“Real-Time Armenia”

Securing Government & Financial Enterprise Operations

Dr David E Probert

VAZA International

\- - - - - - - - - - - - - -

Armenian ICT Leaders Meeting

**** 21st to 22nd February 2009 ****

\- - - - - - - - - - - - - -

"Real-Time Armenia": *Securing Government & Financial Enterprise Operations*

Dr David E Probert – ***VAZA*** International – www.***VAZA***.com

(1) Current Armenian Security Situation – Economic, Electronic, Physical & Political:
Electronic Security will be critical to all aspects of the growing Armenian Economy, Enterprises and Government during the coming months & years. It is an honour to speak at this important international meeting of Armenian ICT Leaders and I offer this White Paper as my personal thoughts and project proposal on this key topic. Every country has a very specific national profile both regarding physical & electronic security so let's summarise the main issues & concerns:

- *Overview of specific security threats including political, criminal, terrorist & natural causes:* Armenia is physically positioned in a region that has various unresolved political issues going back almost 20 years. In addition the proximity to certain Middle Eastern Countries such as Iraq, Syria and Lebanon also boosts the need for Armenia to upgrade both physical & e-Security. Close to Yerevan is the aging Metsamor Nuclear Power Station based upon the Soviet Type VVER440 reactors which despite reaching the end of their original planned life still pose a residual national security risk. And of course this week – 7th December – is also the 20th anniversary of the tragic Gyumri Earthquake which destroyed so many lives, & resources.

- *Importance of e-Security to the Sustainable Growth of the Armenian Economy:* Increasing proportions of global business is being conducted electronically on the Internet, whilst most Governments are migrating citizen services such as taxation, vehicle licences, land registry, & related services to on-line applications that both reduce costs & speed up delivery & cash flows. Later in this White Paper I propose that Armenia extends e-security through a Project that I've provisionally code-named the **"Electronic Diaspora"**. Now is the time & opportunity for Armenia to leverage the strength & scope of its worldwide Diaspora as a stealthy, secure & profitable response to the global financial crisis. All business & trade is built upon trust, so e-security needs to be embedded at the heart of the proposed electronic Diaspora trading network.

- *The value of implementing a distributed security network spanning government & enterprises:* Security cannot be delivered in a box! It needs implemented at all levels of both government & enterprise networks. Every data centre, router, network link, mobile device needs to be secured according to the applications, information and risks related to their use. This paper recommends that Armenia gives serious consideration to significantly upgrading its security through a Government – Enterprise Partnership that develops e-security policies, and works closely with State Bodies & Major Enterprises on their step-by-step implementation over 2 to 3 years.

In summary, this Security White Paper focuses upon the practical project steps required to upgrade Armenia's ICT Infrastructure to support a fully secure and resilient "Real-Time" 21st C e-Armenia. linked with on-line trading enterprises of the proposed global network of the "Electronic Diaspora"!

(2) Further ICT Security Analysis: The international marketplace and most Western Governments have leveraged the "net" and migrated over 10 years to be fully functional and secure with physical & virtual networks supporting e-Business in EVERY market sector from finance, to travel, manufacturing, retail, as well of course Government, Education and Medicine. The good news for Armenia is that, subject to investment from Western partners & Diaspora Partners, the migration to next generation networks will not involve too much legacy integration due to the lower ICT investment for the much of the last 15 years. However the catch-up ICT & security programme will need to be expertly managed in order to be fully operational within the next 2 to 3 years.

In some Government Departments, Agencies and Enterprises there are absolutely world class ICT implementations, whilst in others the infrastructure & facilities probably goes way back to the Soviet Era. In addition, the current Government and Business infrastructure is not adequately connected, and neither are there sufficient international connections or bandwidth to support the operation of Armenia as a global trading economy. There are simply too many single points of failure within the current networks, coupled with a small but growing professional ICT skill base. Hence in-depth security education and training, as in neighbouring Georgia, should be one of the top goals of the Real-Time Armenia & Electronic Diaspora Projects, as well as the evolution & eventual compliance with internationally recognised security policies & standards such as ISO 2700x.

An underlying theme in this paper is that of securing distributed networked systems. In the past era of Web1.0, a dual firewall with DMZ (De-Militarised Zone), and Proxy Server was all that was necessary to secure your main servers, intranet, e-mail and documentation. Now in this new era of Web2.0, the secure perimeter is less well defined as most professionals carry a range of gadgets – 3G Mobile phones, iPod, Memory Sticks, Laptops, and other Wi-Fi, Bluetooth & Wireless Devices.

In summary, due to largely historic & political reasons and critically low ICT investment during the last 15 years, the current security of government & enterprise applications is often unacceptable. Mission critical applications within the government as well as financial & commercial enterprises are too often open to cyber attack from security threats listed below including Distributed Denial of Service (Ddos), Virus/Trojan Attacks, Hacking Wireless Networks & Routers, Potential Loss of information through minimal back-ups, and attack through poorly secured end-user ICT devices.

(3) Extended Security for Real-Time Armenia – The "Electronic Diaspora": My first awareness of the international scope of Armenia came many years ago when, as a teenager, I was introduced by my piano teacher to the piano works of the brilliant Armenian Composer – Aram Khachaturian – and his wonderful Toccata from 1932. Now after more recent research I understand that not only is Armenian Music global in extent, but also its Diaspora which spreads over more than 50 countries.

