…"21stC Georgia"…

…"Cyber-Vardzia"…

- -

"Integrated Cyber & Physical Security"

*** *for* ***

… e-Government, e-Society & e-Georgia.

- -

Author*: Dr David E Probert – VAZA International*

- -

* Integrated Cyber & Physical Security Systems for 21stC Georgia *

Author: *Dr David E Probert – VAZA International*

- -

(0) Executive Summary

In this White Paper I argue that for Georgia to secure its national borders and to protect its critical national infrastructure in the 21stC, that it should develop its cybersecurity & physical security within the framework of an integrated security organisation with charter from highest levels of Government.

The paper briefly reviews the major cybersecurity and physical security technologies and solutions, and then discusses the more complex security threats that can only be detected through the operational integration of the cyber and physical security organisations.

I then consider examples of ways in which cyber and physical security solutions can be operationally & technologically integrated to provide a more effective response to evolving cybercriminal threats. Following this generic review of integrated security, I move to a more detailed discussion of the security requirements on a sector-by-sector basis, focusing on those sectors that are critical to the national economic & political infrastructure including: government, telecommunications, banking, energy, transportation, education, police and defence.

My personal vision for this project is based upon the Georgian Historical Cave City of Vardzia!...

......Significant investment is being made by international agencies and countries into the Georgian Economy, and already much progress has been achieved during the last 3 to 5 years. However in parallel there needs to be incremental investment to upgrade both Georgian physical and cyber security for its critical national infrastructure. There remains an international perception that Georgia's borders & cyber-networks are still not fully secured....

...... So just as the 12thC **Vardzia** Cave Complex protected the country for several hundred years during the medieval period, so this new integrated security programme will dramatically increase Georgia's protection against cyber-attacks and potential invasions during our 21stCentury!

Finally I summarise some of the major benefits for Georgia to consider cybersecurity and physical security within the same organisational and operational framework, and suggestions for next steps.

- -

(1) Background

Practically every country in the world is now planning to implement upgraded physical and cyber security in order to defend their critical national infrastructures against penetration and attack. Traditionally the fields of cybersecurity and physical security have been managed as separate spheres of operation. Back in the 20thC Cybersecurity was managed by the ICT Department, whilst Physical Security, which would include building access, CCTV, fire and emergency alarms, would come under day-to-day security operations.

In this White Paper I consider the reasons and benefits for managing cybersecurity and physical security within the same overall strategic and operational framework. I already have some personal experience of security operations in Georgia through a comprehensive Security Audit of the Georgian Parliament (Sept 2007), and subsequently an in-depth strategic review of the National Government Cybersecurity (Dec 2009), under the auspices of the Georgian Ministry of Economic Development. It is not my aim to repeat or duplicate this previous work but instead to provide a basic framework and architecture for the Georgian Government and Major Commercial Enterprises to extend their security operations to include both cyber & physical security during the next 3 to 5 years.

In this paper I'll explore the portfolio of cyber & physical security solutions, and potential ways which these solutions can be integrated within real world scenarios. I'll try and make these as concrete and practical as possible by considering their applicability within the most critical government and business sectors including energy, telecommunications, transportation, education and defence.

- -

(2) Security Technologies and Solutions

We first need to prepare the security foundations through a quick summary of the primary physical and cyber security technologies that are commonly deployed by governments & corporations today. Then we consider the various ways in which cyber & physical security solutions can be interfaced in order to boost security and thence to further minimise the risks.

a) Physical Security Technologies and Solutions

i) CCTV – Closed Circuit TV is now increasingly deployed with High-Definition Digital Images, Remotely controlled (Pan-Tilt-Zoom), and compressed digital back-up and archiving. Camera arrays are linked to control centres that will typically manage government ministries, enterprise offices, business parks, shopping malls, university campuses, or city regions. In order to reduce the demands on human operators, the CCTV software is increasingly support intelligent object, and person recognition so that unusual events can be automatically detected and alarms raised.

ii) RFID – Radio Frequency ID Devices. RFID tags and cards have mainstreamed in the physical security world during the last 10 to 15 years, with associated international ISO standards. RFID chips can be inserted to electronically tag practically any object or person including ID cards, clothing, food produce, vehicles, pharmaceuticals and drugs. Powered versions of RFID chips can be used to provide remotely triggered actions "at a distance" depending on the size of radio antennas and power supply. Such tags are now being proposed for use in airline baggage handling, and also by newly discussed EU regulations to indicate the freshness, and "use by date" of fruit, vegetables, fish and meat.

iii) ANPR – Automatic Number Plate Recognition – ANPR Solutions are really a subset of Intelligent CCTV Recognition Systems. ANPR is typically used by the police authorities in many countries to detect vehicle ownership and insurance details in real-time based upon the on-line vehicle registration details. In addition, it is used by governments, enterprises and public facilities to manage vehicle any associated parking charges. Another use within certain cities, such as London, is to manage the vehicle congestion charges which serve to reduce vehicle movements during weekday busy periods.

iv) Building Access – Most Government offices and Enterprise have some form of staff & visitor control system which may include a combination of turnstiles, ID Cards, scanning systems & screens. Such building control and alarm systems are now typically deployed within an overall IP networked environment, and managed from the same operations centre as the networked digital CCTV systems. In this way, events from the CCTV next to building and secure entrances/exits can be directly linked to specific ID cards and persons. In addition, in the event of emergency alarms relating to fire, flood, or theft, the CCTV system can again provide real-time viewing of nearby activities, as well as prior video surveillance materials.

v) Perimeter Fences – Easily forgotten is this most basic version of physical security which goes right back to the medieval moats and portcullises that protected fortified towns and cities. In the 21stC perimeter fence technology is now really hi-tech with embedded optic-fibres within the fencing materials to detect and locate any hostile disturbance or movement. Again, intelligent CCTV, infrared and laser systems may also be co-located with the perimeter fences to provide upgraded security for airports, military installations or other top security civilian and government facilities.

vi) Security Guards – Alongside perimeter fences, physical security personnel and body guards are also fundamental in all security implementations however far they are integrated with cyber solutions. The security guards will be equipped with secure multimedia mobile communications, and an appropriate level of personal defences. To be effective, security guards for government installations need to be fully trained in operational security policies and procedures including regular simulation exercises with a range of alert scenarios. In many organisations, the physical security guards & physical security assets are managed by a separate organisation from the ICT & Cybersecurity Teams. As we'll see later in the White Paper, this leaves a multitude of innovative ways in which the more creative cybercriminals can access physical premises such as banks, airports, power stations, telecoms network operations centres, government & military installations.

vii) Detection Systems – All critical national facilities such as government ministries, power stations, airports, and financial centres require a range of "detection systems". These will range from basic X-ray scanning, to more advanced testing for chemical, biological agents and drugs. In addition we've seen that the increasing terrorism threat in many countries is leading to the introduction of more comprehensive low-energy body-scanning devices that provide 3D real-time body images. System software can be programmed to recognise objects or features that fall outside the range of the accepted pre-set security parameters and policies.

viii) Biometrics – The last 5 years has seen and enormous growth in biometric security solutions, with dedicated conferences such as Biometrics 2010 held now annually in London, UK. Biometrics range from the classic fingerprints, to retinal & iris eye scans, 3D facial scans, 3D vein ID, and DNA. Despite being based upon physical body and cellular features, they all require quite significant computing power, and are one of the first to demand real-time integration with cyber databases.

ix) Personality Profiling and Interviews – Another powerful security tool that is also often undervalued is the classic technique of personality profiling, interviewing and interrogation. This can be used in a variety of ways such as passenger profiling and interviewing that is deployed by some international airlines. New personnel working in secure facilities, including airports, financial centres, and telco network operations will also need to be interviewed and vetted to agreed levels of security clearance dependent upon their role and responsibilities.

