for Co-Existence in Sri Lanka, which has appointed monitors throughout the country, all involved in both monitoring and response, through, for example, local mediation.

   The shift is from hierarchical systems, where information is gathered and fed upwards to institutions with the aim of initiating prevention and response, to more horizontal structures, which enable early response by those directly affected by violence.

Two of the larger scale systems, FAST and FEWER, were operational during the earlier part of the last decade and were ambitious in scale and reach.

Their closure (FEWER in 2003 and FAST in 2008) has left a gap in the field. This is now being filled with fourth generation, more people-centred, conflict-located and bottom-up early warning systems, as defined by early warning expert Patrick Meier, increasingly using crowdsourcing and crisis mapping approaches and powered by Web 2.0 platforms, such as FrontlineSMS (www.frontlinesms.org) and Ushahidi (www.ushahidi.com).

The Ushahidi platform, which developed in response to the post-election violence in Kenya in 2008, involves visually mapping reports from the web and mobile phones, providing an instant and visual timeline of events unfolding and alternative sources of information to the mainstream media.

Ushahidi has now been used in many different contexts including humanitarian disaster response in Haiti and the Pakistan floods, election monitoring in Sudan, immigrant harassment in Arizona, and monitoring violence in South Africa, Democratic Republic of Congo (DRC), Pakistan and Gaza.

The recent launch of the Satellite Sentinel project in South Sudan provides an interesting addition to the field of early warning. It combines analysis of satellite images of the border area by experts at UNOSAT with local reports of incidents.

An example of a highly micro-level project is the Voix des Kivus pilot project (http://cu-csds.org/projects/event-mapping-in-congo/), which uses mobile phones to link up villages in South Kivu, DRC, with a view to examining how this might assist in monitoring events, and possible response and prevention. Mobile phones have been issued to people in fifteen villages and data is submitted weekly to report events, including disease outbreaks, population movement and conflict incidents. Sensitive information is shared with development organisations in DRC. A key objective of the project is to learn whether the system is seen to be of value to its users.

A major independent global operation is the International Crisis Group. Their Crisiswatch Bulletins and Reports, together with high-level lobbying, have developed throughout the period from first to third generation, evolving from headquarters-based into regional reporter-based operations. ICG's reports on threats and developing events include both the local reporter perspective from the ground and expert analysis.

David Nyheim's overview of early warning systems in the OECD report 'Preventing Violence, War and State Collapse', warns that despite much progress in the field, particularly in data collection and analysis, it is difficult to monitor success and effectiveness and it cannot be stated with confidence that an event like the Rwandan genocide would be prevented through current early warning systems.

Other Early Warning Systems: Summary

This review suggests that:

1) Although a lot of work has been done in this area, no early warning digital system as ambitious as PAX has been attempted.

   Ushahidi's work has been groundbreaking in establishing the potential for crowdsourcing to improve the information flows from conflict-affected communities, as demonstrated by their work on monitoring violence in Kenya, and their deployments in DRC, Gaza and South Africa.

   Its platform has proved to be applicable to many different data-gathering situations, including election monitoring and natural disaster response.

   PAX would seek to complement or collaborate with Ushahidi's work in monitoring violent incidents and take it the next stage by (a) focusing only on violent conflict, (b) doing so on a world-wide basis, and (c) helping to ensure that warning alerts reach those able to respond, from governments and organisations with influence, locally, regionally and internationally, through to those directly affected by the conflict.

   PAX would also need to complement or collaborate with the Satellite Sentinel project, if it is extended to other areas after Sudan. The points of difference would be that PAX's prime target would be emerging rather than existing conflicts, and that its main focus would be communications data.

2) Work in this field demonstrates the importance of including on-the-ground local evidence of threats and events.

3) Lessons from the projects developed so far emphasise the importance of having a 'mixed economy' approach – having both automated computer analysis and manual, expert evaluation.

9. Conclusion

1) The rapid growth of digital communications means that a large and growing volume of information is coming out of actual and potential conflict areas – even in less developed parts of the world.

2) This data and information includes uploads from mobiles and the internet, information on public websites, postings on social networks, and/or feeds from global alert and information organisations.

3) A PAX digital system could be developed that mined this information – through automated and sophisticated keyword searches and data filtering.

4) This raw flow of data could be evaluated, first, by registered volunteer evaluators on the PAX website and, then, when a conflict reaches the 'Tension' point, by paid specialist experts selected by the PAX team.