So in responding to the current financial crisis I propose the following project – "Electronic Diaspora" to leverage the geographical scope and economic diversity of the Armenian Diaspora:

- *Armenian Diaspora within the extended secure e-Business Community:* During these conference presentations and discussions, Armenian Enterprises and Government Bodies are seeking ways to positively respond to the challenges of the worldwide financial crisis. There are currently numerous excellent websites devoted to international Armenian Business, as well as Web2.0 style social network sites such as www.cilicia.com . The next step is to establish and extend e-commerce trading networks from Armenian Banks & Enterprises to International Partners.

- *Leveraging & Securing Trading Links with Armenian Businesses Worldwide:* Whilst some countries & regions are moving into economic recession, others are still experiencing strong growth. The Top 20 countries of the Armenian Diaspora are spread over many economic zones, and hence investment in this worldwide business network offers a way of spreading the risks as a form of balanced trade portfolio. So whilst physical Armenia is constrained by the national boundaries and population, now is the time for Armenia to extend its electronic and virtual State which will not only provide economic & financial benefits, but also develop renewed political strength within International Trade & Government Organisations.

- *The "Electronic Diaspora" as a fully secure e-Trading Network:* Whilst the rest of the world wrestles with the financial crisis and recession, I propose that Armenia stealthily plans and implements a secure global "internet based" network. This will be based upon secure data centres, network gateways and a range of enterprise grade trading applications that are managed locally by International Armenian Business Partners. This can be implemented in phases maybe starting with the TOP 10 Diaspora Countries, and then extending to the TOP 20 and eventually the TOP 50 according to the strength of local Armenian Business & Population. An excellent overview of the Diaspora Facts is at: en.wikipedia.org/wiki/Armenian_diaspora . Once the e-DiasporaNet is complete, membership of this worldwide secure electronic trading organisation could be granted through grades of membership – Bronze, Silver & Gold – with various trading rights such as bank credit / loan options and delivery logistics support. Yerevan Banking Organisations & Government State Bodies would be at the Global Trading Hub of the worldwide eDiasporaNet. This would significantly boost the Armenian Economy, GDP, and financial status on the world stage. So whilst centres such as London, New York, & Hong Kong are weak through recession, Armenia may hope to use the inter-regnum of the crisis to stealthily secure its own economic renaissance through strategic planning & building during 2009 to 2014.

- *Securing the Boundaries of Real-Time Armenia and the Electronic Diaspora:* Historically, looking back over the last 1000 years, Armenia has struggled to secure its physical geographical boundaries with invaders from all directions of the compass – Turkey, Persia, Russia & more! We've already commented that Armenian lies in a vulnerable region of the world, where boundaries in the Caucasus are fragile as demonstrated by events in Georgia earlier this year. It should be understood that electronic boundaries & e-Security is no less important for Armenia. The success of projects such as Real-Time Armenia and the Electronic Diaspora is built upon bullet-proof secure foundations. Trade is built upon Trust! In the following sections we'll

identify the Top Security Threats that Armenia faces both in the Government & Enterprise Networks. Serious Denial of Service Attacks have taken place in many countries during the last year of which those in Georgia and Estonia are probably most worthy of comment since they're both ex-Soviet Republics and developing e-Government & e-Business Trading Networks. So e-security is absolutely key to Armenia's success. It is both insurance against cyber-attack, as well as providing for the continuity of Business & Government Services following potential natural or human disasters (earthquake, nuclear accident, fire, flood, terrorist or criminal attack).

(4) e-Security for Armenian Banks and Financial Institutions: Since the focus of this conference for Armenian ICT Leaders is e-Financial Services, I'll quickly give an overview of some of the Top e-Security issues and concerns in this market sector. It is already well understood that future growth in the Armenian marketplace for Banking & Financial Services requires significant new investment in electronic network, data centres and security. In addition, it is also clear that international trade and transactions, maybe through the proposed e-DiasporaNet will also provide key contributions to growth in Armenian Trade & GDP. So let's list some of the key topics for Financial Institutions:

- *Information and Data Integrity:* Financial & bank account data is extremely important & valuable! All forms of electronic banking data needs to be secured against secret or malicious alterations, or the possibility of fake transactions & bank transfers. Protection methods may include Digital or e-Signatures, as well as PKI Encryption, Biometrics & Mirror Systems.

- *Identity & Data Theft:* A growing problem on e-Banking Networks is the problem of Personal and Company Identity Theft which can potentially create losses amounting to $$$ millions. In addition, the theft of credit / debit card details from on-line transaction records is also a significant problem for US/European Banks and likely to be a growing problem for Armenia too.

- *Cyber Criminal Attacks:* Criminal gangs have been targeting electronic bank account now for more than 10 to 15 years, with increasingly sophisticated methods. The risks are low for the almost invisible criminals (apart from their fake IP Address & proxy net routing!), whilst the rewards are enormous. In addition, the crimes can be carried out in "safe" remote countries in which the laws regarding cybercrimes, and police counter measures may be extremely weak.

- *Denial of Service Attacks:* These attacks are difficult for banks to protect against unless the IT management have already installed specialised security software (for deep-packet inspection), and duplicate IP addresses and real-time back-up data systems.

- *Sleeping Trojan Agents:* In my view, these are amongst the most dangerous of the security problems for both financial institutions as well as State Bodies. The sleeping software agent is injected by the "enemy" through some email attached script embedded within an "exe", "php", "gif" or poisonous fake web-link! Once safely smuggled into the financial data centre, the Trojan may be programmed to track certain accounts, execute illegal transfers, and communicate

sensitive financial account information & passwords back to the "enemy" through emails sent via an innocent looking Internet proxy server located in a "safe" country outside Armenia.