x) Back-Up Operational Facilities – These can range from a standard fireproof safe for documents and electronic media, through to a deep underground bunker that is built to withstand earthquakes and missile attacks. For 21stC security, such facilities are possibly even more important than in the 20thC as real-time back-up cyber operations centres. They will typically be co-located near to hi-security military bases and remote from any cities, government offices or exposed civilian settlements.

b) Cybersecurity Technologies and Solutions

i) IDS - Intrusion Detection Systems – The traditional form of cybersecurity is the detection and prevention of malicious attacks within both the communications networks and host systems & servers. Many of the following cybersecurity solutions represent ways in which to automatically detect and respond to specific cyber threats. Malicious attacks can include computer viruses, trojans, advertising malware, spam mail, key loggers, firewall port penetration, SQL injections, and more recently the hacking of Web2.0 Applications such as Facebook, MySpace, Yahoo, LinkedIn and similar sites.

ii) Encryption – Data & Communications – Despite the widespread availability of low cost encryption solutions, it is quite amazing how little use is still made of encrypted solution for the secure protection of government and enterprise documentation & communications. There is a range of commercial solutions based upon international standards, including those using PKI – Public Key Infrastructure. Encryption is of particular benefit for the protection of mobile comms, such as Wi-Fi, 3G, and devices such as 8GB Memory Sticks, and external hard-drives. Security for all government mobile devices is imperative using strong encryption standards ranging from AES-128 to AES-256. Critical government & corporate documents should allow be archived & back-up on strongly encrypted storage devices.

iii) DDoS Attack Management – Distributed Denial of Service – Such attacks have been of particular concern to the Georgian Government, as well as the Financial, Banking & Telecomms Sectors. They are caused by armies of "bots" that typically reside on millions of infected PCs across the world. The "botnet" manager is able to activate these malicious software "bots" and to direct them to send continuous messages to designated IP addresses of the targeted host systems. These targets are typically website, or the main access points to government or banking communications networks. There are various solutions available that can monitor all in-coming comms in real-time using recently developed techniques of "deep-packet inspection" to determine malicious IP packets.

iv) Web2.0 Applications – Back in the 20thC it was sufficient to simply deploy firewalls to protect government & enterprises networks. However, most end-users now have accounts on the social networking sites using Web2.0 style applications, as well as mobile iPhones, and Android powered devices. This generates a new level of network complexity, that is even mathematically chaotic, and provides a multitude of ways for determined hackers to compromise and gain control of end-user accounts, and hence ID theft. Today, there are international cybersecurity vendors that can help to secure Web2.0 social & business networking applications, and hence prevent the leakage of secure government & corporate information.

v) BCP - Business Continuity Planning – All government and business information should be backed-up at least on a 24 hour cycle. More critical information such as that relating to banking transactions or national intelligence will need to be mirrored in real-time on duplicate blade server farms, which will in turn be backed-up on a remote server site, with auto-fail-over in the case of alert or emergency. The more recent developments of server virtualisation & cloud computing can both be of considerable technical benefit in the provision of economic BCP solutions for government & major enterprises.

vi) Disaster Recovery – During the last 10 years Georgia has experienced several "disasters" that have impacted computing & telecoms systems including earthquakes, and cyberattacks. The significant international political tensions within the Caucasus Region mean that Georgia needs to make significant investments in cybersecurity in order to minimise the risks of bad events & "disasters". All major computer vendors provide well architected scalable solutions to support governments & large enterprises to deploy networked disaster recovery solutions to international standards.

vii) End-User Management – All governments & major enterprises in Georgia have sizeable networks of end-user PCs & similar devices connected by wired Ethernet, Wi-Fi and other mobile networks. These end-user devices need to be managed through Active Directory Services, including some form of user ID certification, as well as applications administration, software upgrades, and auto-back-up of designated end-user document, applications & mail folders. Controls also need to be placed upon the movement of end-user devices, including PCs, laptops, memory sticks, hard-drives, DVDs and mobile PDAs. There have been numerous cases across Europe and USA during the last 5 years of mission critical military, banking and sensitive government databases being lost by senior officials who mislaid their laptop or memory stick in a taxi, restaurant, airport or train-station! All such devices need to be equipped with encrypted drives, and auto-traceable through pre-installed software, so that in the event of theft, all data in the device can either be deleted, or the device otherwise disabled.

viii) Virtualisation & Cloud Computing – Virtualisation allows applications and processes to be optimally distributed and "virtualised" across the networked server farm which allows both processes and storage devices to be used much more efficiently than in a conventional environment. In the world of cloud computing, all the end-user processes and applications are effectively virtualised and outsourced to remote networked computer resources. With regards to cybersecurity this certainly improves the potential for improving BCP/DR, as well as reducing the problems with end-user systems administration. However, governments and enterprises will need to be careful that mission critical information is only accessible by approved personnel on remote virtualised "cloud" systems. And the remote host facilities should be fully physically secure with linked CCTV & access controls.

ix) Counter-Terrorism & Cybercrime – On-Line Global Networks have opened up a whole new pandora's box of "business" opportunities for criminals. Within Georgia, there is already a significant EU financed programme underway that started mid-2009 in collaboration with the Ministry of Justice that is updating Georgian Laws to meet the goals & objectives of the EU Convention on Cybercrime. Cyberterrorism and Cybercrime can be directed towards Georgia both by within the country, as well as from practically any other country in the world with a developed IP network infrastructure. I'll show later in this White Paper that countering the CyberTerrorism and Cybercrime threats requires the comprehensive integration of both cyber & physical security operations on a 24/7 deployment.

x) Digital Certificates and Signatures – All on-line financial and secure eGovernment transactions should be implemented with some form of digital certificate within the context of PKI, implemented using a solution such as the world renowned VeriSign Inc. In addition, the creation and editing of secure government documents, laws, military plans, national budgets etc, should be undertaken using operational processes that use PKI certificates & digital signatures to fully secure critical information. The Georgian Government should define and communicate the recommended standards for digital certificates & signatures and ensure that they are suitably deployed for all eGovernment Applications as well for the National Georgian Banking Networks & On-Line eCommerce Transactions. In general, I'd recommend self-regulation, and policing as the preferred way forward for cybersecurity operations and policies within major enterprises and the commercial world, with occasional government audits.

xi) CERT – Computer Emergency Response Team – The Georgian Research and Academic Networking Organisation – GRENA established the CERT-GE in 2006 to manage emergency responses within the educational and research sector. These CERT operations need to be urgently extended across all other sectors that are critical to national infrastructure including banking, transportation, telecoms and the power utilities which are all analysed later in this White Paper. Again, the national Georgian CERT operations should be driven from a senior level of Government, maybe the newly established Data Exchange Agency, and be responsible for the co-ordinated national response to all significant cyber threats and attacks. In addition, the CERT will need to be linked with physical security, regional & national operations so that the civilian emergency services – police, fire and ambulance can be quickly mobilised for certain events & disasters.

xii) Cybersecurity Organisation, Operations & Policies – Prior to the deployment of cybersecurity technologies such as those listed in this section, it is imperative that the government and major enterprises implement their own cybersecurity organisation, strategy and security policies. With cybersecurity growing in national & international importance during the early 21stC, it is recommended that security strategy and policy is defined, agreed and authorised at the highest levels of Government. At the same time, I would suggest that the Government works with the higher educational sector and ICT Security Businesses, to organise in-depth cybersecurity training to international professional standards, both for technical & operational staff.

