



21stC Georgia – “*Cyber Vardzia*”

“Integrated Cyber & Physical Security”

for e-Government & e-Georgia

Dr David E. Probert
VAZA International

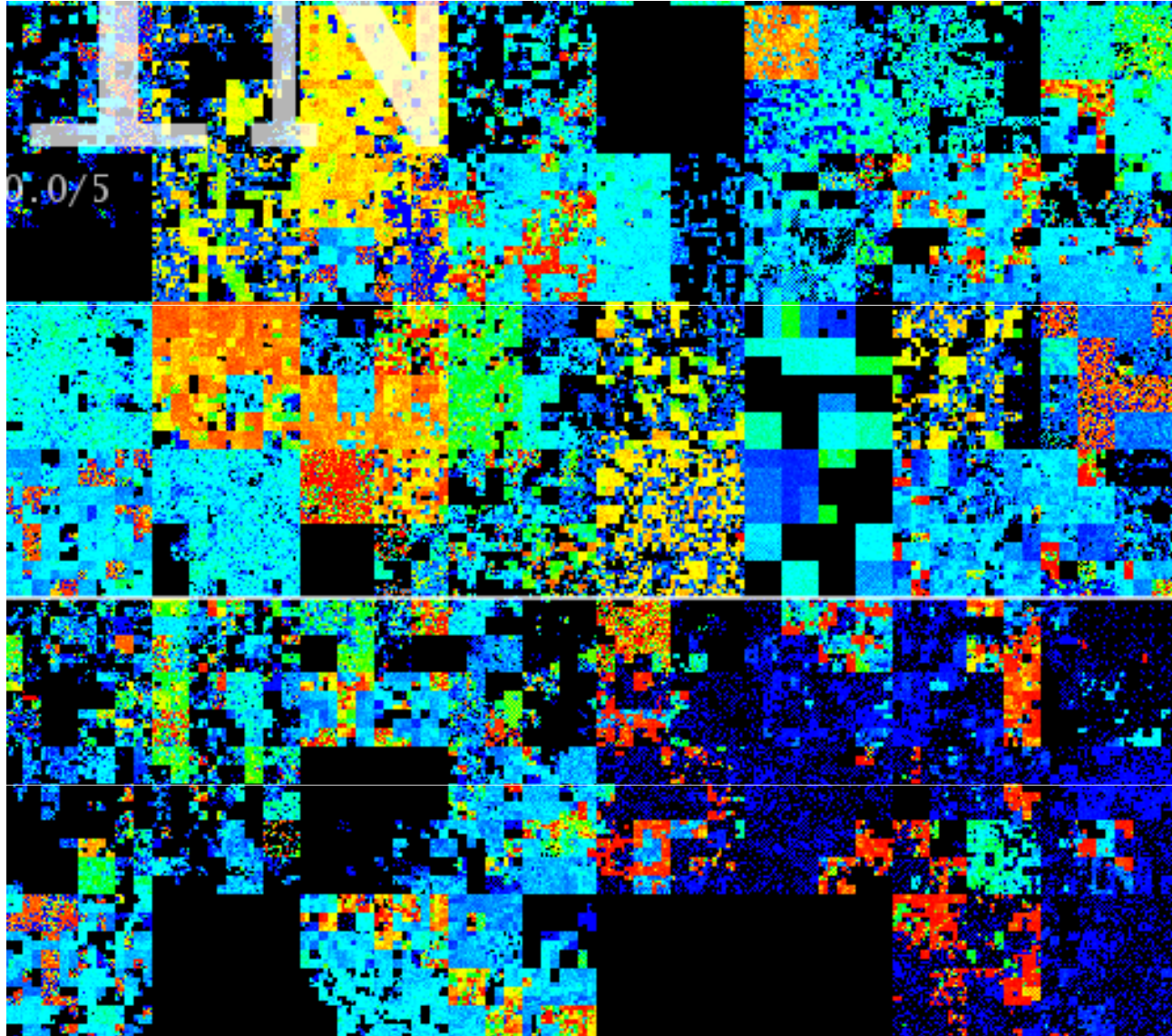


... 21stC Georgia : “*Cyber-Vardzia*” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



...or the Challenging Complexity of Securing Georgian Cyberspace!...



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

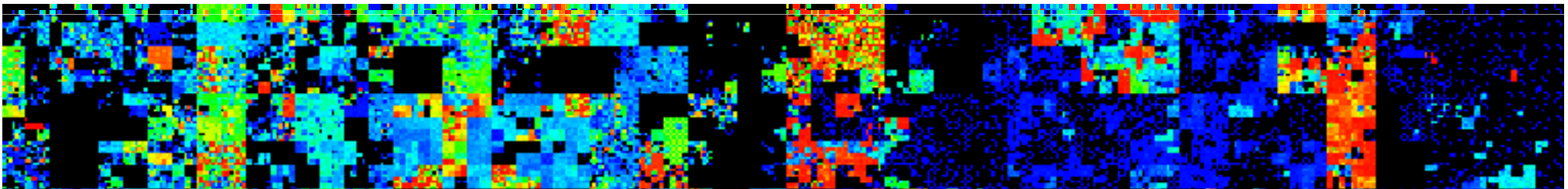
© Dr David E. Probert : www.VAZA.com ©



Integrated Cybersecurity for 21stC Georgia



1 – Background Perspectives	2 – Global Cyber Challenge	3 – Cybersecurity Case Studies
4 – From 20thC to 21stC Security	5 – 21st C “Cyber-Vardzia”	6 – Critical Service Sectors
7 – Integrated Cyber & Physical	8 – Towards “Neural Society”	9 – Next Steps for Georgia



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Background Perspectives

■ **Project Initiatives: 2007 to 2009:**

- In-Depth Cybersecurity Review of Georgian Parliament – Sept 2007 (EU/TACIS)
- Outline Review of Cybersecurity for Georgian Government & Critical Information Infrastructure (Banking, Telecommunications, ISPs, Education) – Dec 2009 (UN/ITU)

■ **Presentation Context:**

- Presents a summary of the Strategic White Paper on “Integrated Cyber & Physical Security”
- Considers the convergence of cyber & physical security solutions for public & private sector
- Briefly reviews some examples of successfully established national cybersecurity agencies
- Presents the ITU “Global Cybersecurity Agenda” as framework for Georgian Government

■ **Future Proposals: 2010+**

- Recommend that Georgia continues to review both cyber and physical security for ALL its critical information infrastructure, and that these are upgraded to international standards
- Use “*Cyber-Vardzia*” as a conceptual framework to build awareness of cybersecurity, and to begin the development of a cybersecurity culture within government, business & citizens



... 21stC Georgia : “*Cyber-Vardzia*” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

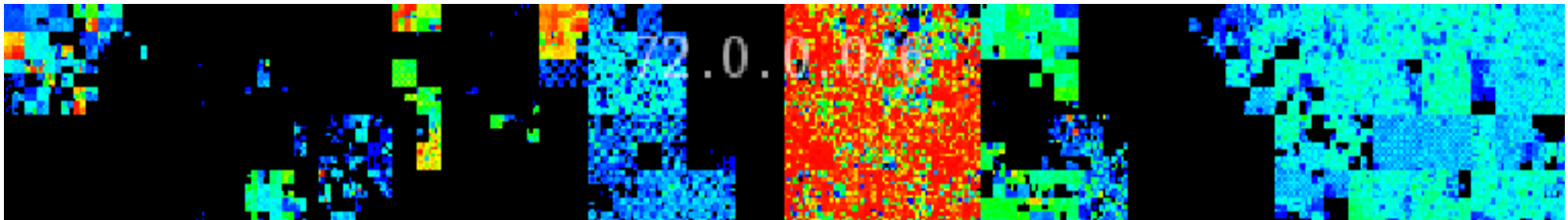
© Dr David E. Probert : www.VAZA.com ©



Integrated CyberSecurity for 21stC Georgia



1 – Background Perspectives	2 – Global Cyber Challenge	3 – Cybersecurity Case Studies
4 – From 20thC to 21stC Security	5 – 21st C “Cyber-Vardzia”	6 – Critical Service Sectors
7 – Integrated Cyber & Physical	8 – Towards “Neural Society”	9 – Next Steps for Georgia



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Cyber Threat Challenges for *Georgia*

- 1) DDoS Denial of Service "Botnet" Attacks
- 2) Phishing Scams such as Advance Fee & Lottery Scams
- 3) Spam eMail with malicious intent
- 4) SQL Database Injection
- 5) XSS Cross-Scripting Java Script Attacks
- 6) Personal Identity Theft (ID Theft)
- 7) Malware, Spyware, Worms, Viruses & Trojans
- 8) Embedded *Sleeping* Software "Zombie Bots"
- 9) Buffer Overflow Attacks
- 10) Firewall Port Scanners
- 11) Social Networking "Malware Apps"
- 12) Wi-Fi, Bluetooth & Mobile Network Intrusion
- 13) Keyloggers – Hardware and Software Variants

