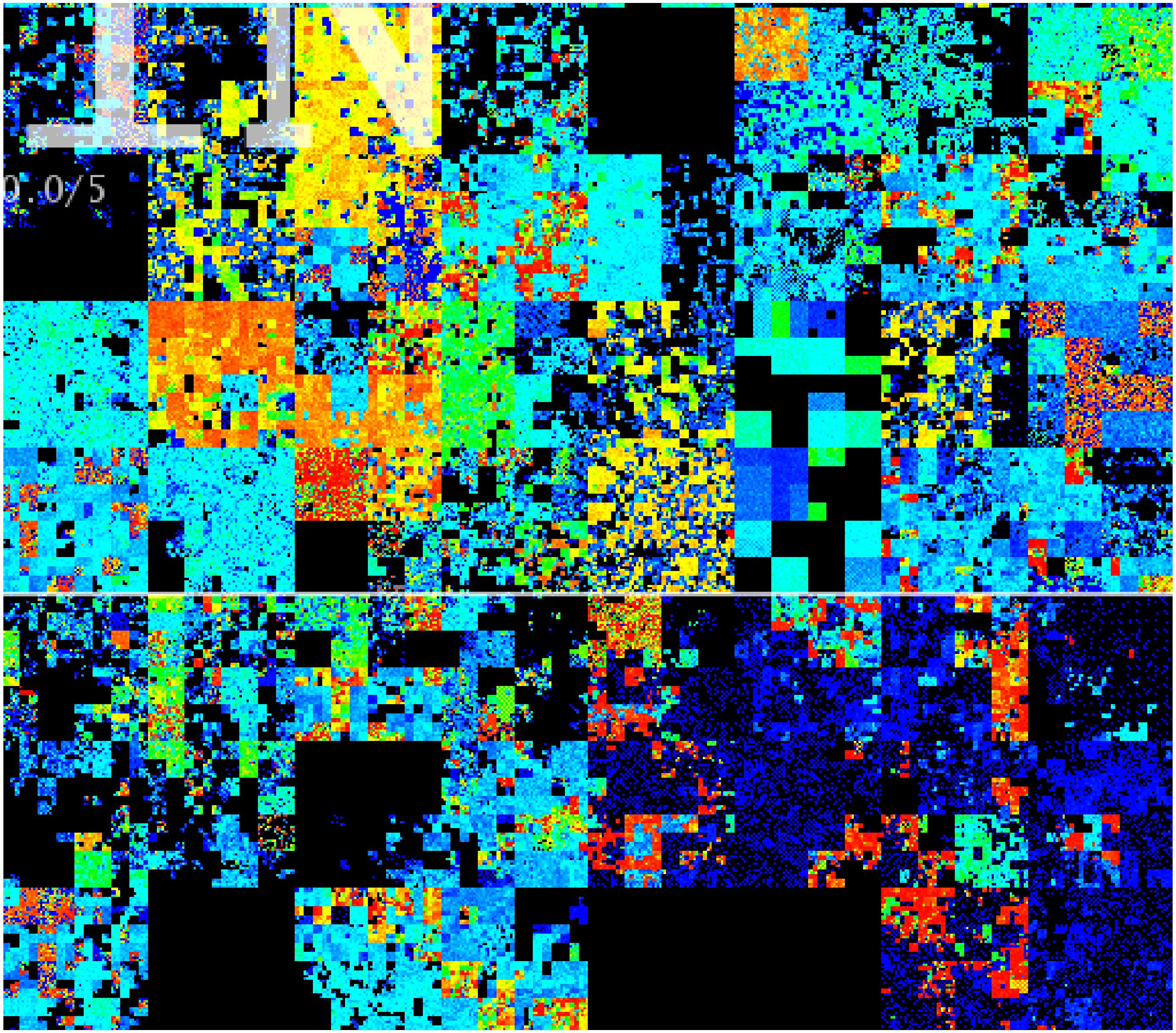
- Smart Sustainable Security -

“Integrating Cyber & Physical Operations”

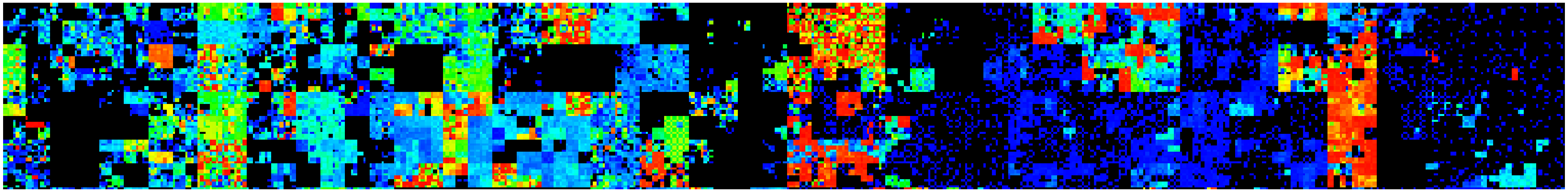
Dr David E. Probert
VAZA International

…or the Challenging Complexity of Securing Armenian Cyberspace!…



Smart Sustainable Security for 21stC Armenia

1 – Background Perspectives	**2 – Global Cybersecurity Challenge**	**3 – Cybersecurity Case Studies**
4 – Transition to 21stC Sustainable Security	**5 – Smart Security: Technology & Process**	**6 – Securing Critical National Infrastructure**
7 – Integration: Cyber & Physical Security	**8 – Towards Smart *"Neural Society"***	**9 – Next Steps for Securing 21stC Armenia**



Background Aims & Perspectives

- ***Smart Security Trends: 2002 – 2012***
  - Smart Security & Cybersecurity have really only become mainstream markets during the last 10 years with the evolution of Web2.0. Back in the 1990s there were some niche solutions for Web1.0 with Firewalls & Anti-Virus Tools, but now cybercrime has become a global threat that all countries & enterprises must ensure protection!

- ***Presentation Context:***
  - The author has been actively involved with Cybersecurity since the early 1990s, including projects across Europe, Middle East , Armenia, Georgia & the Americas, So this presentation is a personal perspective that focuses upon case studies & *"smart security".*

- ***The Future 2012+***
  - No system can ever be 100% secure either in physical or cyber space, so I propose the concept of "Smart Sustainable Security" in which the security investment is made in order to ensure *"sustainable"* & *"continuous"* enterprise & government operations

…The "Smart Economy" & "Smart Governance" are both ultimately dependant upon the integrated security of operations & services.

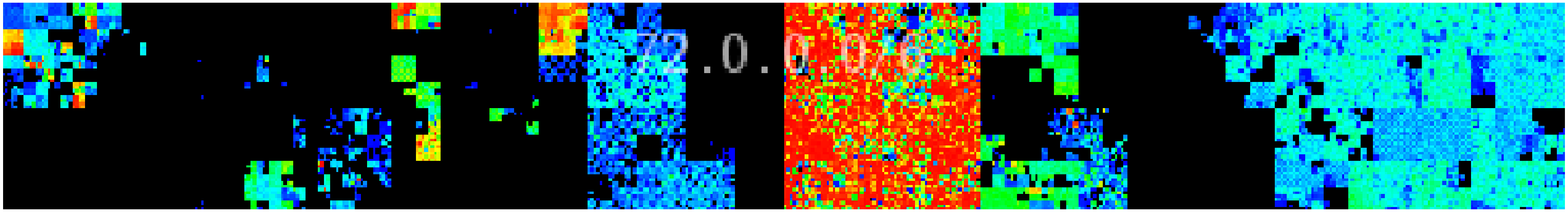
Cyber Threat Challenges for *Armenia*

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

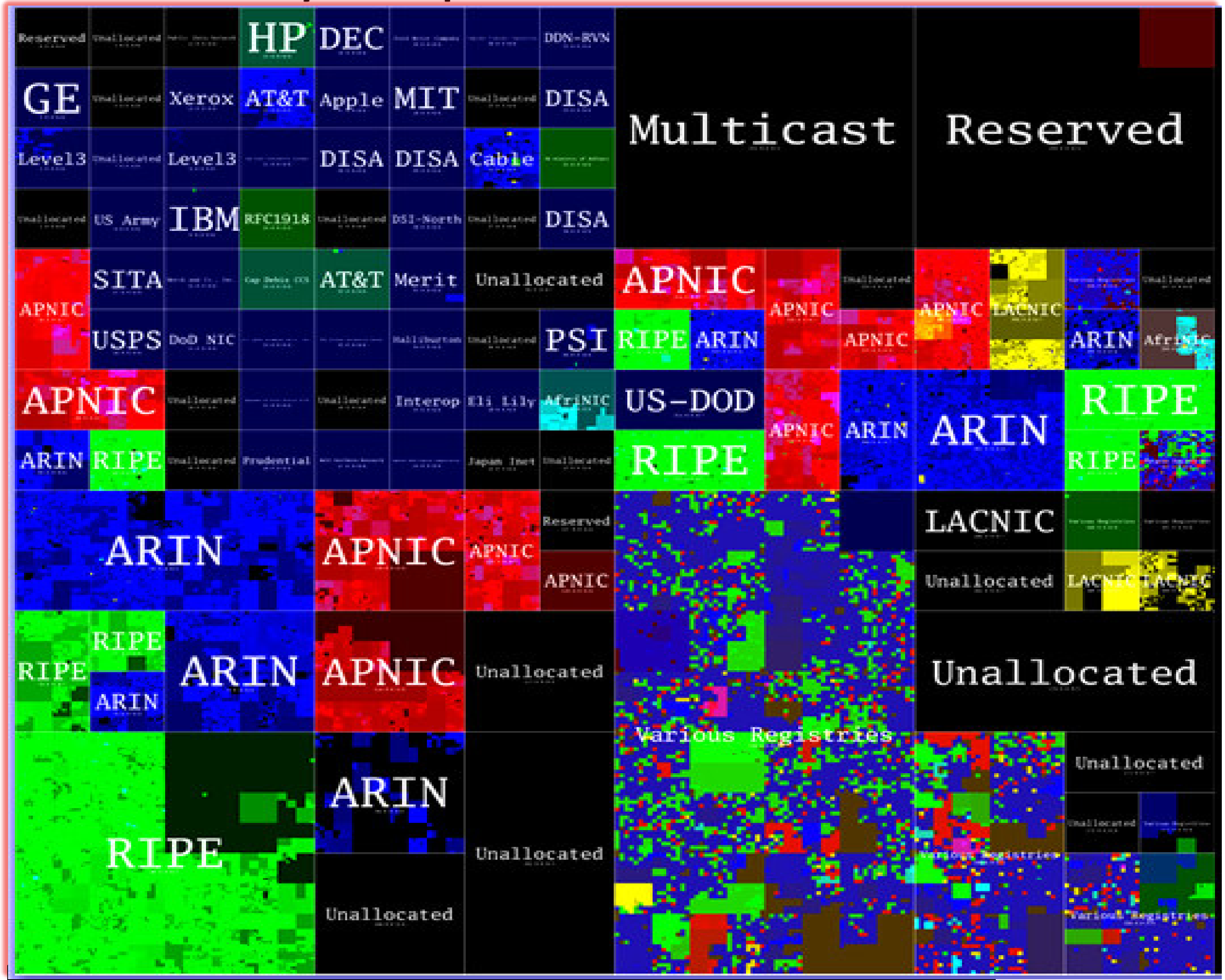
……New Cyber Threats will emerge as ICT solutions grow smarter!

