

"Integrated Cybersecurity & Physical Security for Governments and Business"

Dr David E. Probert
VAZA International

Dedicated to the Memory of Edwin James Williams

30th International East/West Security Conference

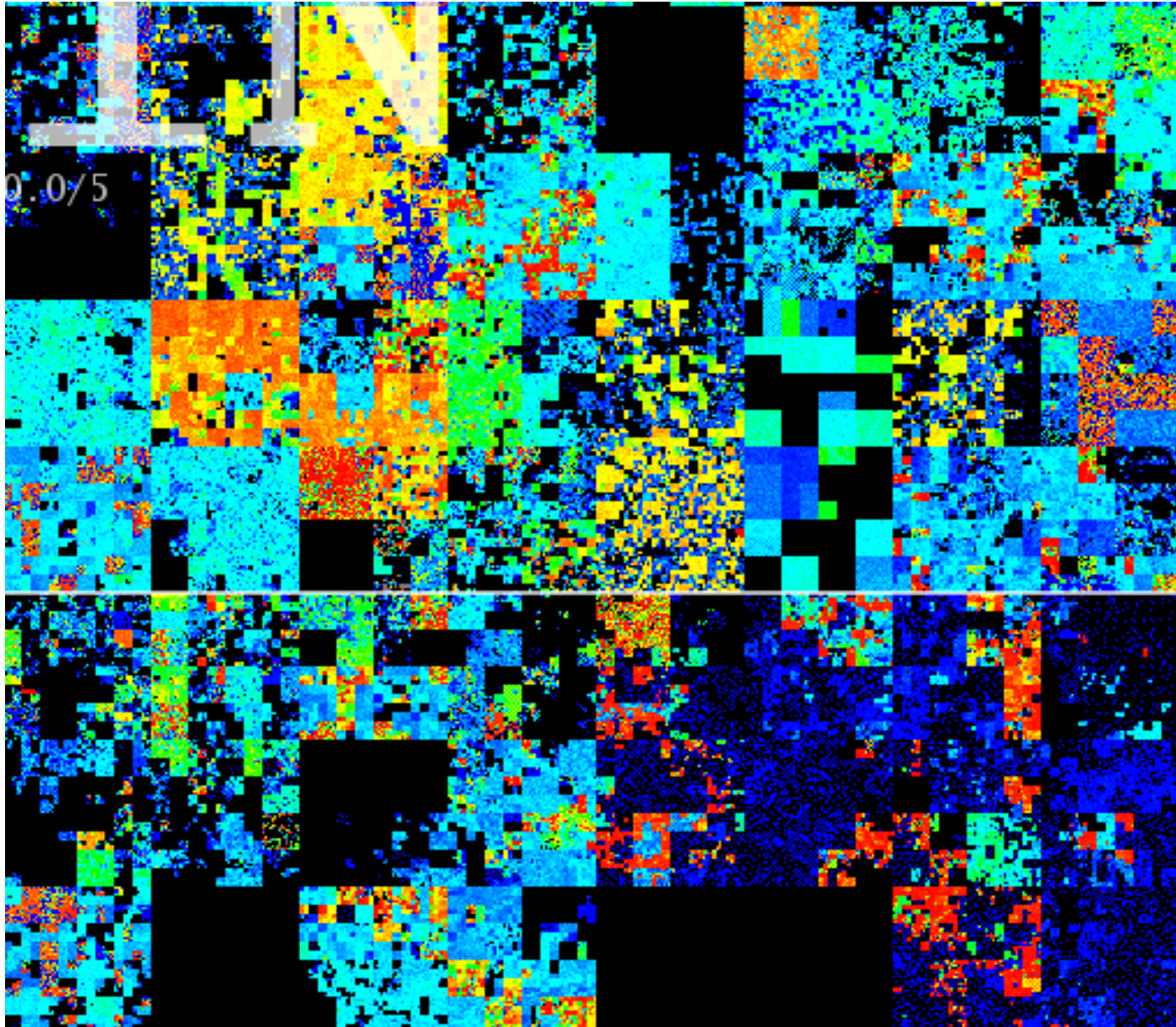
**"Integrated Cyber-Physical Security for
Governments and Business"**

Paris, France – 13th & 14th October 2014

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



*...or the Challenging Complexity of Securing Government & Business in **Cyberspace**!...*



30th International East/West Security Conference

**"Integrated Cyber-Physical Security for
Governments and Business"**

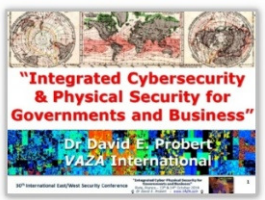
Paris, France – 13th & 14th October 2014

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



Smart Sustainable Security – “Theme Trilogy”

Theme (1) – **Smart Security** : Integrated Cybersecurity and Physical Security



- Understanding and Mapping the Worldwide Cyber Threats
- Transition to Smart Systems : Embedded Networked Intelligence
- Emergence of Smart Security: Hybrid Cyber-Physical Applications

“Operational Convergence”

13th Oct: 09:10 – 09:50

Theme (2) – **National Security** : Strategy, Models, and Road Maps

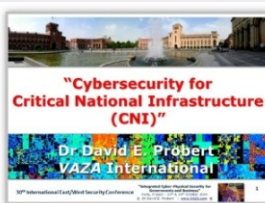


- UN/ITU – Global Cybersecurity Agenda and Guide
- Operations, Technology, Legal, Training, Partnerships
- Case Studies of “National Cybersecurity Agencies”

“Architecture & Standards”

13th Oct: 14:30 – 15:10

Theme (3) - **Critical Security** : Sector Threats and Smart Solutions



- Smart Security for Critical National Infrastructure (CNI):
- Finance, Transportation, ITC, Energy, Defence and more!...
- Engineering Smart Technical and Operational Solutions

“Intelligent Applications”

14th Oct: 11:15 – 11:55

Download Slides: www.valentina.net/East-West2014/

30th International East/West Security Conference

“Integrated Cyber-Physical Security for Governments and Business”

Paris, France – 13th & 14th October 2014

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



Personal *“Eastern Experiences”*: 1991 - 2014



- Armenia
- Belarus
- Bulgaria
- Czech Republic
- Georgia
- Hungary
- Kazakhstan
- Poland
- Romania
- Russia
- Slovakia
- Ukraine

Projects including *Cybersecurity, eGovernance & Internet Solutions*

30th International East/West Security Conference

“Integrated Cyber-Physical Security for Governments and Business”

Paris, France – 13th & 14th October 2014

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



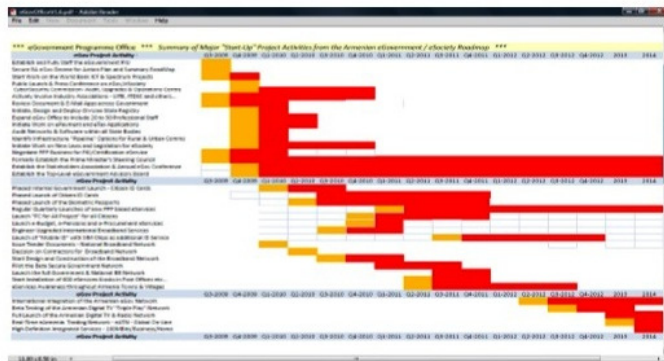
Cybersecurity for Armenia and Georgia

*** "Proposals for e-Government, e-Commerce and e-Security Development in Armenia" ***



"Roadmap for Real-Time Armenia"

E-Government, E-Commerce and E-Security



"Increasing Business Opportunities for the Armenian ICT Cluster through the development of E-Government, E-Commerce and E-Security"

*** Report Prepared by: Dr David E Probert – VAZA International ***

Author: Dr David E Probert : Final Report to USAID/CAPS : June 2009 : Page 1

Link: www.valentina.net/vaza/CyberDocs/
30th International East/West Security Conference

*** "Real-Time" Georgia : Securing Government & Enterprise Operations ***



"Real-Time Georgia"

Securing Government & Enterprise Operations



Dr David E Probert

VAZA International

1st Georgian IT Innovation Conference

Tbilisi : 29th & 30th October 2008

1

Author : Dr David E Probert

Copyright : www.vaza.com – Oct 2008

"Integrated Cyber-Physical Security for Governments and Business"

Paris, France – 13th & 14th October 2014

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



USAID eGovernance and Cybersecurity Mission:

Mt Aragats – South Summit (3879m) – Armenia



30th International East/West Security Conference

**"Integrated Cyber-Physical Security for
Governments and Business"**

Paris, France – 13th & 14th October 2014

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



UN/ITU - *Cybersecurity* Mission to Georgia, Caucasus



30th International East/West Security Conference

"Integrated Cyber-Physical Security for Governments and Business"

Paris, France – 13th & 14th October 2014

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



Network Project Team: *Almaty, Kazakhstan*



30th International East/West Security Conference

**"Integrated Cyber-Physical Security for
Governments and Business"**

Paris, France – 13th & 14th October 2014

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



Satellite & Wireless Networking Project – *Kazakhstan*

digital

FEATURES

European Business Group links Central Asian republic to Net via satellite and radio and 'mesmerises' sceptical locals

Kazakhstan defies remoteness by hooking up to the Internet

In the shadow of the Tien Shan mountains, within sight of China and 2,000 kilometres from the open sea, an Alpha server is being prepared to release a whole world of information on one of the remotest states on earth.

When Kazakhstan's Internet service opens early in 1996, it will be the culmination of a ten-month programme by Reading-based members of Digital's European Internet Business Group (IBG).

The project has linked organisations in three continents and led to star billing at a pioneering NATO conference for Dave Probert, European director of the IBG.

The conference was staged in Almaty, capital of Kazakhstan. It was attended by 150 high-ranking political and technical figures from across the Caucasus and Central Asia regions. They'd come from Russia, Georgia, Armenia, as well as from Azerbaijan, Uzbekistan, Kirghizstan, Turkmenistan and Tajikistan.

Action

Many had expected a lot of talk and not much action dur-



■ Dave Probert in front of the 3500-metre peak near the Cosmos and Scientific Research Station in the Tien Shan mountain range

Campus Network Project Team:

- *Donetsk Technical University* -



30th International East/West Security Conference

"Integrated Cyber-Physical Security for Governments and Business"

Paris, France – 13th & 14th October 2014

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



“Probert” Family History: *“Hughesovka”*



Machine Workshop: *Donetsk – c1890*

Great Grandfather : Edwin James Williams

19thC “Troika Trip” Near “*Hughesovka*” with
Great Grandfather (Edwin James Williams)

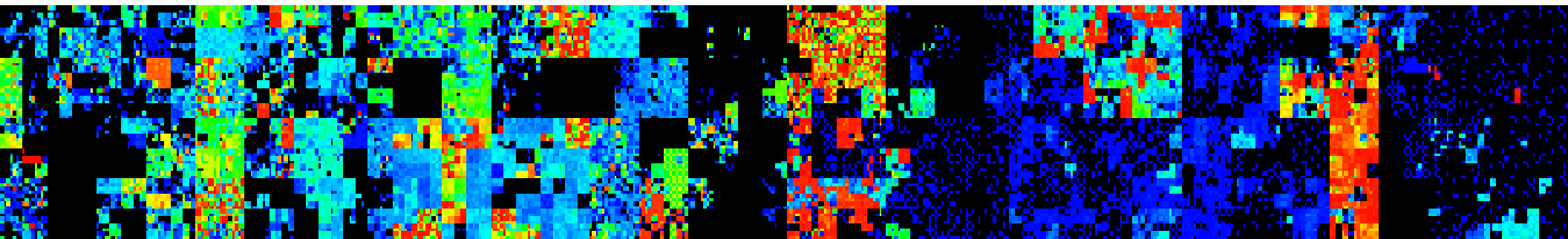


“Troika” — Near Hughesovka (now Donetsk, Ukraine) — c1890 — www.Valentina.Net/e-archive.html

Smart Sustainable Cyber-Physical Security



1 – Background Perspectives	2 – Mapping Cyber Threats in Cyberspace	3 – Hybrid Cyber-Physical Security Threats
4 – Practical Models for Smart Security	5 – Transition to 21stC Smart Security	6 – Smart Security: Technology & Process
7 – Integration: Cyber & Physical Security	8 – Towards Smart “Neural Society”	9 – Next Steps for Smart Security



Background Perspectives: *21stC Cyber World*

- **Cultures:** Cyber and Physical Security have developed as quite separate management operations, applications and cultures
- **Cyber Birth:** Cybersecurity has mainstreamed during the last 20 years since the birth of the worldwide web, search & social media
- **Smart Security Operations:** This talk will show how government and business can significantly reduce 21stC security risks through Smart & Resilient *Cyber-Physical Security* applications and operations
- **21stC Security Models:** During my “trilogy” of talks during the conference I’ll present some practical 21stC security models, solutions and architectures for both Governments and Business



Contrast between our Physical & Cyber Worlds

Convergence to 21stC “Intelligent Worlds” will take time!

Physical World

- Top-Down
- Dynamic
- Secrecy
- Territorial
- Government Power
- Control
- Direct
- Padlocks & Keys
- Convergent
- Hierarchical
- Carbon Life
- Tanks & Missiles
- Mass Media

Cyber World

- Bottom-Up
- Self-Organising
- Transparency
- Global
- Citizen Power
- Freedom
- Proxy
- Passwords & Pins
- Divergent
- Organic
- Silicon Life
- Cyber Weapons & Botnets
- Social Media

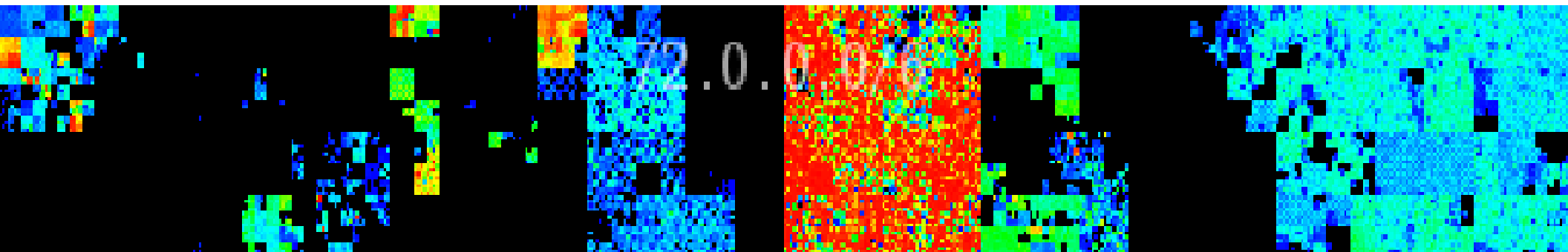
“Smart Resilient Security” will require Embedded Networked Intelligence in ALL devices



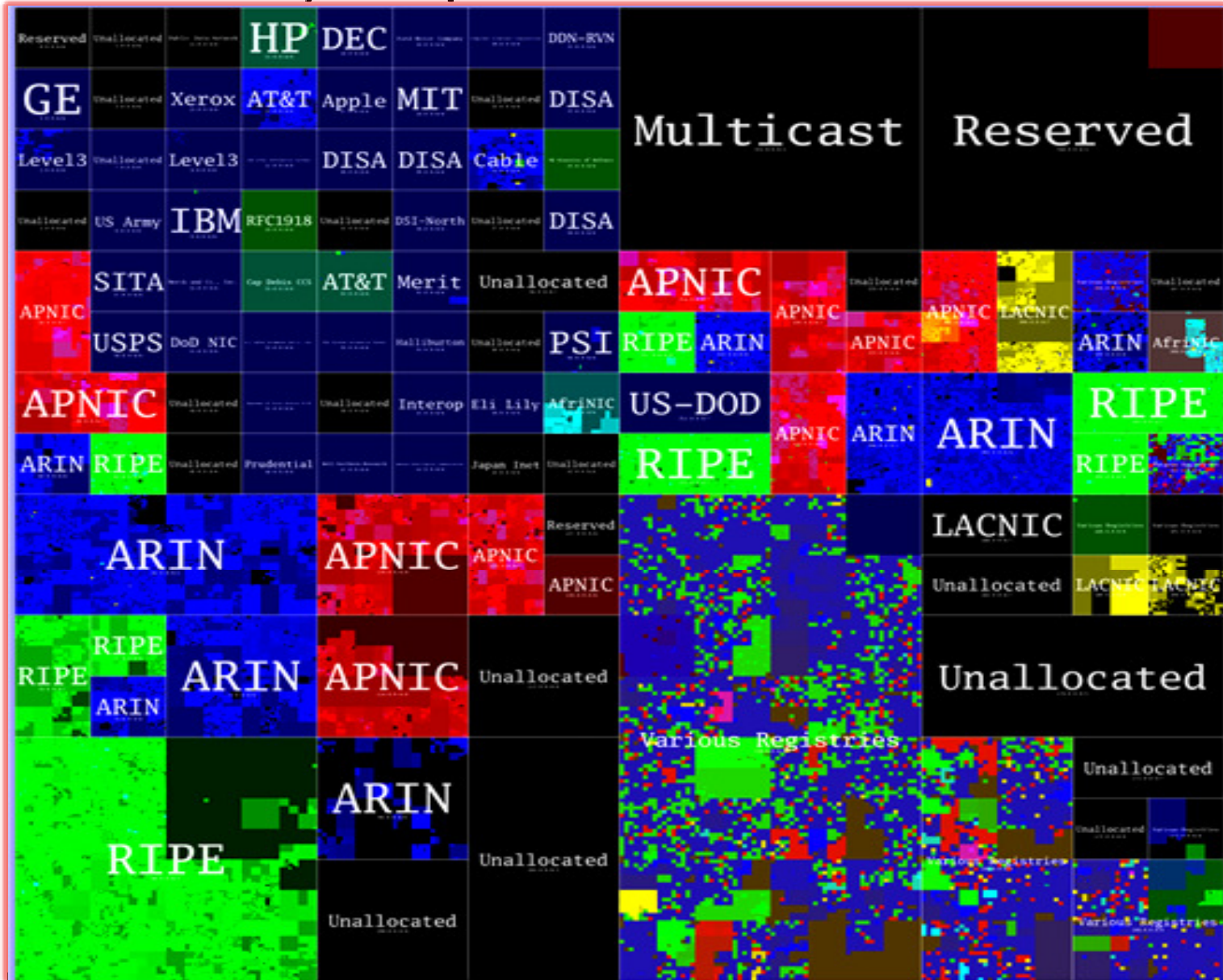
Smart Sustainable Cyber-Physical Security



1 – Background Perspectives	2 – Mapping Cyber Threats in Cyberspace	3 – Hybrid Cyber-Physical Security Threats
4 – Practical Models for Smart Security	5 – Transition to 21 st C Smart Security	6 – Smart Security: Technology & Process
7 – Integration: Cyber and Physical Security	8 – Towards Smart “Neural Society”	9 – Next Steps for Smart Security

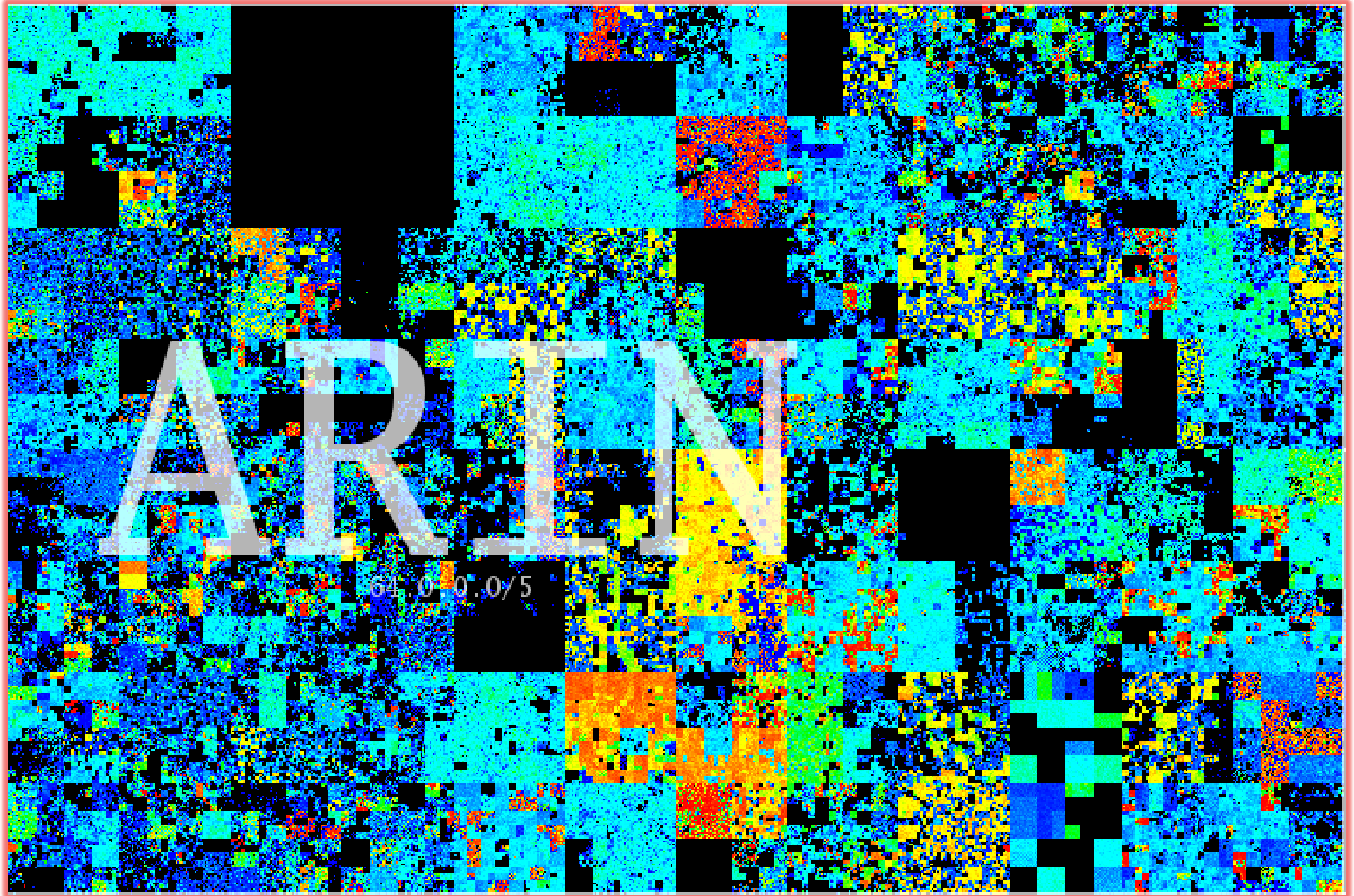


“Visualisation of Cyberspace”: *Global IP “WHOIS” Addresses*



...From 20thC Physical World To 21stC Cyberspace! ...