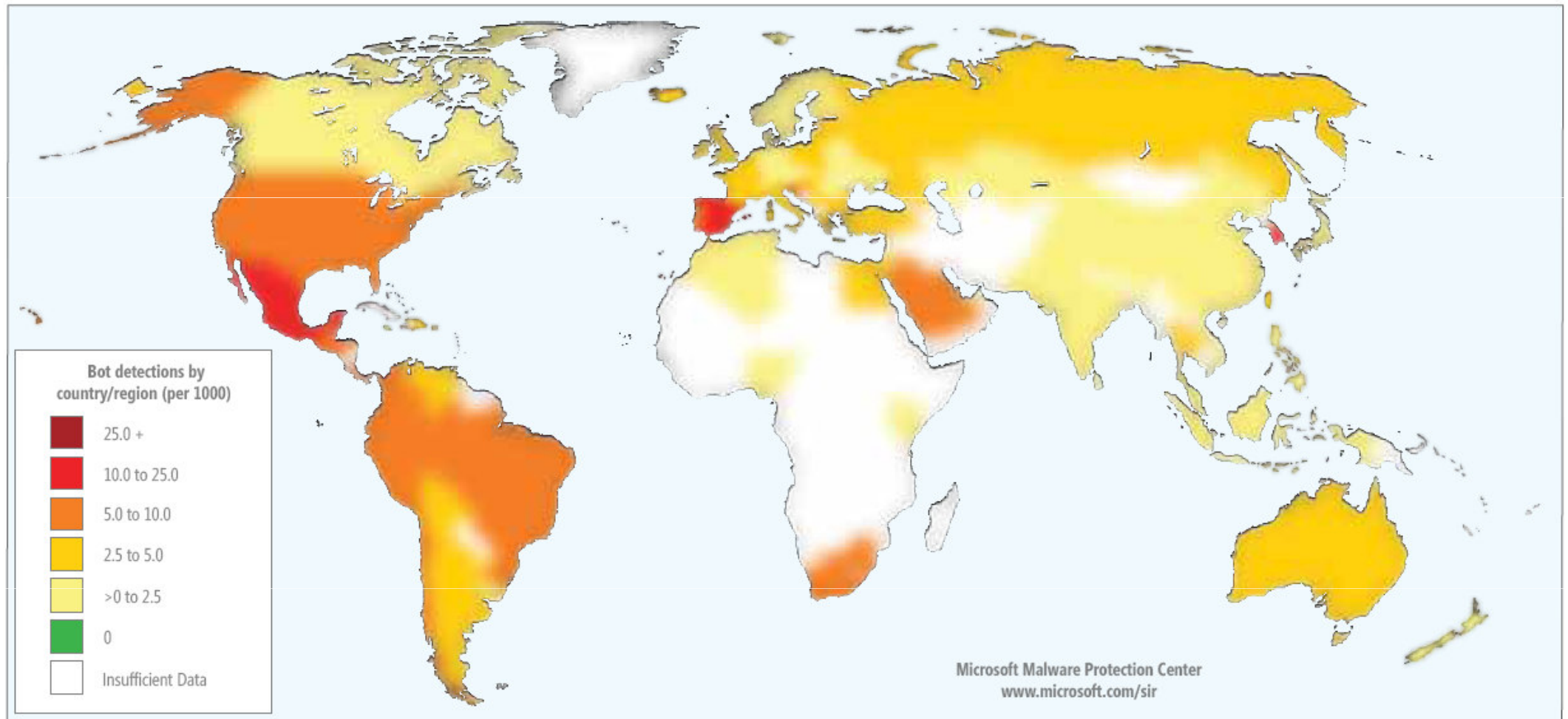


... 21stC Georgia : "*Cyber-Vardzia*" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Worldwide “Bot” Infections: 2Q 2010



Source: Microsoft – Security Intelligence Report - 2010



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Worldwide Security in Cyberspace!

- (4) - Capacity Building

- (1) -
Legal Measures

- (2) -
**Technical
&
Procedural
Measures**

- (3) -
**Organisational
Structures**

- (5) - Regional and International Collaboration



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©




Latin America & Caribbean: CITELE/OAS

Regional ITU-CITEL Cybersecurity Workshop – 1st November 2010 – Argentina

- Within Latin America & Caribbean, CITEL and the OAS are working together on Regional Cybersecurity Strategy & Plans with ITU support:
- CITEL = Inter-American Telecomms Commission
- OAS = Organisation of American States



Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

 [Antigua and Barbuda](#)

 [Costa Rica](#)

 [Haiti](#)

 [Saint Lucia](#)

 [Argentina](#)

 [Cuba](#)¹

 [Honduras](#)²

 [Saint Vincent and the Grenadines](#)

 [Barbados](#)

 [Dominica](#)
(Commonwealth of)

 [Jamaica](#)

 [Suriname](#)

 [Belize](#)

 [Dominican Republic](#)

 [Mexico](#)

 [The Bahamas](#)
(Commonwealth of)

 [Bolivia](#)

 [Ecuador](#)

 [Nicaragua](#)

 [Trinidad and Tobago](#)

 [Brazil](#)

 [El Salvador](#)

 [Panama](#)

 [United States of America](#)

 [Canada](#)

 [Grenada](#)

 [Paraguay](#)

 [Uruguay](#)

 [Chile](#)

 [Guatemala](#)

 [Peru](#)

 [Venezuela \(Bolivarian Republic of\)](#)

 [Colombia](#)

 [Guyana](#)

 [Saint Kitts and Nevis](#)



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



ITU: Cybersecurity Workshop – Jamaica - Sept 2010



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

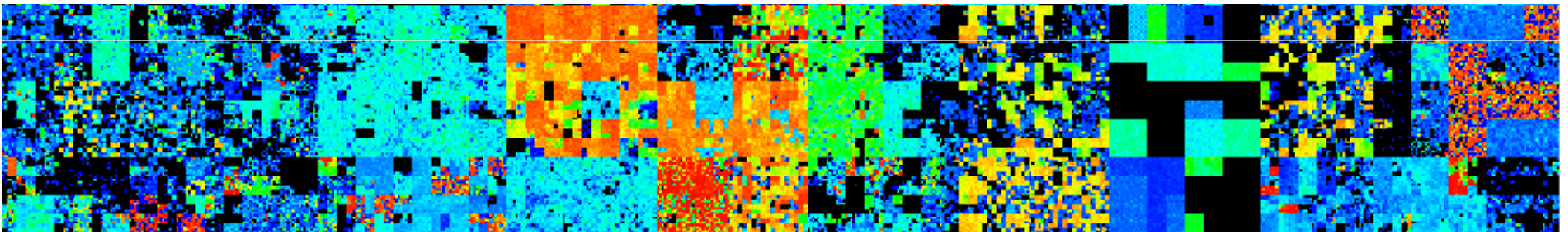
© Dr David E. Probert : www.VAZA.com ©



Integrated CyberSecurity for 21stC Georgia



1 – Background Perspectives	2 – Global Cyber Challenge	3 – Cybersecurity Case Studies
4 – From 20 th C to 21 st C Security	5 – 21 st C “Cyber-Vardzia”	6 – Critical Service Sectors
7 – Integrated Cyber & Physical	8 – Towards “Neural Society”	9 – Next Steps for Georgia



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



National Cybersecurity Case Studies

- **UK Government:** Cybersecurity Strategy for the UK – Safety, Security & Resilience in Cyberspace (UK Office of Cybersecurity – June 2009)
- **US Government:** Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure – May 2009
- **Canada:** Canadian Cyber Incident Response Centre (CCIRC) – Integrated within the Strategic Government Operations Centre (GOC)
- **Australia:** Australian Cybersecurity Policy and Co-ordination Committee (CSPC – Nov 2009), within the Attorney-General’s Government Dept
- **Malaysia:** “Cybersecurity Malaysia” – Mosti : Ministry of Science, Technology & Innovation, and includes the MyCERT & Training Centre
- **Singapore:** Cybersecurity Awareness Alliance & the IDA Security Masterplan (Sept 2009) -Singapore Infocomm Technology Security Authority - SITSA
- **South Korea:** Korea Internet and Security Agency (KISA – July 2009)
- **Latin America :** CITEL/OAS has developed regional cybersecurity strategy
- **European Union:** ENISA – European Network and Information Security Agency (September 2005) tackles all aspects of cybersecurity & cybercrime for the countries of the European Union and beyond



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



US Government : Office of CyberSecurity (CS&C)

- Following the June 2009, US Government Policy Review, the Department of Homeland Security (DHS) has responsibility for hosting the *"Office of Cybersecurity and Communications" (CS&C)*. Within this large organisation is the *"National Cyber Security Division" (NCSD)*:

- *National Cyberspace Response System*

- National Cyber Alert System
- US-CERT Operations
- National Cyber Response Co-ordination Group
- Cyber Cop Portal (for investigation and prosecution of cyber attacks)

- *Federal Network Security*

- Ensuring the maximum security of executive civilian departments and agencies

- *Cyber-Risk Management Programs*

- Cyber Exercises: Cyber Storm
- National Outreach Awareness
- Software Assurance Program



....The US Government DHS also has a National Cyber Security Center (NCSC) which is tasked with the protection of the US Government's Communications Networks



... 21stC Georgia : *"Cyber-Vardzia"* ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Canadian Government : CCIRC

- The Canadian Cyber Incident Response Centre (CCIRC) monitors the cyber threat environment around the clock and is responsible for coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents. The Centre is a part of the [Government Operations Centre](#) and a key component of the government's all-hazards approach to national security and emergency preparedness.



- CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analytical releases, as well as a variety of information products and services specifically for IT professionals and managers of [critical infrastructure](#) and other related industries.



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©

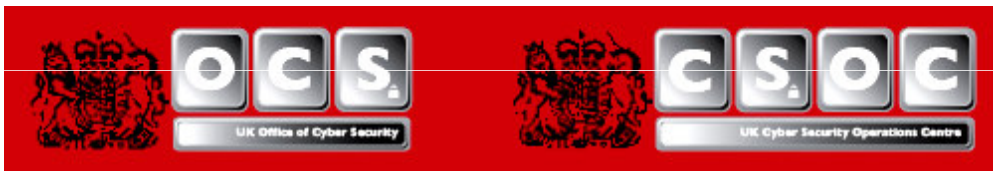


UK Office of Cybersecurity – OCS & CSOC



Cyber Security Strategy of the United Kingdom

safety, security and resilience in cyber space



To address the UK's cyber security challenges, the Government will:

- **Establish a cross-government programme**, with additional funding to address the following priority areas in pursuit of the UK's strategic cyber security objectives:
 - Safe Secure & Resilient Systems
 - Policy, Doctrine, Legal & Regulatory issues
 - Awareness & Culture Change
 - Skills & Education
 - Technical Capabilities & Research and Development
 - Exploitation
 - International Engagement
 - Governance, Roles & Responsibilities
- **Work closely with** the wider public sector, industry, civil liberties groups, the public and with international **partners**;
- **Set up an Office of Cyber Security (OCS)** to provide strategic leadership for and coherence across Government;
- **Create a Cyber Security Operations Centre (CSOC)** to:
 - actively monitor the health of cyber space and co-ordinate incident response;
 - enable better understanding of attacks against UK networks and users;
 - provide better advice and information about the risk to business and the public.



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Australian Government : CSPC

- The **Cyber Security Policy and Coordination (CSPC) Committee** is the Australian Government committee that coordinates the development of cyber security policy for the Australian Government. The CSPC Committee:
 - Provides whole of government strategic leadership on cyber security
 - Determines priorities for the Australian Government
 - Coordinates the response to cyber security events
 - Coordinates Australian Government cyber security policy internationally.



Cyber Security Operations Centre (CSOC)



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Malaysian Government: MOSTi



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Singapore Government : SITSA



The screenshot shows the Singapore Government website with the SITSA announcement. The header includes the Singapore Government logo and navigation links. The left sidebar lists various categories like News, Events, and Publications. The main content area features a 'Press Releases' section dated 30 September 2009, titled '1 October 2009: Singapore Infocomm Technology Security Authority Set Up to Safeguard Singapore against IT Security Threats'. The text describes the establishment of SITSA on 1 Oct 2009 to safeguard Singapore against infocomm technology (IT) security threats. It outlines SITSA's mission to secure Singapore's IT environment, especially vis-à-vis external threats to national security such as cyber-terrorism and cyber-espionage. The announcement is divided into four numbered points detailing SITSA's responsibilities, the role of the National Infocomm Security Committee (NISC), and SITSA's areas of focus, including IT Security Consultancy, Partnership Development, Critical Infocomm Infrastructure Protection, Technology Development, and Singapore's planning and preparedness against major external cyber attacks.