Smart Sustainable Security for 21stC Armenia

1 – Background Perspectives	**2 – Global Cybersecurity Challenge**	**3 – Cybersecurity Case Studies**
4 – Transition to 21st C Sustainable Security	**5 – Smart Security: Technology & Process**	**6 – Securing Critical National Infrastructure**
7 – Integration: Cyber and Physical Security	**8 – Towards Smart *"Neural Society"***	**9 – Next Steps for Securing 21stC Armenia**



"Visualisation of Cyberspace": *Global IP "WHOIS" Addresses*

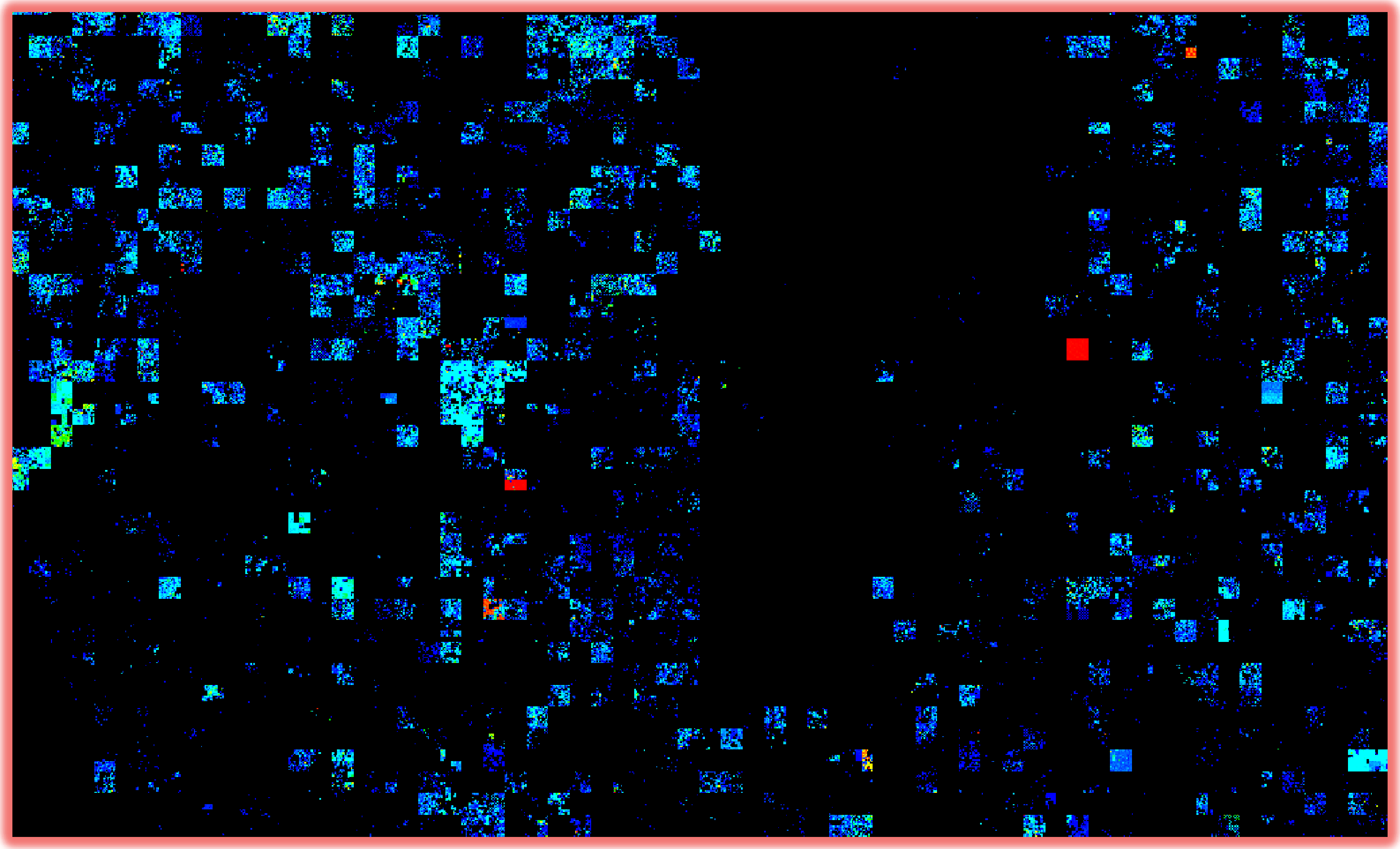


...From 20thC Physical World To 21stC Cyberspace! ...

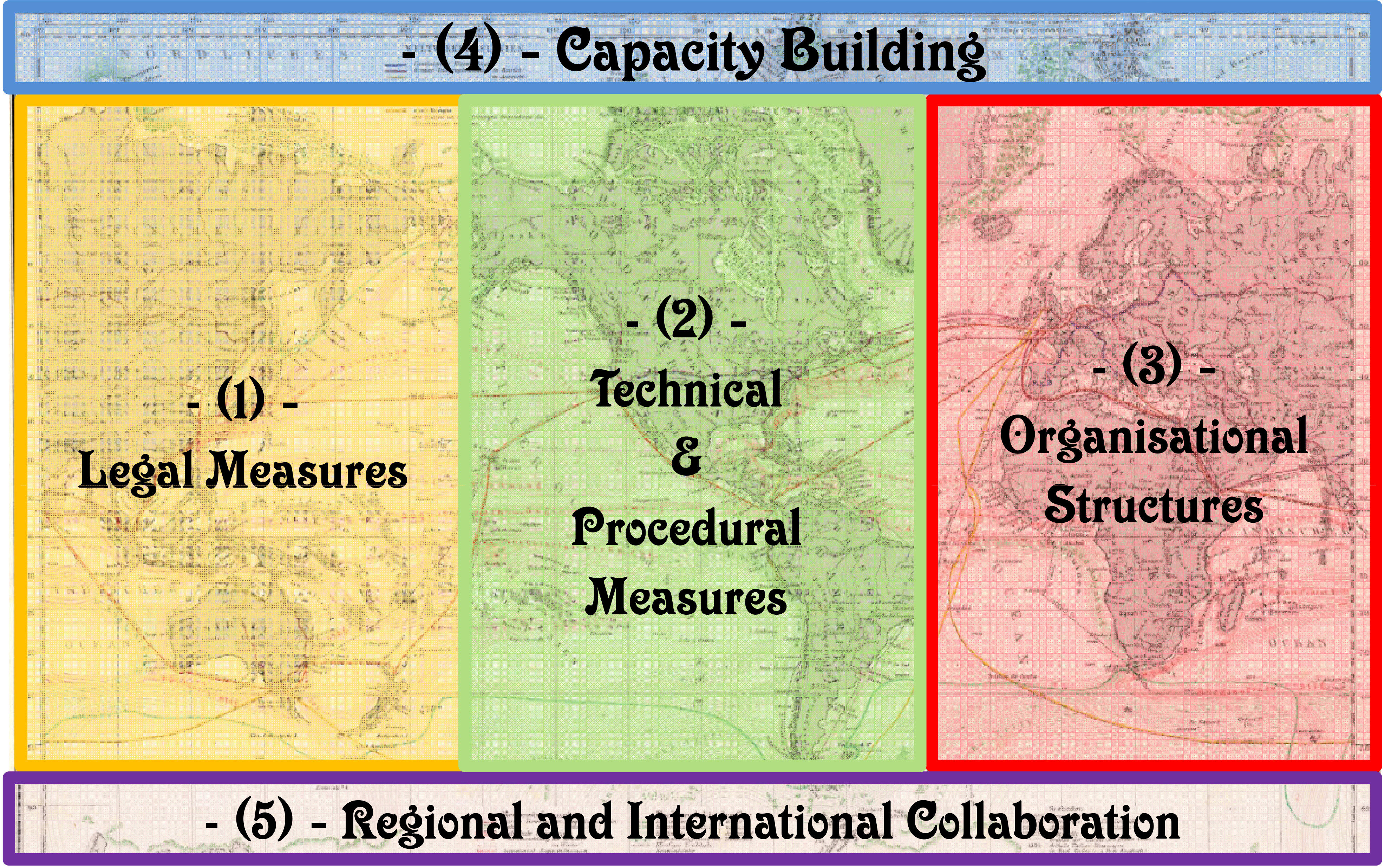
Active Internet Domains: *"American IP Registry"*