Active Internet Domains: *“American IP Registry”*



30th International East/West Security Conference

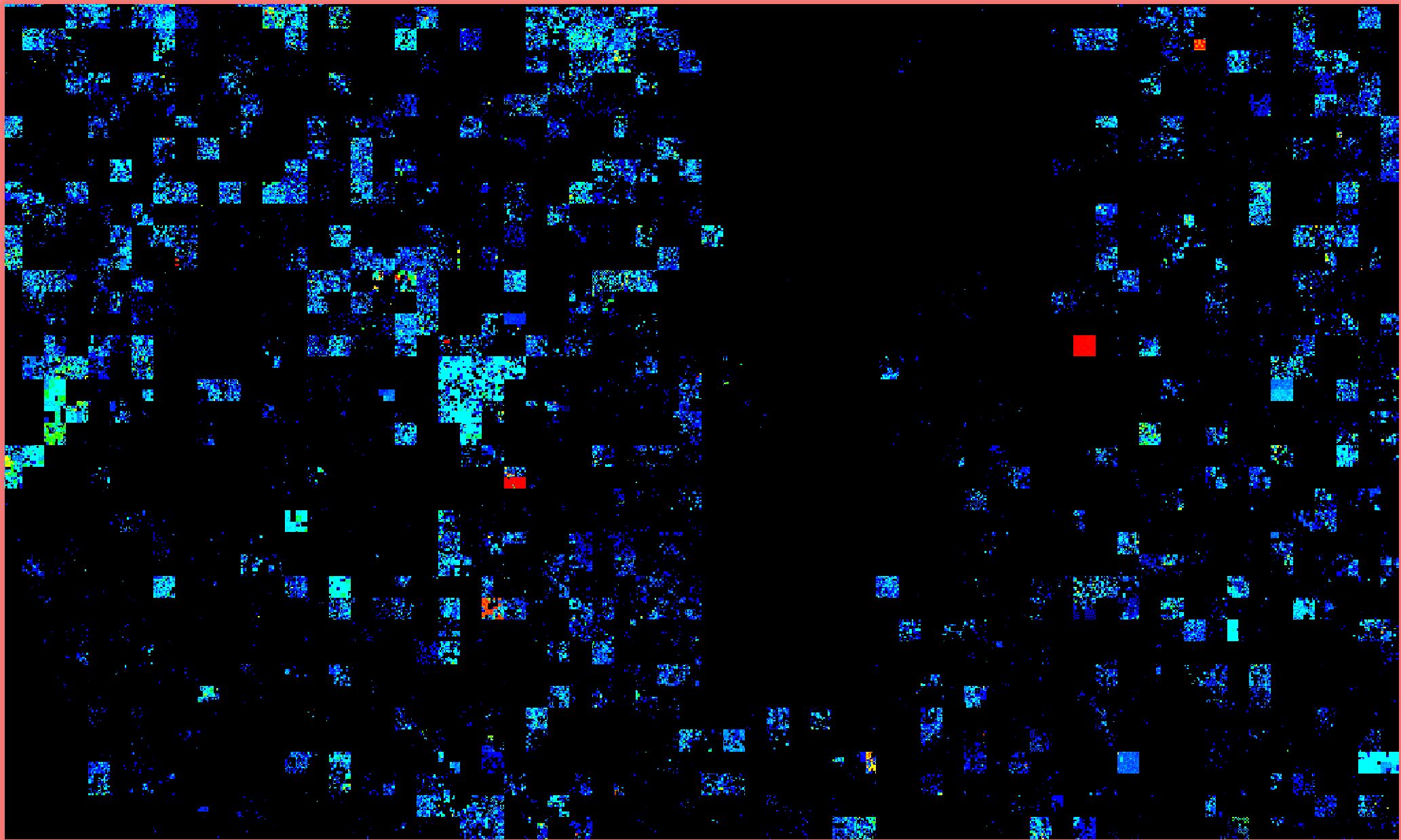
**“Integrated Cyber-Physical Security for
Governments and Business”**

Paris, France – 13th & 14th October 2014

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



“Outer Galaxies of Cyberspace” – *Other IP Registries*



30th International East/West Security Conference

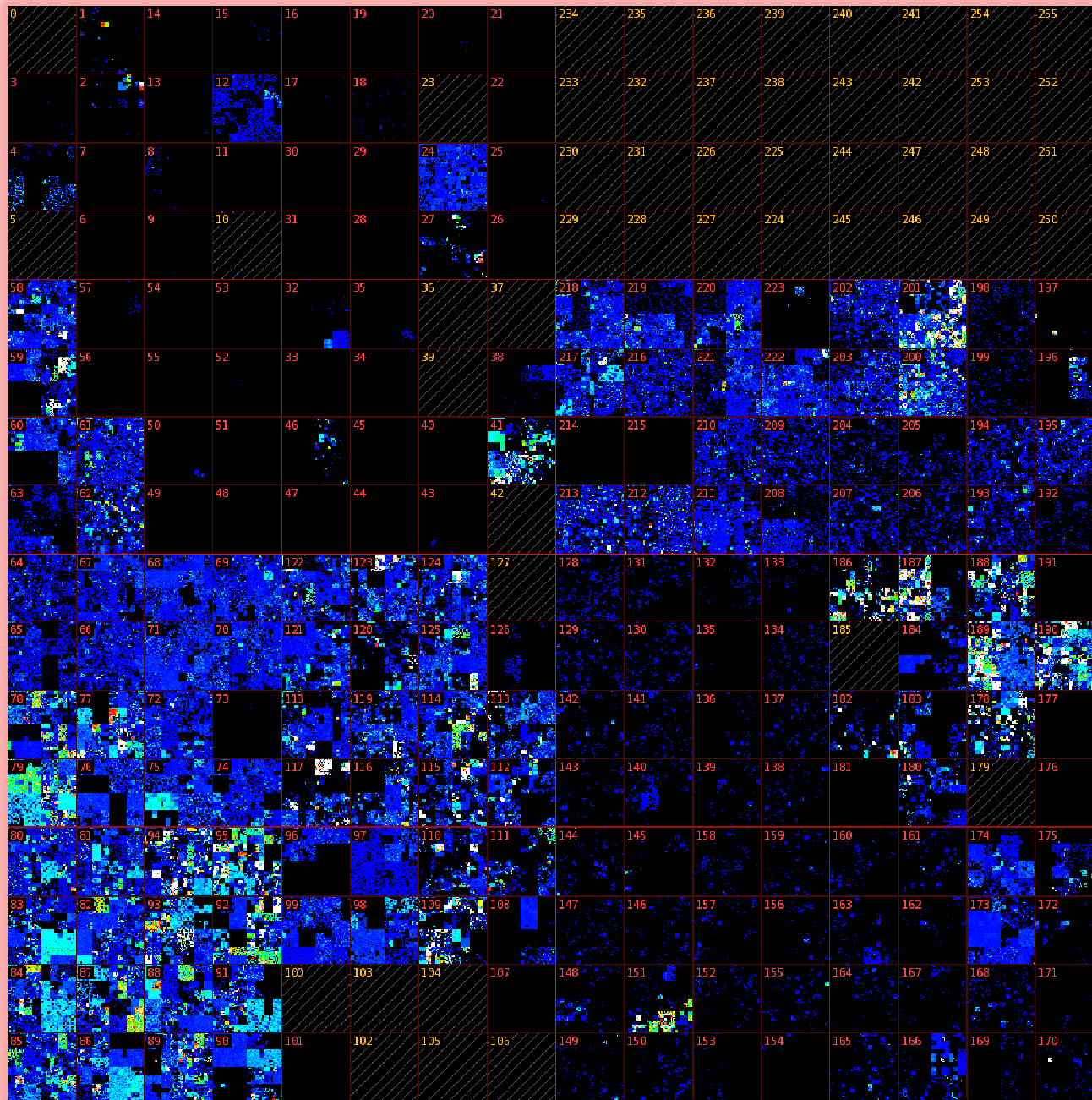
**“Integrated Cyber-Physical Security for
Governments and Business”**

Paris, France – 13th & 14th October 2014

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



Malicious Cybercrime Activity in *Global Cyberspace*



Key: Hilbert Space-Filling Curve Process

Link: www.team-cymru.org

30th International East/West Security Conference

"Integrated Cyber-Physical Security for Governments and Business"

Paris, France – 13th & 14th October 2014

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



Categories of *Cybersecurity* Threats

- The complexity of cyber threats means that several complimentary frameworks have been developed that classify cybersecurity risks
- For this presentation we'll focus on the categorisation developed by the *UN/ITU Telecommunications Study Group 17* as follows:

Category 1 : Unauthorised Access – *The systems & networks are accessed by persons or “bots” that do not have legal access or permissions*

Category 2 : Distributed Denial of Service Attacks (DDoS) – *Such attacks are used to target & disable a specific website or server using an army of infected machines*

Category 3 : Malicious Code – *Malware such as trojans, viruses & spyware are embedded within host machines for both commercial & criminal purposes*

Category 4 : Improper Use of Systems – *In these cases, the systems are being used for access and applications against the communicated policies*

Category 5 : Unauthorised Access AND Exploitation – *Many attacks will fall into this category when the hacker will penetrate systems and then use the acquired data, information & documents for cybercriminal activities*

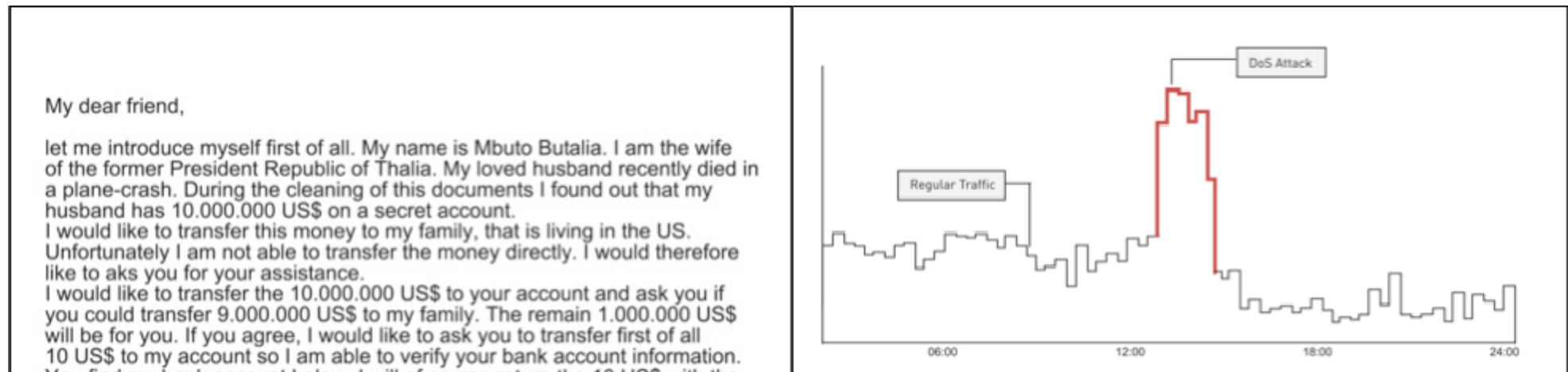
Category 6 : Other Unconfirmed Incidents – *These are alerts that require further investigation to understand whether they are actually malicious*

Typical Cybercrime Threats



(a) – Hardware & Software Keyloggers

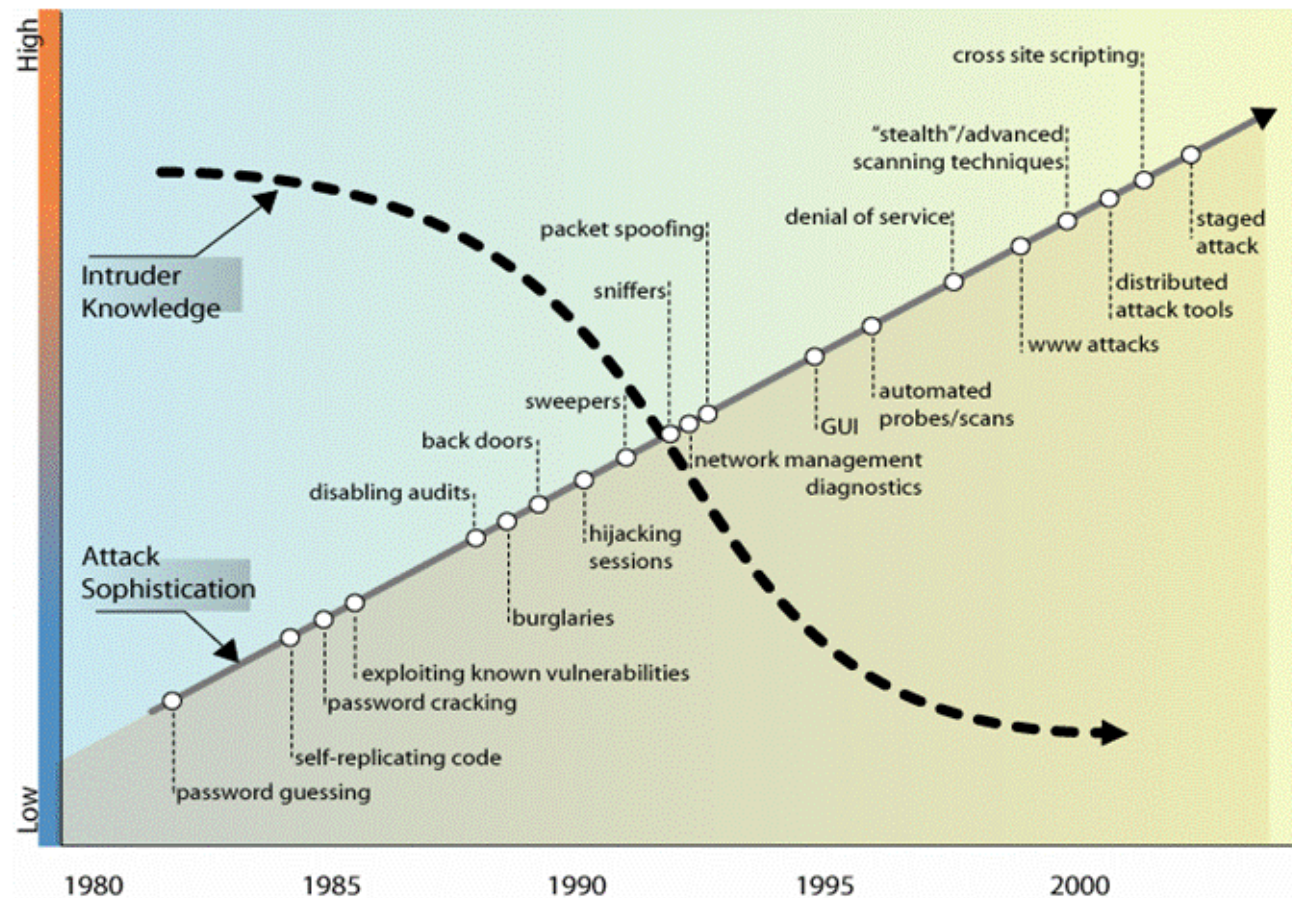
(b) – Email Phishing



(c) – Advance Fee Scam

(d) – Denial of Service

Attack Sophistication v. Intruder Knowledge



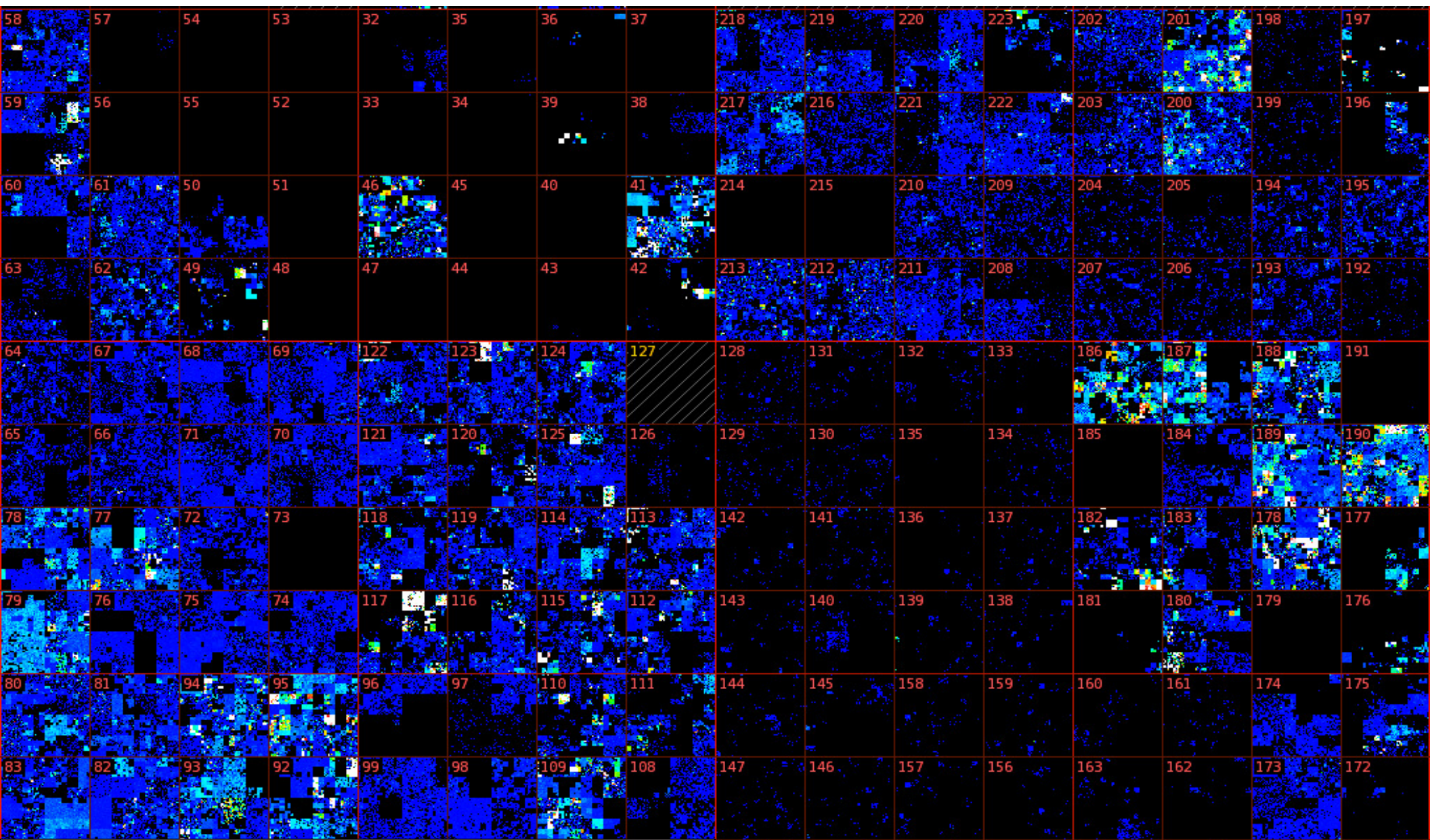
Source: www.cert.org



6



Map of *Recent* Malicious Activity in “*Cyberspace*”



www.team-cymru.org : - *Malicious Activity over 30 days - Sept 2014*

30th International East/West Security Conference

“Integrated Cyber-Physical Security for Governments and Business”

Paris, France – 13th & 14th October 2014

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



Recent *Cyber* Threats & Security Flaws

- **SHELLSHOCK** – Discovered *24th Sept 2014* – Security flaw in “Bash Software” that is present in the Apple Mac OS X, Unix and Linux. Allows execution of malicious code that could allow access to private data and remote control of server for orchestrated DDOS “BOT” attacks to targeted victim networks.