5) The automated keyword searches would look for 'danger' words in potential conflict languages. The main sections of the website would be in the UN's six languages.

6) Measures would be taken in the development of the PAX digital system to adopt the latest computer security systems to seek to identify misinformation and prevent cyber-attacks. As none of these systems can provide 100% security, it is important that the PAX Alarm and report stage of the process is produced by editorial staff with the appropriate expertise.

7) The latest anonymising and circumvention software and techniques would be used to try to protect the identity of people uploading information. However, this remains a serious issue, and PAX would have to warn uploaders about the risks involved.

8) Satellite imagery could currently be used as a verification tool by PAX's specialist experts, if terms can be agreed with the satellite companies. In the future, satellite data could become an important part of PAX's automated process.

9) We believe that – as our case studies suggest - the distribution of timely and trusted PAX Alarms could make a difference, and have an impact on emerging conflicts.

10) We have demonstrated that although other websites and organisations are involved in conflict prevention, none have so far matched the ambition and breadth of the PAX proposal – to set up a global digital system that mines and evaluates data sources, and then sends out alarms to those with influence.

11) PAX would require extensive profile-raising and promotional activities, to ensure that the service becomes known.

12) A major question is whether PAX could attract enough funding to cover its costs.

10. Next Steps

The PAX project team propose the following next steps:

1) This document will be circulated to the Steering Group, Google, all those who contributed to the study, and a list of other interested people and organisations. A printable PDF version will be available on the PAX project website (www.pax2011.org).

2) Feedback from this circulation and from the 'Tell Us What You Think' page on the project website will be collated in February/March 2011, and lead to the production of an updated and final version of the Feasibility Study.

3) The project team would then focus on the following activities:

   - Continue to refine the proposals in the light of further feedback and technological and digital developments.
   - Seek funding for the Development phase of the project (as outlined in Section 7).
   - Support the holding of a technical summit meeting with other organisations active in this field to explore areas of collaboration.

Appendix 1 – PAX Background

Background to PAX

In 2009/10, the UK documentary-maker Brian Lapping proposed setting up a website to help prevent wars through the use of mobile phones and satellite images.

He wrote a series of proposal documents and distributed them to media, government and academic contacts. He requested feedback, and adjusted his proposals accordingly.

This led to a workshop hosted by Google in London in May 2010. The meeting was attended by people with experience in the UN, the British government, NGOs, the media, universities, and international strategy organisations.

Following this meeting, a PAX Steering Committee was set up – and Google provided funds for the Feasibility Study and project website.

The Feasibility Study Document

This document has been edited by Brian Lapping and Nigel Dacre – and written by them and Catherine Dempsey. Tony Curzon-Price contributed to the PAX algorithm section, and Ashok Shah to the budget section.

The branding and graphics were designed by Hazel Dormer of Ikonika. The project website was designed and developed by the Ten Alps company DBDA.

PAX Steering Group

The Steering Group has the following members:

Tony Curzon-Price	Editor-in-Chief, openDemocracy. Founded Arithmatica at UCL, and moved it to Silicon Valley.
Nigel Dacre	CEO, Inclusive Digital TV and former Editor of ITV News and founder CEO Teachers TV.
David Elstein	Chairman of openDemocracy and DCD Media plc. Former CEO of Channel Five, and Head of Programming at BSkyB and Thames TV.

Scilla Elworthy	Founder Peace Direct and Oxford Research Group.
Sir Lawrence Freedman	Professor of War Studies and Vice Principal (Research), King's College London.
Lucian Hudson	Former Director of Communications, Foreign and Commonwealth Office.
Nigel Inkster	Director of Transnational Threats, International Institute for Strategic Studies.
Brian Lapping	Chairman, Brook Lapping Productions.
Robert McFarland	Former CEO BOC Group South Asia, the Middle East and Africa.
Paul Mitchell	Documentary Television Producer.
Edward Mortimer	Senior Vice President at the Salzburg Global Seminar. Former Director of Communications, UN.
Dan Smith	Secretary General, International Alert.

Appendix 2 – Acknowledgments

Many organisations and individuals have put forward thoughts and ideas on the PAX proposal. We would like to thank the PAX Steering Group, those listed on this page, and others who spoke to us 'off the record', for their advice and contributions.