ARIN
64.0.0.0/5

"Outer Galaxies of Cyberspace" – *Other IP Registries*



- Worldwide Smart Security in Cyberspace! -



- (4) - Capacity Building

- (1) - Legal Measures

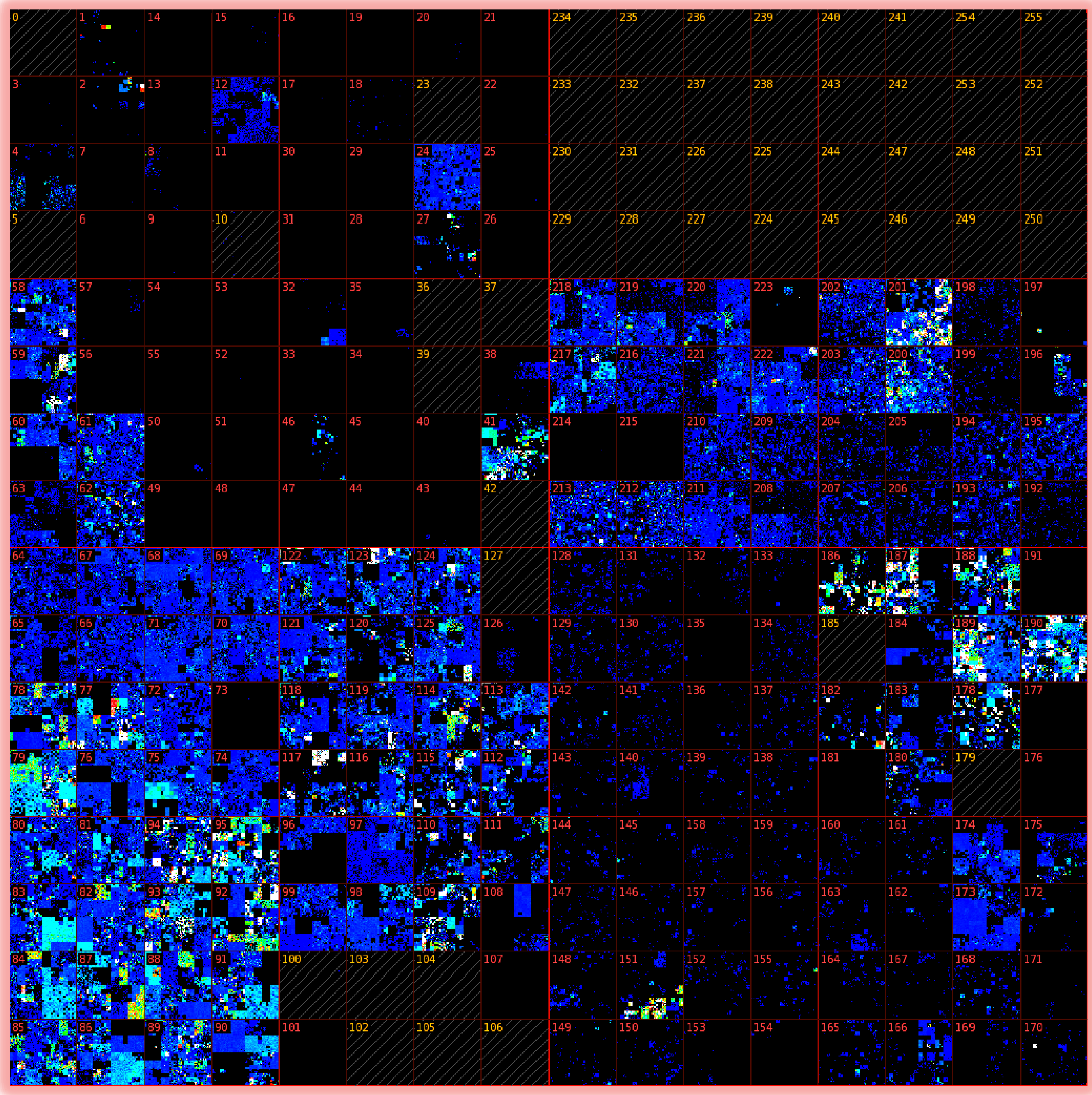
- (2) - Technical & Procedural Measures

- (3) - Organisational Structures

- (5) - Regional and International Collaboration

United Nations/International Telecommunications Union: *"Global Cybersecurity Agenda"*

Malicious Cybercrime Activity in Global IP Cyberspace



Key: Hilbert Space-Filling Curve Process

Link: www.team-cymru.org

Cyber Attack using Global Botnets

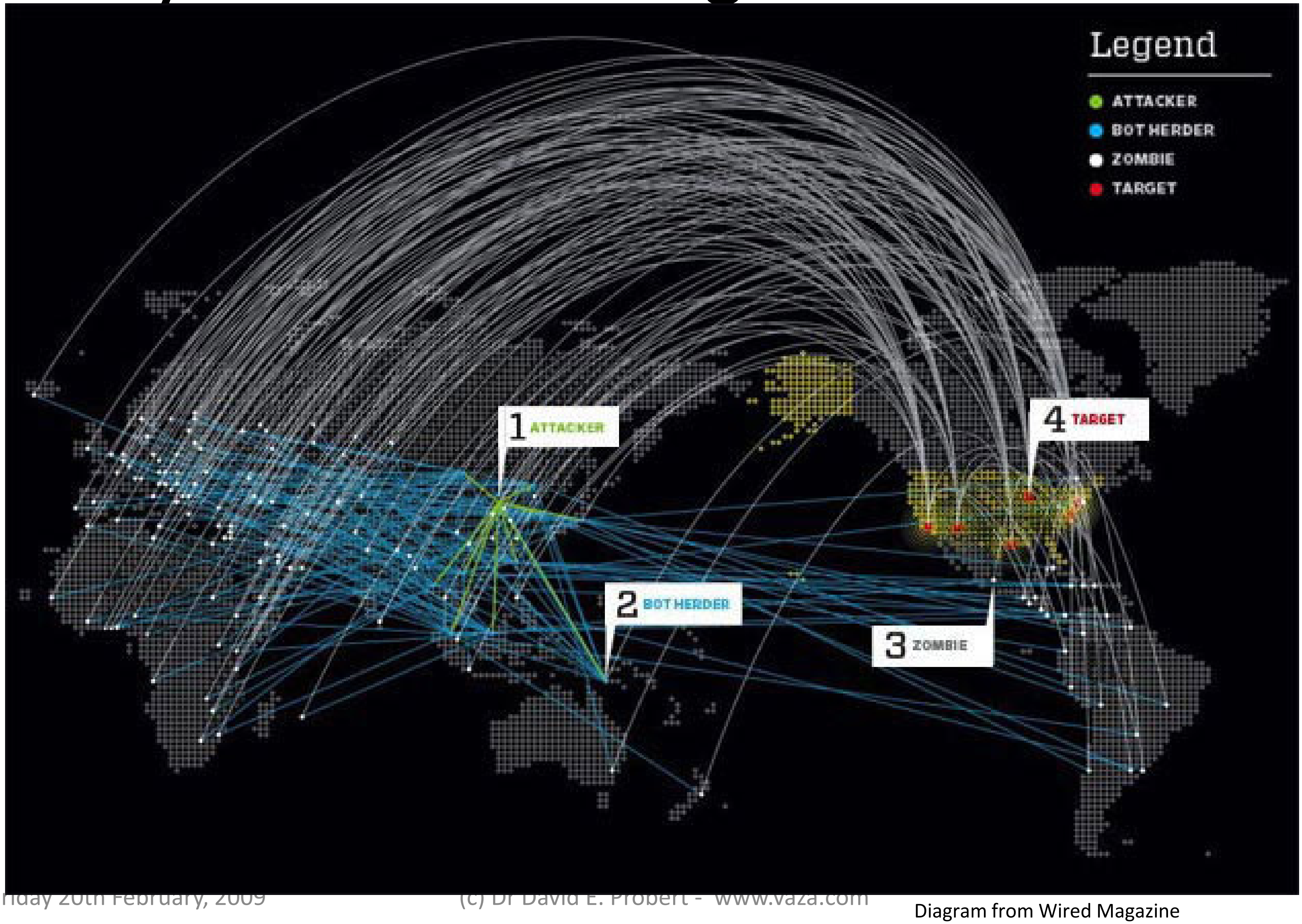
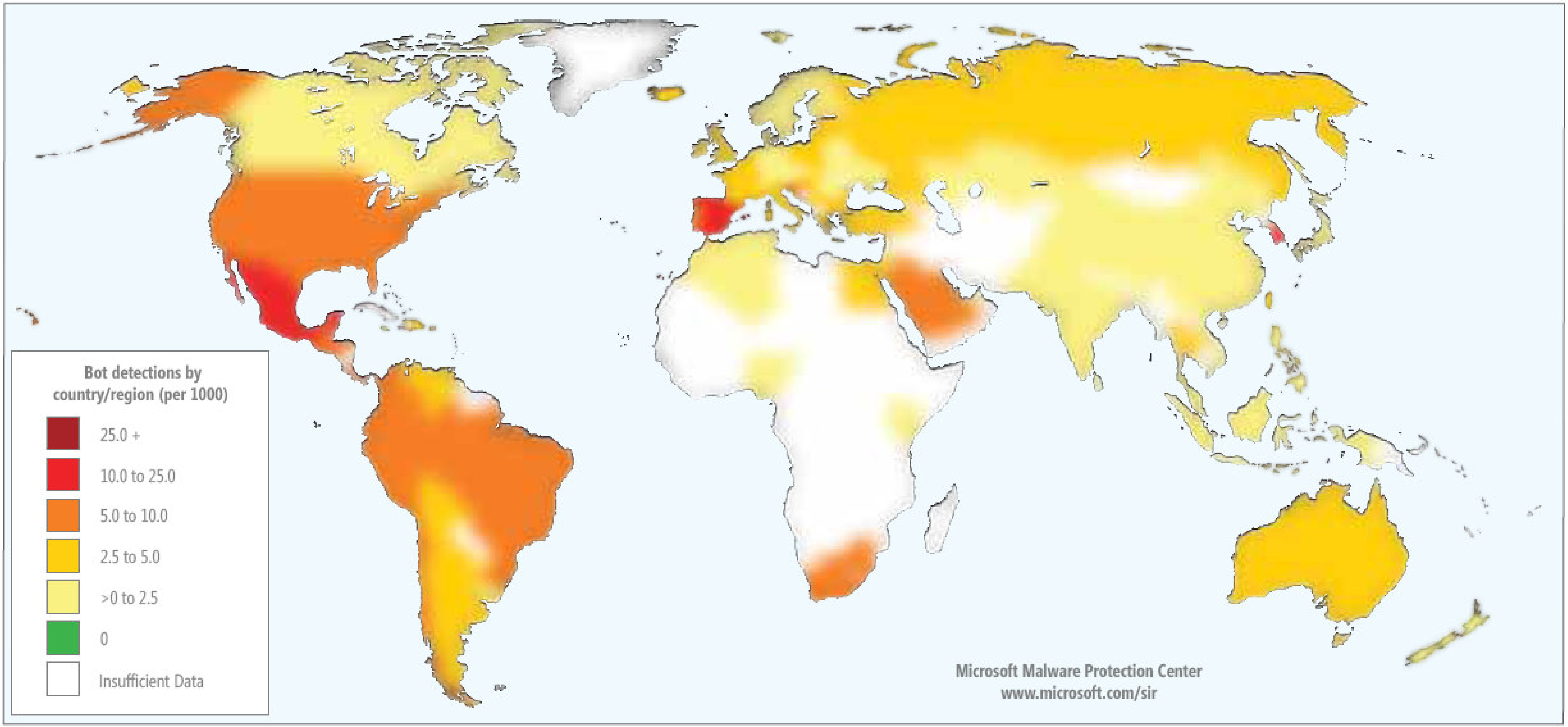