1 October 2009: Singapore Infocomm Technology Security Authority Set Up to Safeguard Singapore against IT Security Threats

SITSA Singapore Infocomm Technology Security Authority (SITSA) will be set up on 1 Oct 2009 to safeguard Singapore against infocomm technology (IT) security threats. SITSA will be the national specialist authority overseeing operational IT security. SITSA's mission is to secure Singapore's IT environment, especially vis-à-vis external threats to national security such as cyber-terrorism and cyber-espionage.

2 SITSA will be responsible for operational IT security development and implementation at the national level. Regulatory agencies will continue to be responsible for IT security-related implementation for their sectors in coordination with SITSA. In the case of the Government and Infocomm sectors, this responsibility will continue to rest with Infocomm Development Authority of Singapore (IDA) in its capacity as the Government Chief Information Office (GCIO) and the government agency responsible for the Infocomm sector. Similarly, other regulatory agencies will continue to be responsible for IT security in their respective sectors.

3 The National Infocomm Security Committee (NISC) will remain as the national platform to formulate IT security policies and set strategic directions at the national level. IDA will continue to serve as secretariat to the NISC and also to promote Singapore as a secure and trusted hub.

4 SITSA will be a division within the Internal Security Department (ISD) of the Ministry of Home Affairs. SITSA's areas of focus will include:

- IT Security Consultancy for strategic Government projects that have national security impact
- Partnership Development to build relationships with key entities strategic to enhancing Singapore's IT security
- Critical Infocomm Infrastructure Protection to systematically harden the CIs in nationally critical sectors
- Technology Development to develop and maintain SITSA's technical competencies and to provide insights on developments in IT security and threats
- Singapore's planning and preparedness, and response, against any major external cyber attack

SITSA's initiatives to harden critical national IT infrastructure and raise national preparedness against external cyber attacks



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
 *** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



South Korea Government: KISA



Font Size + ■ - | [HOME](#) | [CONTACT US](#) | [KOREAN](#)

Greetings | Organization | Location | Main Activities

KISA = “Korean Internet & Security Agency”

Organization

Organization >

Organization



```

graph TD
    President[President] --> SPO[Strategic Planning Head Office]
    President --> ICC[International Cooperation Center]
    President --> ICPO[Internet Convergence & Policy Head Office]
    President --> IPIH[Internet Promotion & Information Security Head Office]
    President --> KISC[Korea Internet Security Center KrCERT]

    SPO --> PCT[Planning & Coordination Team]
    SPO --> MST[Management Strategy Team]
    SPO --> PRT[Public Relations Team]

    ICC --> ICP[International Cooperation Planning Team]
    ICC --> IOT[International Organization Team]
    ICC --> IGC[Intergovernmental Cooperation Team]
    ICC --> GBT[Global Business Team]

    ICPO --> ISPD[Internet & Security Policy Division]
    ICPO --> ICD[Internet Convergence Division]
    ICPO --> MED[Management & Education Division]

    IPIH --> IPD[Internet Promotion Division]
    IPIH --> IPIPD[Internet Infra & Personal Information Protection Division]
    IPIH --> PSD[Public Security Division]

    KISC --> IIR[Internet Incidents Response Division]
    KISC --> IIPD[Internet Incidents Prevention Division]
          
```

• Spam Response Team
 • Web Security Team
 • PC Security Team

• Network Monitoring Team
 • Hacking Response Team
 • Code Analysis Team
 • Response & Security Planning Team

• Knowledge & Information Security Industry Team
 • Electronic Signature & Authentication Team
 • Security Evaluation Team
 • Public Security Service Team
 • Public Security Planning Team

• Internet User Right Protection Team
 • Internet Service Protection Team
 • Enterprise Information Security Management Team
 • Personal Information Protection Technology Team
 • Personal Information Protection Planning Team

• System Management Team (KRNIC)
 • Internet Name Policy Team (KRNIC)
 • IP Policy & Management Team (KRNIC)
 • Internet Ethics Team
 • Internet Planning Team

• KISA Academy Team
 • General Administration Team
 • Human Resource Management Team

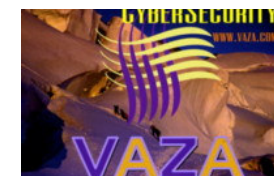
• Convergence Security R&D Team
 • Wireless Internet Team
 • New Business Contents Team
 • Future Internet Team

• Legal Research Team
 • Research & Analysis Team
 • Policy Development Team

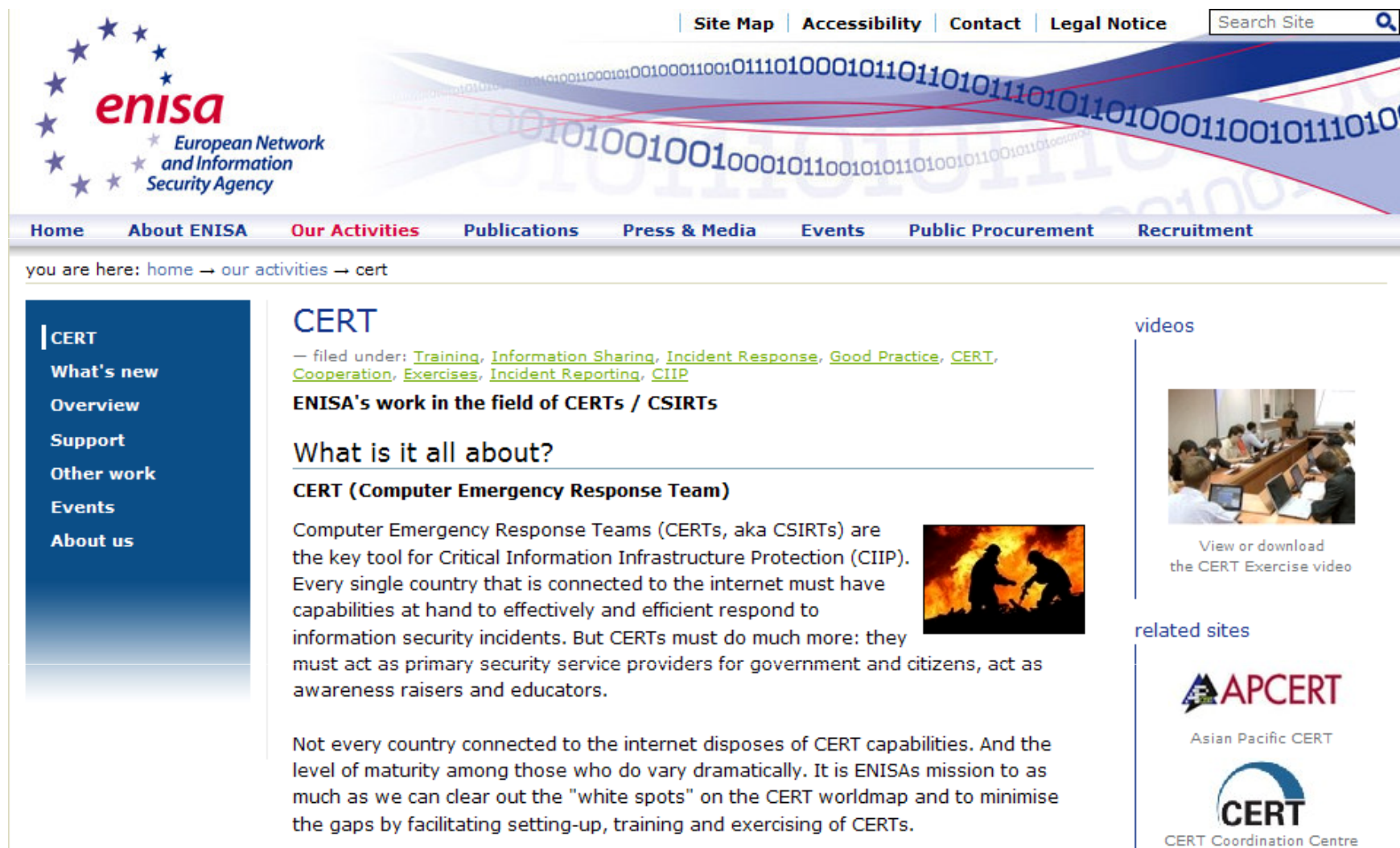


... 21stC Georgia : “Cyber-Vardzia” ...
 Integrated Cyber & Physical Security for e-Government & e-Georgia
 *** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***




© Dr David E. Probert : www.VAZA.com ©



European Network and Information Security Agency: ENISA



The screenshot shows the ENISA website with the following elements:

- Header:** ENISA logo (European Network and Information Security Agency) and navigation links: Site Map, Accessibility, Contact, Legal Notice, Search Site.
- Menu:** Home, About ENISA, Our Activities (highlighted), Publications, Press & Media, Events, Public Procurement, Recruitment.
- Breadcrumb:** you are here: home → our activities → cert
- Left Sidebar:** CERT, What's new, Overview, Support, Other work, Events, About us.
- Main Content:**
 - CERT**
 - filed under: [Training](#), [Information Sharing](#), [Incident Response](#), [Good Practice](#), [CERT](#), [Cooperation](#), [Exercises](#), [Incident Reporting](#), [CIIP](#)
 - ENISA's work in the field of CERTs / CSIRTs**
 - What is it all about?**
 - CERT (Computer Emergency Response Team)**
 - Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the internet must have capabilities at hand to effectively and efficient respond to information security incidents. But CERTs must do much more: they must act as primary security service providers for government and citizens, act as awareness raisers and educators.
 - Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is ENISA's mission to as much as we can clear out the "white spots" on the CERT worldmap and to minimise the gaps by facilitating setting-up, training and exercising of CERTs.
- Right Sidebar:**
 - videos**
 - 
 - View or download the CERT Exercise video
 - related sites**
 - 
Asian Pacific CERT
 - 
CERT Coordination Centre



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



National Cybersecurity Agencies: Common Roles

- Common roles and responsibilities for all these national cyber agencies:
 - **Cyber Alerts:** Management of the National Response to Cyber Alerts, and Attacks
 - **Education:** Co-ordination of the National Awareness and Skills Training Programmes
 - **Laws:** Leadership role in the development and approval of new cyber legislation
 - **Cybercrime:** Facilitation for building a National Cybercrime or e-Crime Unit
 - **Standards:** Setting the national cybersecurity standards and auditing compliance
 - **International:** Leadership in the promotion of international partnerships for
 - **Research:** Support for research & development into cybersecurity technologies
 - **Critical Sectors:** Co-ordination of National Programmes for Critical Infrastructure

...Next we consider the benefits from integrated physical and cybersecurity!