- *Business Continuity & Disaster Recovery:* The Armenian Banks & Financial Institutions are increasingly based upon real-time transactions and operations. This means that ICT interruptions of even a few minutes can be mission critical their successful trusted operations. So a key element of security is the installation of real-time back-up systems that mirror ALL transactions in real-time. For improved security, these systems will be located remotely from the main data centre, possibly in some secure "unmarked" underground facility, 10 - 20kms from Yerevan. Back-Up Facilities should have dual network connections to the main centre, as well as being essentially "earthquake proof through vibration proof mounting of the system server racks.

(5) Electronic Security Threats: Technological and Operational: In previous sections I've analysed some specific security issues relating to Government, Banks, & Financial Institutions. Now I'll extend the analysis more generally to cover the full range of e-security topics. The Top 10 major security threats likely to face the Armenian Government and Major Commercial Enterprises are:

a) Top 10 Security Threats: i) Distributed Denial of Service ii) SQL Database Hacking iii) Targeted Trojan Horses iv) Theft of Secure Information v) Fake Web Sites and Internet IP addresses vi) Destructive Viruses vii) Password, Encryption Key & ID Theft viii) Physical destruction of computer servers & network systems (Fire, Bombing, Terrorism) ix) Loss of International Internet Connections x) Remote enemy and terrorist intercept & secret control of Government & Military ICT and web resources. In fact there are many other levels of electronic & technological security threat, but the above Top 10 is probably of most direct relevance to Armenia's situation.

b) Counter Measures: Armenia needs to urgently deploy a diverse electronic army of security counter measures to detect, and prevent the TOP 10 Security Threats. Some can be implemented within a couple of weeks, whilst a full Business Continuity & Disaster Recovery Programme will take several months of computer upgrades coupled with comprehensive staff training. In the longer term, the aim should be to meet International Security Standards including the ISO27000, as well as "best practice" from NATO and ASIS for Business Continuity & Disaster Recovery.

c) Operational Security Threats: It is generally agreed amongst security professionals that at least 40% of security issues arise not from technological hacking or electronic theft, but from poor operational implementation, human error and theft, sometimes amongst the ICT staff themselves. The Top Operational Security Risks for the Armenian Government include:

i) Loss of Critical Information due to poorly implemented or executed Back-Up Procedures.

ii) Data Integrity whereby information, or databases can be secretly altered by staff or criminals.

iii) Systems Failure & Data Loss due to natural events such as earthquakes, fires or floods.

iv) Loss of Documents & Archives due to the theft of physical devices such as memory sticks, laptop computers, Mobile Phones, or ANY device that can store information & contact details.

v) Theft of Passwords, Encryption Keys, Access Cards & physical building keys by staff, or visitors.

Again, the operational risk list is potentially endless, but the key point is that the technological solutions below will only ever be part of the solution, and a continuous programmes of operational security training has to be an ESSENTIAL part of any complete security programme for Armenia.

(6) Technological Solutions: Fortunately today there are "off the shelf" technological solutions from companies such as Symantec, Hewlett Packard and their local partners such as the Tbilisi-based Orient-Logic Ltd that cover and defend against an extremely broad range of security risks including those discussed above in section (5). If we take the Top 10 Security Threats in turn:

i) Distributed Denial of Service – There is no single solution against invasion by alien invading Botnets, but real-time inspection of message headers, coupled with deep-packet inspection will provide an early alert to attack, and allow operators to quickly divert the attack to alternative destinations, whilst switching servers and databases to remote back-up mode. Re-setting IP address to alternative ranges, linked with re-defining the DNS for the domains are also possible solutions.

ii) SQL Database Hacking – It is unfortunate that many attacks on SQL servers occur since the admin passwords are never changed from their defaults! In any case, this form of Database hacking is one of the easiest and most common on both government and business installations, and is the way in which massive databases of credit card details or maybe military records have been stolen. Again solutions from the major security software vendors protect against such SQL security risks.

iii) Targeted Trojan Horses – These are becoming increasingly sophisticated, and are the root cause of PC infection within the Botnet community. Indeed infection is more likely to come from running computer games, and home use on computing devices that are really designated for Government or Business use only. Locking out the Admin Logon Option is an excellent 1st step, as well as including local and remote access through enterprise directory services. A further issue for the Armenian Government is the risk of dormant Trojan software "bots" planted possibly by criminals, enemy agents or terrorists, that then filter and transmit selected secret information over the net at defined times – either over physical or wireless network connections. Only an ultra-detailed forensic examination of data, scripts and IP Routing Address analysis will ultimately detect such Trojans, coupled with routine real-time scanning of all communications & files.

iv) Theft of Secure Information – From a technical perspective, this can be linked to the passive or dormant embedded Trojan Horse. Such Trojans can be routinely detected by industry standard security software, but this should still be implemented within a professionally defined security policy whether it is the Armenian Parliament, Government Ministry or Commercial Enterprise.

v) Fake Web Sites and Internet IP addresses – It seems that there is an exponential increase in the numbers of fake web sites, SPLOGS (Spam Blogs), as well as other forms of fake IP address which are sites that maybe screen scraped from real branded sites, but with a few subtle changes to ID and password entry data fields. Again, this is protected against using "off the shelf" software, but end-users should still remain alert in the case of "phishing" emails & web pages and never disclose confidential personal, government or business information unless they are 100% absolutely sure.