Diagram from Wired Magazine

Worldwide “Bot” Infections: *2Q 2010*



Source: Microsoft – Security Intelligence Report - 2010

ITU: In-Depth Cybersecurity Workshop – *Jamaica - Sept 2010*

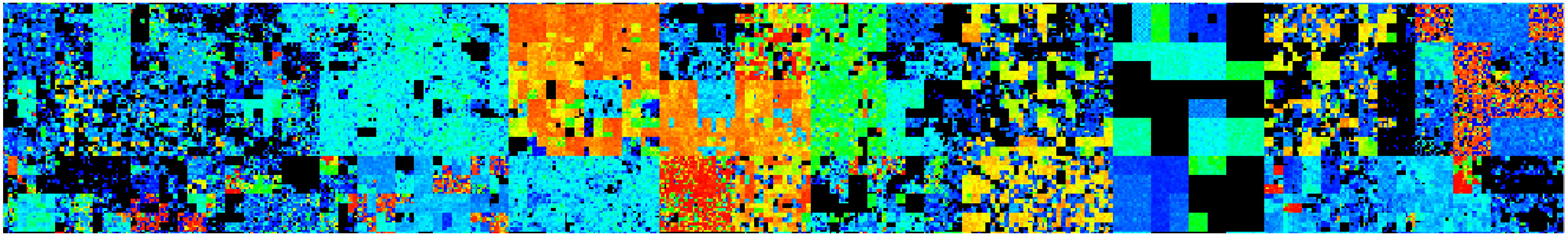
Cybercrimes against Critical Economic Sectors

- ***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!

Smart Sustainable Security for 21stC Armenia

1 – Background Perspectives	2 – Global Cybersecurity Challenge	**3 – Cybersecurity Case Studies**
4 – Transition to 21stC Sustainable Security	5 – Smart Security: Technology & Process	6 – Securing Critical National Infrastructure
7 – Integrating Cyber & Physical Security	8 –Towards Smart *”Neural Society”*	9 – Next Steps for Securing 21stC Armenia



National & Regional Cybersecurity Case Studies

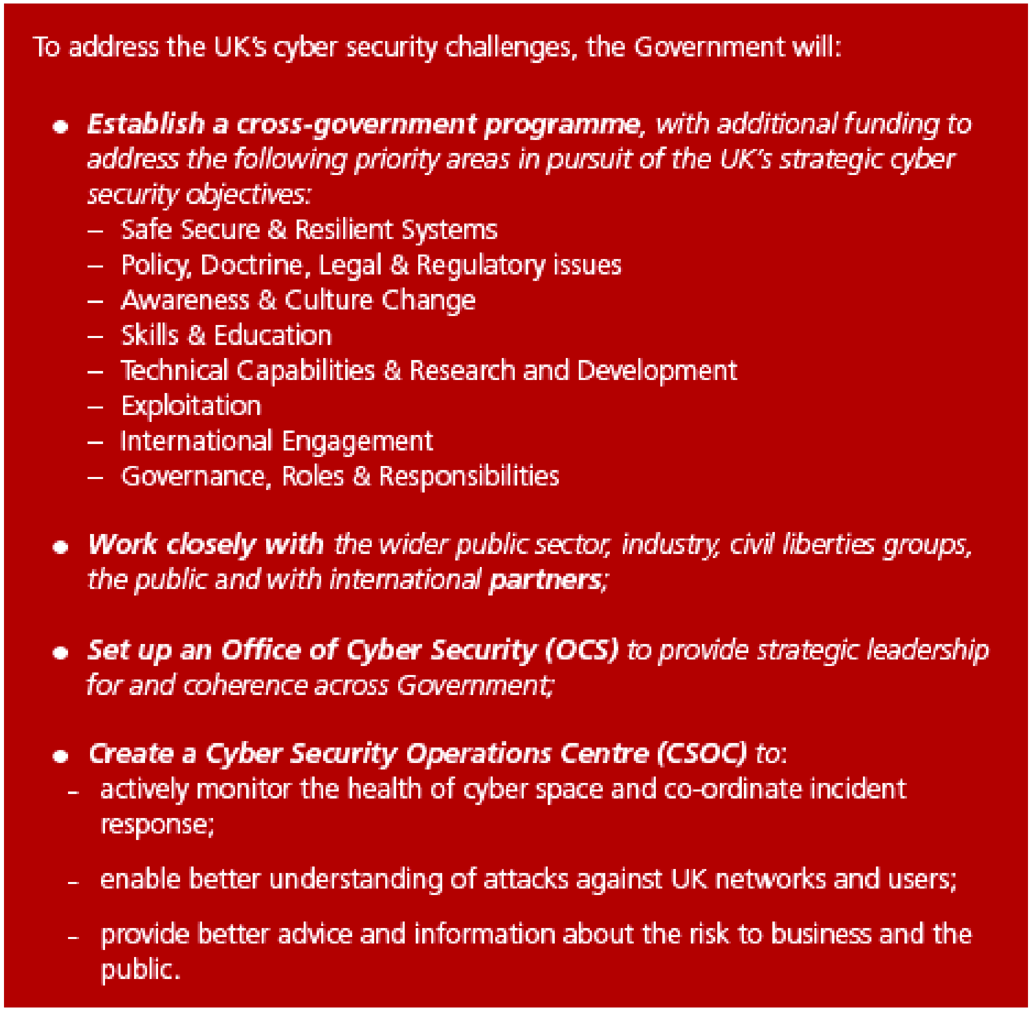
- ***UK Government:*** Cybersecurity Strategy for the UK – Safety, Security & Resilience in Cyberspace (UK Office of Cybersecurity – June 2009)
- ***US Government:*** Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure – May 2009
- ***Canada:*** Canadian 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 Techology Security Authority - SITSA
- ***South Korea:*** Korea Internet and Security Agency (KISA – July 2009)
- ***Latin America :*** CITEL/OAS has developed regional cybersecurity strategy with dedicated events
- ***European Union:*** ENISA – European Network and Information Security Agency (Sept2005) tackles all aspects of cybersecurity & cybercrime for the countries of the European Union and beyond

UK Office of Cybersecurity – OCS & CSOC

Cyber Security Strategy of the United Kingdom

safety, security and resilience in cyber space

OCS
UK Office of Cyber Security
CSOC
UK Cyber Security Operations Centre



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.