- -

(3) Integrated Security Threats

Criminals, Terrorists and Defence Forces are now starting to develop their creative skills both to attack & penetrate physical security systems, and more importantly advanced cyber security systems. In addition, such forces understand that the penetration, manipulation and disablement of cyber systems can significantly reduce the subsequent risks during physical penetration and attacks. In this section we give some possible examples of ways in which criminal agents might gain access to supposedly "secure" systems in order to gain economic or political advantage & control.

In the previous sections (1 – Physical Security), and (2 – Cyber Security), we've assumed that the technologies and solutions are independently managed through separate Cyber Operations, and Physical Security Operations. This is indeed still surprisingly the typical situation in most enterprises & government agencies across the world today! So here we consider ways in which the determined criminal hacker, terrorist or foreign agent can penetrate, manipulate and possibly disable mission critical systems within the Georgian Government Ministries and Major Enterprises & Institutions.

a) Cyber to Physical Attacks

Here we consider ways in which criminals might gain access to cyber systems in order to subsequently carry out some physical attack, transaction or theft.

i) Sleeping Trojan "Bots" : The criminal or hostile agent hacks into the cyber operations through an open firewall port, SQL injection, cross-scripting error, or hacked password, and installs a sleeping "Trojan" or software "bot" to the end-user system. These are usually pre-programmed to carry out specific secret functions on the host system that can be remotely triggered. The "bot" may be programmed to continuously screen & filter host system databases for passwords, personal IDs, biometric information, financial transactions & banking account codes, or even military plans. So with regard to our agenda in this White Paper, some specific physical objectives could be:

- Physical Plans for secure Government, Banking or Enterprise Facilities, including location of security assets such as CCTV cameras, infrared & laser beams, sound & movement detectors, and network access ID & pass codes.
- Access to Detailed Personnel Information in order to secure the necessary information to manufacture fake ID building access cards, credit cards or any other personnel ID asset.
- Determination of timings for secret & sensitive events such as Presidential & Ministerial Travel plans, visits from overseas governments, or top-level commercial, economic & political negotiations.
- Access information regarding the transportation of valuable or politically sensitive cargoes that could include financial bullion, military supplies, and the movement of prisoners.

You'll understand from the above examples that autonomous sleeping software agents can be extremely powerful & dangerous Trojans that are often also quite difficult to detect unless the cyber operations team have top-level professional training & rigorously enforced security policies.

ii) Destructive Cyber "Bots" – Whilst the sleeping Trojans above are typically passive and not intended to "kill" the host system, the destructive "bots" are deliberately targeted at the host systems of critical national infrastructure (CNI) in order to partially or completely disable operations. Some typical applications of such hostile cyber "bots" are:

- Access the operations control systems for energy power plans, and thence to disable and close down the national electrical power grid.
- Hack into the national banking clearing network, and manipulate & randomize data in such a way that the financial transaction network is closed down for some days or weeks. In order to avoid early detection the hostile agent but initially make only minor adjustments to financial transactions and accounts, with increasing activity over time.
- Inject hostile "bots" into the civilian and military telecommunications networks to disable "comms" prior to possible physical attack on civilian & military facilities and national assets.

iii) Denial of Service Attacks – Usually referred to a DDoS or Distributed Denial of Service – These are triggered by zombie "bots that can be secretly installed on innocent host PCs & servers, and which may be simultaneously triggered to continuously send messages to the target host IP address.

- Denial of InfoCommunications for Government, Banking & Commercial Websites, resulting in shut-down of the eGovernment and eBanking Services, and disablement of commerce.

- Massive DDoS attacks will effectively lead to a rapid shutdown of physical business, shipments, wholesale & retail operations. Practically all business today is 100% dependent upon on-line stock control, credit card authorizations, government ID databases and electronic certificate authorities for user & transaction authentication.

- DDoS attacks are often accompanied by the mass defacement of websites, and subtle manipulation of mission critical documents, security settings and operational parameters.

iv) Spam Mail & Phishing Attacks – Criminals and Hostile Agents will literally send millions of spam emails with link to fake or "look-alike" websites in order to phish for personal, banking & password data. Once the information is transmitted & receive by the criminals, it will be used to gain access to physical bank accounts, cloned credit cards and possibly even to manufacture access ID cards to secure government or corporate facilities. The exponential rise in social networking sites is making such phishing attacks much easier. Users will typically enter all the necessary information (Date of Birth, Gender, Address Postcode, & Photo) for criminals to fake their identity for bank loans & social support grants, especially when combined with other easily available on-line directory info.

v) Time-Based "Bots" – In certain situations, hostile agents & criminals simply need to disable some physical facility or asset for a short period of time in order to gain access to secure premises. Remotely managed software "bots" implanted on the target host systems are programmed to autonomously either disable or ideally simply manipulate security parameter settings for short periods of time specified by the hostile agents.

- Access airports (civilian or military) by disablement of perimeter fence cyber operational controls that may include CCTV, light beams, fibre-optic cables, and ground vibration alarms. This could be implemented several weeks before the event through a combination of cyber hacking, and the presence of compromised computer staff working for the hostile forces.

- Entrance to mission critical facilities through temporary disablement of network access & ID controls in which the fall-back option is authentication of fake ID cards by security guards.

- Disable national energy supplies or telecoms networks for short periods to compromise or spoil key national political or commercial events. Following the short "time-out" the cyber software "bots" can be eliminated so that there is minimal evidence of the hostile agents. Again this shows the importance of logging all I/O transactions 24/7 and permanently be on alert & sniffing for hostile activity, with back-up log files on fully secure remote host servers.

vi) National Cyber-Attack – During the last 3 years both Georgia and Estonia have experienced massive cyber attacks on their government, banking and telecommunications networks. In future wars this is likely to become the preferred way of launching a pre-emptive attack with the intention of complete disablement of the target national critical infrastructure – energy, banking, government, telecommunications and transportation. If this is successful then it is likely that the targeted national military forces will be relatively impotent in the absence of power, communications & intelligence.

- Future wars will not necessary be triggered by isolated nation states, but by distributed networks of terrorist cells that are challenging to identify, and counter-target. Such terror-cells may exploit cyber skills to target national critical infrastructure with the dual aims of creating national chaos, and hence a fertile environment for national uprising & civil insurrection. This may sound hypothetical, but unless vulnerable nations, such as Georgia, implement in-depth cybersecurity precautions, both operational & technological, then the risks of such hostile events will increase year-by-year.

- The concept of cyberwar was originally developed by late 20th Science Fiction writers. However, many of the ideas, themes and strategies of cyberwar have analogies in the much quoted work of Carl von Clausewitz in his famous 19thC book – "On War" - which examines all aspects of physical military warfare and combat. I'd personally predict that cyberwarfare and cyberdefence will become of equal if not greater importance to physical warfare during the 21stC since modern society is now becoming 100% dependent upon computing networks!

- Georgia should consider the more recent actions and decisions in other Western Countries such as UK and USA where dedicated Cybersecurity Organisations have been established at the highest levels of government. In the USA this includes a new CyberSecurity Command within the US Defence Organisation, whilst NATO itself is also well advanced in the implementation of cyberdefence and potentially cyberoffensive operations for member states. The US DOD's Architecture is also worth consulting for background reading. This was originally designed in the mid-1990s as C4ISR – Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance. This architecture has since been updated and re-launched as the Department of Defence Architecture Framework DoDAF. It is particularly useful as a framework for distributed real-time military command & control.