- Ken Banks, kiwanja.net and FrontlineSMS
- Peter Barron, Google
- Charlie Beckett, POLIS, London School of Economics
- Ronnie Bregman, Department of War Studies, King's College London
- Gerhard Brey, Centre for Computing in the Humanities, King's College London
- Lars Bromley, UNITAR/UNOSAT
- Lesley Calmels, Brook Lapping Productions
- Kasey Chappelle, Vodafone Group
- Denis Corboy, Caucasus Policy Institute, King's College London
- Steve Crawshaw, Amnesty International
- Katy Cronin, The Elders
- Laura Crow, Vodafone Group
- Winston Fletcher, advertising marketing and communications
- Joel Gabri, Peace Direct and Insight on Conflict
- Nik Gowing, BBC World News
- Carolyn Hayman, Peace Direct
- Gerd Hagmeyer-Gaverus, Stockholm International Peace Research Institute
- Knut Holm, African affairs expert
- Florence Iheme, ECOWARN
- Gulalai Ismail, Aware Girls
- Bhupendra Jasani, Department of War Studies, King's College London
- Peter Kellner, YouGov
- Joanna Kidd, International Centre for Security Analysis, King's College London
- Raymond Kitevu, CEWARN
- Heinz Krummenacher, Swisspeace
- Anne Lapping, Executive Producer
- Americo Lenza, Vodafone Group
- Chris Locke, GSM Association
- John Lotherington, Salzburg Global Seminar
- Geir Lundestad, Norwegian Nobel Institute
- Ross Macdonald, PalmTree Technology
- G Mcquaid, Vodafone Group
- Neil Melvin, Stockholm International Peace Research Institute

- Patrick Meier, Ushahidi
- Christoph Meyer, FORESIGHT, King's College London
- Tina Micklethwait, Salzburg Global Seminar
- Julie Minns, Three
- Hanna Ucko Neill, International Institute for Strategic Studies
- Landry Ninteretse, Amahoro Youth Club
- Ruairi Nolan, Peace Direct and Insight on Conflict
- David Nyheim, International Conflict and Security Consulting Ltd
- Chiyedza Nyahue, Envision Zimbabwe Women's Trust
- Jean Oelwang, Virgin Unite
- Lord Owen, former British Foreign Secretary
- Norma Percy, Brook Lapping Productions
- Robert Picciotto, Conflict, Security and Development, King's College London
- Dan Plesch, SOAS
- Oliver Ramsbotham, Conflict Resolution, University of Bradford
- Gabrielle Rifkind, Middle East Programme, Oxford Research Group
- Adam Roberts, President, British Academy
- Paul Roberts, ForgetMeNot Software
- Harold Short, Department for Computing and Humanities, King's College London
- Mike Short, Telefonica Europe and MDA (Mobile Data Association)
- Kishor Silwal, Youth Alliance for Peace and Environment
- John Sloboda, Iraq Body Count, Oxford Research Group
- Andrew Stroehlein, International Crisis Group
- Martin Sweeting, Surrey Satellite Technology Ltd
- Steve Titherington, BBC World News
- Jeremy Tunstall, formerly of City University
- Staff at Videre
- Stefan Voigt, German Aerospace Center
- Veronica Wadley, Chairman, Arts Council, London and former editor Evening Standard
- Tim Williams, Vodafone Group
- Mark Wood, Future Publishing, formerly ITN and Reuters

References

The following reports, blogs and articles have been read as part of the desk research carried out for the Feasibility Study:

- Lars Bromley, 'Relating violence to MODIS fire detections in Darfur, Sudan' (International Journal of Remote Sensing, 31:9, 2277 – 2292, May 2010)