vi) Destructive Viruses – Many destructive software "bots" are distributed through disguised "exe" files, and are often embedded as jpg or gif image files, or as some form or executable script. However, the damage they cause can be immense though 1st infecting every server on the network, and then successively wiping all the information at the byte level, as well as emailing itself to everyone on the network contact list. Again, industry solutions such as those from Symantec will provide real-time pro-active defence against such virus threats through virus definition directories.

vii) Password, Encryption Key , Access & Biometric ID Theft – These forms of personal identity theft are extremely dangerous since the criminal can impersonate a senior government staff member or maybe business person, and then gain access to highly sensitive & possibly secret information. Protection needs to be a combination of technical defence, coupled with improved operational procedures and comprehensive staff training, particularly in the military or intelligence groups. It should be noted in particular that mobile phones and Wi-Fi networks are specifically vulnerable and frequently targeted by criminals, terrorists and enemies of the state. ALL high security Government & Financial Mobile, Wireless, Radio and Satellite networks should be FULLY secured through a combination of PKI Encryption, Biometric ID and electronic end-user certification (IEEE802.1x).

viii) Physical destruction of computer servers & network systems (Earthquakes, Fire, Bombing, Terrorism) – It is well known Armenia and the whole Caucasus lie in a region that has high likelihood of high intensity earthquakes. So ICT systems should be installed such that they are resilient to at least minor earthquakes through the use of special vibration dampening foundations, and reinforced ceilings. In cases of physical destruction, the risk is considerably reduced through backing-up ALL data, email, and information on remote storage facilities at least some kilometres away in a secret unmarked facility, possibly underground and secure "lights-out" operation.

ix) Loss & Hacking of International Internet Connections – By its nature, internet communications can be routed over any network connection. The growth of VoIP (Voice over IP), and other media over IP creates further risks and vulnerabilities. Any sensitive or secret government or business information should ALWAYS be encrypted according to a sufficiently powerful algorithm & key. Armenia also needs to invest, in alternative routes & higher-speed international broadband IP communications in order to reduce the risk of both agent monitoring, hacking & denial of service.

x) Remote agent intercept & secret control of Government & Military ICT and web resources – This risk may sound rather unlikely, but in fact many supposed secure facilities have been hacked at least once in most developed nations, and facilities in some countries, including USA, UK & Israel,

are under almost continuous attack. It is almost certain that Armenia will experience some form of DDoS attack during the coming few years either from criminals, terrorists or foreign enemies. The implementation of a Government Security Data Centre would certainly help to provide the necessary detailed forensic technical resources to minimise the risks of such cyber attacks, as well as to train up a substantial skill base of Armenian professional security specialists.

(7) Operational Solutions: An essential component of developing and maintaining a defensive security shield is the implementation and communication of in-depth security policies linked to the technological security solutions summarised above.

i) Business Continuity Programme: The loss of critical information can be prevented through upgrading the data centre with real-time data duplication, and longer term back-up on tape-drives. Data storage architectures have advanced dramatically over the last 10 years, with corresponding decreases in cost/GByte. The current generation of disk arrays, clusters, and virtualisation "middle-ware" allows information to be efficiently & economically backed-up both locally and remotely.

ii) Digital Signatures: A key issue for all businesses, but particularly for government and financial institutions is the prevention of secret changes to maybe the national laws, sensitive plans, or financial bank accounts. In short, information security is linked to the integrity of the original data. Operational solutions available today include "off the shelf" Digital Signatures, encrypted files linked with Private/Public Key Solutions, as well as Biometric Access through finger prints, retinal scans and other forms of electronic access system.

iii) Disaster Recovery: Events in Armenia during the last 20 years will have demonstrated the critical importance of planning for potential disasters whether natural (earthquakes, fires, floods), or due to political events (war, terrorism). Increasingly the electronic infrastructure is seen to be a legitimate target by enemy agents, and devastating cyber attacks upon government, military and financial ICT infrastructure will usually occur before and during any physical invasion. In fact, in the case of Georgia I discussed this critical topic of cyberwarfare with senior Government decisions makers and Commercial CIOs from back in September 2007, and the subsequent events from August 2008 have unfortunately proved such forecasts to be correct.

Organisations such as ASIS International have excellent documentation including a Disaster Preparation Guide, and Business Continuity Guidelines. So as well as installing full back-up systems, and remote data centres, it is imperative that all relevant staff are fully trained for evacuation, fall-back procedures, and technical drills to maintain communications and access to mission critical data during & following disasters.

iv) Electronic Asset Management: Today, most staff and decision makers carry a range of portable devices with sensitive and sometimes secret information. Unfortunately such devices and gadgets sometimes go missing, or are deliberately stolen, including memory sticks, laptops, portable disks, mobile phones and PDAs. No single operational procedure will prevent such data loss, but such

devices need to be tightly managed under operational procedures and policies. These could include RFID tagging, encrypted disc drives, and restrictions on the transportation of portable devices outside government, military or financial institutions. It is simply amazing how often such devices are "lost" in trains, taxis, or airline lounges, and all too often with sensitive & secret information!

v) Physical Building Security: Most Western Government Offices, Banks and high profile corporate offices and covered by real-time CCTV systems, as well as entrance/exit security often linked to RFID cards and biometric access devices. In the past these were run on separate networks by the building security teams, but the evolution of IP Access Networks has led to a rapid convergence of Physical and ICT Security Requirements. Now the Broadband IP CCTV images, fire alarm systems and access control can run on the same high-speed IP LANS/WANS, and use facilities in the same data centre for multimedia storage, analysis and back-up. So in planning for the next 3 years, I'd recommend that Armenia gives serious consideration to the development of integrated systems for ICT & Physical Building & Site Security. This would for example allow visitors & staff to be tracked through facilities, with controlled access according to RFID & Personal Biometric Data, hence significantly reducing the risk of theft of electronic assets & sensitive data & documents.