- For the civilian sector, the UN Agency – International Telecommunications Union (ITU) – has taken the lead in the development of the recommended Global Cybersecurity Agenda (GCA) for all UN member states. The ITUs GCA is fully comprehensive, covering cybercrime, cyberlegislation, cyber training and generic technological security solutions.

b) Physical to Cyber Attacks

Here we consider ways in which criminals may gain access to physical facilities, or members of operational staff in order to access the cyber systems, processes and databases.

- Theft & Modification of Physical Assets – This would typically include the theft of laptops, and other mobile assets that contain passwords, personal information and possible sensitive and secret documents and plans. In addition the hostile agents may try to obtain examples of physical ID cards, passports and the security details and plans for secure facilities. Mobile assets such as memory sticks, external drives and intelligent mobile PDAs (iPhones & iPads) are particularly vulnerable to theft through criminal diversions, and classic hustle scams in public places such as cafes, airport lounges, taxi cabs, and reception areas. All mobile assets with sensitive data should be encrypted to at least AES256 standards, with the potential for ALL data to be deleted in the event that a hostile agent connects to the internet or mobile net. Failure to "kill" such stolen or lost mobile assets could result in them being used as "fake" nodes to communicate on secure VPNs with other staff & data nodes, and then to phish for more sensitive information or to be used for the installation of alien Trojan software "bots".

- Fake Maintenance Staff – Many organizations, both government and civilian, have minimal security for computer & security maintenance staff. Skilled staff can be compromised and used as physical human trojans to install back-door software and "bots" to target host systems. This is a particular problem for remote offices & facilities that may in turn have lower levels of security training & professional staff. Such regional or local offices would be the natural choice for hostile agents wishing to install software "bots" that can network with "secure" central government or corporate host systems, and is a particular risk for national eGovernment and eBanking networks with remote office nodes in rural locations.

- Compromised Operations Staff – The classic way for criminals & terrorists to secure access to secure premises such as banks, Telecomms Centres, Power Stations and secure server & storage rooms is to compromise and then "recruit" a vulnerable member of operations staff. Such an inside physical agent can provide operations & cyber support for the hostile agents. Once again such problems are more easily detected if the cyber and physical security operations are tightly co-ordinated to provide integrated security that minimizes risks.

- Guests and Visitors – In general, special precautions and policies should be implemented for all visitors and guests to secure government or corporate facilities. There are clearly a number of ways in which security might be compromised, but a particular risk is for guests to use mobile devices to logon to weakly secured internal Wi-Fi Local Networks, and download "bots" that can then open firewall ports or other back-doors once the "guest" has left the premises. Alternatively, it only takes a couple of minutes to download up to 8GBytes of document folders from an open staff laptop to a compact USB memory stick. A smart guest might even plug in a Wi-Fi Access Point to an open PC or Host System that can be accessed from outside the premises. It is quickly seen that fully secure facilities will demand that visitors leave ALL mobile devices, including memory sticks, phones, cameras & laptops with the front reception desk! In addition, cybersecurity staff should permanently monitor the airwaves for rogue Wireless Access Points, and for any non-secured & encrypted Wi-Fi nodes. Generally, government & corporate wireless networks should be authenticated with end-user PKI-style certificates based upon international standards such as IEEE802.1X.

Some of those reading through the above hostile agent scenarios will maybe feel they have too much in common with Hollywood Movies like "Mission Impossible" or "Ocean's 11" than the real world. However, the current 21stC reality is that all the above scenarios are absolutely possible today, and cybercriminals and terrorists are using such techniques on a weekly if not daily basis to boost their economic wealth and political leverage in those nation states with weak cyber defence shields. Military and Banking facilities in developed nations receive many thousands of mini-cyber attacks everyday in which hostile agents are seeking out weak points & back-doors into the secure networks. Increasingly such governments & major corporations are integrating their organisational and operations for cyber and physical security in order to counter the risk & threats from major attacks.

- -

(4) Integrated Cyber-Physical Security Themes

In previous sections we've listed most of the major physical and cyber security technologies and solutions. In reality these are not really such distinct categories, and in this section we start to explore the ways in which physical and cyber security can work positively together to significantly increase overall national government and corporate security, as well as reducing operational running costs. In addition, the integration of cyber and physical security solutions will result in earlier detection of alarms, and consequently mean speedier real-time response to emergency alerts.

i) Integrated Cyber-Physical Security Operations – At the highest level of security organisation and management it is imperative that both cyber and physical security events & alarms are considered within the same operational environment. We've seen in the previous section how physical facilities can be penetrated through cyber hacking and vice versa. Hence in order to generate early warnings and forecasts of future events it is becoming critically important to analyse cyber events as possible predictors of physical alarms, thefts, emergencies and even territorial invasions.

Integrated security operations may be networked across a range of cyber and physical control rooms, but all the critical & abnormal events should be immediately relayed to integrated control for action.

ii) Adaptive 4D Real-Time Security Modelling – The technologies solutions and assets are only useful in the context of an overall security model and architecture. Some international security vendors are now developing & deploying powerful 4D "computer game" style multi-media displays of large facilities such as airports, university campuses, power stations, industrial oil & chemical plants, military bases and government ministries. These can then be rolled back in time to check on how emergencies unfolded. In addition such 4D models can be used in the simulation of future "What if Scenarios?" for training purposes, and in the real-time forecasting of possible decision options.

In such 4D models all the security assets such as CCTV, gateways, ICT systems, staff & visitor movements, and other tagged assets are shown within an intelligent multimedia virtual world, just like a navigable display from the well known multi-player "social-networking game - Secondlife". Such models make it far easier to integrate cyber & physical security assets & events, as well as providing a basis for operational teams to discuss response plans from distributed locations & control rooms.

Finally, I should add that 4D security simulation modelling is an excellent medium for teams to debrief following an emergency event which can be replayed using the archived security event logs. I'd expect that such 4D security models will mainstream as "best practice" during the coming 5 to 10 years for most major government and corporate security operations.

iii) Integrated Building Access Controls – Most security vendors now offer integrated IP networked access controls for office receptions, door controls, fire alarms, motion alarms, CCTV and RFID cards. However, as noted in the previous section, these physical alarms & security assets should also be networked with the cybersecurity operations if the government or enterprise is to "outsmart" the hostile agents, criminals and hackers who will exploit every security "loophole & back-door".

iv) Critical National Infrastructure (CNI) – This is a key security topic in its own right which we consider in more detail later in the White Paper when we explore specific examples such as airports, national energy grids, banks and national defence. In the 19thC & most of the 20th C it was simply necessary to protect the perimeter of critical facilities with high barbed-wire or electrified fences. Similarly in cyberspace, government & companies installed dual hi-spec firewalls with a virtual DMZ. In the 21stC neither the physical perimeter fence, nor the cyber DMZ with dual firewalls will be sufficient to protect critical infrastructure from attack!