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

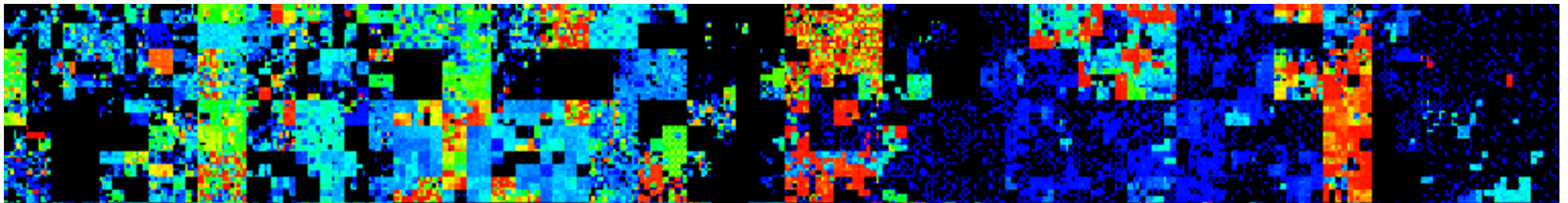
© Dr David E. Probert : www.VAZA.com ©



Integrated CyberSecurity for 21stC Georgia



1 – Background Perspectives	2 – Global Cyber Challenge	3 – Cybersecurity Case Studies
4 – From 20 th C to 21 st C Security	5 – 21 st C “Cyber-Vardzia”	6 – Critical Service Sectors
7 – Integrated Cyber & Physical	8 – Towards “Neural Society”	9 – Next Steps for Georgia



... 21stC Georgia : “Cyber-Vardzia” ...
 Integrated Cyber & Physical Security for e-Government & e-Georgia
 *** GITi – “Georgian IT Innovations”– Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Transition from 20thC to 21stC Security

- **Cybersecurity 2010-2020:**

- Every country in the world will need to transition from the traditional 20thC culture & policy of massive physical defence to the connected “neural” 21stC world of in-depth intelligent & integrated cyber defence solutions

- **Georgia 2010-2015:**

- Georgia has already experienced the weakness in its “cyber defence shield” during the August 2008 conflict. Upgrades will be a 3 to 5 year programme

- **National Boundaries:**

- Traditional physical defence and geographical boundaries are still strategic national assets , but they need to be augmented through integrated cyber defence organisations & assets.

- **Critical National Information Infrastructure:**

- 21stC national economies function electronically, & yet they are poorly defended in cyberspace, and very often open to criminal & political attacks

- **Multi-Dimensional Cyber Defence:**

- Georgia needs to audit its critical infrastructure – government, banks, telecomms, energy, & transport – and upgrade to international cybersecurity standards based upon “best practice” (ISO/IEC & UN/ITU)



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



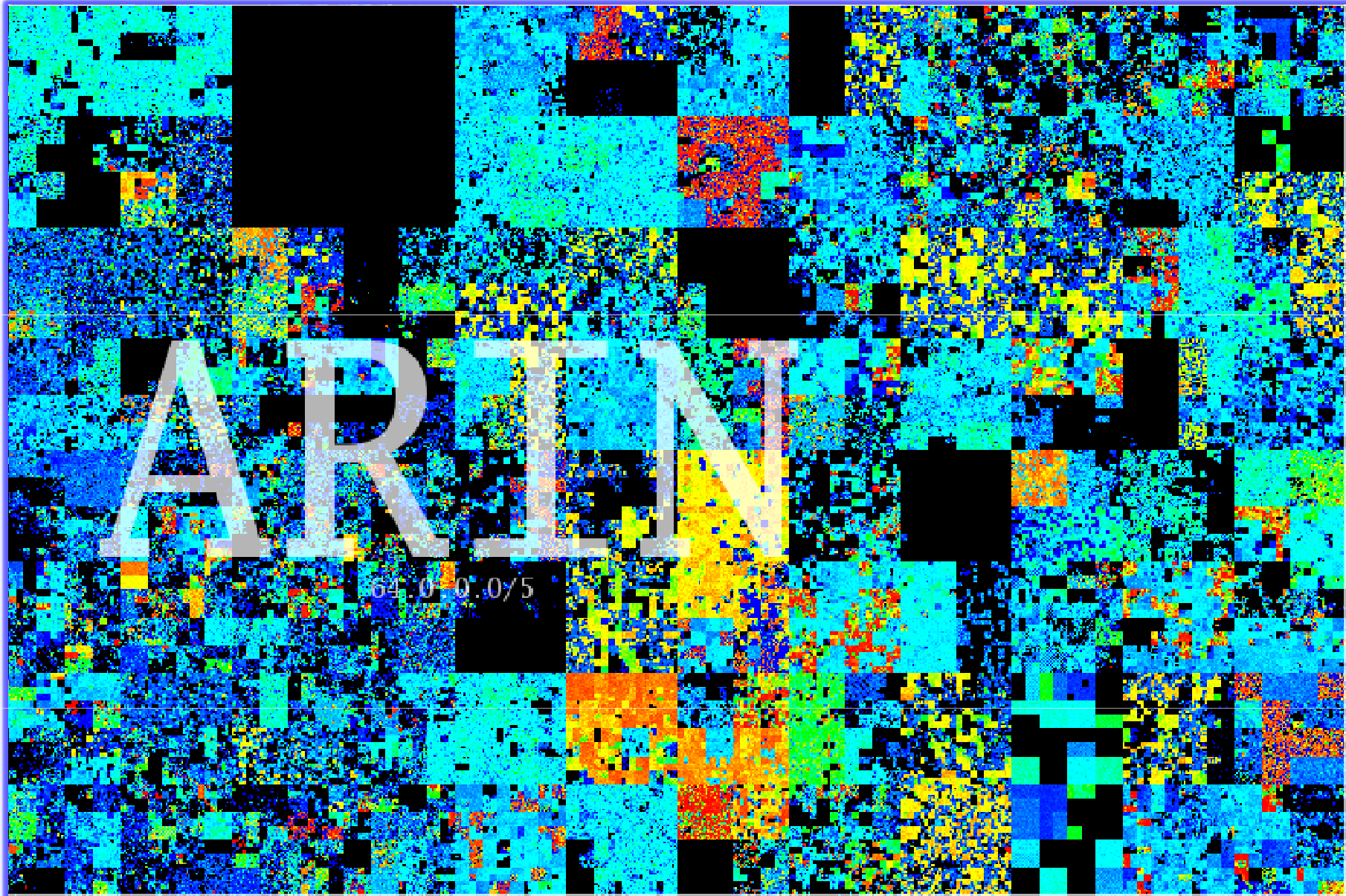


Integrated Cyber & Physical Security for e-Government & e-Georgia

© Dr David E. Probert : www.VAZA.com ©



Active Internet Domains – “American IP Registry”