- Diane Coyle and Patrick Meier, 'New Technologies in Emergencies and Conflicts, The Role of Information and Social Networks' (UN Foundation-Vodafone Group Foundation Partnership, 2009)
- Sokari Ekine, 'SMS Uprising, Mobile Phone Activism in Africa' (Pambazuka Press, 2010)
- Joshua Goldstein and Juliana Rotich, 'Digitally Networked Technology in Kenya's 2007 – 2008 Post-Election Crisis (Berkman Center Research Publication, September 2008)
- Caroline Hargreaves and Sanjana Hattotuwa, 'ICTs for the Prevention of Mass Atrocity Crimes' (ICT for Peace Foundation, October 2010)
- Jessica Heinzelman and Carol Waters, 'Crowdsourcing Crisis Information in Disaster-Affected Haiti' (United States Institute of Peace, October 2010)
- International Crisis Group, 'The Pogroms in Kyrgyzstan' (Asia Report No 193, 23 August 2010)
- International Crisis Group, 'Negotiating Sudan's North-South Future' (Africa Briefing No. 76, 23 November 2010)
- International Telecommunication Union, 'Informatiom Society Statistical Profiles 2009 Africa' (ITU, 2009)
- International Telecommunication Union, 'Measuring the Information Society (ITU, 2010)
- Sheila Kinkade and Katrin Verclas, 'Wireless Technology for Social Change: Trends in Mobile Use by NGOs' (UN Foundation-Vodafone Group Foundation Partnership, 2008)
- Agnieszka Konkel and Richard Heeks, 'Challenging conventional views on mobile-telecommunications investment: evidence from conflict' (Development in Practice, Vol 19 No. 3, May 2009)
- Patrick Meier and Jennifer Leaning, 'Applying Technology to Crisis Mapping and Early Warning in Humanitarian Settings' (Harvard Humanitarian Initiative Working Paper Series No. 1, September 2009)
- David Nyheim, 'Preventing Violence, War and State Collapse, The Future of Conflict Early Warning and Response' (OECD, 2009)
- David Nyheim, 'The Global Balance Sheet: Emerging Security Threats and Multilateral Response Capabilities' (The Stanley Foundation, Working Paper, October 2009)
- Ivan Sigal, 'Digital Media in Conflict-Prone Societies', (Center for International Media Assistance report, October 2009)
- Lawrence Woocher, 'Preventing Violent Conflict Assessing Progress, Meeting Challenges' (Special Report United States Institute of Peace, September 2009)

Blogs and Articles:

http://irevolution.wordpress.com/
http://earlywarning.wordpress.com/
http://www.bbc.co.uk/blogs/podsandblogs/2008/08/south_ossetia_in_social_media.s
http://www.opendemocracy.net/article/citizen-war-reporter
http://globalvoicesonline.org/2010/06/03/georgia-social-media-deployed-for-local-elections/

http://globalvoicesonline.org/-/world/central-asia-caucasus/georgia/
http://www.centerforsocialmedia.org/blog/future-public-media/where-hostile-governments-meet-public-media
http://www.opendemocracy.net/od-russia/madeleine-reeves/breaking-point-why-kyrgyz-lost-their-patience
http://www.usip.org/events/crisis-in-kyrgyzstan-perspectives-kyrgyz-and-uzbek-youth
http://www.registan.net/index.php/2010/06/23/digital-memory-and-a-massacre-2/
http://www.registan.net/index.php/2010/04/08/why-kyrgyzstan's-social-media-matters/
http://globalvoicesonline.org/2010/04/10/morrire/
http://globalvoicesonline.org/2010/06/13/kyrgyzstan-uzbekistan-initial-coverage-of-the-osh-massacre/
http://en.rian.ru/analysis/20100621/159517114.html
http://www.eurasianet.org/node/61004
http://3dblogger.typepad.com/osce_unbound/2010/04/yes-kyrgyzstans-red-blood-tulip-revolution-is-a-twitter-revolution.html
http://ibrahimbadawi.com/2010/03/31/can-twitter-bird-fly-in-sudan/
http://southsudaninfo.net/2010/04/girifna-political-activism-is-a-brave-proposition-in-sudan/
http://pulitzercenter.org/articles/challenge-sudanese-ruling-party-student-activists-rally-democracy

Organisations consulted:

http://mobileactive.org/
http://www.ushahidi.com/
http://acd.iiss.org/
http://www.systemicpeace.org/warlist.htm
http://www.ploughshares.ca/imagesarticles/ACR10/98204_armed_conflict87-09.pdf
http://www.usip.org/files/resources/preventing_violent_conflict.pdf
http://cu-csds.org/projects/event-mapping-in-congo/
http://www.crisisgroup.org/
http://www.girifna.com/
http://shr.aaas.org/geotech/
http://unosat.web.cern.ch/unosat/asp/prod_free.asp?id=23
http://unosat.web.cern.ch/unosat/asp/prod_free.asp?id=101

Disclaimer

This document has been prepared solely for the purpose of providing general information about PAX. PAX 2011 Ltd reserves the right to make changes to PAX and its proposal. To the best of PAX 2011's knowledge the information contained in this publication is accurate; however, we do not assume any liability whatsoever for the accuracy or completeness of such information. To the extent permitted by law, PAX 2011 Ltd disclaims all warranties.

PAX will accept no liability either directly or indirectly for any consequential damages from any use of this document including without limitation any loss of profits, business interruption, or otherwise.

This document is not intended to and does not create any legal or other relationship between PAX 2011 Ltd and any third party.