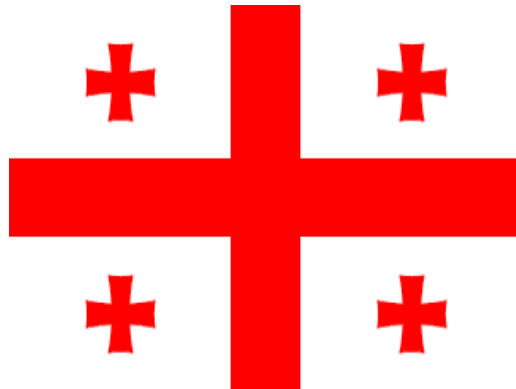




“Real-Time Georgia”

Securing Government & Enterprise Operations



Project Vardzia

Dr David E Probert

VAZA International

“Real-Time Georgia”: Securing Government & Enterprise Operations

(1) Introduction: The security of Georgia will be critical to the future economic growth and development of this new democratic nation. This Security White Paper focuses upon the practical project steps required to upgrade Georgia’s IT, Computing & Communications Infrastructure to support a fully secure and resilient “Real-Time” 21st C e-Government, linked with electronically trading enterprises both in Georgia & Globally.

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 well all carry a range of gadgets – 3G Mobile phones, iPod, Memory Sticks, Laptops, and other Wi-Fi, Bluetooth & Wireless Devices.

There are parallels with the historic position of Georgia in which the Caucasus provided a physical firewall against invasion from the North, whilst in the South, religious cave complexes such as [Vardzia - ვარძია](#) - were constructed in the 12th Century to provide relatively secure life against invasion from the Southern Borders. In fact, this ancient Vardzia Architecture still provides a useful analogy since in the 21stC, instead of securing a 3D network of caves on a cliff-face, we are securing a highly complex multi-dimensional network of servers, databases, and end-user devices. Vardzia stands on the beautiful Kura River which flows through onward through Georgia to the capital Tbilisi, and then to Rustavi, close to another even older 6th Century cave complex of [David Gareja](#). So now we’re securing electronic caves (servers), full of valuable information resources, and I’ll take the liberty of referring to the proposed programme to develop & fully secure “Real-Time” Electronic Georgia - e-GE - as Project Vardzia! A bridge between the 12thC and our current 21stC!

Historically, there had been minimal investment in the IT infrastructure, particularly with regards to the security support, data back-up, duplication, and adherence to international ISO Security standards. The tragic events of the last 6 months will have demonstrated the urgent requirement for significant investment in both the Government & Enterprise IT & Security Infrastructure, since the current networks are extremely fragile, with minimal resilience to cyber attacks or other disasters.

(2) Current Security Situation: The international marketplace and most Western Governments have leveraged the Internet and migrated over the last 10 years to be fully functional and largely secure physical and 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 Georgia is that, subject to investment availability from Western partners, the migration to next generation networks will not involve too much legacy integration due to the relatively low 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.

Based upon my recent experience in Georgia, the current levels of security within both Government & Enterprise is largely inadequate, and well below recognised international ISO 27000 Security Standards. This White Paper presents a summary programme proposal – Project Vardzia – to rapidly and efficiently upgrade the technological and operational security infrastructure to be fully resilient, and to evolve to the required operational security standards by around 2012 – a 3 year plan!

In some Government Departments, Agencies and Enterprises there are absolutely world class ICT implementations, whilst in others the infrastructure & facilities goes way back to the Soviet Era from nearly 20 years ago. 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 Georgia as a global trading economy. There are simply too many single points of failure within the current networks, coupled with a relatively small professional ICT skill base outside the Government and Major Commercial Enterprises. Hence security education and training, as in Estonia, should be one of the top goals of the 3 year e-Georgia Government project.

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) Security Threats : Technological and Operational : The Top 10 major security threats likely to face the Georgian 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 Georgia's situation.

b) Counter Measures: Georgia 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 Georgian 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 Georgia.

(4) Technological Solutions: Fortunately today there are “off the shelf” technological solutions from companies such as Symantec & Hewlett Packard that cover and defend against an extremely broad range of security risks including those discussed above in section (3). 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 Georgian 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 Georgian 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.

viii) Physical destruction of computer servers & network systems (Earthquakes, Fire, Bombing, Terrorism) – It is well known Georgia 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.

Georgia 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 some facilities are under almost continuous attack. It must be assumed that in the case of Georgia that DDoS and related attacks will continue at intervals for many months & years to come, and that both Government & Commercial Enterprises will be targeted. The implementation of the proposed NATO Security Data Centre will 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 Georgian professional security specialists.

(5) 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 : Recent events in Georgia 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, I discussed this topic of cyberwarfare with senior Government decisions makers and Commercial CIOs from Georgia back in September 2007, and events during August 2008 have tragically proved such forecasts 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 Georgia 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 the proposed NATO 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 Georgian Government and Major Enterprises. The implementation and operation of the CERT will be directly 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 Vardzia" we continuously emphasis the urgent need to build up a strong skill base of native Georgian security specialists that may work with Tbilisi based Prime IT Contractors such as Orient-Logic Ltd. Investment in this IT Security Shield will be a critical success criteria for the proposed e-Georgia!