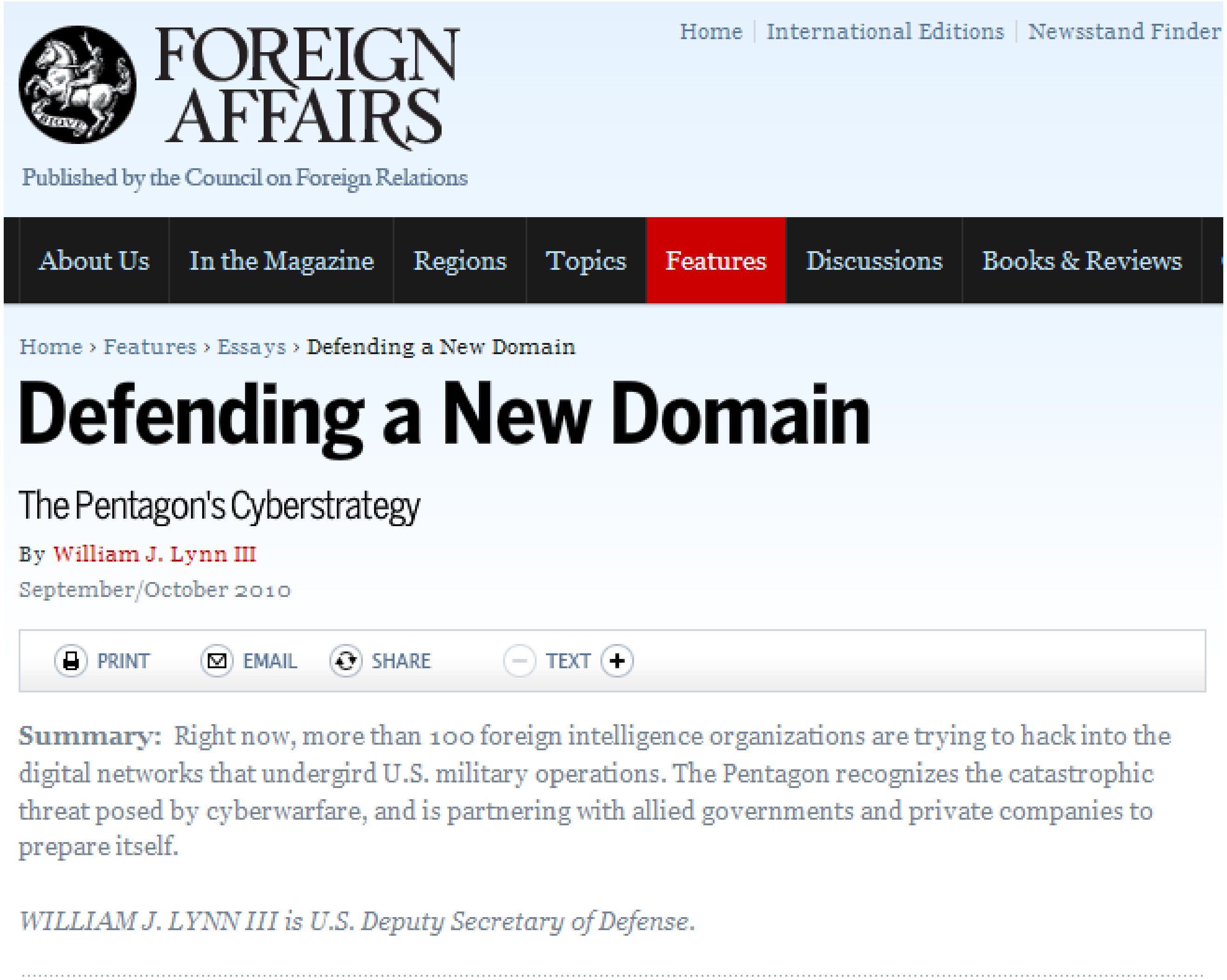
US Government : *Office of CyberSecurity (CS&C)*

- Following the June 2009, US Government Policy Review, the Department of Homeland Security (DHS) has responsibility for hosting the *"Office of Cybersecurity & 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

Evolving Cybersecurity for US Defence:

"The Pentagon's Cyberstrategy"


FOREIGN AFFAIRS
Published by the Council on Foreign Relations
Home | International Editions | Newsstand Finder
About Us
In the Magazine
Regions
Topics
Features
Discussions
Books & Reviews
Home › Features › Essays › Defending a New Domain
PRINT
EMAIL
SHARE
TEXT

Defending a New Domain

The Pentagon's Cyberstrategy

By William J. Lynn III

September/October 2010

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.

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.

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.

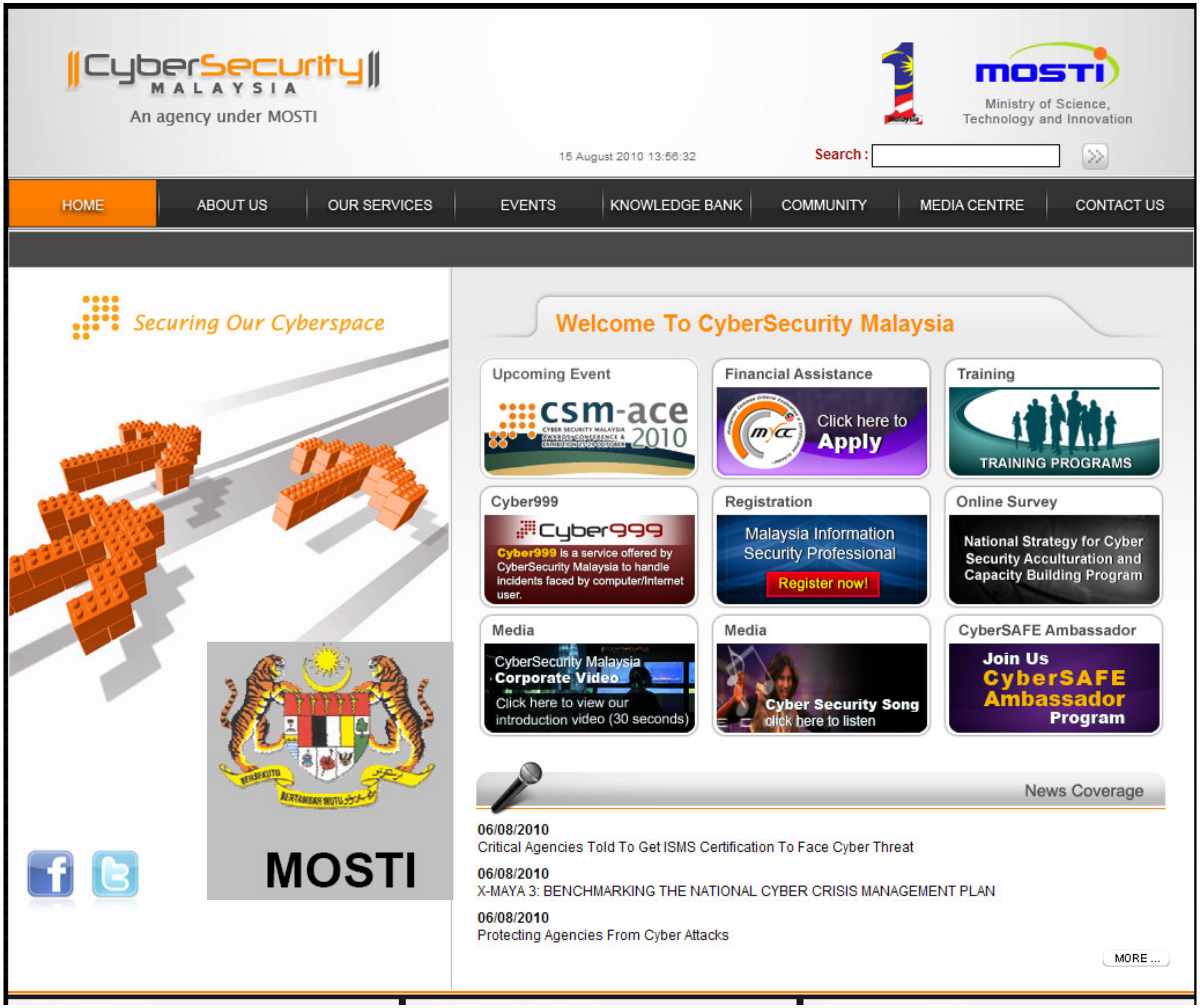
Cyber Security Operations Centre (CSOC)

Australian Government

CERT Australia

AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

Malaysian Government: *MOSTi*



CyberSecurity MALAYSIA

An agency under MOSTI

MOSTI Ministry of Science, Technology and Innovation

15 August 2010 13:56:32

Search :

HOME | ABOUT US | OUR SERVICES | EVENTS | KNOWLEDGE BANK | COMMUNITY | MEDIA CENTRE | CONTACT US

Securing Our Cyberspace

MOSTI

Welcome To CyberSecurity Malaysia

Upcoming Event: csm-ace 2010

Financial Assistance: Click here to Apply

Training: TRAINING PROGRAMS

Cyber999: Cyber999 is a service offered by CyberSecurity Malaysia to handle incidents faced by computer/Internet user.

Registration: Malaysia Information Security Professional. Register now!

Online Survey: National Strategy for Cyber Security Acculturation and Capacity Building Program

Media: CyberSecurity Malaysia Corporate Video. Click here to view our introduction video (30 seconds)

Media: Cyber Security Song. click here to listen

CyberSAFE Ambassador: Join Us CyberSAFE Ambassador Program

News Coverage

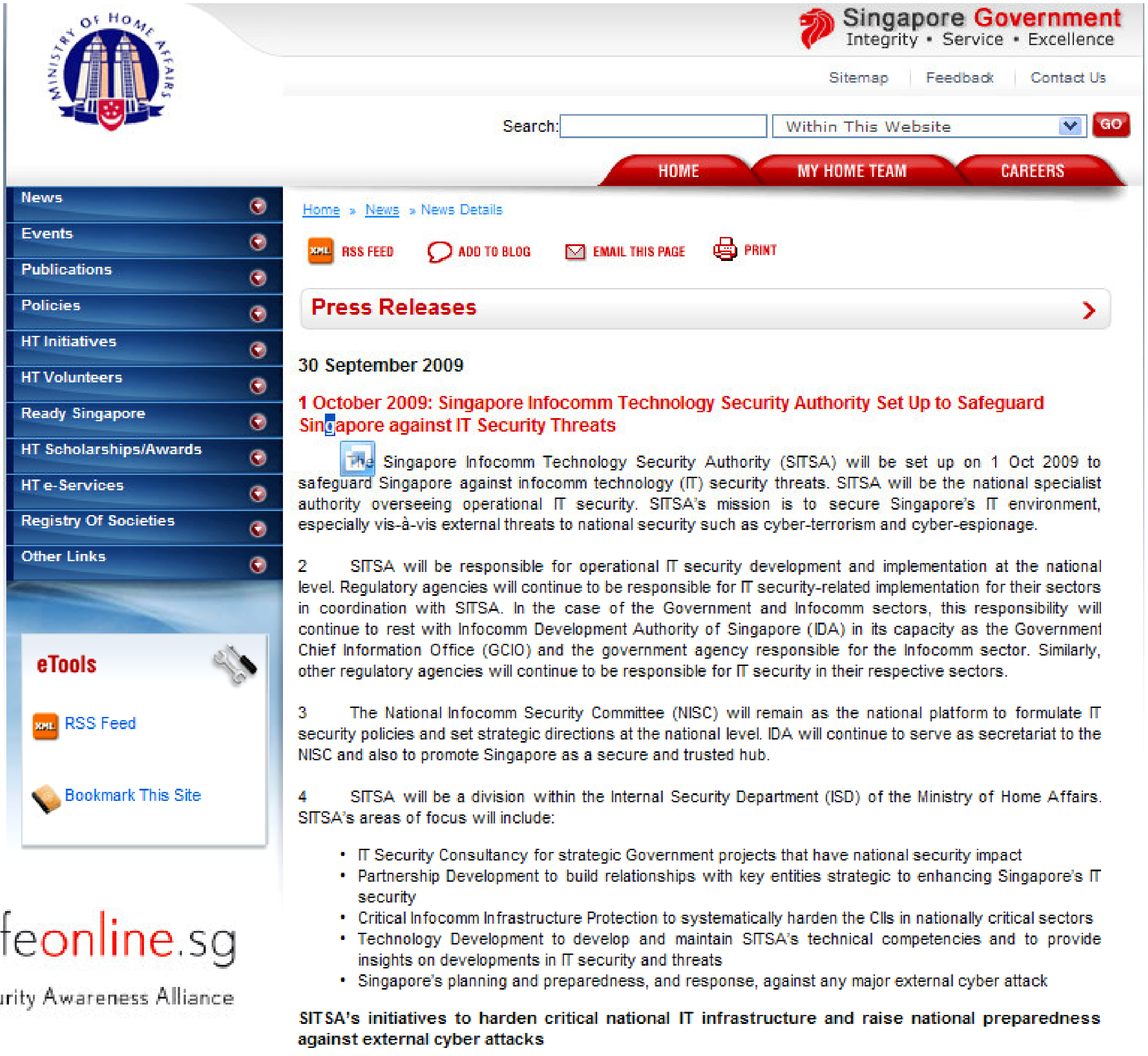
06/08/2010
Critical Agencies Told To Get ISMS Certification To Face Cyber Threat