In the 21stC, every critical national infrastructure requires its own integrated cybersecurity organisation that is responsible for setting the security policies, training staff, and establishing fail-safe security operations based upon security solutions already discussed in this White Paper. The national government should take responsibility for setting the top level standards and security architectures that should be rolled-out across all designated Georgian CNI facilities & assets.

v) Integrated Digital Forensics & Legislation for Cybercrime – The investigation and prosecution of cybercrime also needs to be integrated within the traditional Georgian criminal legislation so that all hostile and terrorist actions can be legally prosecuted to the fullest extent of the law. Today it is likely that some of the potential hostile actions hypothesised in section (3) on security threats are not yet captured within Georgian Laws. I understand that most, and hopefully all of these loopholes & shortcomings will be closed following major cybercrime collaboration by the European Commission & Georgian Ministry of Justice. The Georgian police authorities will also need to extend their professional skills to include both digital & physical forensics in order to collect the criminal evidence necessary for prosecution of legal cases that bridge the real and cyber worlds.

vi) Intelligent Surveillance – CCTV & ANPR – During the last 20 years we've seen the deployment of CCTV operational control rooms that are covered with a moving 2D matrix of "live" CCTV cameras from the target monitored environment. Now with digital CCTV on IP networks, we can use smart software to identify moving targets, and issue automatic alerts with regard to abnormal events. A particular example of such smart software is ANPR (Automatic Number Plate Recognition) which can provide the facility management, police or military authorities with real-time information regarding vehicle registration, insurance and owner. During the coming 5 years I'd predict that CCTV will become ever smarter as a key security asset for the 3D surveillance of critical infrastructure, and city regions such as those around the Georgian Parliament, Government Ministries & Military Bases.

vii) Identity & Mobile Asset Management – RFID & Biometrics – Essentially we're talking here about ways in which to intelligently tag & monitor mobile physical assets and persons so that we can minimise the risks of hostile events within the target security environment. All government and company mobile cyber assets such as memory sticks, external drives, and laptops should be RFID tagged, and movements tracked through the secure facility. Ideally, such assets should remain in the facility, but those that need to exit should be strongly encrypted so that only selected authenticated users can open up the secured folders, applications or documents. The movements of staff, contractors & visitors should also be tracked in the most secure government & military facilities through active RFID cards & smart CCTV. These can be complemented by Biometric Body ID Parameters such as Facial, Retina, Iris, Vein or Fingerprints to make sure all those individuals are 100% authenticated.

viii) Integrated Real-Time Defence Operations – Earlier in the White Paper I made reference to the US Dept of Defence – C4ISR & most recent DoDAF Real-Time Architectures. The primary focus of this White Paper is to outline security issues relating to government and civilian enterprises. However, I'll briefly discuss the critical importance of cyber and physical security integration for the National Georgian Military and Defence Organisations. Only during the last 5 years have most Western Governments & International Development Agencies really taken cybersecurity seriously as a key aspect of national defence, crime prevention, economic resilience and growth.

Today, the physical armies & national defence forces are potentially vulnerable to the threat of cyberattacks which can potentially disable military Command and Control Networks and real-time intelligence systems prior to a hostile attack and territorial invasion. In fact, as already mentioned, intensive cyber attacks are relatively low cost and low risk, and used as an offensive cyber weapon they significantly lower entry barriers for terrorists and hostile forces. In addition, cyber weapons will most often be used prior to any physical attack in order to cripple the critical infrastructure, both military and civilian of the target region.

So the conclusion is that national defence forces in every nation need to augment their physical strength with a cyber operations room that is fully integrated with the traditional real-time Command & Control systems. All physical assets and military facilities should also be regularly security audited to check that there is minimal possibility of cyber penetration to the access controls, wired, radio & satellite communications & on-line networked weapons control systems. Such integration of national cyber and physical defence needs to be organised & orchestrated at the highest levels of government.

ix) Augmented Reality Solutions (AR) – Now we consider a couple of future directions for integrated security solutions for the coming 5 to 10 years. First we briefly review the developments

"Augmented Reality" in which real-time cyber-intelligence is overlaid on the real world and typically presented to the user through head-up displays, smart glasses, or mobile wireless screen such as the iPhone or iPad. Such cyber-solutions are already in use in some military, police & emergency organisations, and they are also being actively researched and further developed in universities & labs around the world.

Augmented Reality complements work on the 4D security simulations since it is the ideal way in which to present real-time digital event updates to mobile users in hostile environments such as a "war zone", "terrorist incident" or natural emergency such as earthquake, flood or fire. In addition it allows a team of mobile workers to communicate, network and take full control of a crisis situation. The classic 20th solution to crisis management was to build a "crisis operations room" within a well protected underground bunker. However, the 21stC will demand that we also develop "virtual crisis centres" for emergency response in which we establish "ad-hoc" networks to both facilities & field based response teams that all have access to the same augmented reality information feeds. So we'll have a hybrid model of hierarchical command & control from the underground control centre, and virtual peer-to-peer networking amongst the mobile & remote team members, all supported by real-time cyber-intelligence feeds viewed through augmented reality 3D devices.

x) 21stC Neural Security - During the next 5 to 10 years, the security solutions will converge to full integration architectures, with increasingly sophisticated 4D real-time modelling and forecasting of future events based upon past events & info archives. I also noted in the previous paragraph that such models will be delivered to peer-to-peer networks of end-users through augmented reality devices.

I refer to such security architectures as *"neural security"* since it has many analogies to the ways in which living cells and organisms manage their biological security operations. Many of these living processes are autonomous in that there is no conscious decision for example to replicate antibodies in response to hostile viruses. However, for high level events in mammals there will be a conscious neural decision to either "fight" or "flee" from an emergency & potentially life threatening situation.

So in developing integrated cyber and physical security solutions during the next 5 to 10 years there will be a requirement for many lower level responses to hostile alerts to be autonomous, and only the high level major hostile threats should be filtered up to the operational team for decision & response.

In summary, we're moving from the 20thC in which security related primarily to the "physical world" to the 21stC in which we are integrating the signals from both the "physical world" and "cyber world". The intelligent responses & actions from emergency alarms & hostile events will then be transmitted in real-time back to a complex combination of networked physical and cyber assets. Key strategic priorities & features in such integrated "neural security" solutions will be:

- Real-Time Operation – Secure and monitor EVERY level of cyber asset and critical physical asset through IP networking, RFID radio tagging, and communicate security status to the designated integrated operations centre.

- Adaptive Modelling – Develop and deploy an operational 4D model of the target security environment which could range from a single building to a city region. Populate and overlay the model with the chosen real-time cyber & physical security assets, and continuously check for abnormal events & alarms. The model will need to be regularly updated & adapted according to the parameters of the security environment such as staffing, and info assets
.

- Fail-Safe Design – All key cyber assets, info servers & storage devices should be replicated with back-up processes to support BCP/DR policies. In some cases there will need to be triplicate systems for certain government, financial and defence information resources.

- BioNeural Metaphors – Existing cyber security solutions already have some similarities with bio processes such as the detection and response to computer "viruses". Increasingly it seems that future integrated cybersecurity solutions will adopt more and more process metaphors from the world of organic living systems. In particular there will be greater focus upon the detection of abnormal events through adaptive "neural networks", and upon autonomous responses to lower level threats, allowing operations staff to focus upon real crisis situations.

- Augmented Reality Solutions – The complexity and scope of the real-time security data feeds means that advanced multimedia interfaces will be required to communicate events, locations, and decision options to mobile staff and teams. Developments in augmented reality displays will be a key feature in allowing quick mobile response & deployment to security situations.

- Hybrid Architectures – Classic Security Solutions were hierarchical and driven through teams of physical security guards managed as a "private army". Integrated cyber-physical security requires the co-working of BOTH hierarchical and peer-to-peer networking. Hierarchical organization provides a guaranteed quick response, whilst peer-to-peer organization is optimal for the synchronization of information across a mobile distributed network. Living organic systems also deploy hybrid architectures of hierarchical & peer-to-peer networks.

In this section I've tried to summarise the ways in which cyber security and physical systems can be integrated to provide security solutions that can respond to the threat scenarios discussed in section(3). I've also given some brief insights to the strategic directions in cyber-physical security solutions.