“SHELLSHOCK” BASH VULNERABILITY COULD HAVE FAR REACHING IMPLICATIONS #shellshock

Command to set environmental variable before execution of Bash command

Tacked-on arbitrary commands which will be executed by Bash

```
env val='() { :; }; echo Unexpected command' bash -c "echo Real command"
```

Unexpected command

Real command


Unexpected command runs first

Expected command runs second

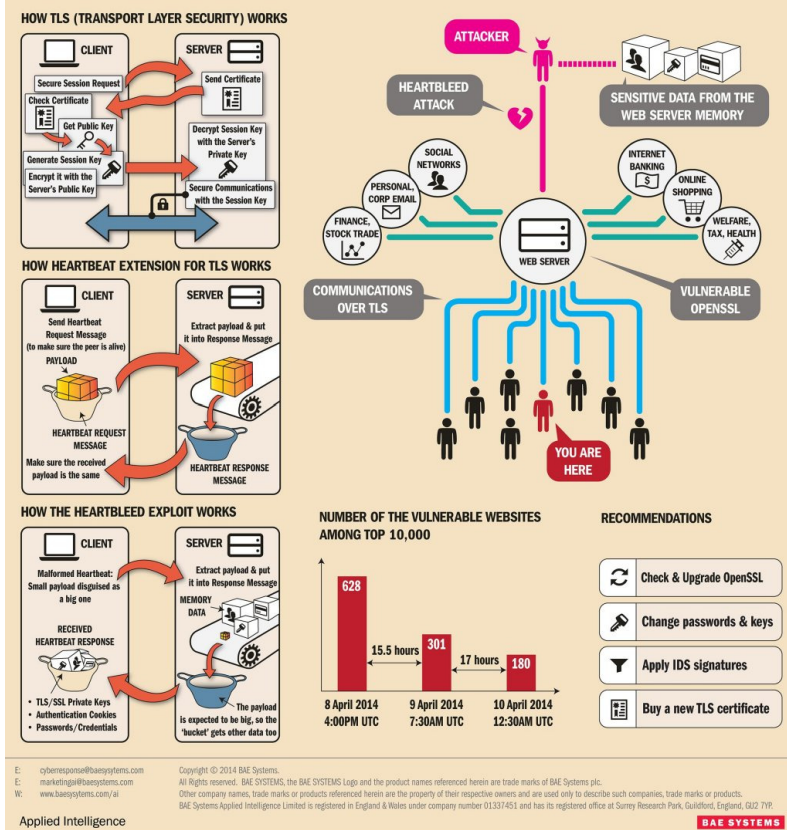
Potential to impact any computer running *NIX operating system. (CVE-2014-6271, CVE-2014-7169)

- Linux
- Unix
- OS X

Check with your software vendor now!

 @threatintel | www.symantec.com

HEARTBLEED - THE OPENSSL HEARTBEAT EXPLOIT



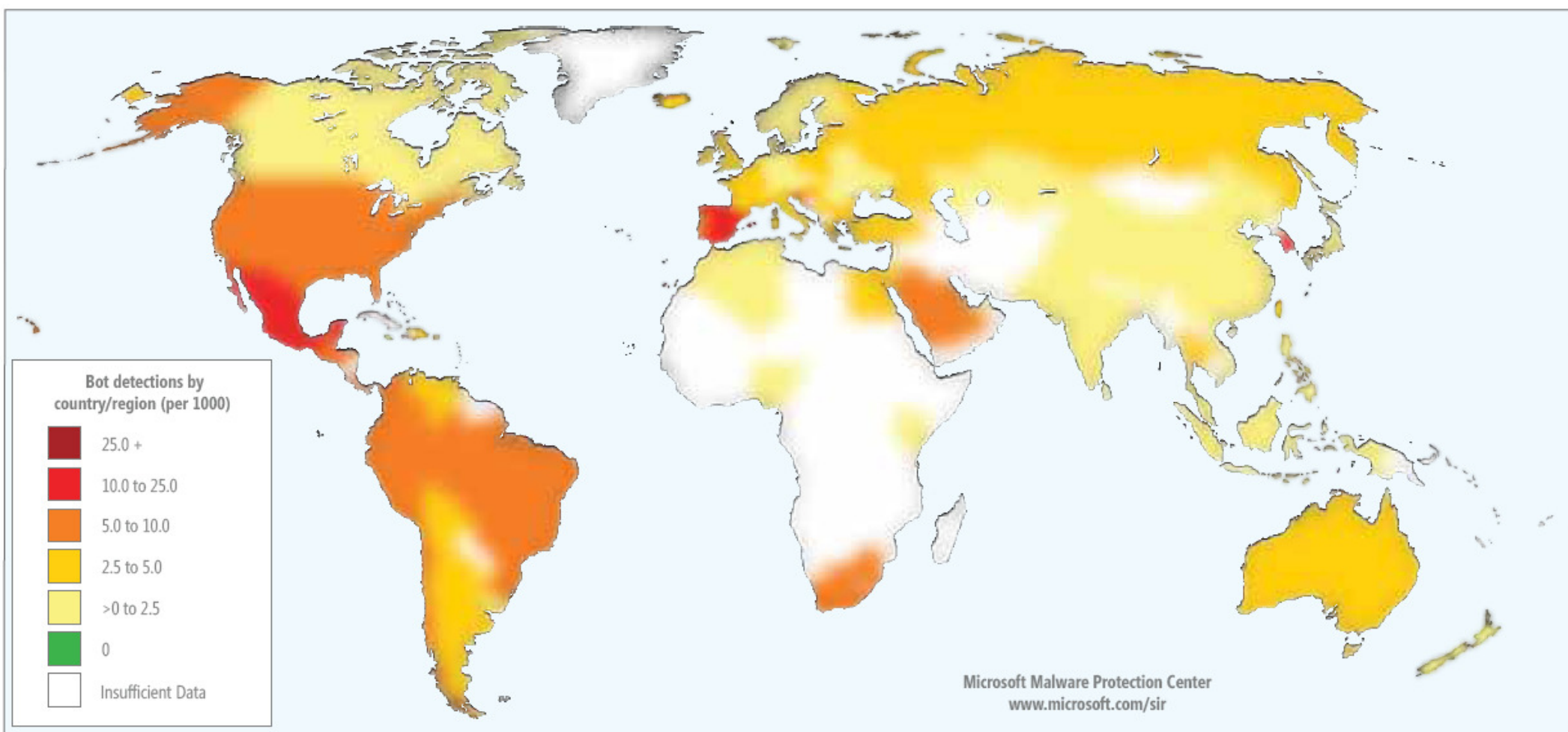
- **HEARTBLEED** – Discovered *April 2014* in OpenSSL Cryptography Library (widely used in Transport Layer Security – TLS) as a buffer over-read security flaw. When exploited this allows the theft of users private encryption “keys”, as well as passwords & session cookies

Commercialisation of “*Cyber Toolkits*”

- Industrialisation and Mainstreaming of Cyber Attacks:
 - *(1) Researchers & Cyber Software Creators of Malicious Codes* : Often creative talented computer scientists that have turned their skills to tools for illegal penetration & control of secure systems
 - *(2) “Botnet” - Farmers & Herders* : They are responsible for the illegal international distribution and infection of target “zombie” networked laptops PCs & Servers within homes and offices. The malicious codes (malware such as viruses & trojans) are spread through spam emails, infected websites and “backdoor” attacks.
 - *(3) “Commercial Botnet Dealers”* : They sell access to herds of “zombie” infected machines. The embedded malicious code can be triggered to stimulate “Denial of Service (DDoS)” attacks on target servers & websites. The aim is usually to maximise economic and political damage upon the targeted nation and associated businesses.

.....For further information see the ITU “BotNet” Mitigation Toolkit(2008)

Worldwide Computer “Bot” Infections: 2Q 2010

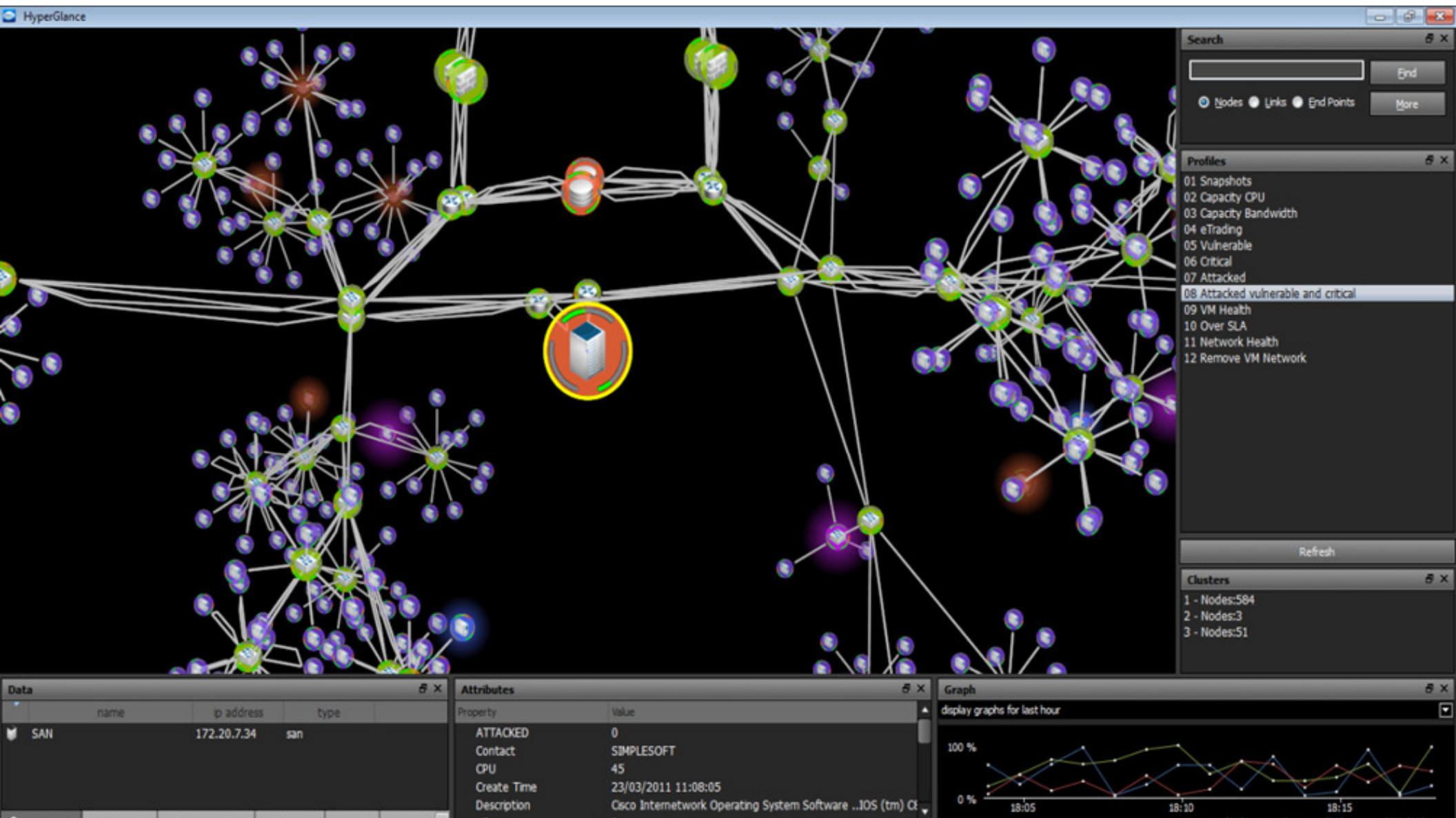


Source: Microsoft – Security Intelligence Report - 2010

Typical Global “*Botnet*” Cyberattack



Smart 3D Network Modelling: *Hyperglance*



Hyperglance Real-Time IT Modelling & Visualisation Software - Intergence.Com - *Cambridge, UK*

30th International East/West Security Conference

"Integrated Cyber-Physical Security for Governments and Business"

Paris, France – 13th & 14th October 2014

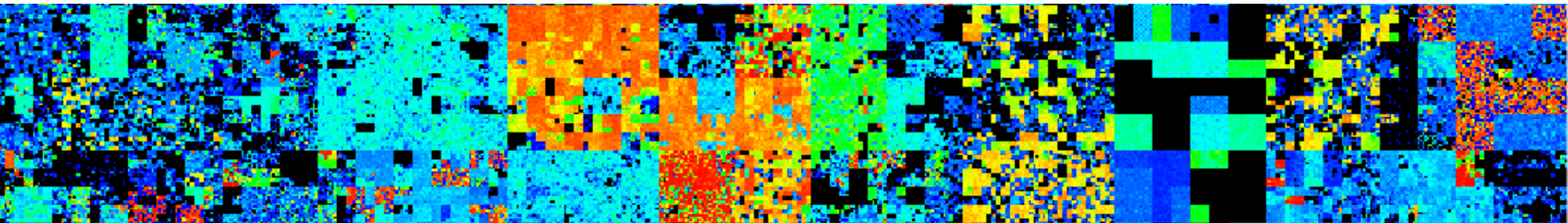
© Dr David E. Probert : www.VAZA.com ©



Smart Sustainable Cyber-Physical Security



1 – Background Perspectives	2 – Mapping Cyber Threats in Cyberspace	3 – Hybrid Cyber Physical Security Threats
4 – Practical Models for Smart Security	5 – Transition to 21 st C Smart Security	6 – Smart Security: Technology & Process
7 – Integrating Cyber & Physical Security	8 –Towards Smart <i>"Neural Society"</i>	9 – Next Steps for Smart Security



Sources of *Cyber* Threats and Attacks

- ***Cyber Criminals:*** Digital Fraud & Forgery, Extortion, Digital “Advanced Fee” Scams, ID Theft, Digital Money Laundering, Offensive & Pornographic Materials, Drug Trafficking, Cyber Stalking & Hate Crimes.
- ***Cyber Terrorists:*** Denial of Service, Website Defacement, Theft of Secret Information & Intelligence, On-Line Blackmail, Disruption of Critical Infrastructure such as Airports, Power Stations, Hospitals, and the National Clearing Banking Networks.
- ***Cyber Warfare:*** Closely related to cyber terrorism, and applied when there is a concerted cyber attack from a region or nation against the infrastructure and citizens of some other defined region or nation.
- ***Cyber Hackers:*** Skilled Individuals and “Researchers” that will initiate malicious attacks for the penetration of secure systems and theft of secret documents & databases from both governments & businesses.



Cyber Threat Challenges for Governments & Business

- 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



“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 has to be closed. Alternatively in the case of an airline check-in and dispatch system, flights are delayed.
 - *National CyberAttacks* – 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 (CNI) Clearly it is important for countries to upgrade their national cybersecurity to minimise the risks of *Hybrid Cyber-Physical Attacks* from terrorists, criminals, hacktivists and political adversaries

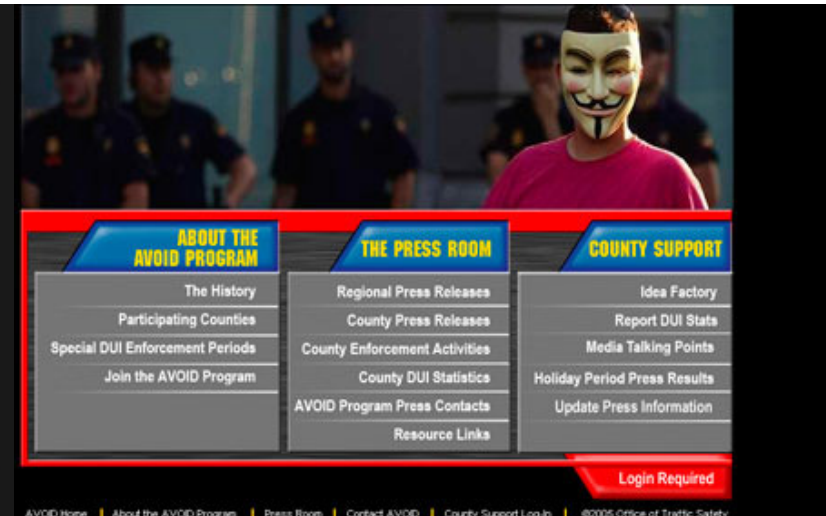


Hybrid Cyber-Physical Hacktivism

“Anonymous” Attacks on BART - Aug 2011



❖ *Physical Protests by International Hacktivist Group – “Anonymous” - coupled with multiple Web-Site Cyber Attacks following incident on Bay Area Transit Network - BART – San Francisco*



“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 devices or extract information, plans and databases to wireless enabled USB chips, tablets or phones!