vi) CERT: Computer Emergency Response Team – An effective CERT needs to be established, probably linked directly to an Armenian Government Cyber Defence Centre. As soon as a security event is identified, a pre-planned emergency procedure is executed by the CERT to minimise disruption, with the Armenian Government and Major Enterprises. The implementation and operation of a CERT will be integrated with the plans for Business Continuity & Disaster Recovery.

vi) Security Training: In the absence of comprehensive training, many technological solutions will be only partially effective since as already mentioned, at least 40% of security failures arise from natural causes & human intervention. So in the proposed programmes for "Project Electronic Diaspora" we continuously emphasis the urgent need to build up a strong skill base of native Armenian security specialists that may work with Yerevan based Prime IT Contractors. Investment in this IT Security Shield will be a critical success factor for the proposed Real-Time Armenia!

(7) International ISO Security Standards: An excellent low cost starting point for standards are the public domain Security Guidelines (372 pages) that are published bi-annually by the UK based Information Security Forum (ISF) – www.securityforum.org . The Guidelines are split into:

- Security Management: Includes Asset Management, Business Continuity & Disaster Planning, Cryptography, e-Commerce, Forensic Investigations, Emergency Response (CERT), Privacy, Intrusion Detection, Malicious Mobile Code Prevention, PKI, Remote Working, Risk Analysis, Security Audit, Training. 3rd Party Access, Virus/Trojan Protection
- Critical Business Applications: Includes Access & Applications Control, Back-Up, Change Management, Confidentiality, PKI Key Management, External Connections, Sensitive

Information, Incident Management, Integrity Requirements, Resilience, Roles & Responsibilities, Service Agreements and 3rd Party Agreements, Web-Enabled Applications

- Computer Installations: Includes Emergency Fixes, Event Logging, Hazard Protection, Host System Configuration, Installation Design, Power Supplies, Physical Data Centre Access, System Monitoring, Sign-on Process, User Authentication and User Authorisation.
- Networks: Includes: Configuration of Network Devices, Back-Up and Service Continuity, External Access, DMZ Firewalls, Incident Management and Network Design, Data & Voice/VoIP Network Documentation, Physical Security, Remote Maintenance, Data & Voice Network Resilience, Voice Controls, Service Providers, Net Audit, Wireless Access.
- Systems Development: Acquisition, Application Controls, Availability Requirements, Confidentiality Requirements, Development Methodologies & Environments, Installation Process, Integrity Requirements, Post Implementation Review, Quality Assurance, Risk Assessment, Specification of Requirements, System Design, System Builds, System Promotion Criteria, Testing and Acceptance Process, and Web-Enabled Development.

The International ISO 27002 Security Standards are essentially similar to the ISF Guidelines with regards to both depth and scope, and require the on-line purchase of the full ISO documentation. Country specific information can be found on-line for UK, Germany, USA with regards to the national security policies and guidelines. For example, the German Government has set up the special dedicated Bundesamt für Sicherheit in der InformationsTechnik - www.bsi.bund.de .

(8) Short Term Programme (6 months to 1 Year): Securing e-Armenia, including Government, Business, Educational Institutions and Hospitals is a long term programme that will require continuous investment akin to the maintenance of national defence & military infrastructure. I've divided the implementation of security for the "Electronic Diaspora" into 3 main phases reaching full operations to recognised international ISO27002 standards within 3 to 5 years (2012 to 2014).

First we list the actions that need to be started and managed immediately to secure the Armenian Government's Computing and Network Resources. This should also include an initial rapid audit & review of the Military Communications and Electronic Networks. The full programme of these urgent actions will probably take 3 to 4 months to fully deploy – Jan 2009 to April 2009.

a) Cyber Security Team: The Security Council should set up a small team leading computer network specialists including both locally based Armenian professionals, and recognised international specialists. The team (max 7 persons), would be responsible for carrying out the URGENT cyber security review across all Government Ministries, Office of the President, the Armenian Parliament, and other designated high profile Financial Institutions & Enterprises.

b) Government Security Review: A full in-depth ICT security review and upgrade plan needs to be replicated in ALL the major Government Ministries including – Foreign Affairs, Finance, Justice,

Internal Affairs, Office of the President, as well as the Military. A thorough cyber security audit will take 2 to 3 full working days, but the team should work in parallel so that everything should be complete in 4 to 6 working weeks.

c) Check List: The team should draw up checklists of security issues as templates for each ministry so that security weaknesses can be immediately identified, and solutions discussed with local teams.

d) Information Back-Up: Checks should be made that ALL government information, databases, email & archives are fully backed up in secure fireproof rooms, and duplicated on secure media.

e) Upgraded Software & Systems: It is likely that most computing servers and network equipment will need some form of security upgrade, with extended RAID-type memory, additional processors, with investigation into the option of virtualised storage for large data centre installations. Local specialist companies should be invited to work with the team to ensure that the most advanced "Best of Breed" Security Software Protection is installed within all Central Government, and Armenian Military Installations, and that data centres are upgraded according to team recommendations. In general, *ALL* computer servers, storage, routers & networks connected should be replicated leaving a minimal number of potential single points of system failure.