06/08/2010
X-MAYA 3: BENCHMARKING THE NATIONAL CYBER CRISIS MANAGEMENT PLAN

06/08/2010
Protecting Agencies From Cyber Attacks

MORE ...

Singapore Government : *SITSA*



Singapore Government
Integrity • Service • Excellence

Press Releases

30 September 2009

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

The 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.

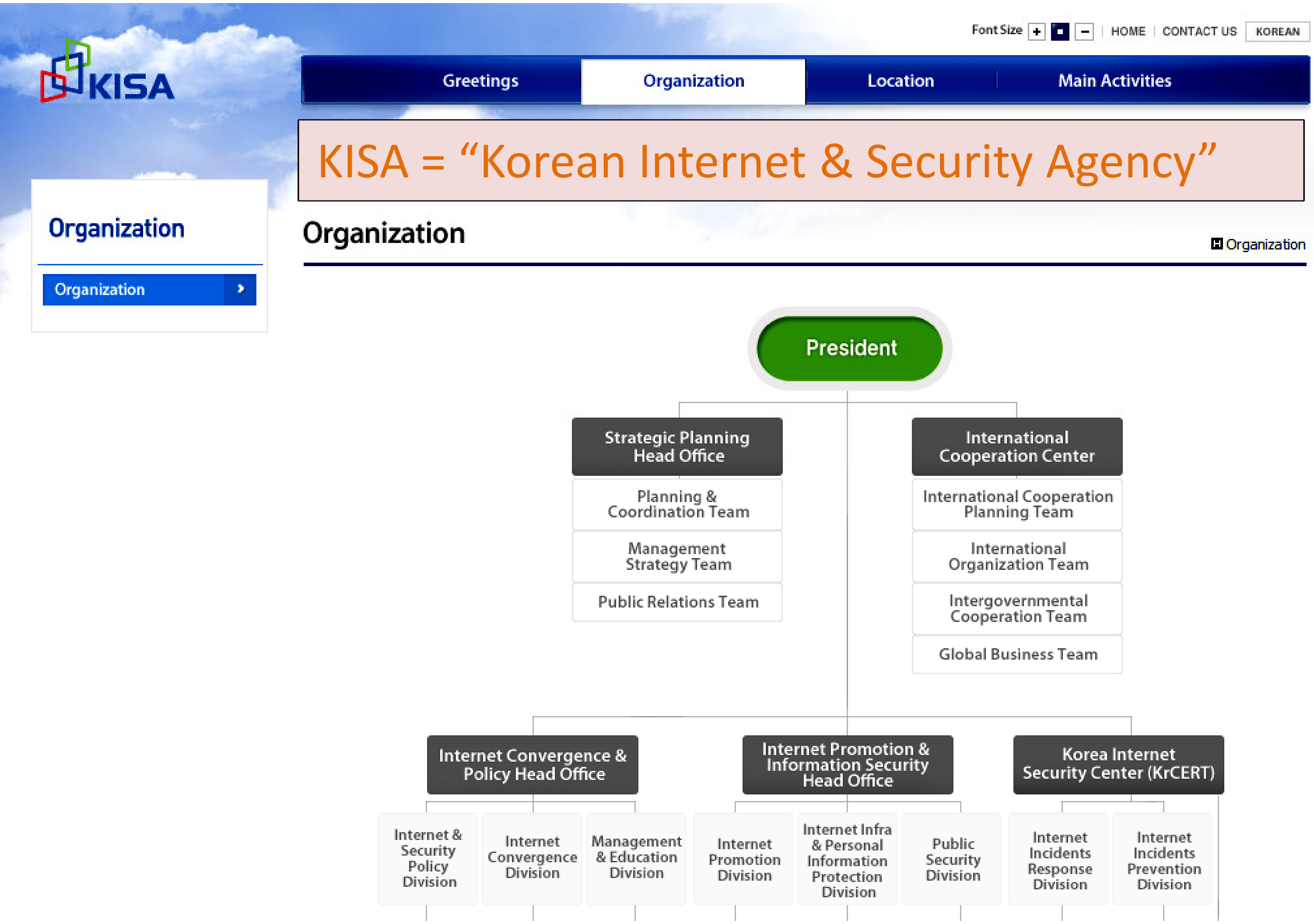
4 SITSA will be a division within the Internal Security Department (ISD) of the Ministry of Home Affairs. SITSA's areas of focus will include:

- 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 CIIs 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

GOsafeonline.sg
Cyber Security Awareness Alliance

South Korea Government: *KISA*



KISA = "Korean Internet & Security Agency"

President

Strategic Planning Head Office
- Planning & Coordination Team
- Management Strategy Team
- Public Relations Team

International Cooperation Center
- International Cooperation Planning Team
- International Organization Team
- Intergovernmental Cooperation Team
- Global Business Team

Internet Convergence & Policy Head Office
- Internet & Security Policy Division
- Internet Convergence Division
- Management & Education Division

Internet Promotion & Information Security Head Office
- Internet Promotion Division
- Internet Infra & Personal Information Protection Division
- Public Security Division

Korea Internet Security Center (KrCERT)
- Internet Incidents Response Division
- 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

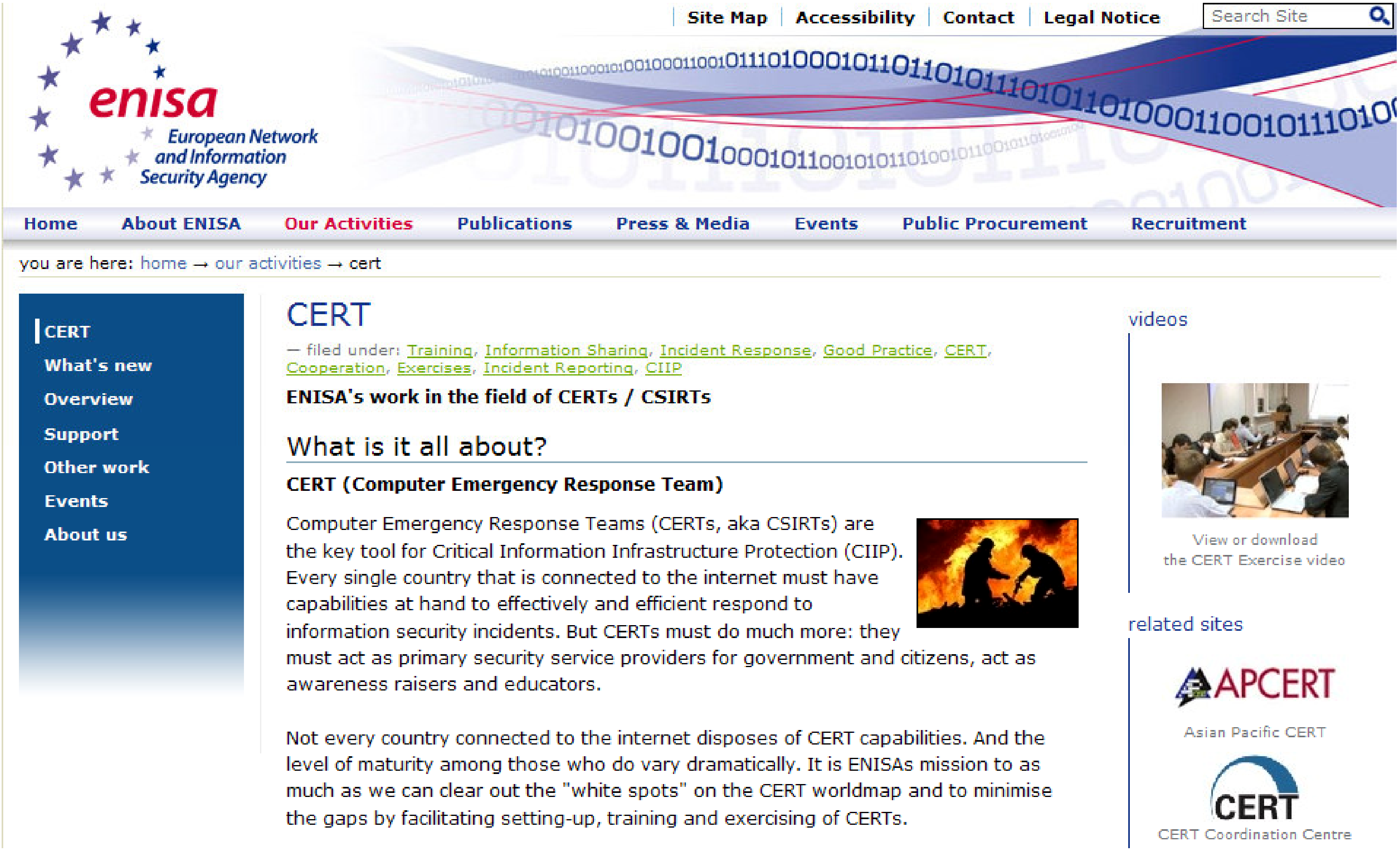
- System Management Team (KRNIC)
- Internet Name Policy Team (KRNIC)
- IP Policy & Management Team (KRNIC)
- Internet Ethics Team
- Internet Planning Team

- 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

European Network and Information Security Agency: *ENISA*



you are here: home → our activities → cert

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 ENISAs 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.