Advanced Physical Perimeter Management

- Critical Infrastructure such as Airports, Power Stations, Ports and Telecommunications Facilities are often sited on large multi-building campuses with a significant physical perimeter fence.
- Modern 21stC Technology can help to secure the perimeter, & prevent access to the electronic cyber assets within the facility:
 - Networked CCTV including Smart Video Analytics for Object Identification
 - Thermal Imaging and Movement Location with HD InfraRed Cameras
 - Optical Fibres for Real-Time Intrusion Location using EM Field Analysis
 - Buried Networked Wired or Wireless Motion Detection Sensors
 - ANPR Vehicle Registration Number Plate Recognition for Perimeter Roads
 - Professional Security Guards that are fully trained & certified in these Security Applications

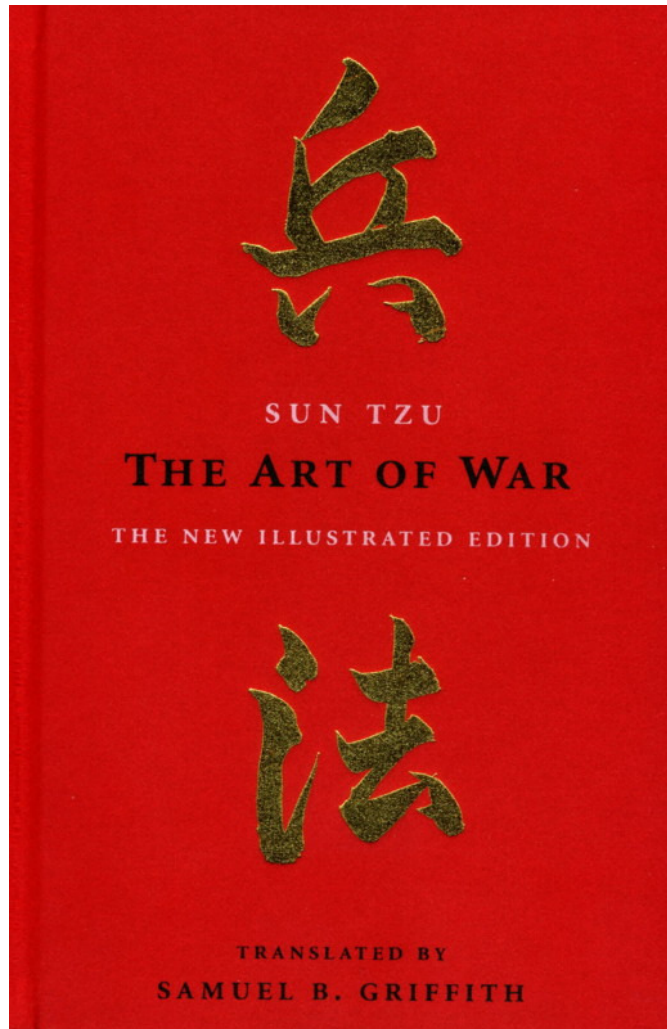


.....In summary, it is important never to neglect upgrading investment in physical perimeter security in order to boost the security of ICT cyber assets

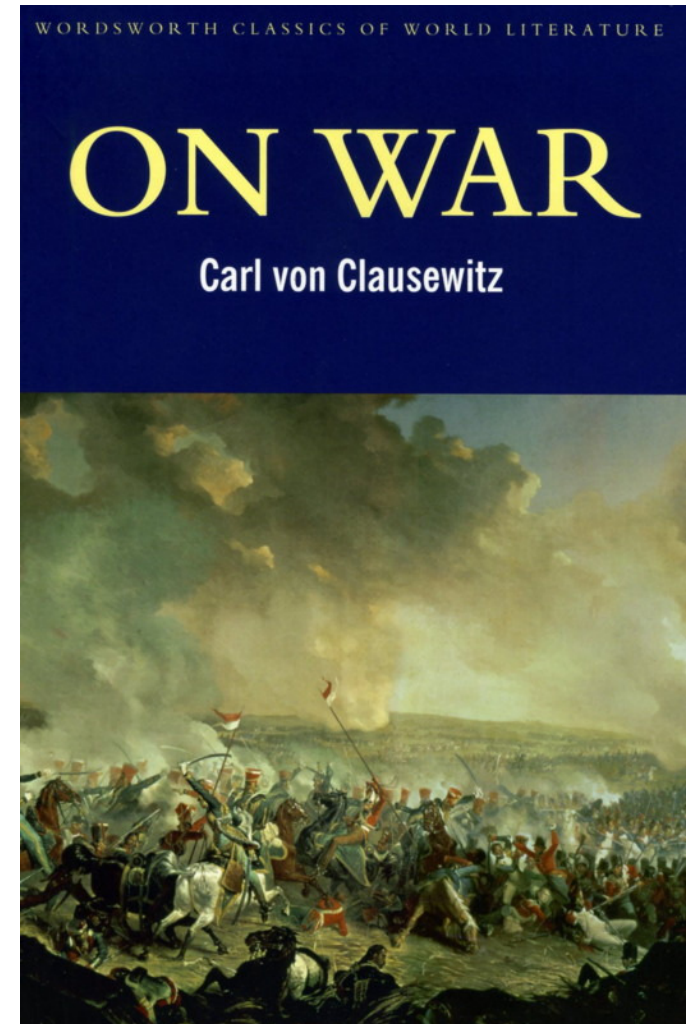
“Historic” Cyber Attack Case Studies

- *Estonia : May 2007*
 - Targeted at Government & Banking Servers – and immobilised national & commercial economic infrastructure for several days. This was one of the earliest “historic” massive DDos attacks (Distributed Denial of Service) from unknown proxy sources.
 - *Georgia : August 2008*
 - Targeted at Government Servers including Parliament & Ministry of Foreign Affairs, and the National & Commercial Banking Network from anonymous proxy sources.
 - *South Korea : July 2009*
 - Targets included the Defence Ministry, Presidential Offices, National Assembly, and Korea Exchange Banks. This attack was also simultaneously targeted at various high-profile US Sites & Servers such as the NY Stock Exchange, White House & Pentagon.
 - *Iran, Indonesia & India : June 2010*
 - Computer worm known as *Stuxnet* discovered in Industrial Logic Controllers in several countries including Iran , Indonesia and India. Stuxnet was the 1st known sophisticated “Designer” Cyber Malware targeted on specific industrial SCADA Systems (Supervisory Control And Data Acquisition). Duqu Malware (2011) is related to Stuxnet.
 - *Middle East : May 2012*
 - Sophisticated Modular Computer Malware known as *Flame* or Skywiper is discovered infecting computer networks in Middle Eastern Countries including Iran, Saudi Arabia, Syria, Egypt,& Israel
-Small scale penetrations & cyber attacks continue on an almost 24/7 against almost ALL countries including government & critical national & industrial infrastructure (CNI)*

“CyberWar” Strategies *from* Classic Works!



Recommended
“Bedtime
Reading”
for
Cybersecurity
Specialists!



...Classic Works on “War” are just as relevant today for Cybersecurity as pre-21th C

Case Study: StuxNet Worm - Industrial SCADA Systems - 2010



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 -

Critical Energy Industry Sector : *“Cybersecurity for Automated Industrial Control & Safety Systems”*



Protection against “Stuxnet” type designer malware that attacks SCADA systems

30th International East/West Security Conference

“Integrated Cyber-Physical Security for Governments and Business”

Paris, France – 13th & 14th October 2014

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

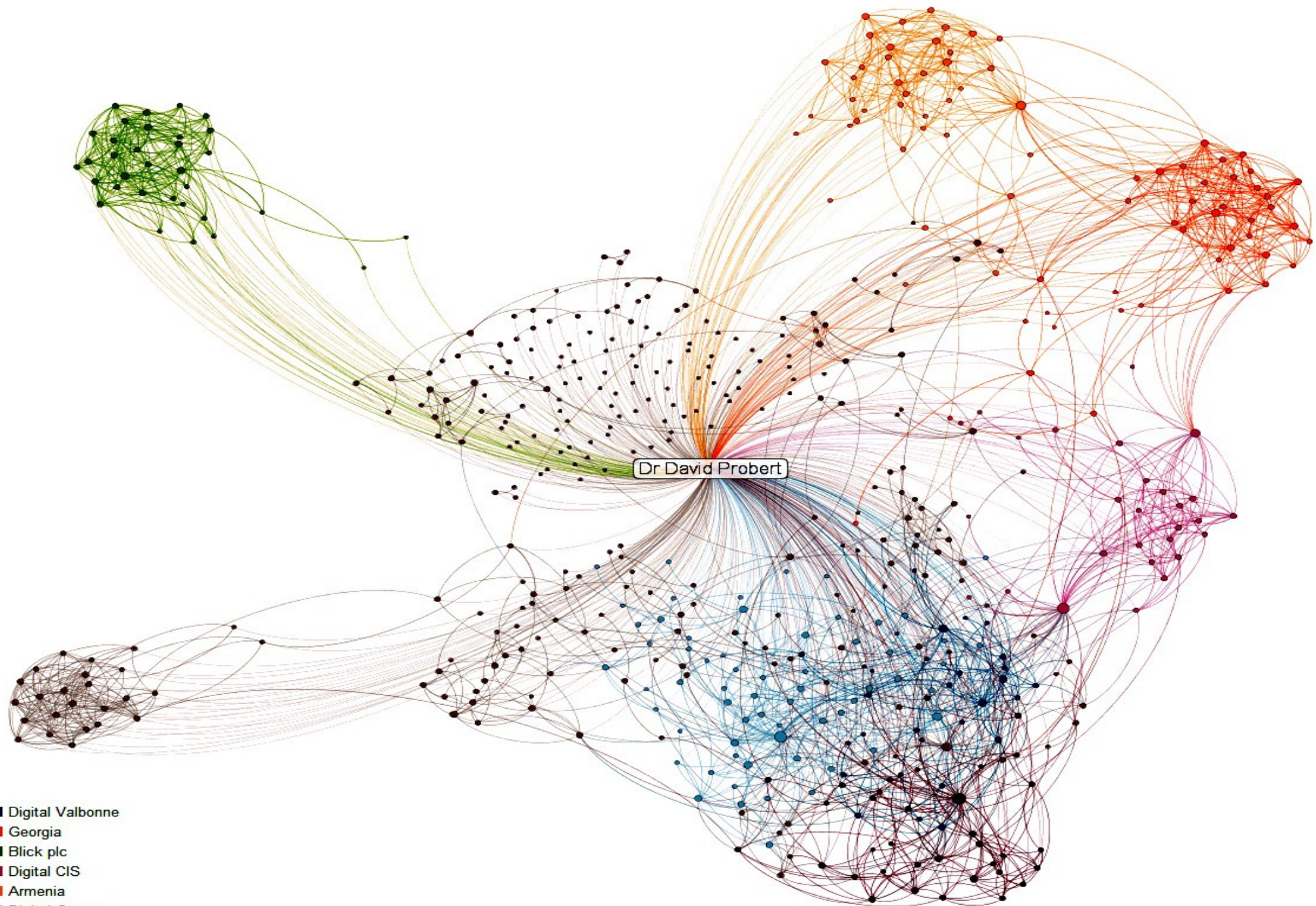


Cybersecurity for Social Networks

- *Social Sites*: During recent years, social & professional networking sites such as Facebook and LinkedIn have become the latest commercial targets for cybercriminals
- *Cyber Scams* include Identity Theft and requests for instant money transfers from parents to support the “release” of children & friends overseas
- *Cybercriminals* also sign-up as “friends” in order to infiltrate student & family networks, and then to secure personal information & account details
- *Paedophiles* also use these social networks in order to cultivate relationships with children and teenagers below the “age of consent”
- *Businesses* may be at risk if employees publish confidential company information on their social network accounts that may easily go public
- *Facebook* now works with child protection authorities in countries such as the UK so that those at risk can quickly contact “help lines”

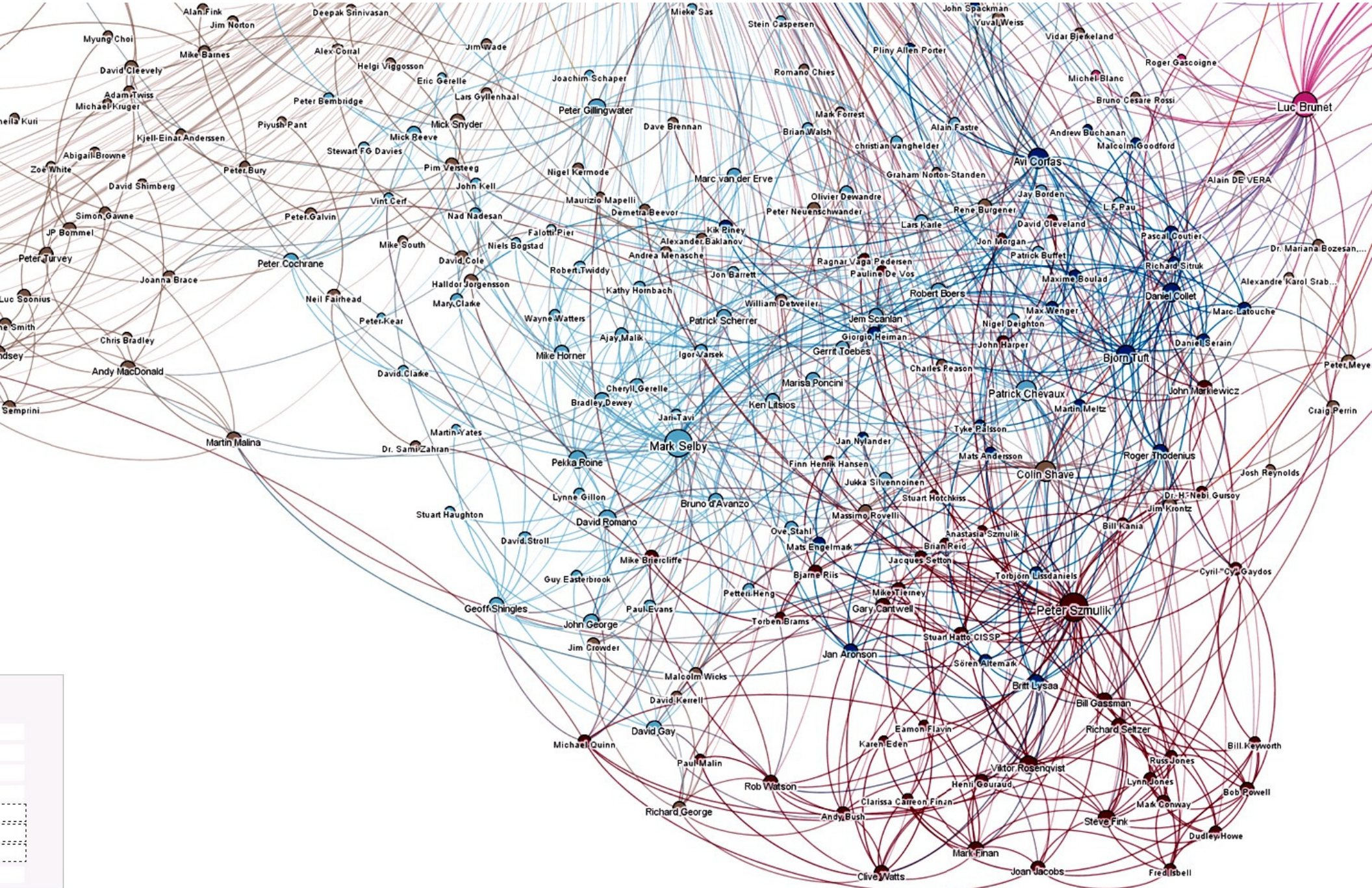
.....Business and Government should consider ways to exploit the power of social networking whilst protecting their own networks against attack.



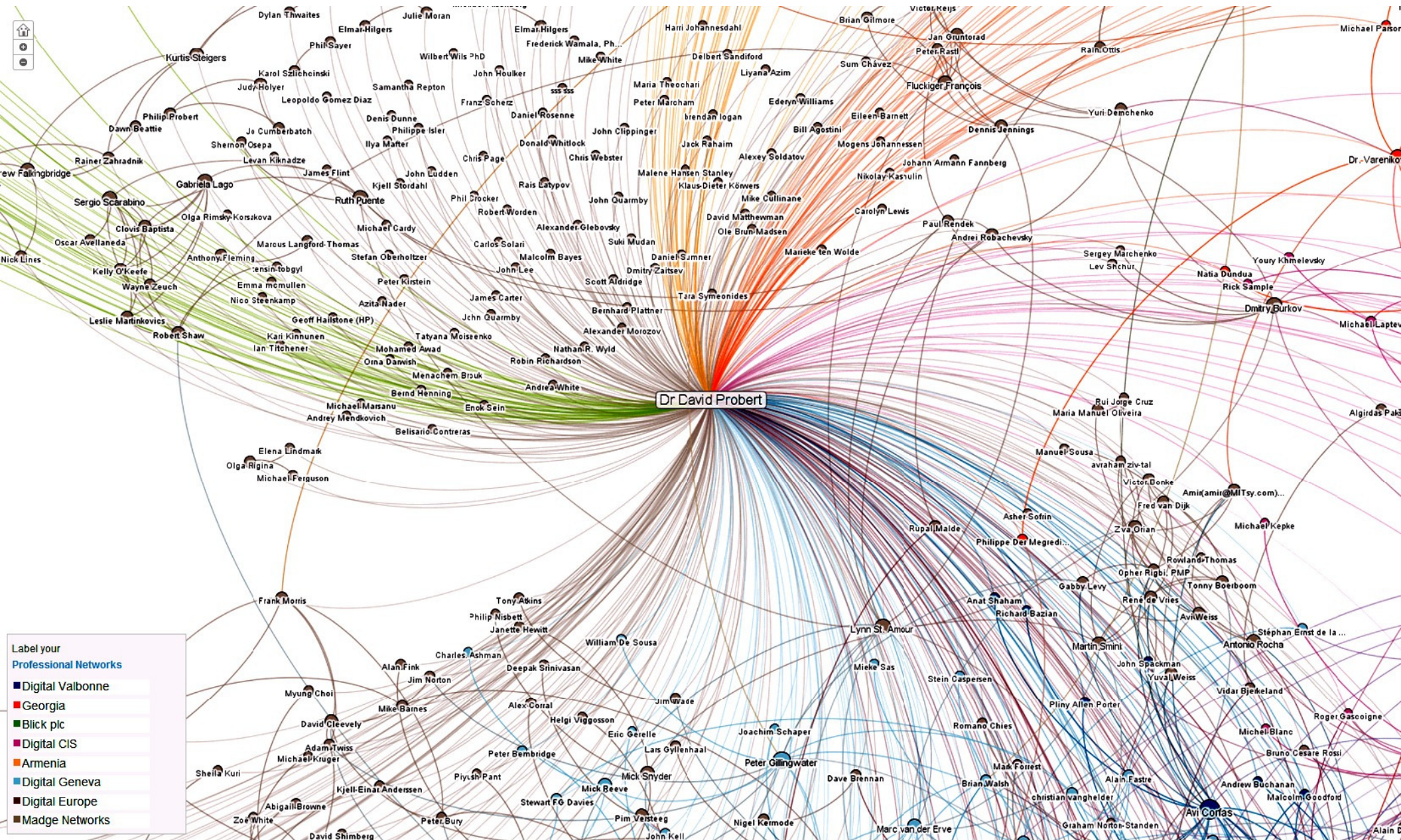


- Digital Valbonne
- Georgia
- Blick plc
- Digital CIS
- Armenia
- Digital Geneva
- Digital Europe
- Madge