f) Network & Wireless Connectivity: This includes ALL physical cables, wireless networks, and satellite links that are currently used by the Armenian Government & Financial Institutions for communication both within Armenia, as well as the secure International Trans-Caucasus Gateways, Radio and Satellite Links. Ideally, IP Addresses, and serves should be replicated with a "secret" alternative back-up set of addresses, and remote warm "back-up" servers available in the event of a serious Distributed Denial of Service or other form of devastating large scale focused Cyber Attack.

g) Back-Up Web Sites & Servers: All web sites should be backed up**,** with a quick (less than 5 minutes) option to switch over the domain, (with an alternative IP Address) to an alternative web server located either elsewhere in Armenia in secure facilities, or within a friendly overseas nation. The alternative web site should ideally have some form of Ddos deep-level packet sensing software with automatic Ddos alert & filter so that alien (cyber attack) IP packets can be intercepted in real-time and dealt with according to agreed security policies. The CERT will provide actions alerts.

h) Database Security: Many commercial & government SQL databases remain with their default passwords and are easily "hacked" and compromised by enemy hackers. Once compromised, the database can either be subtly altered, stolen, or simply deleted. Hence all government databases should be checked to ensure that they sit behind a full double firewall with electronic DMZ (De-Militarised Zone) & proxy IP addresses.

i) Information Integrity: The enemy hackers will sometimes enter the database, and simply make small, though strategic changes to the database which may initially be undetectable by the operational staff. This is particularly dangerous if the hacker deploys a Trojan horse to route certain data back to their own computer which frequently occurs when banking and financial systems are

hacked. However, in the case of the Armenian Government, this means that enemy criminal, political or terrorist agents may *ALREADY* have secretly & invisibly compromised Ministry Information systems & Financial Institutions and then transmit critical & secret information (referenced by keywords) back to their home servers. The appointed Cyber Security Team will thoroughly check that Government & Financial Data Systems have not yet been compromised in this dangerous way by foreign agent or criminal Sleeping Trojan Cyber "bots".

These urgent short term actions need to be completed, at latest, within the next 3 to 4 months

(9) Medium Term Programme (2 to 3 Years): Following the comprehensive Government-Wide security audit by the Cyber Security Team, it is expected that the State may support the establishment of a national Cyber Defence Centre that will serve both as the Armenian CERT, Advanced Training Centre and overall Centre of Security Excellence (COE). Of course, any comprehensive security architecture needs to be fully distributed so whilst the COE might act as the central "church" of security protection, all other network nodes, servers, storage and end-points also need to be "real-time" monitored and fully secured. All these actions are essential to support the project of ***"Real-Time Armenia"*** and the Foundations for the Project – ***"Electronic Diaspora".***

Specific medium term topics that need to be addressed and managed by the cyber security team are:

a) Data Centre Storage & Virtualisation: It should be understood that the Armenian Government, with financial & resource support from its allies in Europe and USA, should invest significantly in the *complete* upgrading of the electronic network and computing infrastructure. This will then act as a reliable & resilient defence shield against any future organised hacker, and cyber terrorist attacks. In particular, significant investments should be planned during the next 3 years into replicated & virtualised data-centres to support the proposed extensive e-Government & e-Business Applications.

b) Regional Government: In the medium term, the electronic security & defences of the Regional Government Offices should be reviewed and upgraded since these are information gateways into the Central Government Ministries. The same applies also to the Regional City Banks, Financial Institutions and Enterprises, since again these maybe weak links and back doors to e-Yerevan.

c) Security Training: Relevant IT & Computing Staff should undergo intensive training in 21st Century cyber security solutions through local courses organised by an Armenian State Cyber Defence Centre in collaboration with local specialist companies & international consultants.

d) Security Standards: There needs to be relevant in-depth training on the details of the various international ISO/ISF security standards that will be implemented during the coming 2 to 3 years.

e) Business Continuity: Events in both Georgia & Estonia have tragically shown how important it is to have pre developed plans and fall back options in to the case of IT systems failures and cyber attacks. The cyber security team will develop these during the next 9 months with each of the

Ministry Departments. In particular, the team should ensure that there is duplication of computing storage, servers, and network connectively in the case of *ALL* mission critical government resources.

f) Disaster Recovery: Closely associated with Business Continuity are the recovery plans for disaster such as on-going cyber terrorist attacks, as well as possible floods, fires and earthquakes. For such disaster contingencies, the Armenian Government should seriously consider building a remote and secure underground computing facility outside Yerevan that can serve as the alternative command post in the case of forced evacuation of the Parliament and Central Government Offices.

g) Distributed Denial of Service (Ddos): It seems likely that the Ddos attacks may continue intermittently for several months, if not years for those politically aligned with the enemies Armenia. Hence, full industry strength protection should be purchased and deployed including dedicated Ddos network hardware that checks and filters *every* incoming IP data packet header and full contents in real-time. Such systems will be required as gateways to each Government Ministry, the Armenian Parliament, and key Military Installations. Consideration should also be given to also making these mandatory for all major commercial Armenian Financial & Banking Institutions.

i) e-Business Ventures & the Electronic Diaspora: Depending on the discussions and outcomes of this Armenian Leaders Conference, it would be expected that the 1st major investments & ventures into e-Business will be launched during the coming year and implemented during the medium term. Based upon my personal IT experience, e-Business will eventually penetrate every aspect of Armenian Business & Enterprise, extending from e-Government, through to e-Health, e-Learning, e-Finance, e-Shopping, and global e-Trade! These electronic trading highways are the "Silk Routes" for the 21st Century, and the establishment of a fully secure distributed network is of fundamental importance to the future resilience and success of Armenia's pioneering e-Business Ventures. Never neglect investment in good e-Security which should ideally be integrated with physical security.

j) NATO Silk Project and ASNET: Excellent examples of electronic networking projects that are already implemented within Armenia are the NATO financed Silk Net Project SilkProject.org and the Armenian Science and Academic Network – ASNET – ASNet.am - together with CERT.am . The organisation and secure network implementation of both Silk Net & ASNet may provide useful reference Security Guidelines for future national & international Armenian Networking Projects.