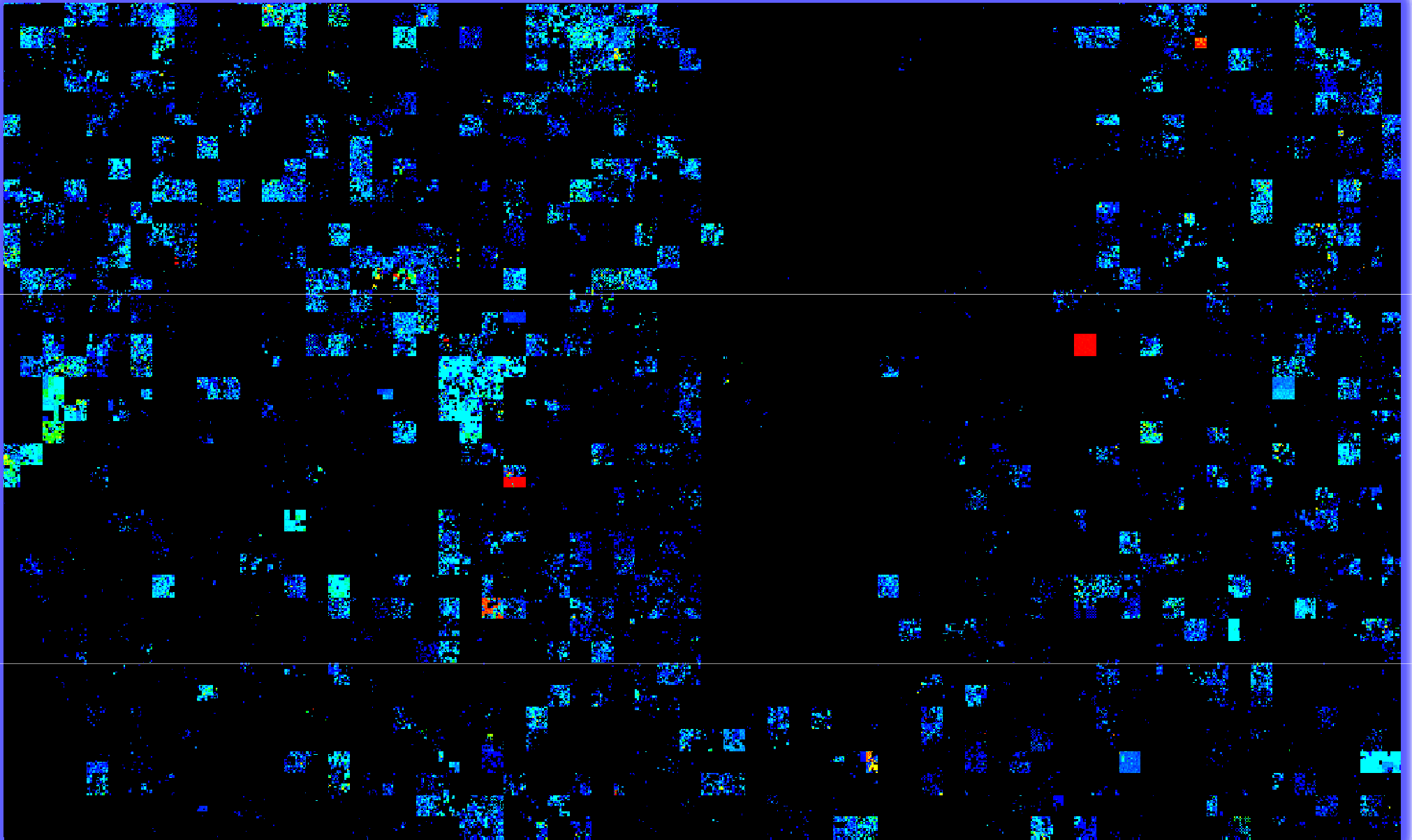


... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



“Outer Galaxies of Cyberspace” – Other Registries

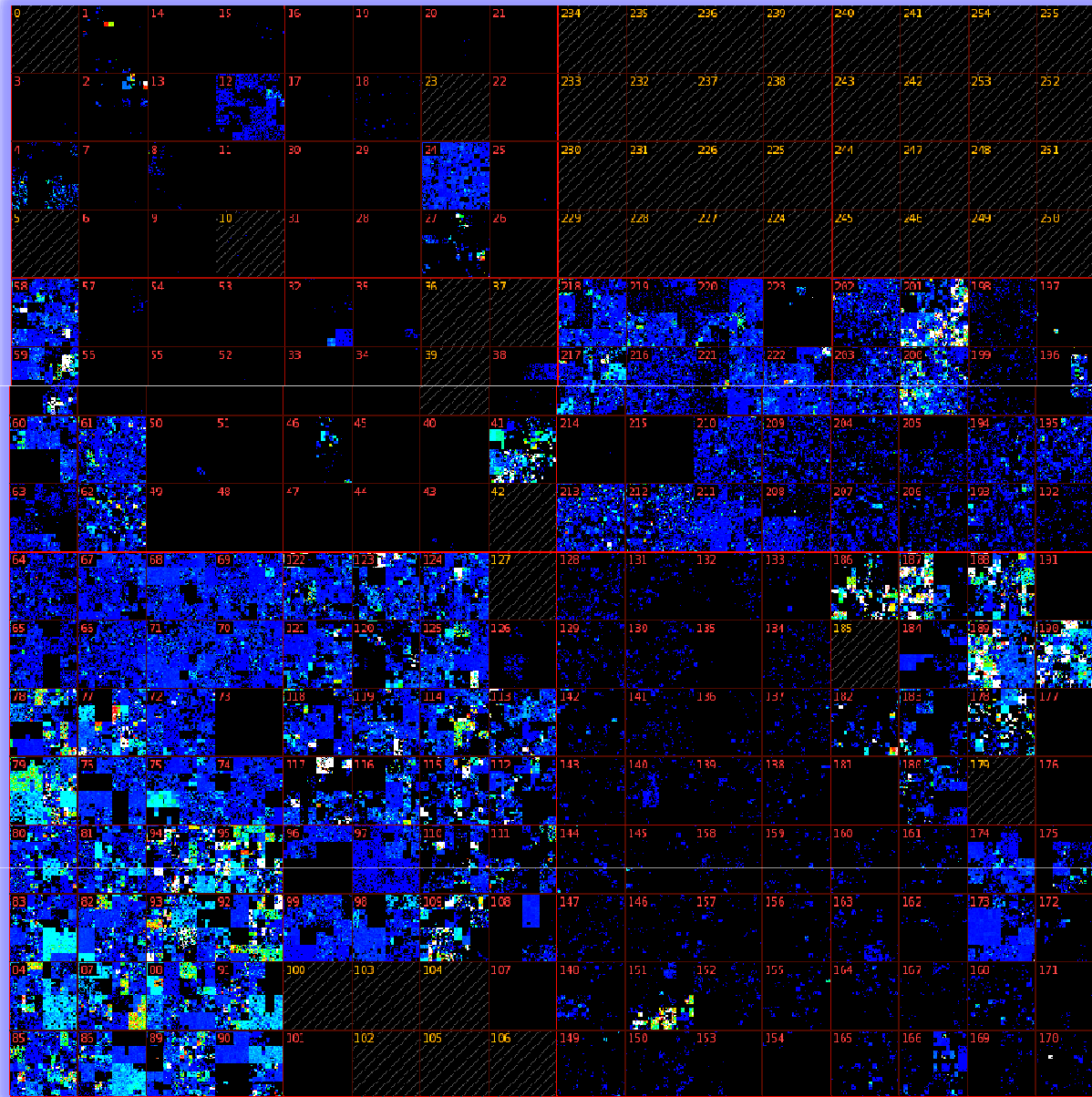


... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

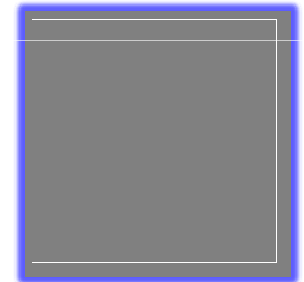
© Dr David E. Probert : www.VAZA.com ©



Malicious Cybercrime Activity in Global Cyberspace



Key: Hilbert
Space-Filling
Curve Process



Link: www.team-cymru.org



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations”– Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



"21st Century Cyber World"

- *Open World:* During the last 15 years we've evolved from the primitive Internet to the complex world of Web2.0 mobile & wireless applications
- *Criminals and Hackers* seek every opportunity to creatively penetrate wired, wireless, mobile devices, and social networking applications
- *The war against cybercriminals* requires us to continuously create new cybersecurity solutions for every conceivable cyberattack
- *Standards, Architectures and Operational Security Policies* all ensure that the "business case for cybercriminals" is much less attractive
- *The DMZ Security Firewalls* of the 1990s are now only a partial solution to the protection of critical information infrastructure

.....*In this presentation we briefly explore the 21st World of Cybersecurity Solutions including their integration with more traditional physical security & surveillance*



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Evolving Cybersecurity for US Defence: “The Pentagon’s Cyberstrategy”



The screenshot shows the top of a web page for the magazine 'FOREIGN AFFAIRS', published by the Council on Foreign Relations. The navigation bar includes links for 'About Us', 'In the Magazine', 'Regions', 'Topics', 'Features' (highlighted in red), 'Discussions', and 'Books & Reviews'. Below the navigation bar, the breadcrumb trail reads 'Home > Features > Essays > Defending a New Domain'. The main title of the article is 'Defending a New Domain', with the subtitle 'The Pentagon's Cyberstrategy'. The author is listed as 'By William J. Lynn III' and the date as 'September/October 2010'. At the bottom of the article header, there are icons for 'PRINT', 'EMAIL', 'SHARE', and 'TEXT' (with minus and plus signs).

Summary: Right now, more than 100 foreign intelligence organizations are trying to hack into the digital networks that undergird U.S. military operations. The Pentagon recognizes the catastrophic threat posed by cyberwarfare, and is partnering with allied governments and private companies to prepare itself.

WILLIAM J. LYNN III is U.S. Deputy Secretary of Defense.

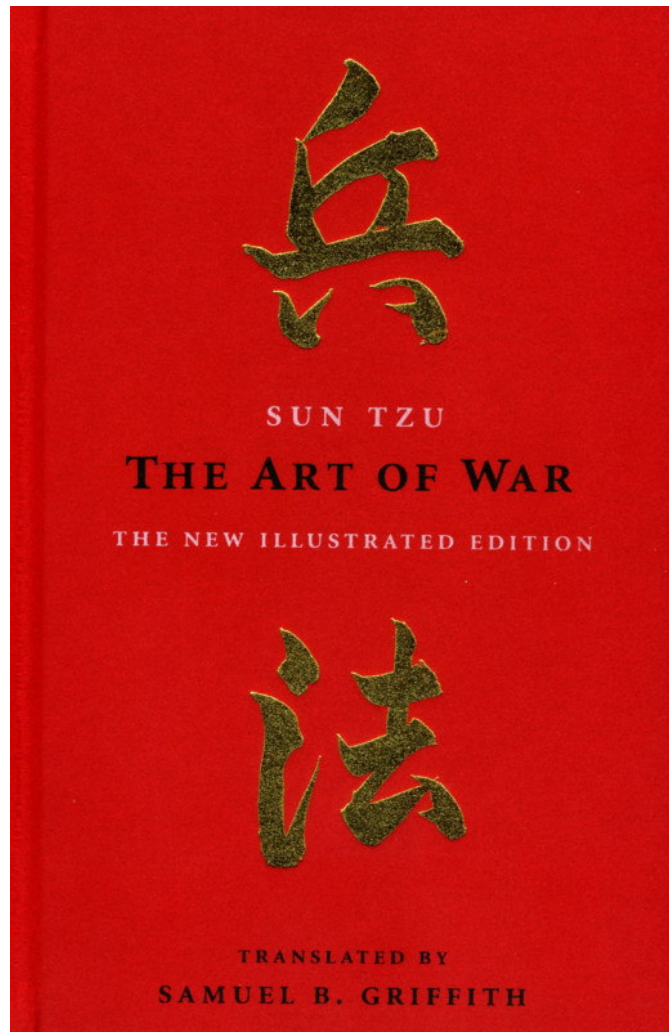


... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

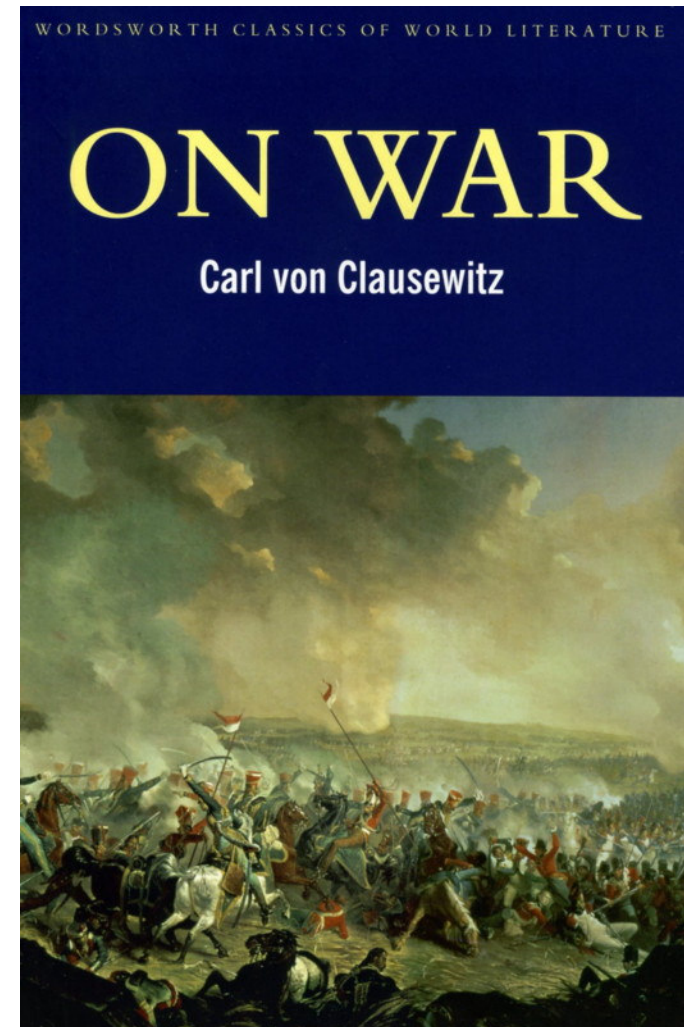
© Dr David E. Probert : www.VAZA.com ©



CyberWar Strategies *from* Classic Works!



Recommended
"Bedtime
Reading"
for
Cybersecurity
Specialists!