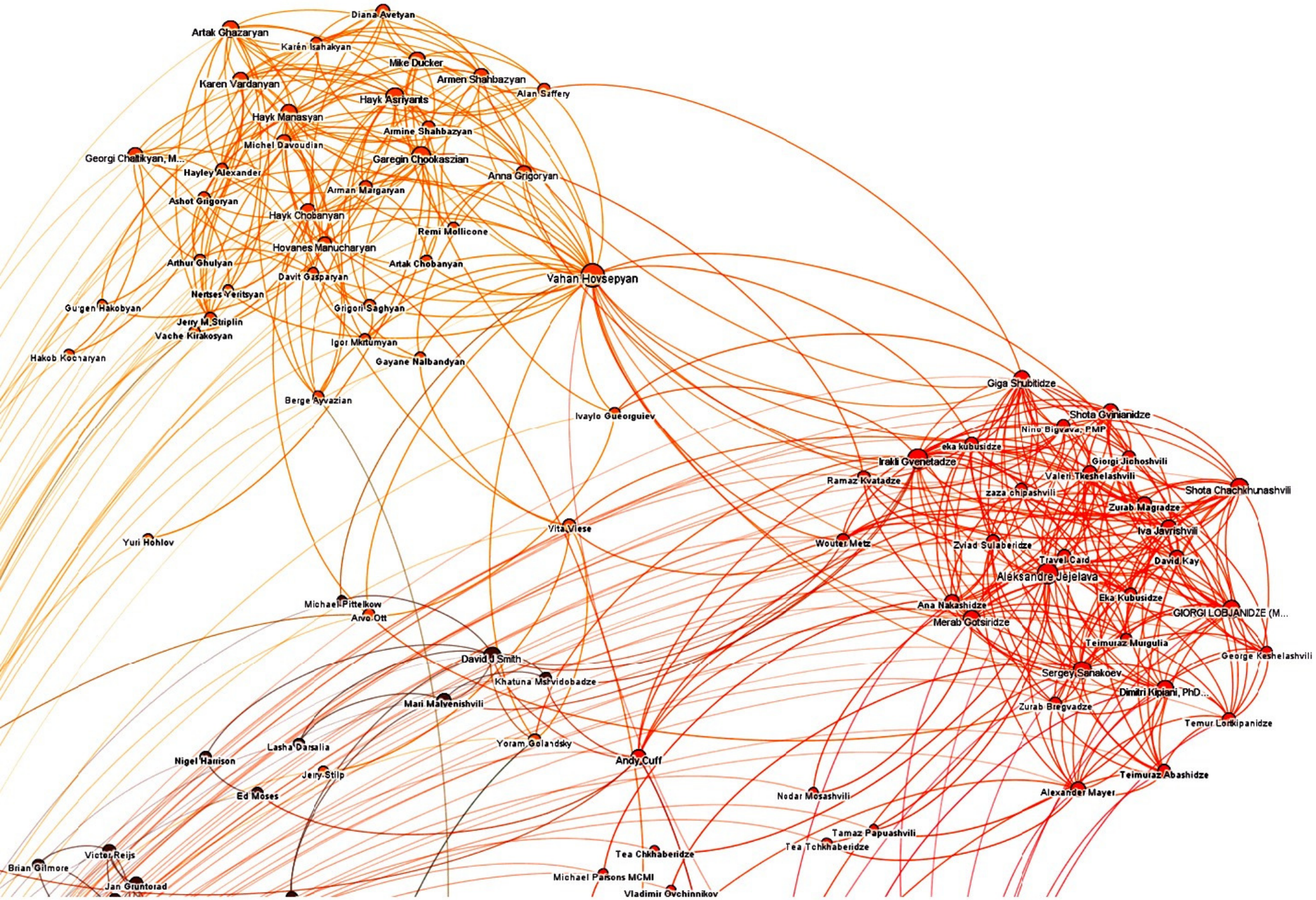
Mapping Social Media Networks: *LinkedIn*



Mapping Social Media Networks



My *Linkedin* Social Media Map : *Armenia & Georgia*



Cybersecurity Operations & Policies for Wireless Networks

- **Perimeter Protection:** Sentry Wireless Access Point Network around office/campus
- **Certificates:** End-User Encrypted Logon Certificates – EAP/802.1X
- **24/7 Scanning:** Permanent Wireless Frequency Sentry Scanning against rogue devices
- **Prohibition:** of attachment of personal wireless nodes (“Bring your Own” – BYO Policy)
- **3G/4G Gadgets:** Management of Business PDAs and Smart Mobile Devices
- **Guests & Contractors:** All guest account access either fully secured or prohibited
- **3G/4G Mobiles:** Sensitive government or business data should always be encrypted and transmitted using secure VPN tunnel to home servers

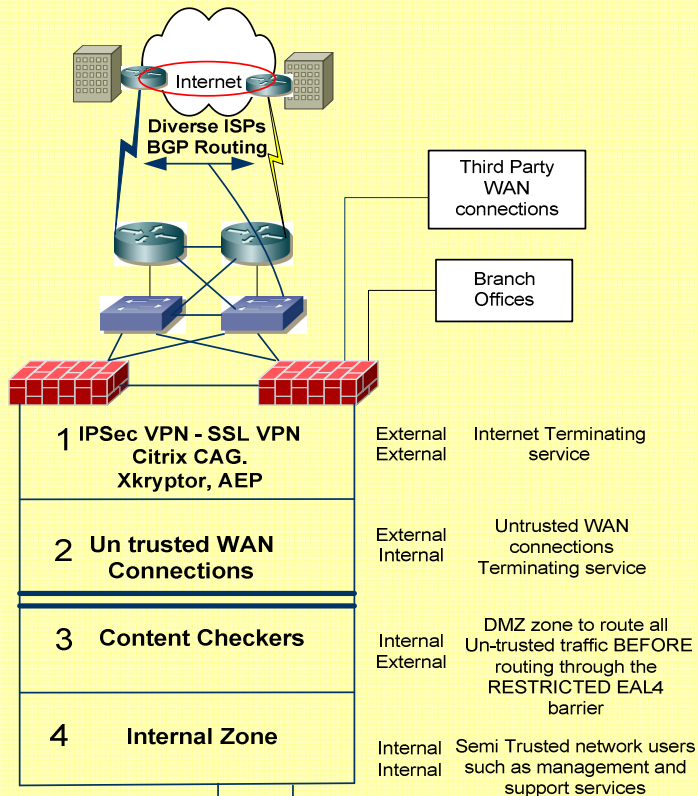
.....All businesses & governments now need to plan their strategies, operations and policies for BOTH Cyber and Physical Security , with some level of sharing & solutions integration



Summary of Cybersecurity Focus, Applications and Solution Benefits

SECURITY Focus	SECURITY Application	CYBERSECURITY SOLUTION Benefits
Access Control		
Boundary Protection	Firewalls	Aim to prevent unauthorised access to or from a private network.
	Content Management	Monitor web, messaging and other traffic for inappropriate content such as spam, banned file types and sensitive or classified information.
Authentication	Biometrics	Biometric systems rely on human body parts such as fingerprints, iris and voice to identify authorised users
	Smart tokens	Devices such as smart cards with integrated circuit chips (ICC) to store and process authentication details
Authorisation	User Rights and Privileges	Systems that rely on organisational rules and/or roles to manage access
System Integrity		
	Antivirus and anti-spyware	A collection of applications that fight malicious software (malware) such as viruses, worms, Trojan Horses etc
	Integrity Checkers	Applications such as Tripwire that monitor and/or report on changes to critical information assets
Cryptography		
	Digital Certificates	Rely on Public Key Infrastructure (PKI) to deliver services such as confidentiality, authentication, integrity and non-repudiation
	Virtual Private Networks	Enable segregation of a physical network in several 'virtual' networks
Audit and Monitoring		
	Intrusion Detection Systems (IDS)	Detect inappropriate, incorrect or abnormal activity on a network
	Intrusion Prevention Systems (IPS)	Use IDS data to build intelligence to detect and prevent cyber attacks
	Security Events Correlation Tools	Monitor, record, categorise and alert about abnormal events on network
	Computer Forensics tools	Identify, preserve and disseminate computer-based evidence
Configuration Management and Assurance		
	Policy Enforcement Applications	Systems that allow centralised monitoring and enforcement of an organisation's security policies
	Network Management	Solutions for the control and monitoring of network issues such as security, capacity and performance
	Continuity of Operations tools	Backup systems that helps maintain operations after a failure or disaster
	Scanners	Tools for identifying, analysing and reporting on security vulnerabilities
	Patch Management	Tools for acquiring, testing and deploying updates or bug fixes

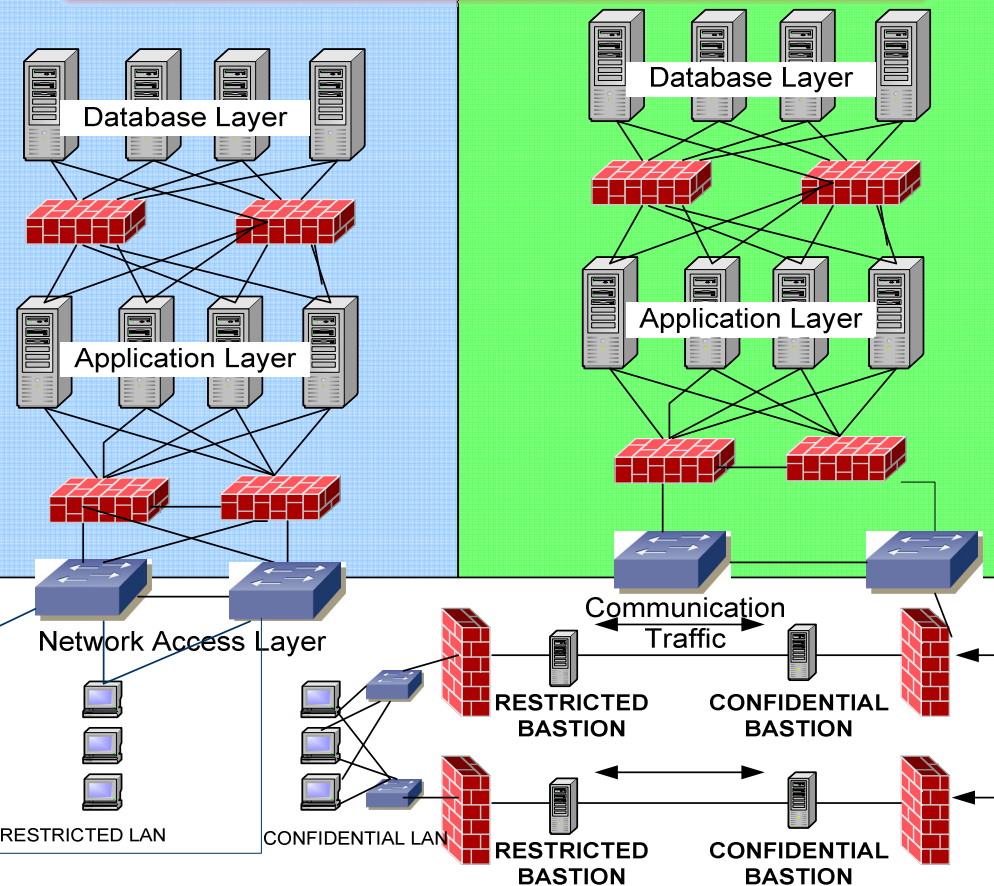
NON PROTECTIVELY MARKED LAN



RESTRICTED LAN

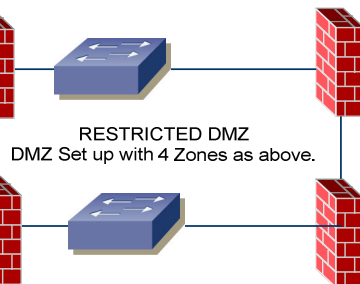
CONFIDENTIAL LAN

Cyber Secure Systems LAN Infrastructure with DMZ for Government or Enterprise



Access to RESTRICTED ZONE via restricted DMZ.

- One way Diodes
- Firewall Rules
- Access List Control
- Protocol Control
- Bastion Devices



"Integrated Cyber-Physical Security for Governments and Business"

Paris, France – 13th & 14th October 2014

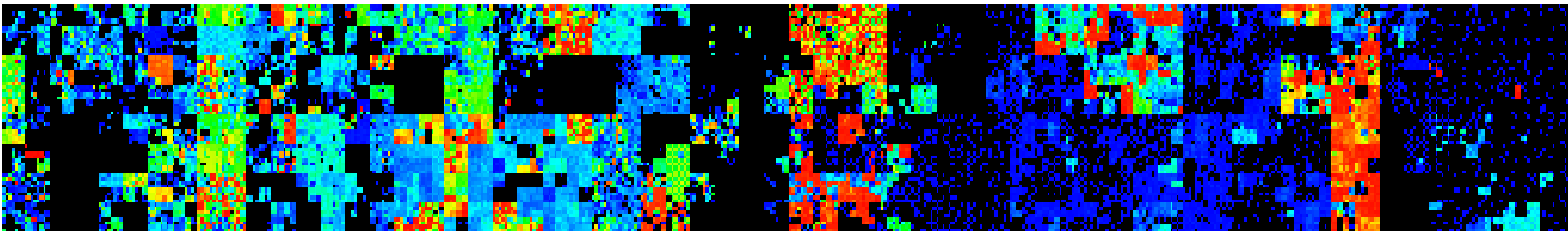
© Dr David E. Probert : www.VAZA.com ©



Smart Sustainable Cyber-Physical Security



1 – Background Perspectives	2 – Mapping Cyber Threats in Cyberspace	3 – Hybrid Cyber-Physical Security Threats
4 – Practical Models for Smart Security	5 – Transition to 21 st C Smart Security	6 – Smart Security: Technology & Process
7 – Integrating Cyber & Physical Security	8 – Towards Smart “ <i>Neural Society</i> ”	9 – Next Steps for Smart Security



21stC Smart Models for Business

- From 1980s onwards, many Enterprises started to deploy ICT networks, and then to “flatten” their organisations from Hierarchical to Hybrid.
- In the 21stC, Business is now starting to fully deploy more advanced ICT Solutions using the *“Smart Design Principles”* that we summarise below:
 - **Space-Time Awareness:** Utilise GPS Location and RFID Technologies to Track and Trace both Products, Staff and all moveable Business Assets to provide Real-Time Corporation
 - **Adaptation** to Markets, New Product Features, Delivery Logistics, Minimise Stock Levels
 - **Massive Memory & Storage:** Low Cloud Storage Costs permit massive data mining on customer orders, profiles, search and buying behaviours. Already used by major international supermarket chains & global on-line players such as Amazon, eBay, Google.
 - **Sustainable Security :** Integrated adaptive management of cyber and physical security
 - **Self-Organisation:** Empower staff for Local Decisions with almost “Flat Organisation”
 - **Scalable Architecture:** Building Business as Cellular Organisation using High-Speed Nets
 - **Systems Integration:** Many Businesses need to integrate their on-line cyber & traditional physical operations to provide a integrated & coherent cyber-physical managed operation

...Now for examples of smart systems – “Self-Organisation” & “Scalability” in science



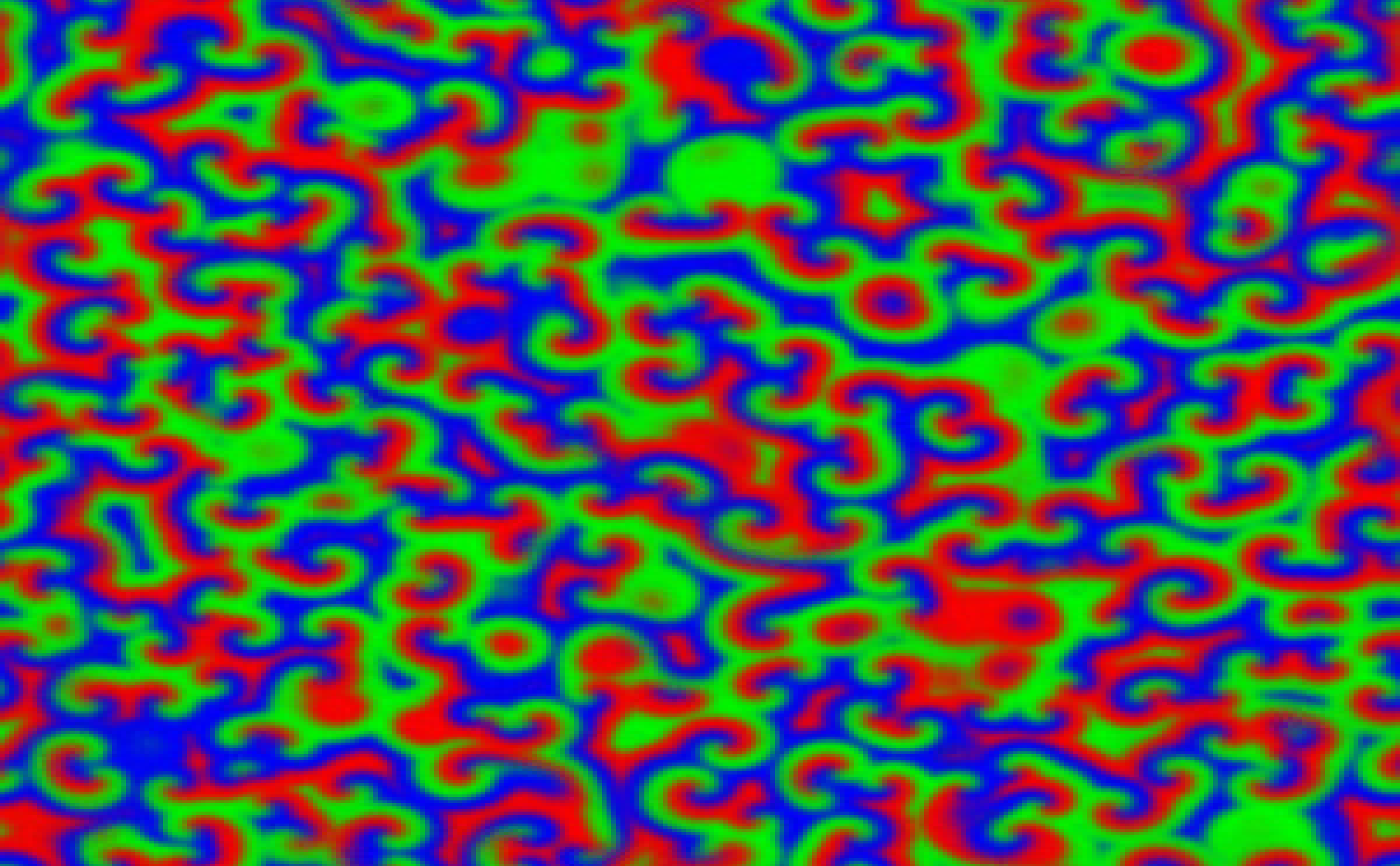
Cellular Automata: *“Game of Life”*

....*“Simple”* Rules may Lead to *“Smart”* Complex Behaviour!