(10) Longer Term Programme (4 to 5 Years): Once the secure foundations of the "Real-Time Armenia" programme are completed, it will be time to expand the **"Electronic Diaspora"** project to provide secure international connectivity with other Major Enterprise & e-Government networks.

a) e-Government European Interoperability Programme - EIF : Many Government activities & programmes reach across international boundaries such as the Ministry of Foreign Affairs, Taxation, Laws, Finance as well as the worldwide network of Armenian Consulates & Embassies. Hence it will be important the practical construction of Armenian's proposed e-Government network & "Electronic DiasporaNet" is undertaken to recognised international computing & software standards

such as those of the IEEE, and the ISO - International Standards Organisation. Other possible trans-national connectivity could include NATO, United Nations, IMF, World Bank, and various international trade organisations. In all these cases, the real-time security defences will need to be negotiated and upgraded to ensure that Armenia is secure against electronic invasion by software "bots", and other intelligent & malicious on-line agents controlled by political & criminal consortia.

b) International e-Trading Hub: A key aim for Armenia's e-Business programme is clearly to boost its economic competitiveness within the international marketplace. Yerevan was established on the physical Silk Trading Route from China to the West, but now such trade, apart from valuable commodities such as oil & gas, is quickly migrating to the internet. Armenia's economic reputation will depend upon the security of these electronic 21stC trading routes, so investment will need to be continuously made into improved intrusion detection systems, enhanced servers, duplicate storage, virtualisation, security training and preparation for possible alerts, emergencies & disasters.

c) Physical & Electronic Security Integration : During the next 5 years it is forecast that most physical security such as CCTV networks and access control will be digitalised over IP networks with hi-resolution cameras, automatic car number plate recognition (ANPR) and satellite imagery all converged into new generation secure data centre applications. Today, in many government and commercial facilities there are separate security organisations for physical and IT security. It is to be hoped that an Armenian State Cyber Defence Center will also inspire the full integration of physical CCTV and electronic IT security as a longer term 3 to 5 year programme

d) Biometric ID and RFID Asset Management: In a previous professional role I was CTO for a major international Security Solutions provider (now Stanley Security Solutions Ltd). Products included biometric finger-print readers and RFID Access Cards for ultra-secure facilities such as prisons & special government facilities. Such biometric devices are now decreasing in cost and generally becoming commoditised and available for all organisations to provide advanced technological control at a uniquely personal level. Earlier this year I participated at the Biometrics2008 Exhibition in Westminster, London with major vendors displaying their latest solutions. It seems clear that such IP networked biometric devices will provide the basis of future innovative security access and control for Armenia's e-Government & e-Business Programmes.

e) Security of End-User Devices & Applications: There is a worldwide computing trend to virtualise data centres, and to place networked servers, storage, services and applications "in the cloud". In addition, the numbers & types of portable intelligent end-user devices looks set to grow exponentially during the coming 5 to 10 years. All these trends mean that the traditional security perimeter that can be firewalled is rapidly vaporising! The leading international security vendors such as Symantec (represented by Orient-Logic Ltd in Tbilisi) are already extending their "off the shelf" enterprise security applications to defend against this new generation of networked threats.

In particular there is a new organisation – the Jericho Forum – which is developing security blueprints for such open networked environments with no traditional IT perimeter. In fact, dual

security firewalls (DMZ) will always be of great utility at the LAN level, but for the extended Campus/Metropolitan/Wide Area Networks, security will need to be embedded deep within every networked end-user device, router, switch, storage device and application. Real-Time Encryption such as RSA/PGP algorithms provide a partial solution, and hence the proposed Armenia Cyber Defence Centre will have a continuous programme of challenges to maintain the security of "real-time" Armenia. This is the core mission of our 5 Year "Real-Time Armenia" & Project "Electronic Diaspora"– to provide a flexible & comprehensive real-time electronic security shield against invading agents, "bots", and cyber criminals!

(11) Next Practical Steps (3 to 6 Months – Jan 2009 to June 2009): In the last 15 pages we discussed a diverse range of security issues, solutions, projects & programmes. Now let's go back to basics and summarise the practical steps Armenia might take to build the necessary secure foundations for e-Government, "Real-Time" Armenia and the ambitious "Electronic Diaspora"!

a) Appoint a full-time team of Government & Banking security professionals (max 7 individuals)

b) Undertake a comprehensive audit of all strategic government & financial ICT facilities. Focus particularly on single points of failure, back-up policies, and opportunities for data theft or hacking.

c) Check-out the electronic logs of any Cyber Attacks & major Denial of Service events that may have previously taken place. Carry out a technical forensic examination of vulnerabilities within the relevant State & Banking ICT computer systems, networks, gateways, routers & servers.

d) Work with Government Departments on a case-by-case basis to ensure that all critical, sensitive and secret information, plans and databases are fully backed-up and replicated on tape or disk.

e) Work with appointed NATO and EU security specialists to establish a national Cyber Defence Centre as a Centre of Excellence for Security Monitoring, Alerts, CERT and Training in Armenia.

f) Based upon the results of individual security & IT audits from the Government Ministries & Agencies, develop detailed engineering plans and requirements for discussion with both approved international consultants & locally based vendors of recognised enterprise-grade security solutions.

g) Commence specialist IT security training courses to significantly boost the national skill base.