- -

(5) Integrated Security Sector Scenarios

In previous sections we gave general examples of the ways in which criminal, terrorists and hostile agents might penetrate critical government and enterprise facilities and cyber systems. We now consider these threats sector-by-sector and summarise ways in which the deployment of integrated solutions can significantly reduce the penetration risks, and provide early warning of potential attacks.

i) National Government – We start with the Government since the overall strategy, standards and architecture for all aspects of integrated security should be driven at the highest levels of Government. Given the importance of the Government sector, I've distinguished below between "Physical to Cyber" Security and ""Cyber-Physical" Security. For example, for "Physical to Cyber" we're interested in securing the physical facilities in order to prevent access to ICT systems, whilst in "Cyber to Physical" we secure electronic information to prevent access to critical infrastructure.

- Government Ministries & Parliament
  - Physical to Cyber – The region around each Government Ministry and the Parliament should be managed as a high-security zone with, security lighting and smart CCTV coverage linked with ANPR to detect possible hostile vehicles. Advanced biometric software such as 3D facial recognition may be used to detect known hostile agents.

  - Cyber to Physical – All computing systems and networks need to be managed to the highest cybersecurity standards in order to prevent hostile intrusions, the installation of intelligent "bots", and the manipulation or theft of documentation & codes.

- eGovernment Services
    - Physical to Cyber – ICT facilities should be fully secured, and computing staff should be vetted to standards related to their operational roles & information access.

    - Cyber to Physical – The eGovernment Services are interfaced with most of the most critical datacenters, including those for citizen data, vehicles, taxation, customs, criminal records and health records. Strong authentication techniques based upon certification within a Public Key Infrastructure (PKI) should be fully deployed.

- National Defence
    - Physical to Cyber – All military bases, and related ICT defence facilities should be protected to the highest security standards with smart perimeter fencing using lasers/optic fibres, linked with HD CCTV and advanced monitoring software. The future deployment of 4D real-time models would also be appropriate to such sites. Contractors and ICT suppliers & maintenance staff should also be security vetted.

    - Cyber to Physical – Clearly all the communications links, both wired & radio should be encrypted and also duplicated with alternative routings in case of hostile events. Particular security risks are all mobile devices (phones, discs, memory sticks, ID Cards…) and these should be encrypted to be fail-safe, so that in the case of loss or theft all data can be deleted if connected to the internet, or incorrect codes used.

- Regional Administrations
    - Physical to Cyber – Just as predators in the jungle will seek out the weakest prey, the hostile agents and criminals will see out the weakest point of entry to ICT networks. Remote Government offices in small towns, and villages will usually have lower grades of professionally trained staff, but will still have connections to the internal Government network and eGovernment Applications. For these reasons, these remote nodes still need to be fully secured, with networked alarms & smart CCTV cameras.
    - Cyber to Physical – Precautions should be taken to ensure that all network access codes for remote facilities are as secure as those in Tbilisi. The risk here is that these remote nodes are “hacked”, and then hostile agents gain the staff ID information, and security plans that allow them to gain access to critical national facilities.

- National Security Standards Authority – The Georgian Government should set the recommended standards for all aspects of both physical and cyber security for designated critical national infrastructure. During the last 3 years, many national governments have established dedicated high-level organizations that are fully responsible for cybersecurity for critical national infrastructure, as well as all aspects of security standards & regulation.

ii) Banking & Financial Services – The financial sector is clearly critical to national economic infrastructure, and today most transactions are carried out over electronic banking networks. If these are penetrated, secretly manipulated or critical files deleted, then the resulting chaos will inevitably destabilise business, whilst trust in the banking system will be significantly reduced.

- Clearing Bank Network – This lies at the heart of the financial sector, and underpins the whole economy. Clearly both the ICT Operations centres, servers and storage require the highest levels of technological security, whilst operational & support staff should be fully vetted and trained to international professional standards. In the case of the Estonian cyberattack during June 2007, the banking & financial services sector was one of the primary targets since it is clearly critical to all business & government operations.

- Branch Offices – Banking branches in the heart of downtown Tbilisi are likely to be well secured against physical attack. However, as in the government sector, there are also significant security risks at the remote bank branch offices where hostile agents might gain access to banking networks through poorly secured nodes, passcodes, and stolen ID cards.

- eBanking – During the last 5 years, many banks in Europe and USA have upgraded end-user authentication to eBanking networks using a combination of passwords, secret phrases, and one-time codes generated by synchronized off-line devices. These "strong" authentication processes certainly reduce the risks of fraud, although the creative "hacker" will still find ways to penetrate the network if they're able to gain access to personal IDs & partial codes!

- International Banking Networks – Cybercriminals are already skilled in laundering massive funds from illegal business transactions through the international banking networks. Suspicious international transactions can be checked through in-depth investigations, according to standard operational procedures. For these reasons, it is critical that the network gateways, servers and storage are continuously monitored for hostile software "bots" & other malicious code that may compromise and potentially "hide" illegal banking activities.

iii) Airports & Transportation

- Civilian Airports – The traditional model for physical airport security is one of successive security search & scanning barriers, with sterile security zones for cleared passengers, and designated security ID zones for staff working airside on baggage handling, or airline operations. However, the advent of cyber attacks means that additional precautions are being taken by airlines to check passenger profiles, IDs and electronic mobile devices such as laptops, phones and cameras. The airport ICT operational systems & networks, as well as the airline registration systems need to be fully secured against secret penetration by "bots". In particular, it is imperative that all Wi-Fi & wireless IP nodes are locked down and encrypted so that hostile agents cannot logon to any of the closed airport ICT operations networks.

- Train, Metro & Bus Stations – These zones around and within civilian transportation hubs have been preferred "soft" terrorist targets in a number of countries during the last 10 years. Physical security can be increased through smart CCTV systems, linked, as appropriate, to ANPR systems to track car, buses and trucks within the designated security zone. The metro system is probably the most difficult to physically secure against attack, but early warnings of possible events can still be provided through smart CCTV linked to advanced monitoring and surveillance software. In the event of high alerts, random passengers & staff could also be searched by civil police for illegal items, and personal IDs & documents checked too.

iv) Telecommunications & Mobile Services – Telco Services have been critical to business now for more than 100 years, whilst mobile services have been critical for now longer than 10 years! Together with the Internet Service Providers it remains vital to business & government that they remain fully operational and free from cyber penetration, info manipulation, info filtering & theft.

- Communications Hubs – Most communications networks are converging to IP backbone networks that support ALL multimedia services – video, voice, broadband & mobile. This is of great economic benefit to operators, but is probably more vulnerable to cyber penetration since all the critical services are now routed through the same network hubs & switches. Network "hackers" that are specialists in IP Nets & ICT devices can often find vulnerable points to secretly attack . Hence telecommunications services, mobile operators & ISPs need to continuously audit the integrity of their networks against such hostile penetrations. In fact one the weakest security links is that of temporary technical staff and maintenance staff that have in-depth access to network hubs. So ALL staff whether temporary or permanent should be vetted before they're issued with IDs that give access to critical network infrastructure.

- Mobile Devices – I've already discussed at some length in this Security White Paper on the vulnerability of end-user mobile devices as potential entry points for cyberattacks. Firewalls are probably now as useful as medieval castle moats & portcullis in securing 21stC networks! Successful cybersecurity policies require all ICT assets, both fixed and mobile, to be secured through embedded security software, with encryption applied according to the security risks.

v) Energy & Water Utilities – It is becoming understood by governments that even the energy utilities, power stations, pipelines and national grids could become attacked by hostile cyber agents.

- Electrical Power Stations – The automated control systems & processes are always programmed to have fail-safe operations, but we've already seen certain nuclear facilities during the last 20thC in which such systems failed to function! More recently there have been massive blackouts in the USA caused by power systems failures. Since these processes are all essentially specialized ICT applications for industrial devices, they are also liable to cyberattack through remote ports, or through the acts of compromised operational staff. Clearly facilities such as power stations should also be physically secured in the same way as National Government Ministries and International Airports, with perimeter fences, CCTV and full staff & visitor ID Access controls.