“Smart” Autonomous Chemical Oscillator:

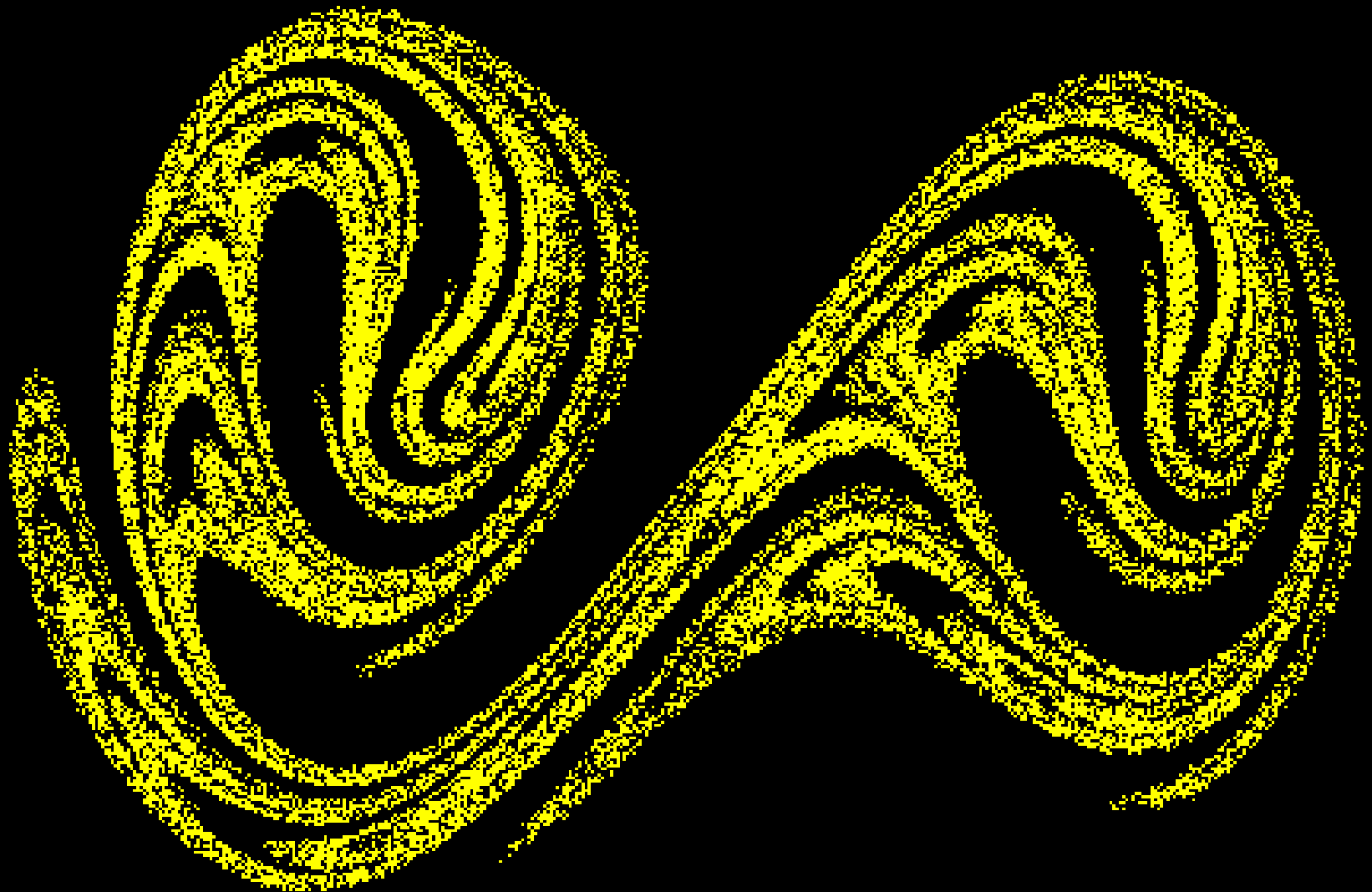
- Belousov–Zhabotinsky Reaction (BZ) -



Chaotic Attractor: *Duffing Oscillator*

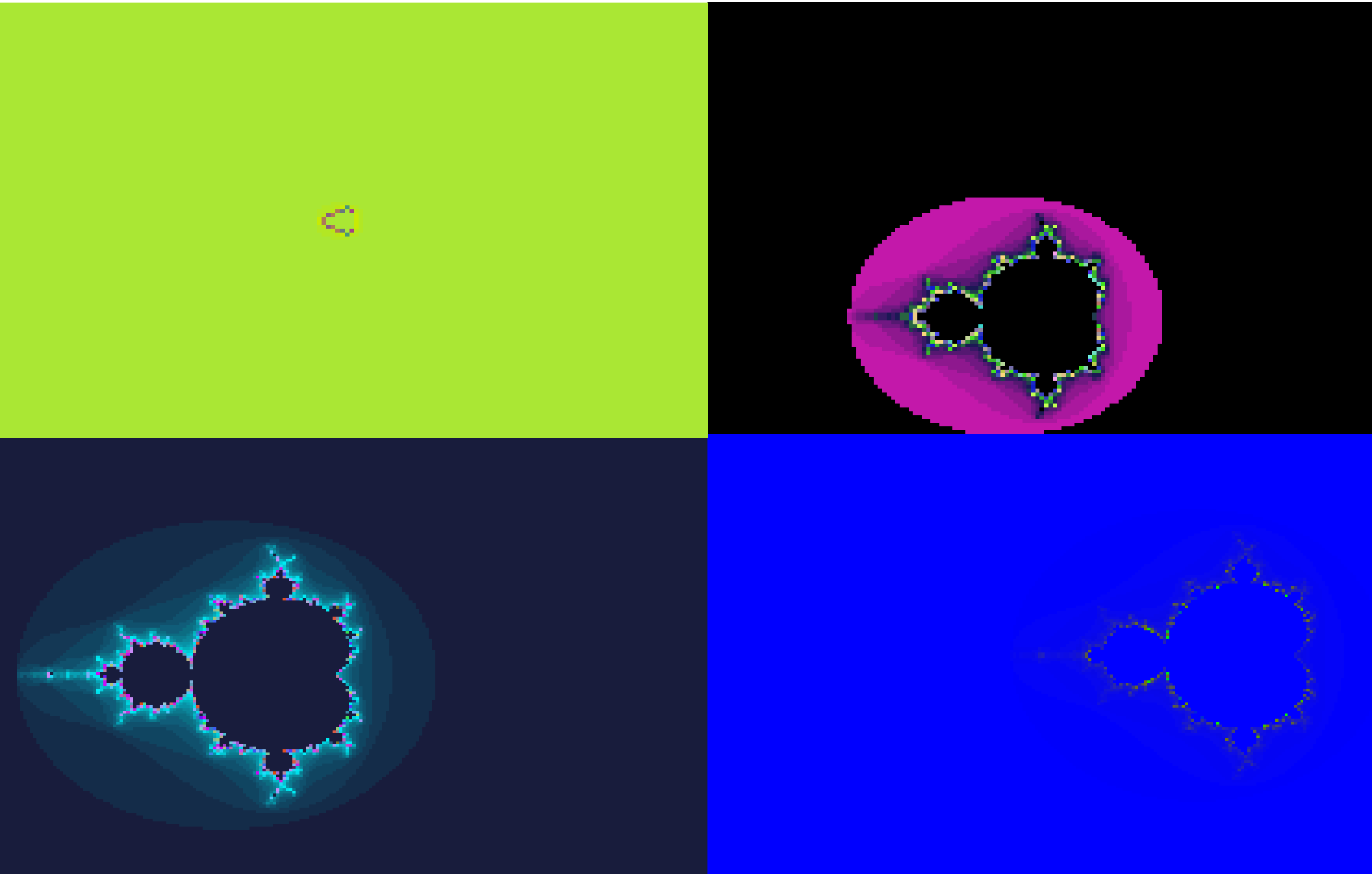
....*"Chaos" is common in "Smart Systems" and "Cyber Communities"*

Dynamic Duffing Equation: $\ddot{x} + \delta\dot{x} + \alpha x + \beta x^3 = \gamma \cos(\omega t)$ - Exhibits Chaotic Behaviour

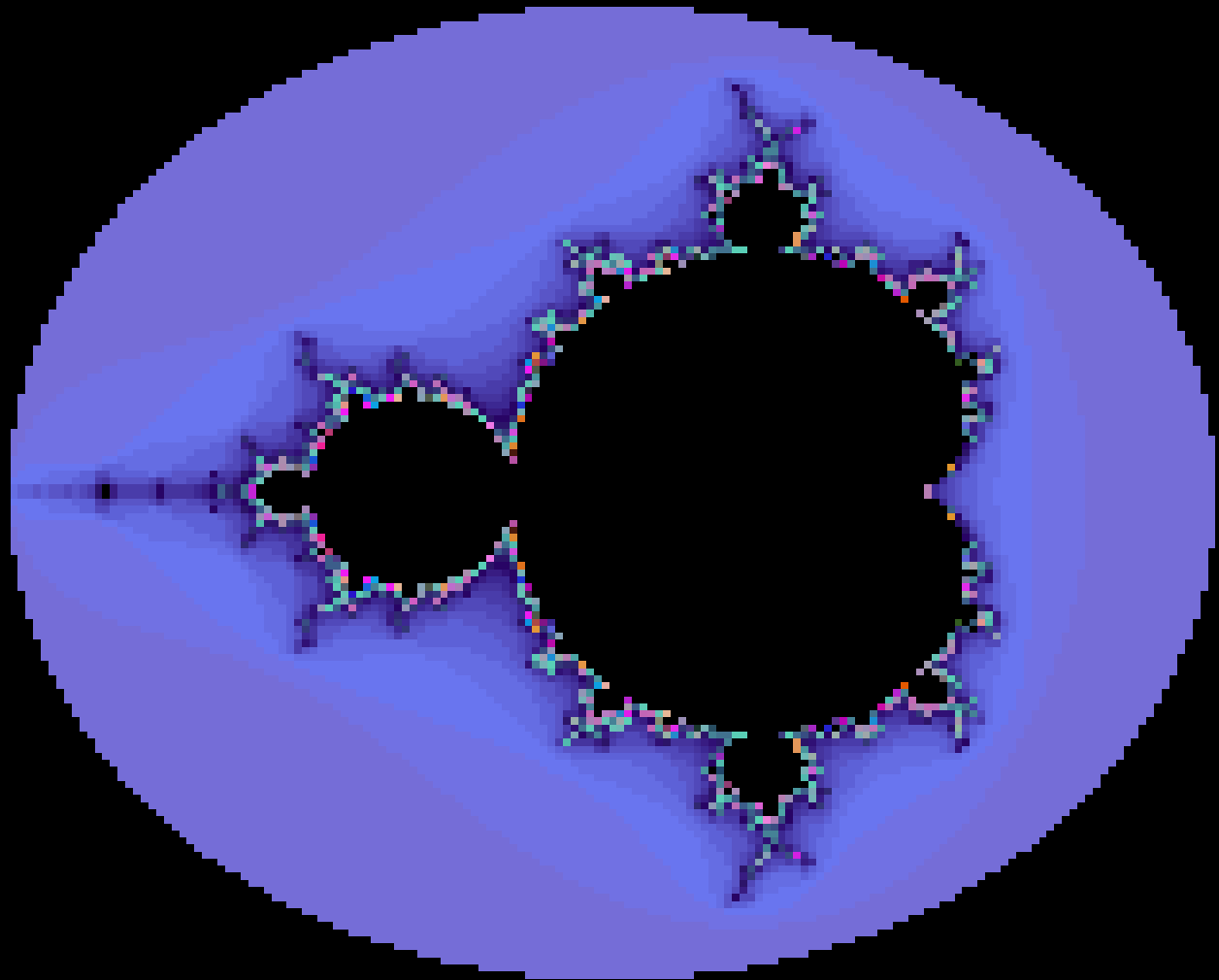


“Smart Scaling”: Fractal Mandelbrot Set

.....Fractal Scaling is frequently found in Nature.....



“Smart Scaling”: Fractal Mandelbrot Set



Cyber “Genes” for *Smart Systems*

- Intelligent Systems, either Artificial or Organic – Living Systems - are based on just a few shared common principles that include:
 - 1) ***Space-Time Awareness:*** Location (GPS) & Real-Time Clocks
 - 2) ***Learning, Adaptation & Self-Organisation:*** Real-Time Intelligence
 - 3) ***Massive Memory & Storage:*** Local & Remote Cloud Storage
 - 4) ***Sustainable Security :*** Embedded Smart Security – *Everywhere!*
 - 5) ***Scalable Networked Architecture:*** Smart Architectures will need to scale in space & time from micro cells to macro solutions
 - 6) ***Decision Focus:*** “Knowledge Lens” for Data Mining & “Big Data” from Social Networks, Search & On-Line Commerce
 - 7) ***Systems Integration:*** Cyber and Physical Solutions & Operations

.....*Advanced ICT Solutions now provide ALL these “Genetic” Functions which will enable us to design **Smart Cyber-Physical Security Solutions***

Smart Decision Principles - “D-Genes”

- **Business Decisions** require focusing & filtering of Big Data sources in Space-Time to create local knowledge (Data Mining). Hence a useful metaphor is the “Knowledge Lens”:
 - Smart Decision “Genes” = Space, Time and Information Focus
 - Conceptual “Knowledge Lens” can filter and focus information in “Space” from searching Big Data Sets to a Small focused Short-List
 - The “Knowledge Lens” can focus information & present in real-time, possibly as an stream of multi-media news or market intelligence
- **“Knowledge Lens”**: This concept can be a useful architectural principle in the design of *smart security*, smart business & smart governance

....21stC Cyber Attacks (such as Denial of Service) occur in real-time @Optical Speeds via worldwide proxy servers, so ultra fast analysis, decisions and action is a must!



Smart Learning Principles - “L-Genes”

- **Smart Learning** requires: Self-Organisation, Adaptation, Memory and Scalable Architecture. The Decision “Genes” are relatively traditional whilst these new Learning “Genes” lie at the heart of Smart Security.
 - **Self-Organisation** & Adaptation are essential principles of living systems and communities which include the well known self-organisation of insect roles in communities such as ants & bees.
 - **Cellular Automata** demonstrate relatively complex behaviour from simple mathematical rules, as in Conway’s “Game of Life”
 - **Simple Dynamic Recursive Maps** such as $x \Rightarrow 4x(1-x)$ also result in complex chaotic behaviour as found in real world insect populations
 - **Scalable Architecture** is also an essential feature of both plants & animal life, and Mandelbrot’s theory of Fractal Curves provides vivid examples.
- **Current Trends:** Research into Learning, Self-Organisation & Adaptation remains extremely active in both ICT R&D Labs & Academic Institutions

“How to Build Smart Security Solutions?”

- Conceptually - Smart Solutions all use combinations of these basic ICT “genes” shared with Intelligent Living Systems:
 - 1) **Hybrid Organisation:** Hierarchical (Pyramid) & Organic (Networked)
 - 2) **Smart Decision Principles (D-Genes):** Space, Time and Focus
 - 3) **Smart Learning Principles (L-Genes):** Memory, Scaling & Adaptation
 - 4) **Smart Solutions & Business Architecture:** Integration of the Decision + Learning “Genes”, within a Secure & Resilient Systems Environment

=> “SMART SECURE BUSINESS”!

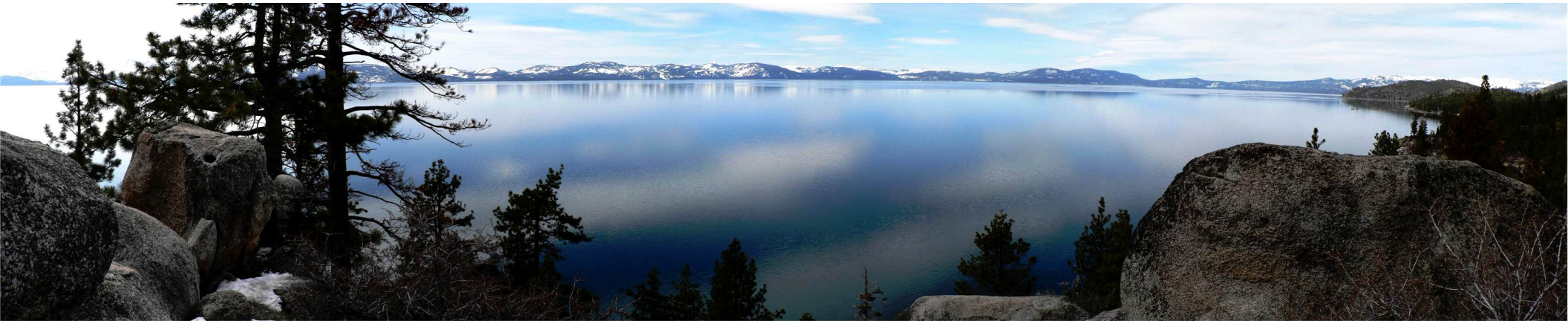


21stC Architectures for Smart Business Sectors

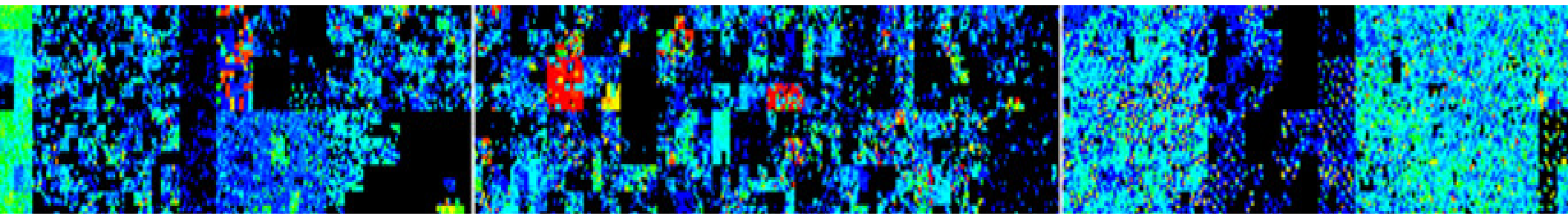
- We can also design new economic architectures using our Smart Design Principles & then customise sector by sector. We focus upon adaptation, scaling, massive data, & network transparency:
 - **Education & Research:** Transition from Monolithic to Niche Networks
 - **HealthCare & Social Welfare:** Telemedicine for towns & villages
 - **Banking & Finance:** “Real-Time” financial & commodity trading
 - **Transportation:** Smart Airports, Roads and Transportation Services
 - **ICT Infrastructure:** Launch 3G/4G Mobile Networks, and maximise Internet Services, Local Wireless Hubs & eGovernance across all supported Regions
 - **National Security & Defence:** Both for Physical Borders & CyberSpace
 - **Travel & Tourism:** Major opportunities for on-line bookings & marketing
 - **Energy & Utilities:** Secure Management of National Energy & Utility Grids
- *Tomorrow morning we'll explore the practical design requirements of Smart Security Solutions for Critical National Infrastructure (CNI)*



Smart Sustainable Cyber-Physical Security



1 – Background Perspectives	2 – Mapping Cyber Threats in Cyberspace	3 – Hybrid Cyber-Physical Security Threats
4 – Practical Models for Smart Security	5 – Transition to 21stC Smart Security	6 – Smart Security: Technology & Process
7 – Integrating Cyber & Physical Security	8 – Towards Smart “ <i>Neural Society</i> ”	9 – Next Steps for Smart Security



Transition from 20thC to 21stC Smart Security

- **Cybersecurity 2015-2025:**

- 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

- **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:**

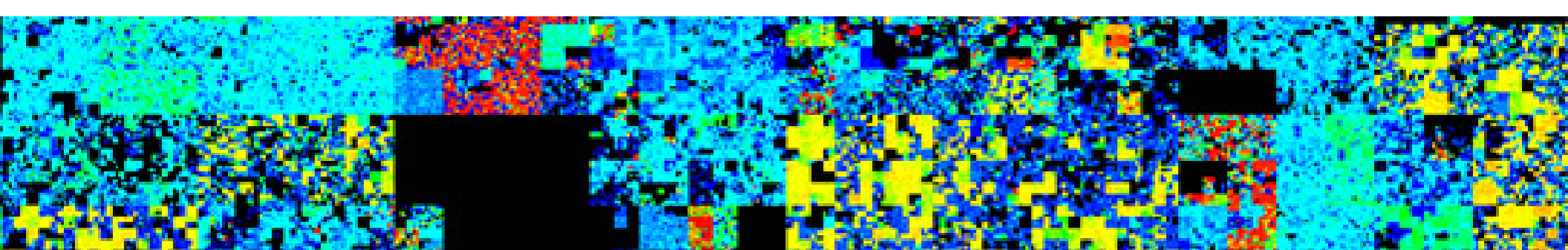
- Nations need to audit their critical infrastructure – government, banks, telecommunications, energy, & transport – and to upgrade to international cybersecurity standards based upon accepted “best practice” (ISO/IEC)



Smart Sustainable Cyber-Physical Security



1 – Background Perspectives	2 – Mapping Cyber Threats in Cyberspace	3 – Hybrid Cyber-Physical Security Threats
4 – Practical Models for Smart Security	5 – Transition to 21 st C Smart Security	6 – Smart Security: Technology & Process
7 – Integrating Cyber & Physical Security	8 – Towards Smart “Neural Society”	9 – Next Steps for Smart Security



Smart Security: *Integrating Cyber & Physical*

- **Dual Operations:** Security is often managed under separate management for physical building & personnel security and IT Computer & Network security. In addition, the risks are continuously evolving so an adaptive model is essential!
- **ISO Security Standards:** *Smart Sustainable Security* requires operational linkages & integration between cyber and physical security in order to meet current ISO 27xxx Security Standards, and to minimise risk of cyber attacks.
 - **Physical Security:** Buildings, People, National Borders, Government Ministries
 - **Cybersecurity:** Computers, Storage, Networks, Applications, Mobile Devices
- *“Smart Sustainable Security” will be discussed “in-depth” later within tomorrow’s session on Cybersecurity for Critical National Infrastructure (CNI)*



Cyber: Integrated Command & Control



- ***Security Operations Command Centre for Global Security Solutions Enterprise***

30th International East/West Security Conference

"Integrated Cyber-Physical Security for Governments and Business"