...Classic Works on "War" are just as relevant today for Cybersecurity as pre-20th C



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

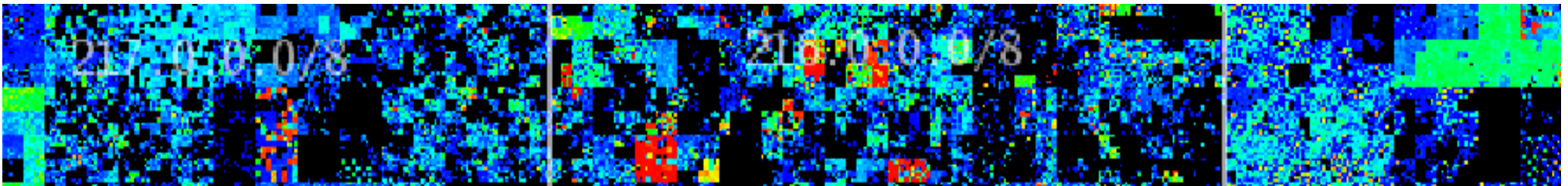
© Dr David E. Probert : www.VAZA.com ©



Integrated CyberSecurity for 21stC Georgia



1 – Background Perspectives	2 – Global Cyber Challenge	3 – Cybersecurity Case Studies
4 – From 20 th C to 21 st C Security	5 – 21st C “Cyber-Vardzia”	6 – Critical Service Sectors
7 – Integrated Cyber & Physical	8 – Towards “Neural Society”	9 – Next Steps for Georgia



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

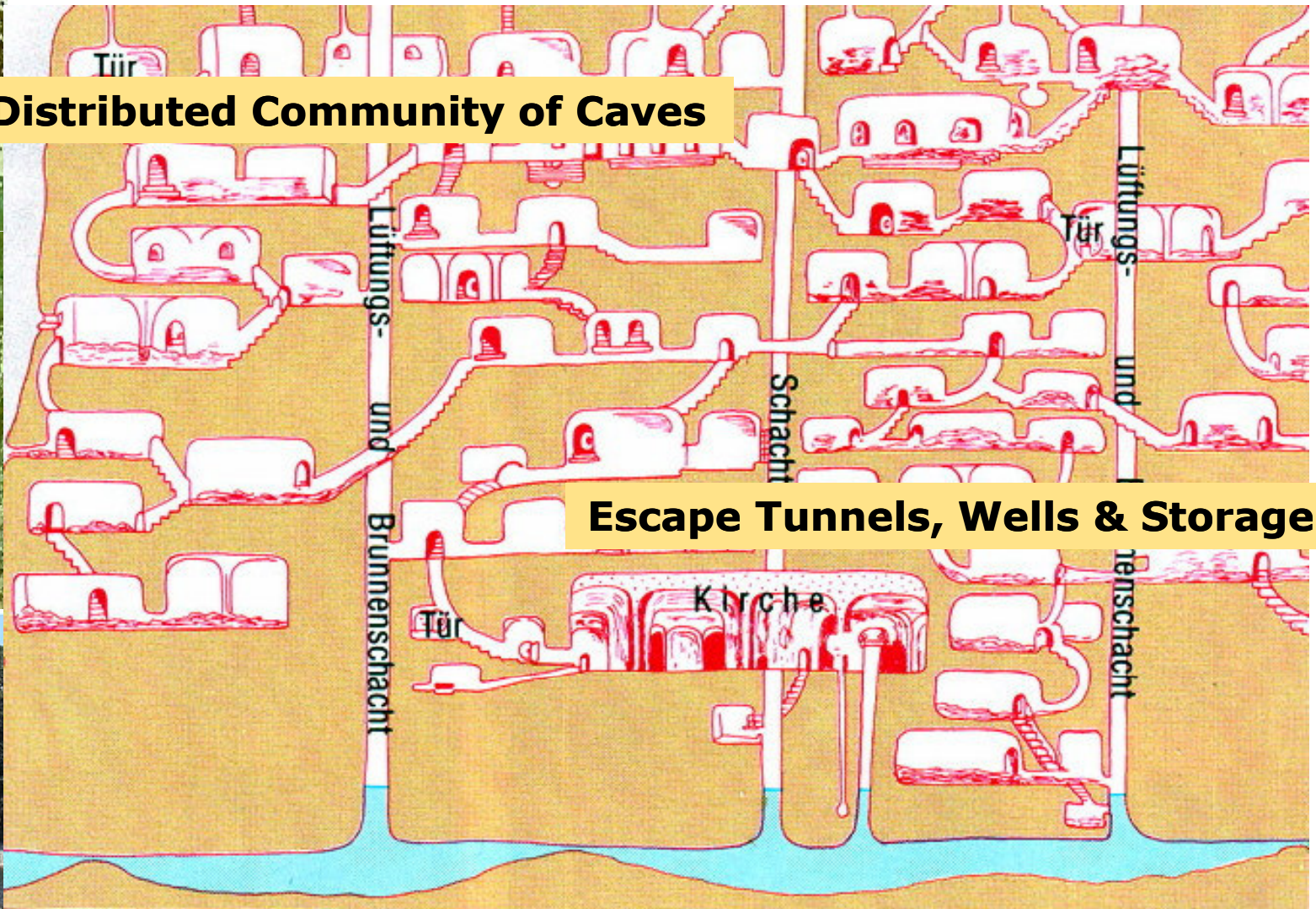
© Dr David E. Probert : www.VAZA.com ©



Vardzia: Secure 12thC Community



Distributed Community of Caves



Escape Tunnels, Wells & Storage



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



"VARDZIA": Architecture for 21stC GEORGIA!

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

Virtual = Virtual world is the World of IP Cyberspace – Globally Virtual & Locally Physical!

Adaptive = 21stC Security solutions need to be deployed with adaptive real-time response.

Distributed = Just as the Ancient Vardzia ვარძია was a distributed cave complex, so 21stC security is built 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 slides that all the physical & cyber security assets and solutions will gradually become smarter with embedded networked intelligence.

Architecture = The integration of cyber & physical security clearly demands an extended architecture. The ITU's innovative Global Cybersecurity Agenda provides a framework spanning cybercrime, cyber legislation, cyber standards & procedures, cyber organizations & partnerships

So, in common with ALL other nations, Georgia will need to upgrade its national defences over the next 3 to 5 years to include cybersecurity within its national security policies & organisation



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

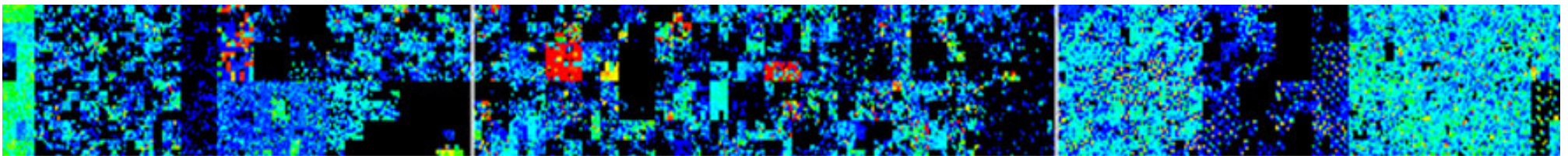
© Dr David E. Probert : www.VAZA.com ©



Integrated CyberSecurity for 21stC Georgia



1 – Background Perspectives	2 – Global Cyber Challenge	3 – Cybersecurity Case Studies
4 – From 20 th C to 21 st C Security	5 – 21 st C “Cyber-Vardzia”	6 – Critical Service Sectors
7 – Integrated Cyber & Physical	8 – Towards “Neural Society”	9 – Next Steps for Georgia

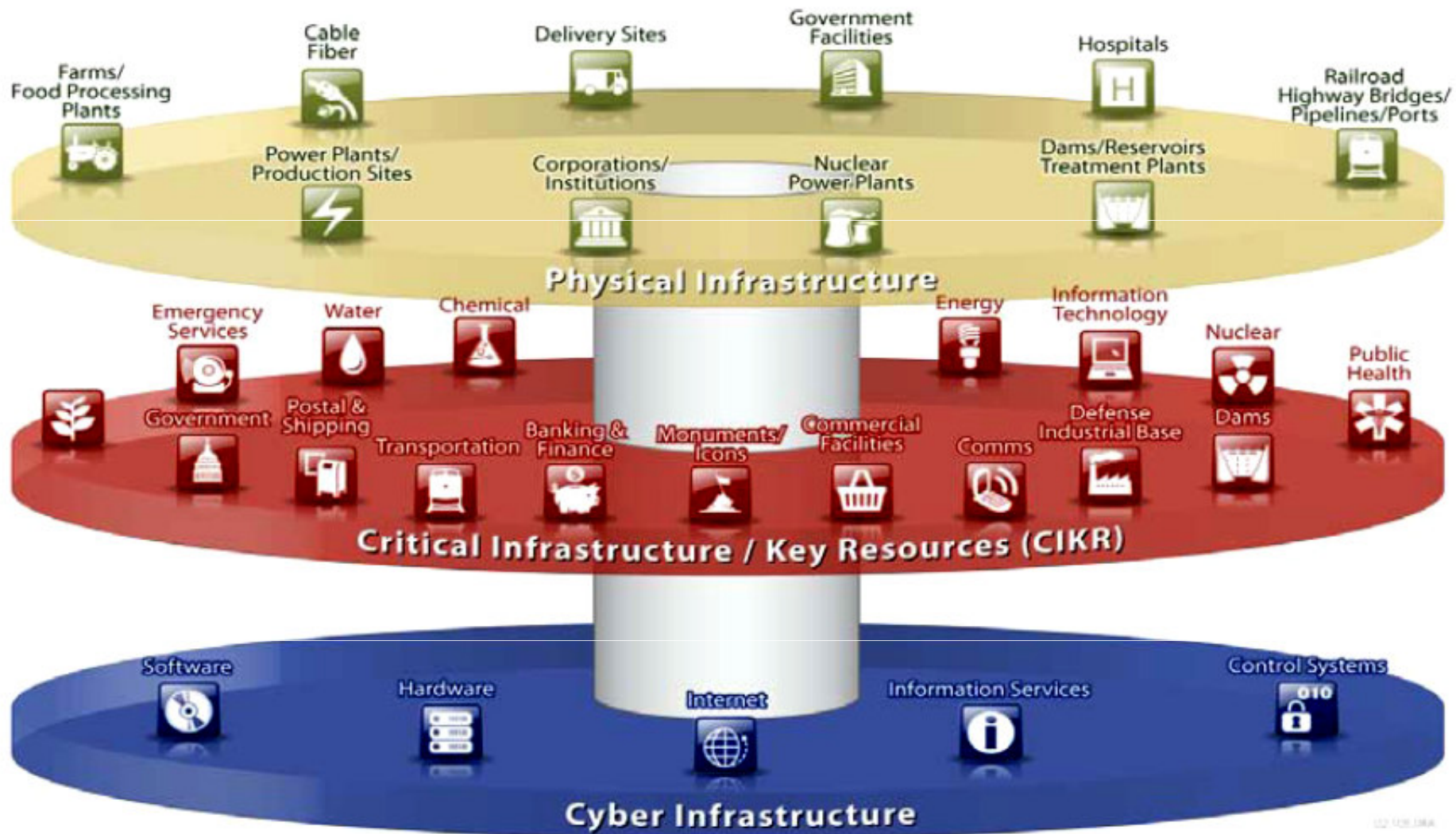


... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations”– Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Critical Sectors and Infrastructure in Cyberspace



Critical Service Sector Infrastructure

- *National Strategies:* Many countries & regions now consider the threat of cyber attacks to be high enough to build national cybersecurity strategies.
- *UK Strategy:* As with physical security & defence, these should be annually updated. For example the UK published its 1st Cybersecurity Strategy (June 2009), and now an updated UK National Security Strategy (Oct 2010).
- *Every Critical Service Sector* should be strategically addressed in-depth:
 - Government (National & Regional)
 - Telecomms/Mobile/ISPs
 - Banking/Financial Services
 - Transportation/Airports/Ports
 - Energy Power Grid & Utilities
 - Healthcare & Emergency Services
 - Police & Law Enforcement Agencies

....The national cybersecurity organisation will include ALL these stakeholders and the CERTs will respond to incidents & communicate cyber alerts across ALL sectors



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Computer Automated Industrial Control & Safety Systems



Case Study: StuxNet Worm - Industrial SCADA Systems



User accesses an infected removable drive; his/her system is then infected by **WORM_STUXNET.A**

Stuxnet Worm : 1st Discovered June 2010



WORM_STUXNET.A drops files onto the *Windows* folder, creates registry entries, and injects codes into processes to stay memory-resident; it also drops **RTKT_STUXNET.A** to hide its malicious routines

WORM_STUXNET.A targets SCADA WinCC systems, which are used to manage industrial operations such as power plants and energy refineries.