(12) Wrap-Up: Success for "Real-Time" Armenia & the "Electronic DiasporaNet" requires significant investment in upgrading and maintaining a fully secure national and international IT infrastructure. This Security White Paper proposes that the Government & Enterprises of Armenia jointly establish a pioneering 3 to 5 year programme - *"**Project - Electronic Diaspora**"* – to ensure that Armenia pro-actively responds to the real challenges of the worldwide financial crisis. This Three-Phase programme: (1) e-Government – (2) Real-Time Armenia – (3) Electronic DiasporaNet will boost economic growth, increase Armenia's political profile, and ensure that the country is fully secure and defended against future electronic Cyber Attacks, Cyber Crime, or other e-Invasions!

Annex: Security References

The following useful references are all available free of charge on-line apart from the full ISO/IEC 27000 Standards which may be purchased on-line from www.iso.org .

a. ASIS International 2005 – Business Continuity Guidelines (includes Disaster Recovery)

b. Information Security Forum – Oct 2007 – Security Guidelines - www.securityforum.org

c. German Government 2004 – IT Security Guidelines (Ministry for Security and IT)

d. ISO/IEC 27001/27002 Guidelines – 2005 and Updates – www.iso.org

e. OECD Guidelines for the Security of Information Systems & Networks – 2002

f. US Congress – Security in the Information Age – May 2002

g. UK Government – Network Defence – 2002

h. UK Government – Security Architecture - Version4.0 – 2002

i. UK Government – Registration and Authentication – Version4.0 - 2002

j. FFIEC – Information Security – IT Examination Handbook - July 2006

k. EIF – European Interoperability Framework for Pan-European e-Government - 2004

l. International Jericho Forum – "Security De-Parameterization" www.opengroup.org/jericho/

m. NATO Advanced Networking Working – Yerevan –Nov 2007 – www.asnet.am/anw2007/

Personal Acknowledgements

I'd like to thank Vahan Hovsepyan from the Armenian Union of IT Enterprises for the invitation to speak at this Armenian ICT Leaders Conference, as well as to Armen Shahbazyan from CAPS for extremely stimulating discussions during the recent Georgian Government IT Conference in Tbilisi. Next I thank my colleagues from Orient-Logic Ltd, especially Dr Dimitri Kipiani and Sergey Sanakoev for their outstanding support in the development of relevant IT Security Programmes, as well as my long time friend & colleague Pavel Khrapkin (Symantec CIS). Finally, my warm thanks to Nodar Mosashvili (Acting World Bank Finance Director – Tbilisi, Georgia) who was my personal introduction, in 1994/95, to the Government & Enterprise ICT Security challenges of the Caucasus.

* *

On-Line Version : Download Security White Paper from: www.valentina.net/vaza/ARMENIA.pdf

* *

Professional Profile: Dr David E. Probert – *VAZA International* – www.vaza.com

- ***Computer Integrated Telephony (CIT)*** – Established and led British Telecom's £25M EIGER Project during the mid-1980s' to integrate computers with telephone switches (PABX's). This resulted in the successful launch of CIT software applications for global telesales operations.

- ***Blueprint for Business Communities*** – Visionary Programme for Digital Equipment Corporation during late-1980's that included the creation of the "knowledge lens" and "community networks". The Blueprint provided the strategic framework for Digital's Value-Added Networks Business that secured significant contracts for enterprise networks.

- ***European Internet Business Group (EIBG***) – Established and led Digital Equipment Corporation's European Internet Group for 5 years, from 1994 to 1999. Projects included support for the national Internet infrastructure for countries across EMEA as well as major enterprise, government & educational Intranet deployments. David was a member of the Trans-European Board for Academic & Research Networking (TERENA) for 7 years (1991 ➔1998)

- ***KolaNet*** – Established and led the KolaNet Project for Nuclear Security within the Arctic Kola Peninsula. The 5 year multi-national project (1992 - 1997) provided Real-Time Internet based monitoring, Training & Web Sites to Government Institutions within Russia & neighbouring countries. The primary KolaNet Applications were the monitoring of radioactivity from the Kola NPP, sea borne reactors as well as other harmful industrial chemicals & heavy-metal emissions.

- ***Supersonic Car (ThrustSSC)*** – Worked with Richard Noble OBE, and the Mach One Club to set up and manage the 1st Multi-Media and e-Commerce Web-Site for the World's 1st Supersonic Car – ThrustSSC – for the World Speed Record – Feb 1995 to Oct 1997.

- ***Secure Wireless Networking*** – Business Director & Vice President for Madge Networks. He launched a comprehensive portfolio of innovative & secure wireless Wi-Fi IEEE802.11a/b/g networking products with advanced technology partners from UK and Taiwan.

- ***Networked Enterprise Security*** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional security & software engineers & a diverse portfolio of hi-tech security products.

- ***Republic of Georgia*** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and Business Continuity Plans & Disaster Recovery relating to the Georgian Parliament.

- *Dr David E. Probert is a Fellow of the Royal Statistical Society. He has a 1st Class Honours Degree in Mathematics (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata) & features in Who's Who in the World.*