Paris, France – 13th & 14th October 2014

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



Physical: Integrated CCTV Surveillance



- ***CCTV Command and Control Operations Centre for Large UK City***

Emerging Physical & Cyber: National Operations Room: - US Transportation Security Administration (TSA) -



Computer Emergency Response Team (**CERT**)

Reactive Services



- + Alerts and Warnings
- + Incident Handling
 - Incident analysis
 - Incident response on site
 - Incident response support
 - Incident response coordination
- + Vulnerability Handling
 - Vulnerability analysis
 - Vulnerability response
 - Vulnerability response coordination
- + Artifact Handling
 - Artifact analysis
 - Artifact response
 - Artifact response coordination

Proactive Services



- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

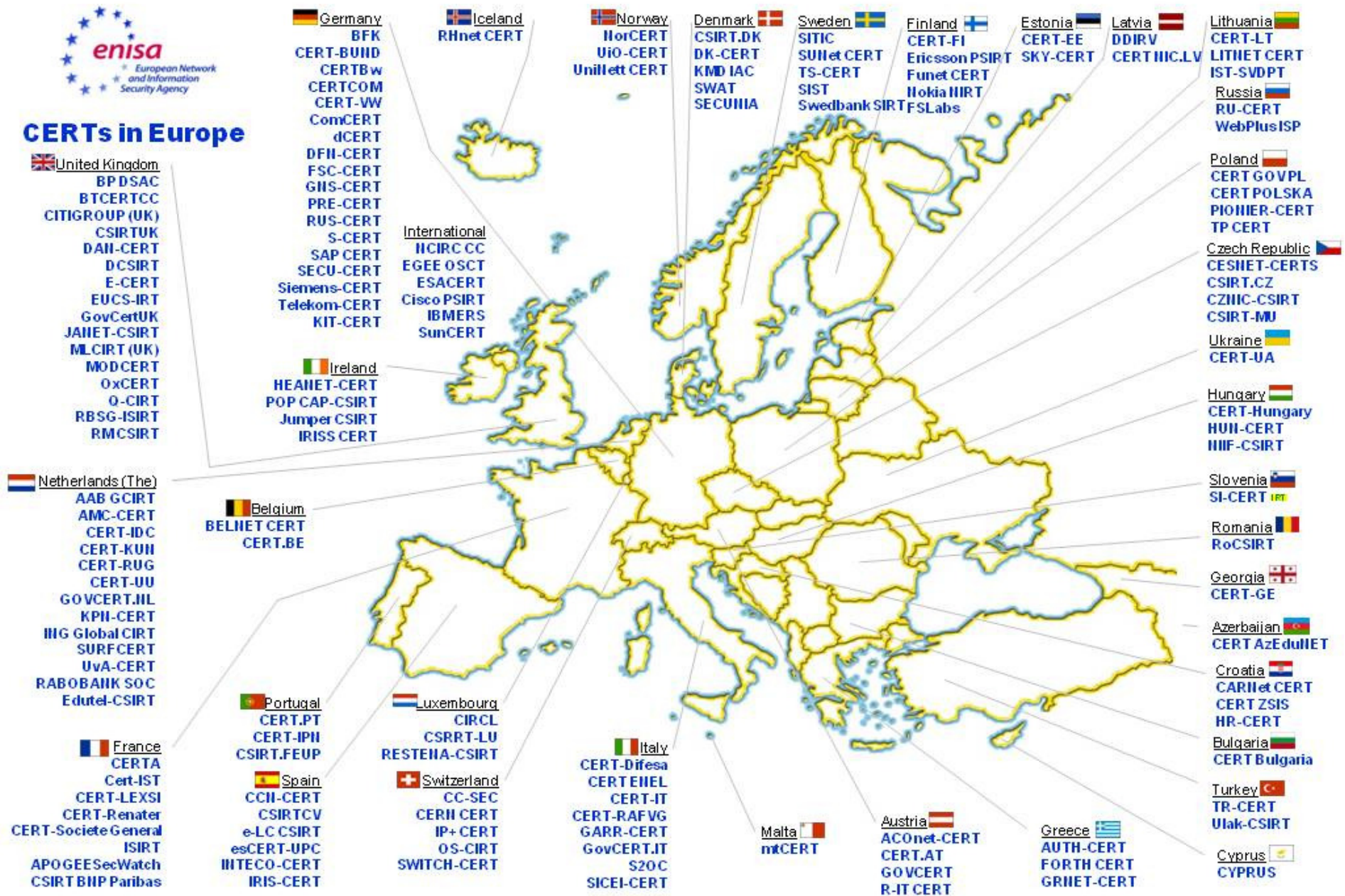
Security Quality Management Services



- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Also known as **CSIRT** : Computer Security Incident Response Team

ENISA: European *CERT* Network



CERTs in Europe map, June 2010 v2.0 <http://www.enisa.europa.eu/act/cert/background/inv> © European Network and Information Security Agency (ENISA)

ENISA: *CSIRT/CERT* Guidebook



A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT

Including examples and a checklist
in form of a project plan

Deliverable WP2006/5.1(CERT-D1/D2)

Index

1	Management Summary	2
2	Legal Notice	2
3	Acknowledgements	2
4	Introduction	3
4.1	TARGET AUDIENCE	4
4.2	HOW TO USE THIS DOCUMENT	4
4.3	CONVENTIONS USED IN THIS DOCUMENT	5
5	Overall strategy for planning and setting up a CSIRT	6
5.1	WHAT IS A CSIRT?	6
5.2	POSSIBLE SERVICES THAT A CSIRT CAN DELIVER	10
5.3	ANALYSIS OF THE CONSTITUENCY AND MISSION STATEMENT	12
6	Developing the Business Plan	18
6.1	DEFINING THE FINANCIAL MODEL	18
6.2	DEFINING THE ORGANISATIONAL STRUCTURE	20
6.3	HIRING THE RIGHT STAFF	24
6.4	UTILISATION AND EQUIPMENT OF THE OFFICE	26
6.5	DEVELOPING AN INFORMATION SECURITY POLICY	28
6.6	SEARCH FOR COOPERATION BETWEEN OTHER CSIRT'S AND POSSIBLE NATIONAL INITIATIVES	29
7	Promoting the Business Plan	31
7.1	DESCRIPTION OF BUSINESS PLANS AND MANAGEMENT TRIGGERS	33
8	Examples of operational and technical procedures (workflows)	36
8.1	ASSESS THE INSTALLATION BASE OF THE CONSTITUENCY	37
8.2	GENERATING ALERTS, WARNINGS AND ANNOUNCEMENTS	38
8.3	DOING INCIDENT HANDLING	45
8.4	EXAMPLE OF A RESPONSE TIMETABLE	51
8.5	AVAILABLE CSIRT TOOLING	52
9	CSIRT training	54
9.1	TRANSITS	54
9.2	CERT/CC	55
10	Exercise: producing an advisory	56
11	Conclusion	61
12	Description of the Project Plan	62
	APPENDIX	64
A.1	FURTHER READING	64
A.2	CSIRT SERVICES	65
A.3	THE EXAMPLES	74
A.4	SAMPLE MATERIAL FROM CSIRT COURSES	78



Designing “*Smart Security*” Operations

- 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 UN/ITU & ISO/IEC Standards:
 - **CERT:** Implementation of National, and Enterprise Computer Incident Response Teams (CERTs)
 - **C&C:** Integrated Command and Control Operations (including fail-over control rooms)
 - **BCP/DR:** Business Continuity & Disaster Recovery (for cybercrimes, terrorism & disasters)
 - **Forensics:** Integrated Digital Forensics, eCrime Unit & Cyber Legislation against Cybercrimes
 - **Access:** Traditional Physical Security Defences (including guards & perimeter fences)
-*Many criminal attacks happen through a penetrating combination of physical & cyber systems.*
- *Breaking into a physical building may allow a criminal to gain access to secure ICT zones*
-*Massive Data Files can be then easily downloaded to chips, phones or other storage drives*



***“Smart Analysis Tools”**: 3D Simulation Modelling for Security Crisis & Disaster Management*



30th International East/West Security Conference

**“Integrated Cyber-Physical Security for
Governments and Business”**

Paris, France – 13th & 14th October 2014

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



Summary of Physical Security & Operational Solutions

- **Networked Solutions:** Physical security and the Operational Solutions are increasingly based upon sophisticated electronic networked solutions, including biometrics, smart CCTV, intelligent fences, and RFID Access Devices
- **Convergence:** Operations for “Physical Security” and “Cybersecurity” will need to be slowly converged & integrated during the next few years both from a personnel, assets, resources and operational budget perspective
- **Security Benefits:** The benefits of integrating cyber and physical security are reduced running costs, reduced penetration risk, and increased early warning of potential attack whether from criminals, hackers or terrorists.

.....Next we'll consider the integration of physical and cybersecurity in some more detail, including the modes of attack & overall benefits



Benefits of Integrated Cyber – Physical Security

- Some of the key benefits from integrating cybersecurity technology solutions with rigorous physical operational processes and policies are:

- *Reduced Operational Costs*, through “Single Security Organisation” under a CSO/CISO
- *Early Warning* of both Physical or Cyber Penetration through comprehensive surveillance
- *Extended Protection* of ALL Critical Physical and On-Line Assets
- *Focused Security Policy* for Government, Businesses and Citizens
- *Risks*: Reduced “Open World” Security Risks from Smart Mobile Devices ,“Apps” & Web2.0
- *CyberCrime*: Comprehensive Management and Control of National Cybercrime
- *CNI*: Critical Infrastructure such as Banks, Power Stations and Airports are better protected
- *National Defence*: Countries now need to be 100% protected both in physical & cyberspace

....In summary, the practical 21st approach to *integrated “smart” security* is a combination of *technological* solutions together with rigorously enforced *operational* procedures, all implemented to recognised international security standards such as those of the UN/ITU and ISO/IEC

....Later we will consider these UN/ITU & ISO/IEC cybersecurity standards in more depth, and also discuss specific organisational models for National Cybersecurity Agencies and eCrime Units



Smart Security Benefits: *Business & Government*

- Improvements in integrated “smart” security will provide significant benefits to National Governments, Business & 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 cyber attacks 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 SCADA control systems
 - **Telecommunications:** Top security of government communications with alternative routings, encryption & protection against cyber attack



- Smart Sustainable Security in the Wild! -



The Sociable Weaver Bird

"World's largest Bird Nests"

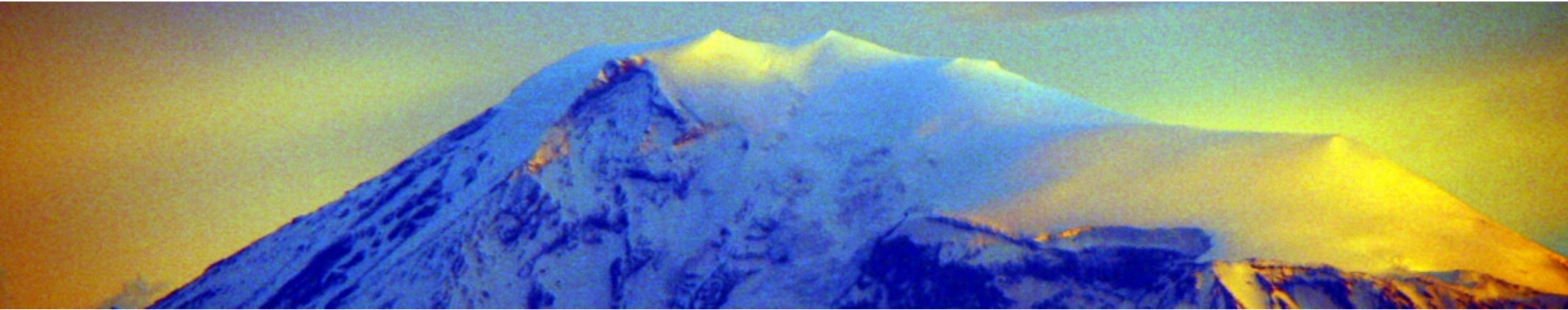
*** Southern Africa ***



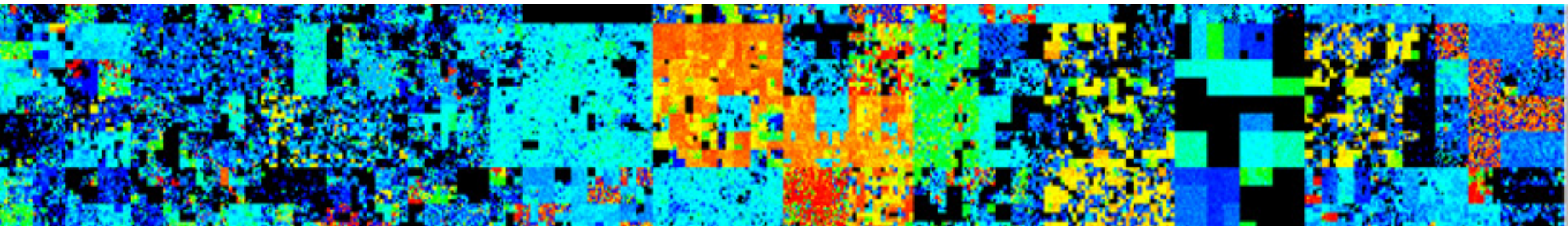
- Secure Living Community
- Self-Organising Architecture
- Fully scalable for long term growth
- Supports 250+ Weaver Birds
- Real-Time Disaster Alert System
- Sustainable in Semi-Desert Steppe
- Robust against "Enemy Risks" such as Eagles, Vultures & Snakes

...all the features of a 21stC-"Cyber Defence Centre"-including Disaster Recovery & Business Continuity!

Smart Sustainable Cyber-Physical Security



1 – Background Perspectives	2 – Mapping Cyber Threats in Cyberspace	3 – Hybrid Cyber-Physical Security Threats
4 – Practical Models for Smart Security	5 – Transition to 21 st C Smart Security	6 – Smart Security: Technology & Process
7 – Integrating Cyber & Physical Security	8 – Towards Smart “Neural Society”	9 – Next Steps for Smart Security



Cyber Integration with *Physical Security Operations*

- Cybersecurity for Government, Business & Critical Service Sectors should be tightly integrated with operational physical security solutions including:
 - 1) Advanced CCTV Camera Surveillance of the Secure Government & Critical Facilities
 - 2) Exterior ANPR (Automatic Number Plate Recognition) Systems for Car Parking & Entrances
 - 3) Integration of the Cyber CERT/CSIRT with physical CCTV & Alarm Control Centres
 - 4) Personnel RFID and/or biometrics office & campus access controls
 - 5) Professionally trained security personnel & guards – 24/7 – for top security facilities
 - 6) Implemented facility security policy for staff, visitors and contractors
 - 7) Intelligent perimeter security controls for campuses and critical service facilities such as airports, power stations, refineries, military bases, hospitals and government institutions
 - 8) On-Line Audit trails and Electronic Log-Files for secure Physical Facilities
 - 9) Focus upon in-depth physical security for computer server rooms, data storage & archives

*.....All critical information infrastructures on multi-building campus sites such as airports, universities, hospitals, military bases, leisure resorts & government agencies require
“Integrated Cyber-Physical Security Operations” = “SMART SECURITY”*



Physical Security & Surveillance Solutions

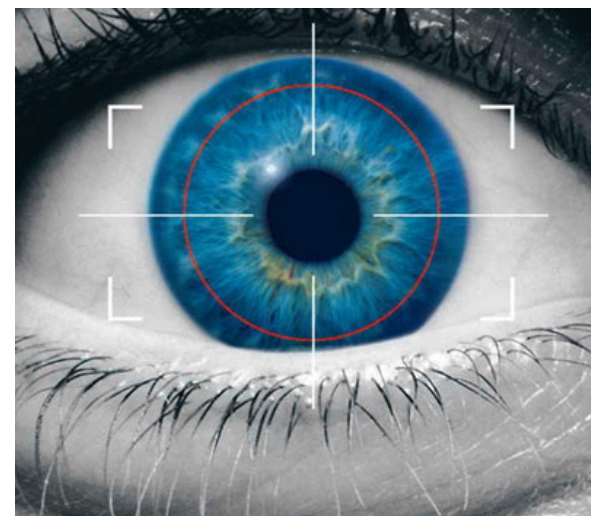
- The comprehensive security of electronic information, data and assets also requires corresponding upgrades in the physical & operational security for the offices, facilities and ICT server & storage rooms:
 - *Reception, Facility and Office Access* for Staff, Contractors and Visitors
 - *Advanced Smart Perimeter Management* for Campus Sites, Airports & Bases
 - *Integrated CCTV/ANPR* Intelligence Surveillance
 - *Biometrics and RFID* Identification for Personnel and Mobile Assets

*.....Traditionally physical security was managed independently from the ICT security.
However, many businesses & governments now understand that security is improved at
lower cost & risks through the integrated management of cyber & physical resources*



Biometrics and *RFID* Security Applications

- *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 shoplifting
 - 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



.....Both *Biometrics* and *RFID* Technology Solutions can be powerful tools against cybercrime

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

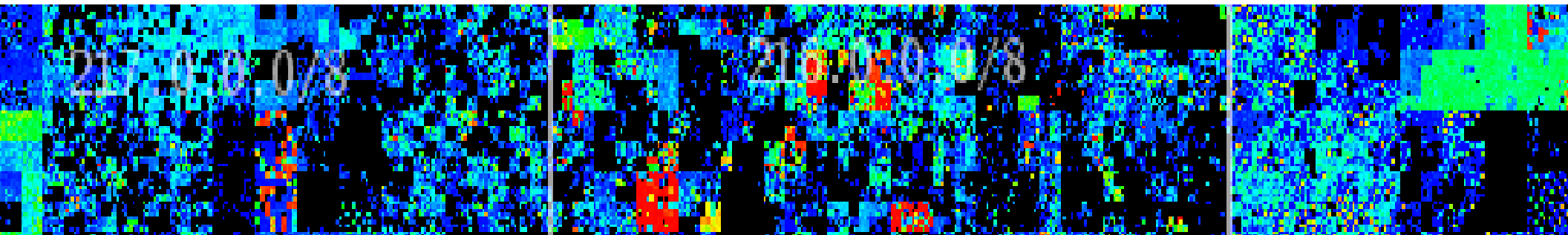
- **Compliance:** Investments in establishing and upgrading cybersecurity defences against cybercrime means that all physical security and associated operational staff should also be reviewed for compliance with policies, and audited to international standards
- **Integration:** Physical and Cybersecurity 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 YOUR National Economy & Enterprises



Smart Sustainable Cyber-Physical Security



1 – Background Perspectives	2 – Mapping Cyber Threats in Cyberspace	3 – Hybrid Cyber-Physical Security Threats
4 – Transition to 21 st C Sustainable Security	5 – Transition to 21 st C Smart Security	6 – Smart Security: Technology & Process
7 – Integrating Cyber & Physical Security	8 – Towards Smart “Neural Society”	9 – Next Steps for Smart Security



21stC Smart Security: *Towards “Neural Society”*

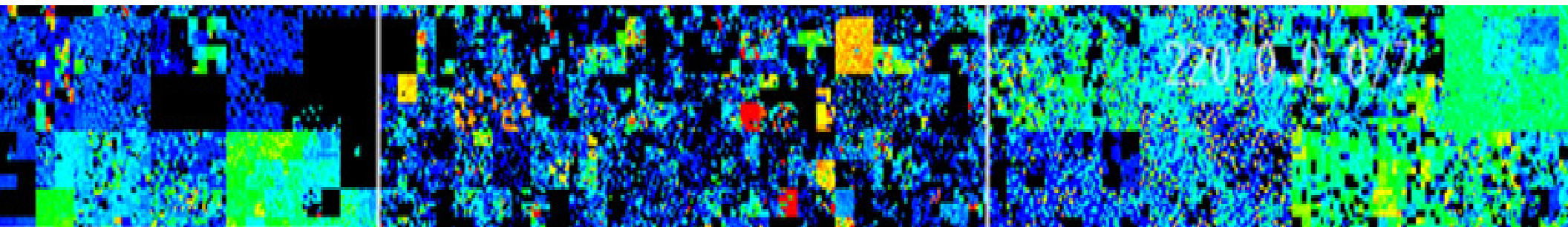
- ***Real-Time Security Operations:***
 - Secure and monitor every cyber asset and critical physical asset through IP Networking, RFID Tagging & communication of status to operations centre
- ***Augmented Reality:***
 - Multimedia virtual world overlays on data from the real physical world, through head-up 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