- National Power Grids – The electrical power grid itself with high-tension cables, and sub stations should also be physically secured through smart surveillance CCTV, laser & optic fibre systems. And the operations centres will need to deploy cybersecurity policies too.

- Oil, Gas & Water Pipelines – A key source of Georgian GDP is the transit oil pipelines from the Caspian to Black Sea, together with the freight trains. Such pipelines are also monitored through supervisory systems that could potentially be compromised & disabled by agents. The 2008 War demonstrated certain vulnerabilities in the pipeline & railroad networks so security improvements through physical surveillance & cyber integration should be a priority.

vi) Police, Cybercrime & Legislation

- Personal Data & ID Protection – The growth of personal identity theft within developed nations has grown spectacularly during the last 10 years since it is relatively easy to obtain personal information such as "Dates of Birth", "Home Addresses" & related details through public on –line databases. Such data is used by cybercriminals to obtain bank loans, order goods, and even to set up new credit card & mobile phone accounts. Such crime is difficult to control unless there are rigorous counter measures & cybersecurity policies that request stronger authentication from citizens such as Photo RFIDs or Biometric ID Cards.

- Cyber Legislation – Cybercrime has increased faster than the supporting criminal legislation. This needs to be urgently fixed so that all the hostile cyber actions that I hypothesized in section (3) are established as being illegal and open to criminal prosecution.

- Police Cybercrime Units – Cybersecurity and Integrated Cyber-Physical Security are complex fields that demand months of professional study to reach certified international standards. National police forces will require dedicated trained professional teams to identify crimes, investigate & secure electronic evidence that will support successful prosecutions. I'd suggest that physical security solutions such as smart CCTV surveillance systems, biometrics and ANPR should also be included as skills that are deployed within a Police Cybercrime Unit.

vii) Educational Institutions – Schools, Universities and other Educational Establishments – Typically these have been extremely open in the past with regards to both physical and cybersecurity. However as schools and colleges are becoming networked there is an urgent need to secure these networks & computing devices both against abuse as well as secret penetration & manipulation by hostile agents.

- Integrated Campus Security – There have been numerous tragic events that have taken place on university campuses around the world in recent years. Clearly it is preferable to keep campuses open than behind barbed-wire perimeter fences. However, the physical security should be upgraded to at least include some level of smart CCTV surveillance, ANPR vehicle checks, and random checks on student ID cards, with occasional bag searches too. University networks are traditionally also the location of some of the most expert cyber hackers, and these networks may be used as the anonymous cyber port of entry to more critical networks. So again some thought might be given to the operational integration of cyber & physical security within major educational institutions to reduce the risks of hostile & tragic events.

- Professional Security Training – Clearly there is a major for the Georgian Universities to play in the creation of a professional cadre of cybersecurity specialists. Course agendas for such Undergraduate & Masters' Level courses could be based upon those already offered by leading Western Universities, as well as the training agenda for professional security organizations such as the CISSP (Certified Information Systems Security Professional).

viii) Healthcare and Emergency Services – Previous economic sectors are all clear candidates for being designated as critical national infrastructure (CNI). However, in this White Paper we also consider Healthcare and related Emergency Services as being within this CNI category too. In the event of natural disasters (earthquake, fire, flood, epidemic), terrorism, civil unrest or war there is clearly a critical operational dependence upon the health, medical & emergency services.

- Medical Devices & Software – All medical equipment & software should be fully secured against the possibility of penetration, hacking & malicious manipulation. Operating theatres are now effectively networked computing facilities so there should always be procedures for business continuity with real-time back-up services during critical operations. Medical computing software should also be certified to international standards since any malfunction or system crashes could potentially have fatal consequences.

- eHealth & Patient Health Records – Many countries are now putting patient medical histories and all related health records on-line. This has strong healthcare benefits for just-in-time treatment, but once again if the records are maliciously altered or data deleted there could be negative outcomes. In the USA, the HIPAA Compliance (1996) provides a comprehensive framework for the protection of electronic health records & information. eHealth is a key service within eGovernment, and closely associated with on-line social welfare. Hence the Georgian Government should secure on-line patient records, multimedia consultations, and the transmission of patient data from X-rays, MRI scans & other on-line diagnosis tools.

- Pharmaceutical Chemicals and Drugs – From the perspective of physical security it is important that there are adequate controls regarding the security and sourcing of all chemicals & drugs deployed within the medical establishments. There have already been various international security incidents relating to nerve gases & toxic chemicals (in Japan), as well as biological terrorist weapons such as those relating to anthrax spores (in USA & elsewhere).

- Hospital Campus Network & Access Security – Most of the same security considerations apply to medical & hospital campuses as for educational institutions and business parks. CCTV linked with ANPR should be deployed to monitor and control vehicle movements, particularly those of delivery trucks, ambulances & other emergency vehicles. Internal movements of both staff, patients & visitors will need to be carefully tracked within hospitals, as well as the access to secure areas such as operating theatres, consulting rooms and storage areas for drugs & medical equipment.

- Emergency Service Communications Networks – The Medical & Healthcare Services are at the core of emergency services that include the fire, police and ambulance services. It is quite possible that these communications and electronic logistics networks could be hacked by terrorists or other enemies in order to create added chaos and disruption following a major emergency alert or invasion.

In summary, the Georgian Government should ensure that hospitals, medical institutions and related emergency services are fully secured against both cyber & physical attacks.

ix) Military and National Defence – The Military Command and National Defence Operations are clearly the most respected and highest level user of advanced security solutions. I stress here that to be successful during the coming 5 to 10 years, the Military Command will need to give urgent consideration to ways in which cybersecurity can be integrated within the overall national security policy, deployment and mainstream defence operations. I should add that I'm not qualified to go into any detail with regard to defence issues, so the following points represent some personal ideas.

- Cyber Early Warning Signals – I mentioned earlier that future hostile actions are likely to be initiated by either a sudden burst of cyberattacks targeted upon critical national infrastructure. And even before the sudden burst, it may well be possible to detect explorative penetrations of software agents that are secretly navigating and manipulating target cyber ICT assets. Failure to detect such early warning cyber explorations could prove catastrophic since a major cyberattack could well disable the national communications, banking & power infrastructure.

- Joint Cyber-Defence Operations – The US Defence Forces have announced that they are integrating Cyber Command within their overall Defence operations. Based upon my earlier comments it is easy to see the logic of such investments of staff and technology to counter the growing cyber threats from both nation states, and distributed networks of terrorist cells. NATO is also extremely active with regards to cybersecurity operations and training, and recently established a dedicated centre in Estonia following the devastating 2007 attacks.

- National Borders in Cyberspace – During the last 10,000 years, the national borders of Georgia have been no more than 3 Dimensional, and have been physically monitored & secured with defensive land, sea and air forces. However, for the last 10 years, the national borders have become multi-dimensional since the networks extend globally in cyberspace. Georgia should now prioritise investment to extend its national defence & military forces to include the defence of its national economic interests & critical infrastructure in cyberspace!