It is also interesting to note that it attempts to access sites related to an online football-betting site. Though this does not pose threats, it may be a diversion tactic to confuse security analysts, causing them to fail to immediately realize the worm's main functionalities.



WORM_STUXNET.A drops copies of itself, a .LNK file detected as **LNK_STUXNET.A**, onto all removable drives connected to an affected system, allowing it to propagate

SCADA = Supervisory Control & Data Acquisition
- Mainly for Power Stations & Industrial Plants -

CyberCrimes against Critical Sectors

- *Government:*

- Theft of secret intelligence, manipulation of documents, and illegal access to confidential citizen databases & national records

- *Banking/Finance:*

- Denial of Service attacks against clearing bank network, phishing attacks against bank account & credit cards, money laundering

- *Telecomms/Mobile:*

- Interception of wired & wireless communications, and penetration of secure government & military communications networks

- *Transport/Tourism:*

- Cyber Terrorism against airports, air-traffic control, coach/train transport hubs, & malicious penetration of on-line travel networks

- *Energy/Water:*

- Manipulation and disruption of the national energy grid & utilities through interference of the process control network (SCADA)

...Cybersecurity is a Critical National Issue that now requires a Global Response!



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Sector Case Study: Banks & Finance

- *Banks & Financial* Institutions are prime targets for cybercriminals.
- *Access* to Accounts is usually indirect through phishing scams, infected websites with malicious scripts, and personal ID Theft.
- *On-Line bank transfers* are also commonly used for international money laundering of funds secured from illegal activities
- *Instant Money Transfer Services* are preferred for crimes such as the classic “Advanced Fee Scam” as well as Lottery and Auction Scams
- An increasing problem is *Cyber-Extortion* instigated through phishing
- *National & Commercial Banks* have also been targets of DDOS cyberattacks from politically motivated and terrorist organisations
- *Penetration Scans*: Banks are pivotal to national economies and will receive penetration scans and attempted hacks on a regular basis.
- *On-Line Banking* networks including ATMs, Business and Personal Banking are at the “sharp end” of financial security and require great efforts towards end-user authentication & transaction network security



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Sector Case Study: Governments

- **Cyber Agencies:** Governments such as UK, USA, Malaysia, South Korea and Australia have all implemented cybersecurity agencies & programmes
 - **eGovernment Services** are critically dependant upon strong cybersecurity with authentication for the protection of applications, and citizen data
 - **Compliance Audit:** All Government Ministries & Agencies should receive in-depth ICT security audits, as well as full annual compliance reviews
- 1) National Defence Forces
 - 2) Parliamentary Resources
 - 3) Land Registry & Planning System
 - 4) Citizen IDs and Passports
 - 5) Laws, Legislations, and Policies
 - 6) Civilian Police, Prisons & National e-Crimes Unit (NCU)
 - 7) National CERT – Computer Emergency Response Team
 - 8) Inter-Government Communications Network
 - 9) eServices for Regional & International Partnerships
 - 10) Establishment of cybersecurity standards & compliance
 - 11) Government Security Training and Certification



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Cybersecurity Benefits: Government

- Improved cybersecurity provides significant benefits to the Government & Critical National Service Sectors including:
 - **eGovernment:** Fully secure & cost effective delivery of on-line services to both citizens and businesses, such as taxes & customs, social welfare, civil & land registries, passports & driving licences
 - **eDefence:** Early warning, alerts and defences against cyberattacks through national CERT (Computer Emergency Response Centre)
 - **Cybercrime:** Investigate, Digital Forensics and Prosecution of cybercrimes such ID & Financial Theft, "Computer Misuse, Laundering, On-Line Drug Trafficking & Pornographic Materials
 - **Cyberterrorism:** Ability to assess, predict and prevent potential major cyber terrorist attacks, and to minimise damage during events
 - **Power & Water Utilities:** Prevent malicious damage to control systems
 - **Telecommunications:** Top security of government communications with alternative routings, encryption & protection against cyberattack



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

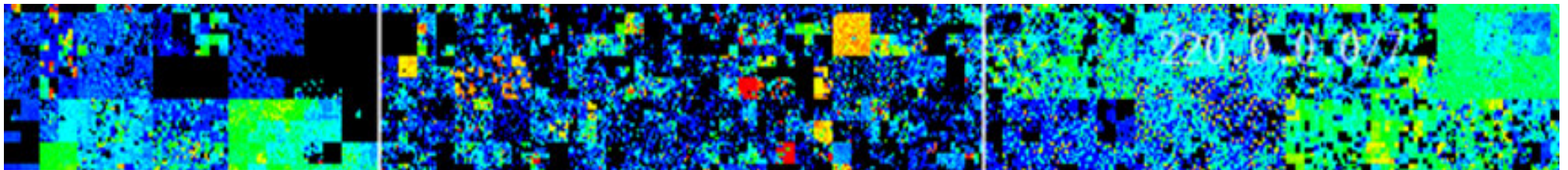
© Dr David E. Probert : www.VAZA.com ©



Integrated CyberSecurity for 21stC Georgia



1 – Background Perspectives	2 – Global Cyber Challenge	3 – Cybersecurity Case Studies
4 – From 20 th C to 21 st C Security	5 – 21 st C “Cyber-Vardzia”	6 – Critical Service Sectors
7 – Integrated Cyber & Physical	8 – Towards “Neural Society”	9 – Next Steps for Georgia



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Traditional “Physical Security” Defences in the context of “Cybersecurity”

- **Compliance:** Investments in establishing and upgrading cybersecurity defences against cybercrime means that all physical security and associated operational staff should also be reviewed for compliance with policies, and audited to international standards
- **Integration:** Physical and Cybersecurity operations should be linked “step-by-step” at the command and control level in the main government or enterprise operations centre.
- **Physical Security** for critical service sectors such as governments, airports, banks, telecommunications, education, energy, healthcare and national defence should be included within the strategy and policies for Cybersecurity and vice versa
- **Upgrades:** In order to maximise security, Government and Businesses need to upgrade and integrate resources & plans for both physical & cybersecurity during the next years.
- **Roadmap:** I’d recommend developing a focused total security action plan and roadmap (Physical & Cyber) for each critical sector within the National Economy & Enterprises



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

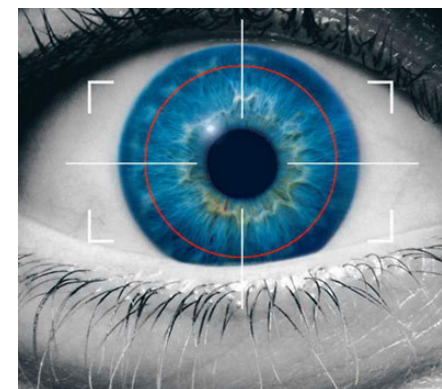
© Dr David E. Probert : www.VAZA.com ©



Biometrics and RFID

- **Biometrics** techniques may include:

- Finger and Palm Prints
- Retinal and Iris Scans
- 3D Vein ID
- Voice Scans & Recognition
- DNA Database – usually for Criminal Records
- 3D Facial Recognition



- **RFID** = Radio Frequency ID with applications that include:

- Personal ID Cards for Building, Facility and Secure Room Access
- Tags for Retail Articles as a deterrence to shop lifting
- Powered RFID Tags for Vehicles to open Barriers, Doors, or switch traffic lights
- Plans to use RFID Tags for Perishable Products such as vegetables and flowers
- Asset Tags to manage the movement of ICT Assets such as Laptops, PDA & Storage

...Biometrics & RFID solutions are powerful tools against cybercrime!

"Cyber to Physical Attacks"

- The illegal penetration of ICT systems may allow criminals to secure information or "make deals" that facilitates their real-world activities:
 - **"Sleeping Cyber Bots"** – These can be secretly implanted by skilled hackers to secure on-line systems, and programmed to explore the directories & databases, and then to transmit certain information – Account & Credit Card Details, Plans, Projects, Deals
 - **Destructive "Cyber Bots"** – If cyber-bots are implanted by terrorist agents within the operational controls of power plants, airports, ports or telecomms facilities then considerable physical damage may result. A simple " *delete *.** " command for the root directories would instantly wipe out all files unless the facility has real-time fail-over!
 - **Distributed Denial of Service Attacks** – These not only block access to system, but in the case of a Banking ATM Network, means that the national ATM network is off-line.
 - **National Cyber Attacks** – Many international organisations such as NATO & US DOD forecast that future regional conflicts will begin with massive cyberattacks to disable their targets' physical critical communications and information infrastructure. Clearly it is important for countries to upgrade their national cybersecurity to minimise such risks



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



"Physical to Cyber Attacks"

- Most "physical to cyber attacks" involve staff, contractors or visitors performing criminal activities in the "misuse of computer assets":
 - **Theft & Modification of ICT Assets:** It is now almost a daily occurrence for critical information & databases to be either deliberately stolen or simply lost on PCs or Chips
 - **Fake Maintenance Staff or Contractors:** A relatively easy way for criminals to access secure facilities, particularly in remote regions or developing countries is to fake their personnel IDs and CVs as being legitimate ICT maintenance staff or contractors
 - **Compromised Operations Staff:** Sometime operational ICT staff may be tempted by criminal bribes, or possibly blackmailed into providing passwords, IDs & Access Codes.
 - **Facility Guests and Visitors:** It is standard procedure for guests & visitors to be accompanied at all times in secure premises. In the absence of such procedures, criminals, masquerading as guests or visitors, may install keylogger hardware devices or possibly extract information, plans and databases to USB memory chips, or steal DVDs!