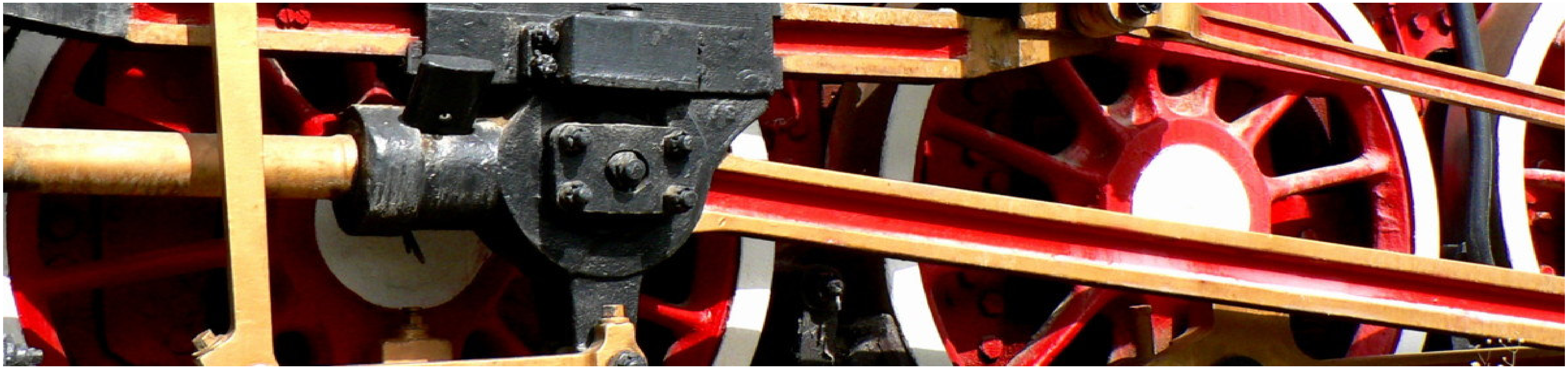
National Cybersecurity Agencies: *Common Roles*

- Common roles and responsibilities for all these national cyber agencies:

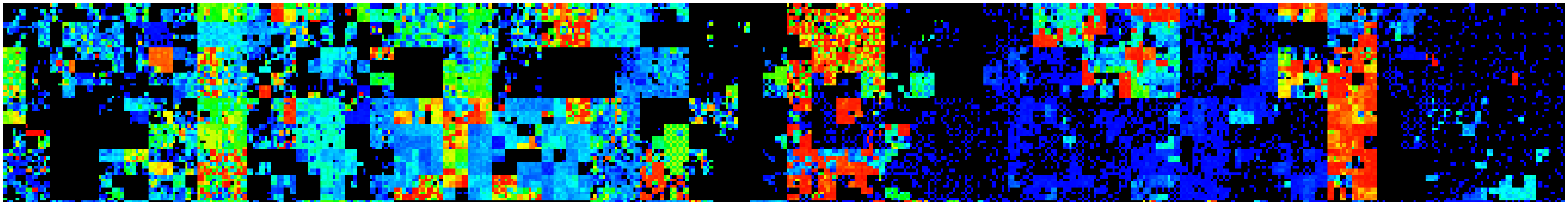
  - ***Cyber Alerts:*** Management of the National Response to Cyber Alerts, and Attacks
  - ***Education:*** Co-ordination of National Awareness and Skills Training Programmes
  - ***Laws:*** Leadership role in the development and approval of new cyber legislation
  - ***Cybercrime:*** Facilitation for building a National Cybercrime of 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!

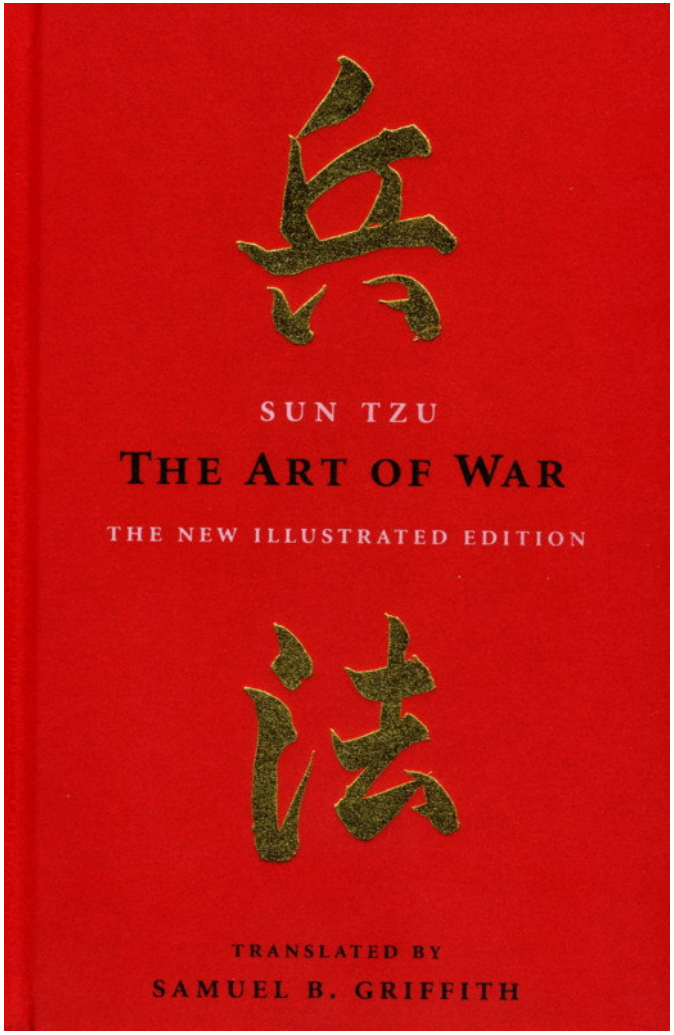
Smart Sustainable Security for 21stC Armenia



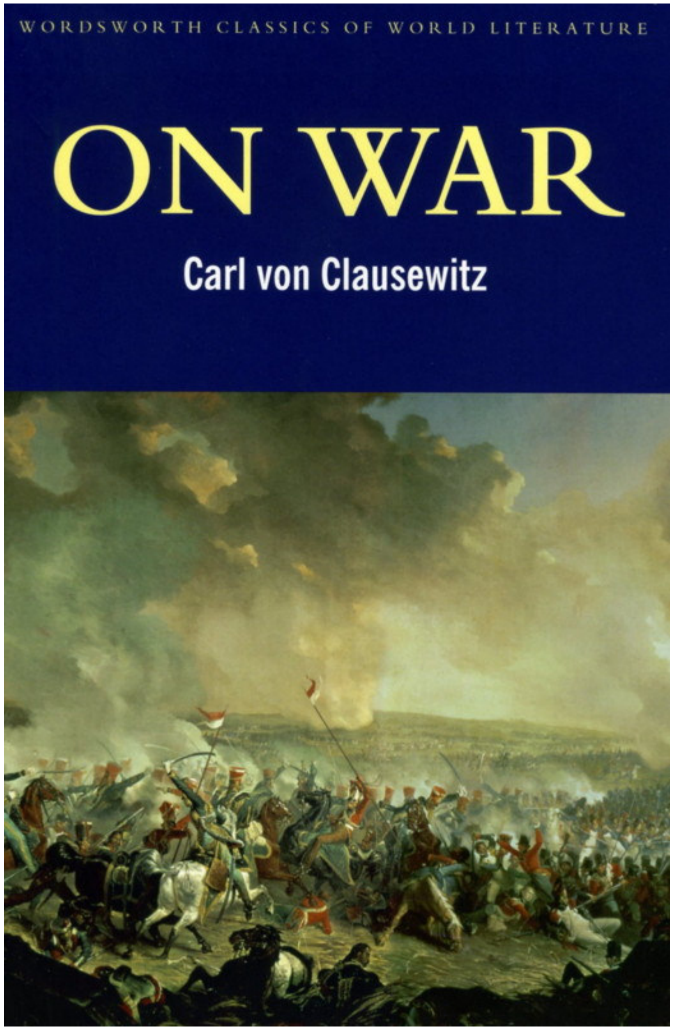
1 – Background Perspectives	**2 – Global Cybersecurity Challenge**	**3 – Cybersecurity Case Studies**
4 – Transition to 21stC Sustainable Security	**5 – Smart Security: Technology & Process**	**6 – Securing Critical National Infrastructure**
7 – Integrating Cyber & Physical Security	**8 – Towards Smart *"Neural Society"***	**9 – Next Steps for Securing 21stC Armenia**



Cyber War Strategies *from* Classic Historical Works!