- -

(6) Integrated Security Benefits

We've now considered the integrated security threats and sector scenarios in some depth. In this section we summarise the main benefits to Georgia in merging security operations for physical and cyber security for both government, and mission critical enterprises such as telecoms, energy, banking and transportation. The top 10 benefits of operational security integration are :

i) Single Security Organisation – Traditionally IT security and the physical site security have been managed by separate organisations. However, the IP networking of site security with smart CCTV, biometric & RFID ID Cards means that it makes sense to establish a single security organisation under the Chief Security Officer (CSO). In countries such as Georgia there is often a shortage of fully trained and certified cybersecurity professionals, so integrating the cyber & physical security organisations may help the country to reach critical mass. In addition it will be useful to have some transfer of knowledge and skills between those in the fields of physical security & cybersecurity.

ii) Reduced Costs – Bringing together cyber and physical security will allow the integration of the supporting IP networking & technology costs. The merger of the IT security & physical site security operations will also result in financial budget savings. Many organisations are starting to converge the cybersecurity and physical security alarm systems for major facilities within a single networked operation centre, supported by a remote fail-over back-up centre in case of major disasters.

iii) Flexible Staffing – Merging the cyber & physical security operations will provide more flexibility in operational staffing & resourcing. There is also likely to be an expanded professional career opportunity for specialist staff. The overall impact will be to re-focus the integrated security programmes, and to place the security strategy & investments at the highest organisational levels.

iv) Early Alarm Warnings – It is quite often the case that physical alarms may be initially triggered by cyber penetration, and vice versa and discussed in the section (3) on integrated threat. Merging security at the operational levels means that the organisation will be aware that if, for example, the network access software & setting have been "hacked" then there is a higher risk of physical building intrusion. Similarly, if laptops & mobile devices are stolen with confidential personal, ID & credit card details, then there will be increased risks of financial cybercrime based upon "faked" IDs.

v) Extended Protection - The integration of cyber & physical security operations will enable greater scope of security protection both geographically, as well as in time. The smart CCTV networks will permit security teams to make some predications regarding potential hostile events. Similarly, the active monitoring of national cyberspace will provide the authorities with indications of possible future cybercrimes, acts of terrorism and threats to national borders & defences.

vi) Focused Security Policy – At present, many enterprises & organisations have somewhat fragmented security policies that are poorly communicated , with minimal audit & regulation. The integration of all security operations within a dedicated high-level team will provide the strategic focus and necessary authority to create an effective & successful security policy for the enterprise.

vii) Reduced "Open World" Security Risks – Security for the 20thC was "closed world" in which physical security meant security guards, perimeter fencing & turnstiles, and Hi-End IT security was all about DMZs with Dual Hi-Spec Firewalls! However, both the physical and cyber worlds have opened up and full protection requires us to analyse signals, alarms & events from both physical & cyber worlds within the same adaptive operational & architecture security frameworks. Neither perimeter fences, nor firewalls will secure national defences!...

.....Now we need to secure the social networking Web2.0 applications, iPhones and Wi-Fi devices. Cybersecurity needs to be embedded as micro-code within EVERY mobile device that connects to the government & enterprise networks. Similarly, every physical security asset also requires upgraded intelligence so that operators can zoom in real-time to incidents on perimeter fences, or within sites using smart tracking, ID & advanced CCTV surveillance technologies.

viii) Cybercrime Control – Cybercriminals & Terrorists are already skilled in the application and deployment of 21stC cyber technologies. Hence both civil & military government authorities need to establish & train-up professional cybersecurity teams with comprehensive skills in order to win the battle against cybercrime & international terrorism. The integration of cyber & physical security operations from multiple government agencies will help to significantly improve the situation just as the US Govt established the focused Dept of Homeland Security after the tragic events of "9/11".

ix) Critical National Infrastructure (CNI) – In my sector-by-sector analysis I discussed how security impacts each of the key economic sectors of banking, telecommunications, transportation, energy & education. The government will need to ensure that each organisation designated as critical national infrastructure has its own integrated security organisation, with effective deployment of its security strategy and policies throughout its personnel & operations. As mentioned previously, it is probably best if this is "self-regulating" with just the occasional government audit since this would be expected to create a "security culture" of responsibility & risk minimisation within the enterprises.

x) Improved National Defences – For the last 1000 years, the mountains of the Caucasus Region have provided the natural security barriers against invasion. Now these physical barriers and armies need to be augmented through equal if not stronger defences of Georgia's borders in cyberspace! In my previous presentation to the 1st GITI Conference in Oct 2008 I defined the Project *VARDZIA*. All native Georgians will know that ***Vardzia*** **-** ვარძია is the 12thC complex of secure caves developed under the wise leadership of Queen Tamar that protected Georgia against invasion for several hundred years. So I thought it might be interesting to now define Cyber-*VARDZIA* as a 21stC security acronym:

***** VARDZIA = (V)irtual (A)daptive (D)istributed (Z)ecurity (I)ntelligent (A)rchitecture *****

- **Virtual** = Virtual world is the world of cyberspace – Globally Virtual & Locally Physical!
- **Adaptive** = 21stC Security solutions need to be deployed with adaptive real-time response.
- **Distributed** = Just as the Ancient Vardzia was a distributed cave complex, so 21stC integrated security is architected as a distributed peer-to-peer network of secure organizations.
- **Zecurity** = We denote the integration of cyber security & physical security as (Z)ecurity!...
- **Intelligent** = We noted in previous sections that all the physical & cyber security assets and solutions will become smart with embedded networked intelligence.
- **Architecture** = The integration of cyber & physical security clearly demands an extended architecture. Within the defence community an excellent example is the classic US DoD – C4ISR / DoDAF Real-Time Operational Architecture. Whilst in the civilian sector the ITU's innovative Global Cybersecurity Agenda provides an outstanding framework to all aspects of cybersecurity including cybercrime, cyber legislation, cyber "bots" and cyber organization.

So, in common with ALL other nations, Georgia will need to upgrade its national defences over the next 2 to 3 years to include cybersecurity within its national security framework & architectures.

(7) Next Steps

In previous papers & presentations I've presented proposals and outline action plans for the implementation of comprehensive cybersecurity within Georgia during the coming months & years. I understand that such plans & proposals are already under discussion by the Government. So to move the discussion forward, I've focused in this new White Paper upon presenting the benefits of integrating cybersecurity operations with those of physical security under a focused organisation.

With regards to the necessary steps towards security integration I suggest that the following 3 phases:

a) Phase 1- Audit & Review: The designated Georgian Government organisation for national security will review & audit all current cyber & physical security systems across Ministries, Agencies and Institutions. Also include the major stakeholders within the critical economic sectors of banking, telecoms, energy, transportation and education. This phase will typically take 3 to 6 months.

b) Phase 2 – Planning: Based upon the audit results, and national security strategy, the Government will work with each organisation to develop its operational & technological plans. These will upgrade the cyber & physical security to international standards, and will take 6 to 12 months to complete.

c) Phase 3 – Deployment: The overall implementation of the national integrated security plans would be expected to take between 2 to 3 years. Each organisation would be responsible for its own upgraded security deployment within standards, policies and architectures set out by the Government. The completed distributed network of integrated security operations across the government & enterprises would conceptually represent a sort of 21stC ***"Cyber-Vardzia"*** as discussed in section (6).

Following completion of this 3 phase implementation plan, the Georgian Government and enterprises will need to continuously review and upgrade cybersecurity on an annual self-regulatory audit cycle. Just as a physical army needs to be continuously trained and resourced with the latest weapons, so the cyber operations, defences & security staff need to receive regular training & the systems upgraded.

In view of Georgia's strategic & geo-political & economic position, I would strongly recommended that the Government, National Institutions, Utilities & Major Enterprises place top priority upon the full deployment of integrated cyber & physical security within their Multi-year investment plans.

- -

Personal Thanks: I would like to personally thank all my friends and colleagues in Georgia that have contributed their ideas, and motivated me to work on this White Paper on Integrated CyberSecurity..

- -