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Operational Security Solutions

- Securing information and assets in the virtual world of cyberspace requires the discipline of rigorous operational security solutions and policies in the real-world according to accepted ITU & ISO Standards:
 - Integrated Command and Control Operations (including fail-over control rooms)
 - Business Continuity & Disaster Recovery (for cybercrimes, terrorism & natural disasters)
 - Implementation of National, and Enterprise Computer Incident Response Teams (CERTs)
 - Integrated Digital Forensics, eCrime Unit & Cyber Legislation against Cybercrimes
 - Traditional Physical Security Defences & Deterrents (including security guards & fences!)

....Many criminal and terrorist attacks are through penetrating some combination of physical and cybersecurity systems. Breaking into a physical building may allow a criminal to gain secure ICT zones, and thence to on-line user accounts, documents & databases...

...Information can then be downloaded to chips or storage drives & stolen with relative ease...



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Cyber: Integrated Command & Control



- Security Operations Command Centre for Global Security Software Enterprise



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Physical: Integrated CCTV Surveillance



Summary of Physical Security and Operational Solutions

- **IP Networks:** Physical security and the Operational Solutions are increasingly based upon sophisticated electronic networked solutions, including biometrics, smart CCTV, intelligent fences, & RFID Devices
- **Convergence:** Operations for “Physical Security” and “Cybersecurity” will slowly converge & become integrated during the next few years both from staff, assets, resources & operational budget perspectives
- **Benefits:** The benefits of integrating cyber and physical security are reduced running costs, reduced penetration risk, and increased early warning of attacks, whether from criminals, hackers or terrorists.

.....the “Cyber-Vardzia” White Paper discusses cybersecurity and physical security in some depth, as well as their convergence and integration!



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



Integrated Cyber & Physical Security: *"The Shopping List"*

- 1) *National Cybersecurity Agency*: Establishment of a CERT & National Government Cybersecurity Agency within the Government Ministries
- 2) *CIIP*: Long Term Critical Information Infrastructure Protection (CIIP)
- 3) *System Upgrades*: Technical Infrastructure Upgrades including Hardware, Software, Databases, Secure Network Links, Biometrics & RFID
- 4) *Back-Up*: Disaster Recovery, Business Continuity and Back-Up Systems
- 5) *Physical* : Physical Security Applications – CCTV, Alarms, Control Centre
- 6) *Awareness Campaign*: Government Campaign for cybersecurity awareness
- 7) *Training*: National Cybersecurity Skills & Professional Training Programme
- 8) *Encryption*: National User & Systems PKI Authentication Programme
- 9) *Laws*: Costs for Drafting and Enforcing Cyber Laws. Policies & Regulations

.....It is important to develop an in-depth economic "cost-benefit" analysis and Business Case in order to understand the "Return on Investment"

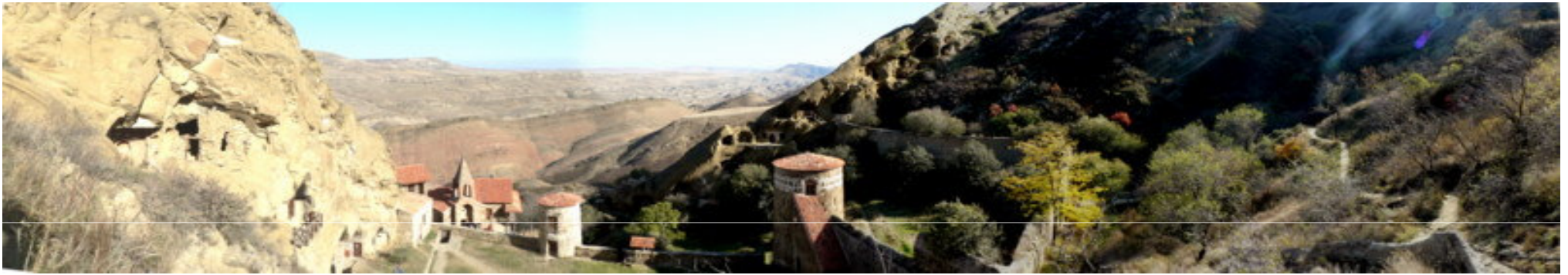


... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

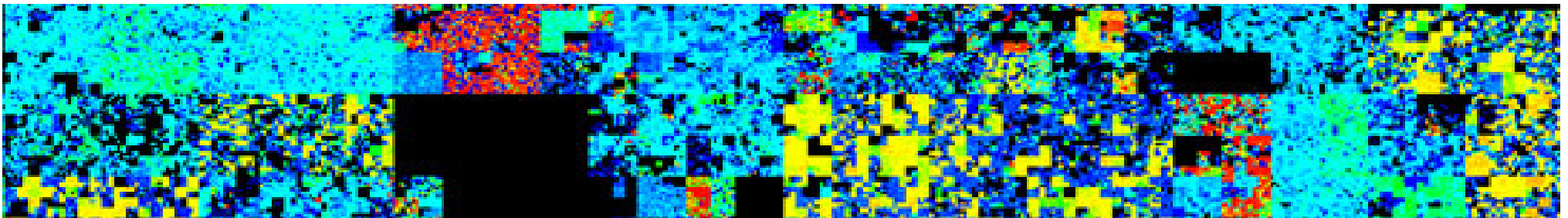
© Dr David E. Probert : www.VAZA.com ©



Integrated CyberSecurity for 21stC Georgia



1 – Background Perspectives	2 – Global Cyber Challenge	3 – Cybersecurity Case Studies
4 – From 20 th C to 21 st C Security	5 – 21 st C “Cyber-Vardzia”	6 – Critical Service Sectors
7 – Integrated Cyber & Physical	8 – Towards “Neural Society”	9 – Next Steps for Georgia



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



The Future: *Towards “Neural Society”*

- ***Real-Time Security Operations:***

- Secure and monitor every cyber asset and critical physical asset through IP Networking, RFID Tagging & communication of status to operations centre

- ***Augmented Reality:***

- Multimedia virtual world overlays on data from the real physical world, through head-up displays & other forms of embedded sensors & displays

- ***BioNeural Metaphors:***

- Further developments of self-organising and autonomous systems for monitoring and responding to cyber alerts & potential attacks in real-time

- ***3D Adaptive Modelling:***

- Adaptive 3D computer modelling of physical buildings, campuses & cities, as well as dynamic models of extended enterprises networks. The aim is to visualise, model & respond to security alerts with greater speed & precision

- ***Hybrid Security Architectures:***

- Effective integrated security requires management through hybrid hierarchical and “peer-to-peer” organisational architectures. Living organic systems also exploit such hybrid architectures for optimal command & control



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

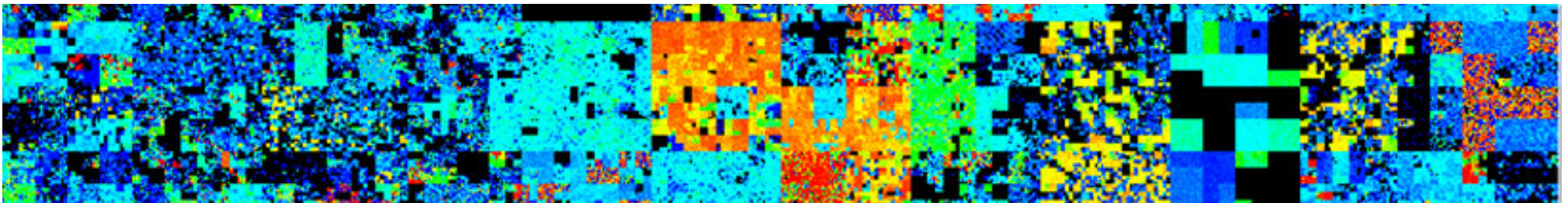
© Dr David E. Probert : www.VAZA.com ©



Integrated CyberSecurity for 21stC Georgia



1 – Background Perspectives	2 – Global Cyber Challenge	3 – Cybersecurity Case Studies
4 – From 20 th C to 21 st C Security	5 – 21 st C “Cyber-Vardzia”	6 – Critical Service Sectors
7 – Integrated Cyber & Physical	8 – Towards “Neural Society”	9 – Next Steps for Georgia



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



White Paper: 21st C Georgia – “Cyber-Vardzia”

* Cyber-Vardzia: Integrated Cyber & Physical Security Systems for 21stC Georgia *

...“21stC Georgia”...



...“Cyber-Vardzia”...

“Integrated Cyber & Physical Security”

*** for ***

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

Author: Dr David E Probert – VAZA International

1 Author: Dr David E. Probert - (c) www.vaza.com - November 2010: V5



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

Download: www.Valentina.net/GITI2010/

* Cyber-Vardzia: Integrated Cyber & Physical Security Systems for 21stC Georgia *

* 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 21st Century!

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.

2 Author: Dr David E. Probert - (c) www.vaza.com - November 2010: V5



Next Steps for e-Georgia: საქართველო: e-Ge

- **Cybersecurity Plans:** Georgia is already engaged in several projects related to the implementation of Cybersecurity both in Government & Critical Enterprises. It is clearly important that these plans are co-ordinated across all stakeholders.
- **e-Government and e-Georgia** are mission critical to Economic Growth, and it is vital the ICT assets are fully secured against cyberattacks and cyberterrorism
- **"Cyber-Vardzia"** White Paper suggests that Georgia reviews & audits the current status of *both* physical and cybersecurity, and that a comprehensive action plan & roadmap are prepared & implemented during the next 3 years.
- **Regional & Global Challenge:** National Georgian Security is also dependant upon the physical & cyber security of the "neighbourhood". Hence the negotiation of regional & international cybersecurity partnerships will be essential to success!

Integrated Security for 21stC Georgia in Cyberspace!



... 21stC Georgia : "Cyber-Vardzia" ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



21stC Georgia : “Cyber–Vardzia”

Georgian IT Innovation Conference – Tbilisi, Georgia

Thank-You!...

White Paper & Slides: www.Valentina.net/GITI2010/



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©



White Paper & Slides: www.Valentina.net/GITI2010/



Thank you for your time!



... 21stC Georgia : *"Cyber-Vardzia"* ...
Integrated Cyber & Physical Security for e-Government & e
*** GITi – "Georgian IT Innovations" – Tbilisi, 10th to 12th November

© Dr David E. Probert : www.VAZA.com ©



International
Telecommunication
Union

Committed to connecting the world

21st C Georgia – “Cyber-Vardzia”

Georgian IT Innovation Conference – Tbilisi, Georgia

BACK-UP SLIDES



... 21stC Georgia : “Cyber-Vardzia” ...
Integrated Cyber & Physical Security for e-Government & e-Georgia
*** GITi – “Georgian IT Innovations” – Tbilisi, 10th to 12th November 2010 ***

© Dr David E. Probert : www.VAZA.com ©