Smart Sustainable Cyber-Physical Security



1 – Background Perspectives	2 – Mapping Cyber Threats in Cyberspace	3 – Hybrid Cyber-Physical Security Threats
4 – Practical Models for Smart Security	5 – Transition to 21 st C Smart Security	6 - Smart Security: Technology & Process
7 – Integrating Cyber & Physical Security	8 – Towards Smart “ <i>Neural Society</i> ”	9 – Next Steps for Smart Security



Integrated Cyber & Physical Security: ***“The Shopping List”*** ***...Smart Security for Business & Government is a Multi-Year Programme!***

- 1) **National Cybersecurity Agency:** Establishment of a CERT/CSIRT & National Government Cybersecurity Agency within the Government Ministries
- 2) **CNI:** Long Term Critical National Infrastructure Protection (CNI)
- 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:** Programme for Drafting and Enforcing Cyber Laws, Policies & Regulations

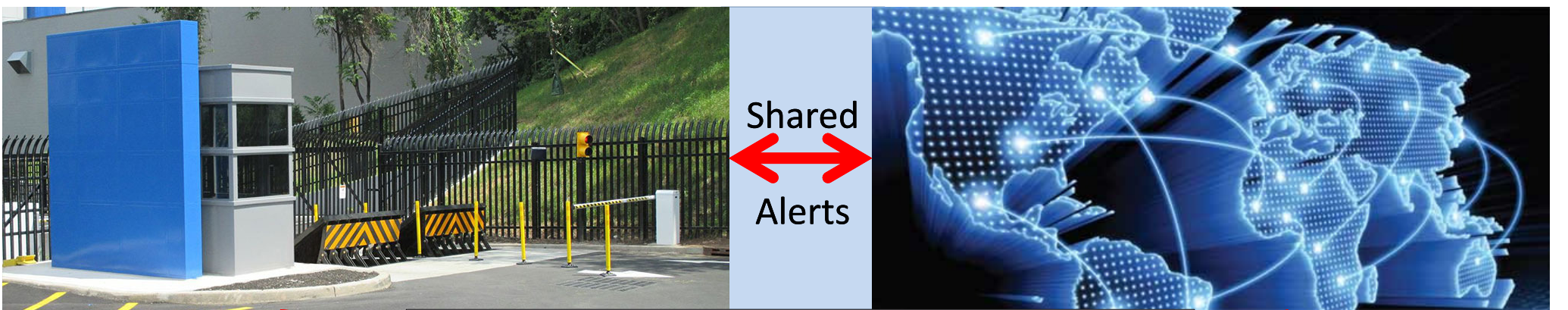
*.....It is also important to develop an in-depth economic **“Cost-Benefit”** analysis and Business Case in order to evaluate the **“Return on Investment”** for Smart Security*

Virtual Integration of Physical and Cyber Security

Integrated CSO-led Management Team – *Merged HQ Operations*

Physical Security Operations

Cyber Security Operations



Smart Security = Virtual Integration

Corporate CSO-led Security Team
ONE – Shopping List!



Integrated Management,
Training, Standards, Plans
ONE – Architecture!

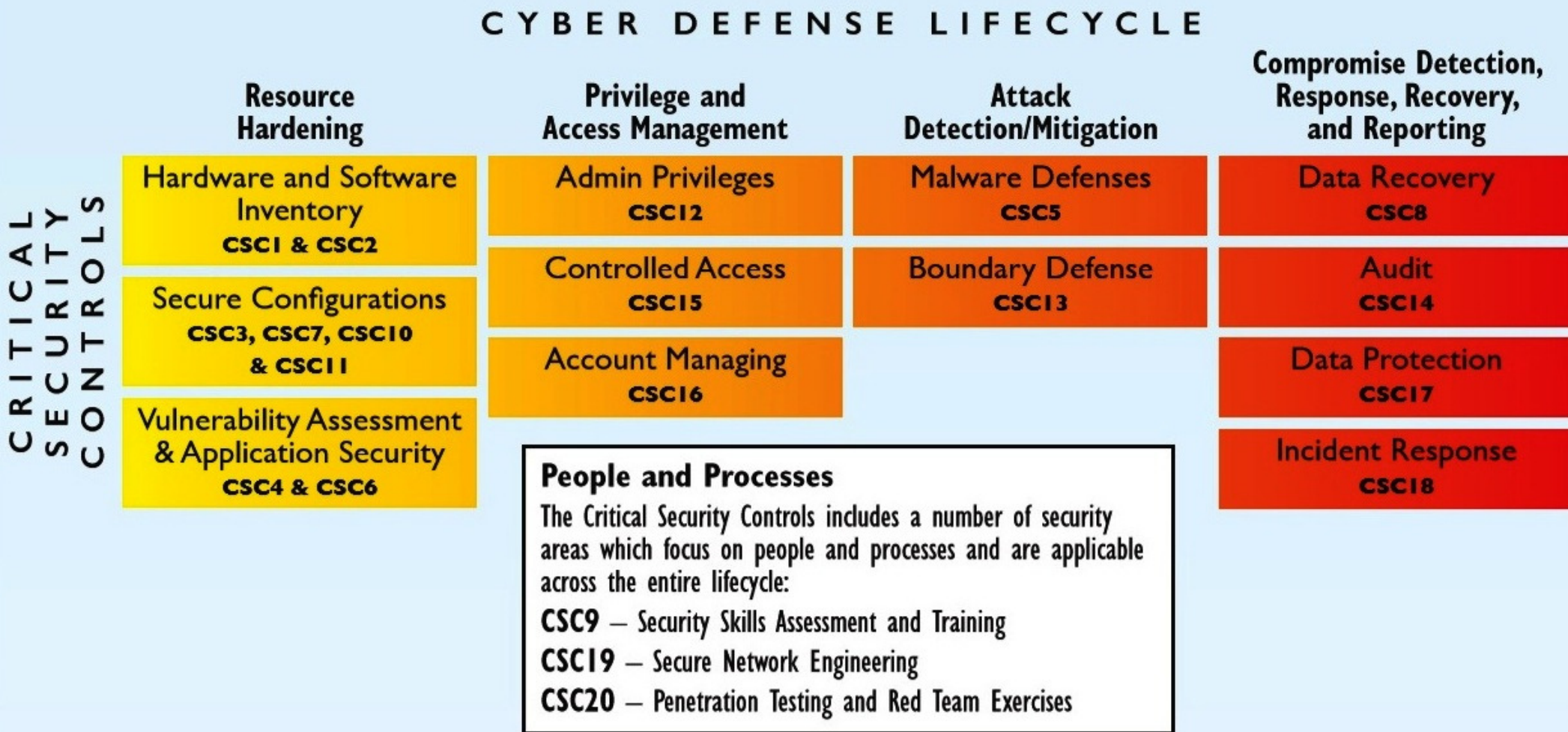
Final phase of *Cyber-Physical Integration* - Embedded Intelligence in ALL Devices - *Internet of Things*



Critical Security Controls (CSC)

Mapping the Controls Across the Cyber Defense Lifecycle

The Critical Controls provide high value across different stages of the typical “Prevent/Detect/Respond” cybersecurity lifecycle. SANS has created a mapping allocating the Controls across four phases:



SANS = SysAdmin, Audit, Networking and Security

Link: www.sans.org/critical-security-controls/

30th International East/West Security Conference

“Integrated Cyber-Physical Security for Governments and Business”

Paris, France – 13th & 14th October 2014

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



“Cyber – Physical Security Operations”

Convergence to Smart Resilient Security Solutions

- **IP Networks:** Physical security and associated Operational Solutions are increasingly based upon sophisticated electronic networked solutions, including biometrics, smart CCTV, intelligent perimeter fences, embedded active & passive RFID Devices and networked real-time sensors
- **Convergence:** CSO-led Management operations for “Physical Security” and “Cybersecurity” will steadily converge & become integrated during the next few years from staff, assets, resources & operational budget perspectives = **“Smart Resilient Security”**
- **Smart Security in 3 Phases:** Cyber-Physical Security Integration will evolve over 5 -10 years
 - 1st Phase – *Virtual Operational Integration* - **CSO** managed Security Team
 - 2nd Phase – *Integrated Architectures* and Standards – **ONE** Cyber-Physical Model
 - 3rd Phase – *Embedded Intelligent Integration of ALL* Devices - Internet of Things
- **Business Benefits:** The benefits of integrating cyber and physical security for both Business and Governments are reduced running costs, reduced penetration risk, and increased early warning of co-ordinated cyber-physical security attacks, whether from criminals, hackers or terrorists.

.....the “*Cyber-Vardzia*” White Paper for Georgia discusses Cybersecurity and Physical security in some depth, as well as their convergence and integration!



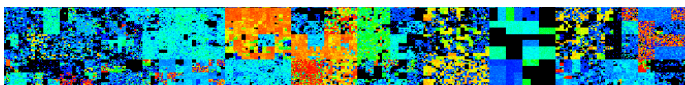
Case Study: White Paper: 21st C Georgia – “Cyber-Vardzia”

* 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

* 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 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.

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

Web Link : www.Valentina.net/vardzia/Georgia2010.pdf



Sunset on the Georgian - *Kakhetian Steppes*



“Integrated Cyber-Physical Security”

30th East-West Security Conference – Paris, France

Thank-You!...

Presentation Slides:

www.Valentina.net/East-West2014/

Presentation Slides:
www.Valentina.net/East-West2014/



Thank you for your time!

Professional Profile – *Dr David E. Probert*

- **Computer Integrated Telephony (CIT)** – Established and led British Telecom's £25M EIGER Project during the mid-1980s' to integrate computers with telephone switches (PABX's). This resulted in the successful development and launch of CIT software applications for telesales & telemarketing
- **Blueprint for Business Communities** – Visionary Programme for Digital Equipment Corporation during late-1980's that included the creation of the "knowledge lens" and "community networks". The Blueprint provided the strategic framework for Digital's Value-Added Networks Business
- **European Internet Business Group (EIBG)** – Established and led Digital Equipment Corporation's European Internet Group for 5 years. Projects included support for the national Internet infrastructure for countries across EMEA as well as major enterprise, government & educational Intranet deployments. Dr David Probert was a sponsoring member of the European Board for Academic & Research Networking (EARN/TERENA) for 7 years (1991 → 1998)
- **Supersonic Car (ThrustSSC)** – Worked with Richard Noble OBE, and the Mach One Club to set up and manage the 1st Multi-Media and e-Commerce Web-Site for the World's 1st Supersonic Car – ThrustSSC – for the World Speed Record. (Oct 1997), which still stands after 17 years!
- **Secure Wireless Networking** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.
- **Networked Enterprise Security** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 50+ professional engineers & a diverse portfolio of hi-tech networked security products across global markets.
- **Georgia** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament. Also appointed by the UN/ITU as expert for in-depth cybersecurity audit & roadmap.
- **Armenia** – Appointed by USAID/CAPS to develop eGovernance, eSecurity, eSociety Report, Roadmap & Action Plan which has since been implemented
- **UN/ITU** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

Dr David E. Probert is a Fellow of the Royal Statistical Society. He has a 1st Class Honours Degree in Mathematics (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata), and his full professional biography is featured in the Marquis Directory of Who's Who in the World: 2007-2015 Editions.

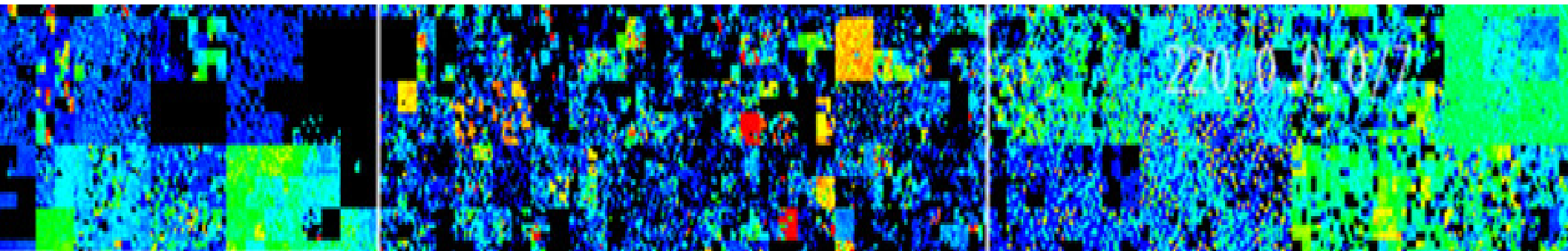


“Integrated Cyber-Physical Security”

30th East/West Security Conference – Paris, France



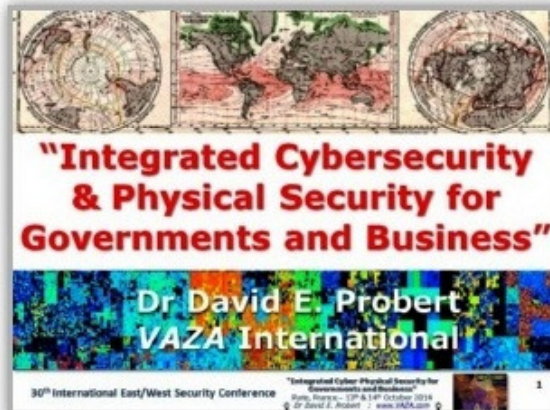
BACK-UP SLIDES



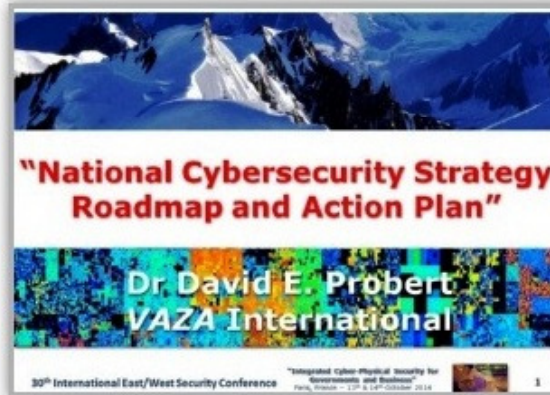
East-West Security Conference – Paris 2014

- *Cybersecurity Presentation Slides (PDF)* -

Smart Sustainable Security - "Theme Trilogy"



(1) Smart Security



(2) National Security



(3) Critical Security

Download Link: www.valentina.net/East-West2014/

Additional *Cybersecurity* Resources

"Master Class - Smart Theory & Practice"	"Master Class 2012 - Smart Design"	"21stC Armenia - 2012: Smart Economy"	"21stC Armenia - 2012: Smart Security"	"21stC Armenia: Smart Governance"
"Real-Time Armenia" - White Paper	"Real-Time Armenia" - Slides	Awesome Armenia: In Photos	Roadmap for Real-Time Armenia- Report	RoadMap for Real-Time Armenia- Slides
"Real-Time Georgia" - GITI 2008 Slides	"Real-Time Georgia" - GITI 2008 Paper	Gorgeous Georgia: In Photos	21stC Georgia: "CyberVardzia" - Paper	21stC Georgia - "CyberVardzia" - Slides
Jamaica: Cybersecurity Technology- Slides	Jamaica: Cybersecurity Strategy- Slides	"Short Professional Bio"	ITU/CITEL: Cybersecurity in the Americas	ITU/CITEL: Cybersecurity Skills Building

Link: www.valentina.net/vaza/CyberDocs

30th International East/West Security Conference

"Integrated Cyber-Physical Security for Governments and Business"

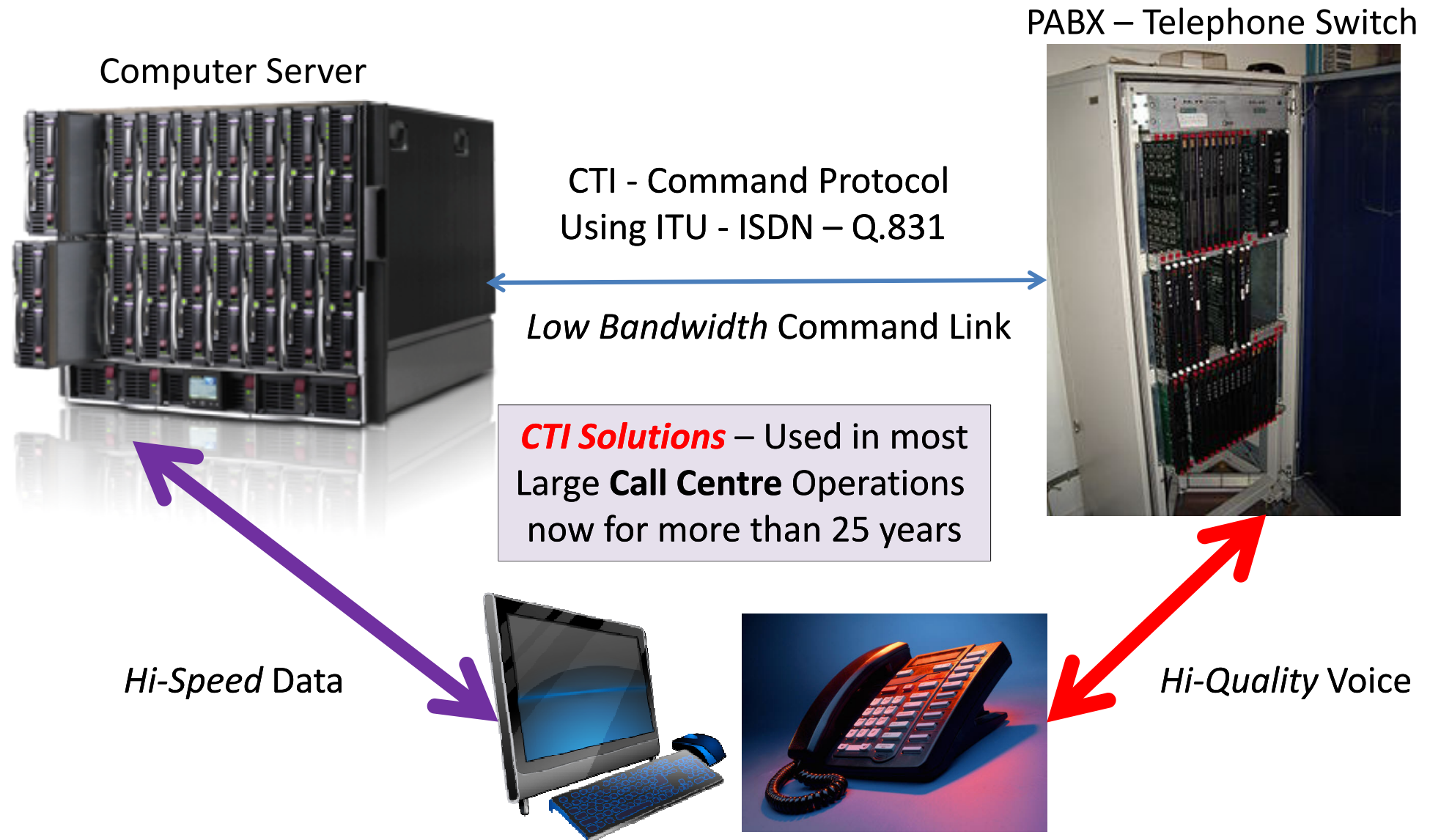
Paris, France – 13th & 14th October 2014

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



Computer Telephony Integration (CTI):

Virtual Integration of Voice-Data via Command Protocol Link



Smart Sustainable Security: Armenia's Coat of Arms

-A Conceptual View of Cyber-Physical Integration-

Cyber World = Eagle
(Artaxiad & Arsacid)



Physical World = Lion
(Bagratuni & Rubenid)

"Eagle flies in the Clouds!"

"Lion hunts on the Land"

Smart Security = Eagle and Lion working TOGETHER!