*** Central Government Crisis Management Centre ***

(1) **Background** – The Central Government has decided to upgrade and establish a new generation crisis management centre using state-of-the-art 21st Century technologies and networked applications. This short proposal summarises an innovative approach to the design of such a new generation real-time architecture that allows for the identification, management and resolution of potential major crises.

(2) **Crisis Definition** – The new centre will need to identify and manage a diverse range of crises that may include the following as well as local and regional emergencies:

a. Environmental Events – Forest Fires, Earthquakes, Tsunamis, Landslides, Avalanches.
b. Transportation Events – Airports, Trains, Cars, and related infrastructure & facilities.
c. Terrorist Incidents – Including biological, nuclear, chemical, kidnapping & similar.
d. Industrial Events – Gas, Poison, Chemicals, Petroleum, Radiation, Fires, Explosions.
e. Utilities Failures – Electrical Grid, Water, Gas, Telecommunications
f. Net Security Attack – Distributed Denial of Service (National Level), Virus, Trojan…

It will be critical that potential & emergent crises are identified quickly and correctly, and that appropriate alerts are issued to a pre-arranged team of networked & trained specialists. In previous 20th century solutions, the crisis centre was typically a large operations room with wall screens, telephones, terminals and databases. These "war room" solutions were very much inspired by the systems architectures of the industrial and information societies. In our innovative proposal we recommending updating the architecture to one that allows the crisis response network to be fully "virtualised" and distributed such that there is always some redundancy in the management control, and the necessary supporting resources.

(3) **Proposal** – We recommend the construction of both a physical "crisis centre", with remote underground back-up, regional offices, and coupled with a fully "virtualised network".

a. **Physical Centre**: Modelled on 20th Century "War Room" (close to Central Government), but with redundant national underground back-up, and regional Government centres. The focus would be real-time access to on-line multimedia intelligence, both nationally and internationally. Intelligent Software agents would be permanently data mining for emergent event detection within the terabytes of dynamic storage area networks. These would be a combination of secure Government, enterprise, and military sources, as well as agreed international intelligence exchanges.
b. **Virtual Crisis Centre**: All resources on-line, and linked through wired/wireless networks to all trained specialists and crisis operators. Multimedia information,

videos, alerts provided and engineered using open source standards to generic mobile devices. Redundant Communications options including WiMax, Wi-Fi, 3G, DSL, to allow team interaction depending on available networks. As the network develops, it is suggested that active consideration be given to the implementation of 3D Virtual Reality environments such as those use in compelling ways for SecondLife and similar MMORG (Massively Multiplayer On-Line Role-Playing Games). These state-of-the-art architectures are most probably ideal and adaptable for enhancing the speed and accuracy of the virtual networked crisis response teams.

c. **Redundancy of Control**: Allow any trained team leader with supported multimedia mobile device to take top-level control of the crisis whether mobile or in a physical crisis operations centre. This means that ALL available crisis intelligence should be available in real-time to the team-leaders & staff whatever their location – 24/7.
d. **Emergent Crisis Identification**: Some situations should always be under review through on-line industrial, Government enterprise sensor networks. These would include those for nuclear, chemical, gas, military, police and transportation facilities as well as certain secure Government facilities, major enterprises and utilities. A virtual networked team would keep such threats under continuous real-time review through intelligent software agent that would detect exceptional events as defined.
e. **Real-Time Virtualised Architecture**: Crisis response always needs to be in "real-time", and the proposed innovative architecture virtualises all aspects of the crisis intelligence such that the response team switch from the real-world to interaction with the simulated virtual world. In certain crisis, aspects of the real physical world could be under attack, destroyed by fire, or unavailable due to nuclear or biological attack. So switching the command, control and response to the computerised virtual world allows for solutions to be discussed, and quickly deployed using available networked resources, both physical and electronic. Virtualisation speeds up the access to resources, as well as the filtering and focusing the real-time intelligence. Decision will be made more effectively, deployed faster and more accurately using this style of 21st century "virtualised" national crisis management centre.
f. **International Interoperability**: Some crisis may extend to international dimensions, including certain environmental and terrorist incidents. Hence the solutions architecture needs to be scalable for European-Wide Interoperability. An excellent starting point would be the European Interoperability Framework (EIF) developed and published by the European Union in 2004. It seems likely that work on the Crisis Centre will provide further innovations to the EIF for the support of Disaster Management and Recovery. The North American, ASIS International, has also published useful documentation regarding Crisis and Disaster Management. In fact,

a real commercial benefit would be the potential commercial replication of the Crisis Management Solution by Enterprises within other Governments.

g. **Training and Scenario Simulation:** Team Training for the new Crisis Centre will be absolutely critical to the successful operation. We'll need to develop realistic crisis scenarios, both for testing the pilot implementation, as well as quarterly on-going response training during the operation of the new Central Government crisis centre.

(4) Milestones – Such an innovative crisis management solution would need to be planned and deployed in several pilot and mainstream phases according to the following timescales:

- **Phase 1 – Jan to March 2008 –** Discussions and Desk exercises. Establish the Project Advisory Board – Government, Enterprise, Military – and IT Specialists
- **Phase 2 – April to June 2008 –** Discuss and agree the real-time crisis management architecture, making sure that it is scalable, redundant, and supports the innovative "virtualisation" process and intelligent agents already discussed in the proposal
- **Phase 3 – July to December 2008 –** Design and Implement pilot solution
- **Phase 4 – Jan to March 2009 –** Review the learning from the Pilot Solution, and revise the architecture and applications as required to improve crisis response.
- **Phase 5 – March to December 2009** – Deploy the full-scale rollout of both the physical and virtual components of the integrated real-time crisis response centre
- **Phase 6 –January 2010 →** Launch the new Crisis Response Centre, and implement the on-going training, and realistic crisis scenario programme

(5) Next Steps – It is suggested that the next step is a 1 or 2 day seminar that brings together the members of a provisional project advisory team to agree the concrete action plan.

- -

Author: Dr David Probert – Qualifications & Experience *- The attached document lists relevant qualifications for acting as an independent consultant and advisor for the project including:*

a. ***Doctorate Degree*** *– "Self-Organising Systems" – Cambridge University*
b. ***TERENA Advisory Board*** *– Trans-European Academic & Research Networks*
c. ***Project Director*** *– International KolaNet Programme – "Quick Response System for Potential Nuclear Accidents" within the Kola Peninsula & Northern Russia.*
d. ***Chief Technical Officer*** *– Blick plc – Networked RFID Security, Access Control & CCTV*
e. ***EU Senior Technical Adviser*** *– Georgian Parliament: IT Security & Disaster Recovery*
f. ***USAID/CAPS Senior Adviser*** *– Armenian eGovernance, Cybersecurity and eSociety*
g. ***UN/ITU Senior Expert*** *– Georgian Cybersecurity: Government & Critical Infrastructure*
h. ***Professional Biography*** *– Marquis' Who's Who in the World – 2007-2012 Editions*

- -