(6) Short Term Programme (6 months to 1 Year): Securing e-Georgia, 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 "Project Vardzia" into 3 main phases reaching full operations to recognised international ISO27000 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 Georgian Government's Computing and Network Resources. This should also include an initial rapid 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 – Nov/Dec 2008 - Jan/Feb 2009.

a) Cyber Security Team: The Security Council should set up a small team leading computer network specialists including both locally based Georgian 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 Georgian Parliament, and other designated high profile Financial Institutions & Enterprises.

b) Government Security Review: Last September 2007, I carried out a full review of the cyber security and some aspects of the physical security for the Georgian Parliament, under the auspices of the EU. This level of in-depth review and recommendation 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 such as Orient-Logic 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 Georgian 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 Georgian Government for communication both within Georgia, as well as the secure International Network Gateways such as those across the Black Sea, Radio and Satellite. Ideally, IP Addresses, and servers 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 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 Georgia 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 policies.

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

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

(7) Medium Term Programme (2 to 3 Years) : Following the comprehensive Government-Wide security audit by the Cyber Security Team, it is expected that NATO will support the establishment of a locally based Cyber Defence Centre that will serve as the National Georgian CERT, Advanced Training Centre and overall Centre of Security Excellence (COE). Of course, any comprehensive security architecture, like the ancient 12thC Vardzia Cave System, needs to be fully distributed so whilst the COE might act as the central “cathedral” of security protection, all other network nodes, servers, storage and end-points also need to be “real-time monitored and fully secured.

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

a) Data Centre Storage & Virtualisation : Based upon my recent experience within the Georgian Parliament, it is apparent that in previous years the potential threat of cyber attacks and cyber warfare was completely underestimated. It should be understood that the Georgian Government, with financial & resource support from its allies in Europe and USA, should investment significantly in the *complete* upgrading of the electronic network and computing infrastructure. This will then act as a reliable & resilient defence shield against 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

- c) Security Training:** Relevant IT & Computing Staff should undergo intensive training in 21st Century cyber security solutions through local courses organised by the National Cyber Defence Centre in collaboration with local specialist companies such as Orient-Logic Ltd.
- 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 of recent months 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 coming 6 to 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 Georgian Government should seriously consider building a remote and secure underground computing facility outside Tbilisi 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 of Georgia. 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 Georgian Parliament, and key Military Installations. Consideration should also be given to also making these mandatory for all commercial Georgian Financial & Banking Institutions.
- i) e-Business Ventures :** Depending on the discussions and outcomes of this 1st GITI 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 Georgian 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 Georgia's pioneering e-Business Ventures. Never neglect investment in good Security!
- (8) Longer Term Programme (4 to 5 Years) :** Once the secure foundations of "Project Vardzia" are completed, it will be time to expand the real-time "e-Georgia" programme to provide secure international connectivity with other e-Government networks, as well global e-marketplaces.
- 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 Georgian Consulates & Embassies. Hence it will

be important the practical construction of Georgia's proposed e-Government network & applications 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 Georgia is secure against electronic invasion by software "bots", and other intelligent on-line agents.

b) International e-Trading Hub : A key aim for Georgia's e-Business programme is clearly to boost its economic competitiveness within the international marketplace. Tbilisi 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. Georgia'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 the proposed NATO 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. Last week I participated at the Biometrics2008 Exhibition and Conference in Westminster, London with all the 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 Georgia'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 Georgian Cyber Defence Centre will have a continuous programme of challenges to maintain the security of “real-time” Georgia. This is the core mission of our 5 Year “Project Vardzia” – to provide a flexible & comprehensive electronic security shield against invading agents, “bots”, and cyber criminals!

(9) Next Practical Steps (3 to 6 Months – Nov 2008 to April 2009) : In the last 10 pages we discussed a diverse range of security issues, solutions, and programmes. Now, based upon my experience with the Georgian Parliament, let’s go back to basics and summarise the practical steps Georgia might take to get build the necessary secure foundations for e-Government & e-Business!

- a) Appoint a full-time team of Government security professionals (max 7 individuals)
- b) Undertake a comprehensive audit of all strategic government IT facilities. Focus particularly on determining any single points of failure, lack of back-ups, opportunities for data theft or hacking.
- c) Check-out the electronic logs of any Cyber Attacks & major Denial of Service events that may have taken place during July/August/September 2008. Carry out a technical forensic examination of vulnerabilities within the relevant IT 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 Georgia.
- 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.

(10) Wrap-Up: Success for “Real-Time” Georgia requires significant investment in upgrading and maintaining a fully secure IT infrastructure. This Security White Paper proposes that the Government of Georgia establishes a 3 to 5 year programme - “*Project Vardzia*” – to ensure that the country is fully defended against future 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/

*** *On-Line Version of Security White Paper in Eng/Geo* : www.orient-logic.com ***

*** *Orient-Logic Limited : 8 Belashvili Street “MIONI” Building, Tbilisi 0159, Georgia* ***