Recommended "Bedtime Reading" for *Cybersecurity Specialists!*



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

“21st Century Smart 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 cyber attack

- ***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 on the distributed mobile internet

…….In this presentation we explore the 21st World of Smart Security Solutions including their integration with traditional physical security & surveillance

Transition from 20thC Industrial to 21stC Smart Security

- **Cybersecurity 2012-2022:**
  - 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

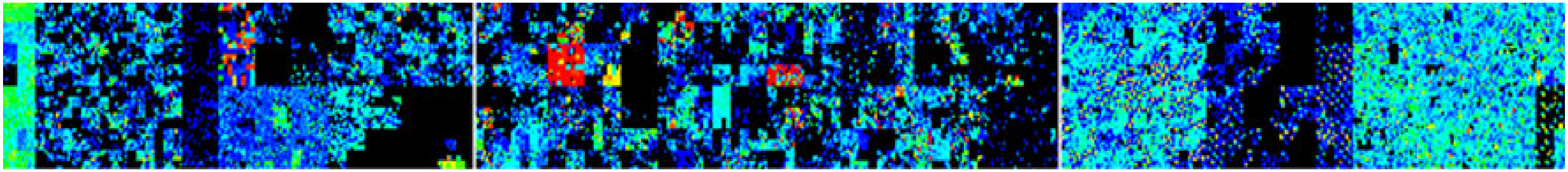
- **National Boundaries:**
  - Traditional physical defence and geographical boundaries are still strategic national assets , but they need to be augmented through integrated cyber defence organisations & assets

- **Critical National Information Infrastructure:**
  - 21stC national economies function electronically, & yet they are poorly defended in cyberspace, and often open to criminal & political attacks

- **Multi-Dimensional Cyber Defence:**
  - *Armenia* will need to audit its critical infrastructure – government, banks, telecommunications, energy, & transport – and upgrade to international cybersecurity standards based upon "Best Practice" (ISO/IEC – 27xxx).

Smart Sustainable Security for 21stC Armenia

1 – Background Perspectives	**2 – Global Cybersecurity Challenge**	**3 – Cybersecurity Case Studies**
4 – Transition to 21stC Sustainable Security	**5 – Smart Security: Technology & Process**	**6 – Securing Critical National Infrastructure**
7 – Integrating Cyber & Physical Security	**8 – Towards Smart *"Neural Society"***	**9 – Next Steps for Securing 21stC Armenia**



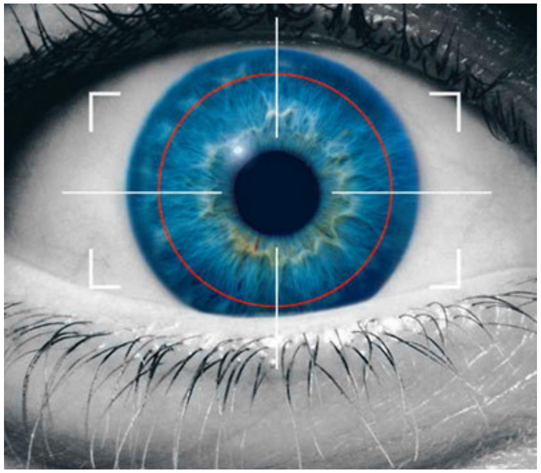
Smart Security: *Technology & Operations*

- ***"Smart Security"*** spans the protection of both physical buildings, staff and cyber facilities, networks & information assets.
  - ***Technologies:*** Advanced ICT Security technologies include Biometrics, RFID Encryption, PKI Authentication, ID Management, DDoS Protection, Malware Detection
  - ***Operations:*** Physical Buildings, Staff and all information & ICT assets need to be secured through solutions such as RFID tagging, Interactive HD CCTV, movement detection and other automatic means for asset monitoring & surveillance
  - ***Critical National Infrastructure Protection (CNIP):*** Most national smart security programmes now focus upon securing critical infrastructure such as banking & finance, airports & transporation, power stations, military & defence facilities, ICT, Mobile & telecommunications services & Government Ministries & Parliament.

…In the next sections we'll explore both CNIP and the Integration of Cyber & Physical Security Operations which is the real essence of "Smart Security"

Smart Technology Example: *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 used 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!

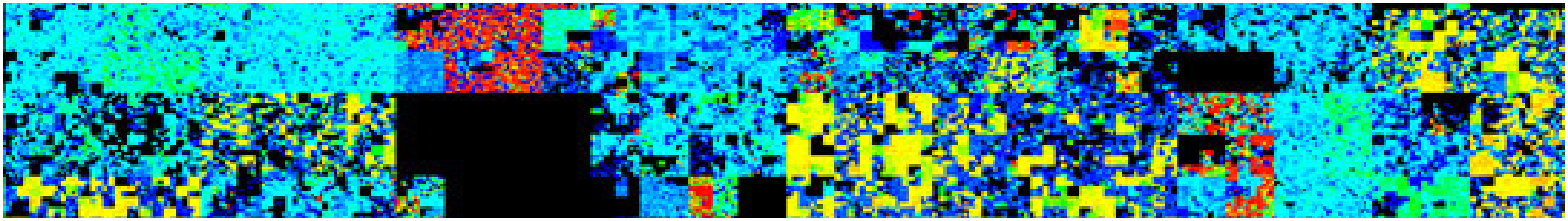
Smart Security Solutions & *ISO Standards*

- 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 *ISO 27xxx 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!)

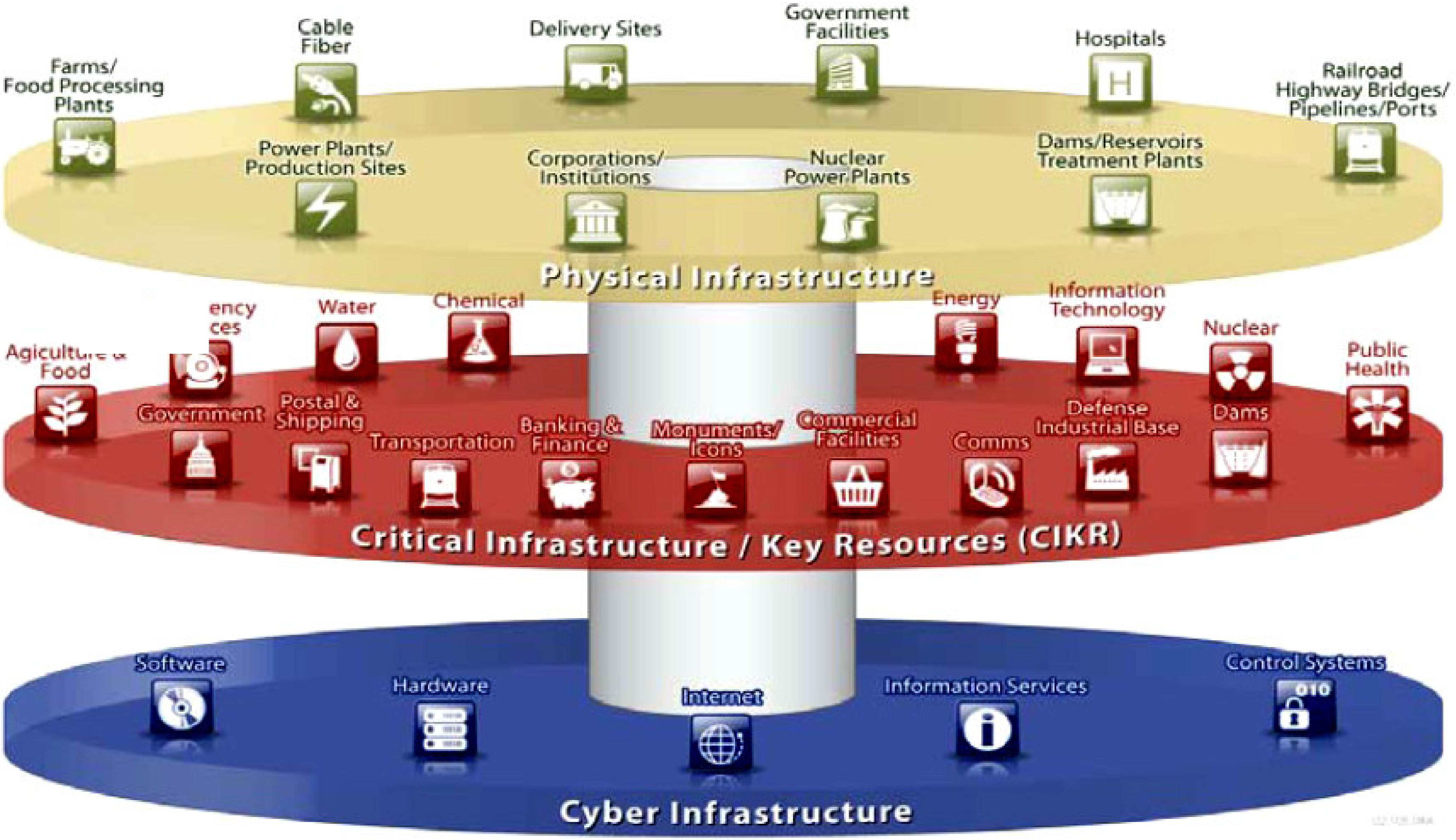
….Many criminal and terrorist attacks are achieved through penetrating some combination of physical and cybersecurity systems. Breaking into a physical building may allow a criminal to gain secure ICT zones, and thence to on-line user accounts, documents & databases…

Smart Sustainable Security for 21stC Armenia

1 – Background Perspectives	**2 – Global Cybersecurity Challenge**	**3 – Cybersecurity Case Studies**
4 – Transition to 21stC Sustainable Security	**5 – Smart Security: Technology & Process**	**6 – Securing Critical National Infrastructure**
7 – Integrating Cyber & Physical Security	**8 – Towards Smart *"Neural Society"***	**9 – Next Steps for Securing 21stC Armenia**



Critical Sectors and Infrastructure in Cyberspace



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

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

Cybersecurity Benefits: *Government*

- Improved cybersecurity & physical security provides significant short & medium term 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 cyberattacks

Critical Service Sector Infrastructure

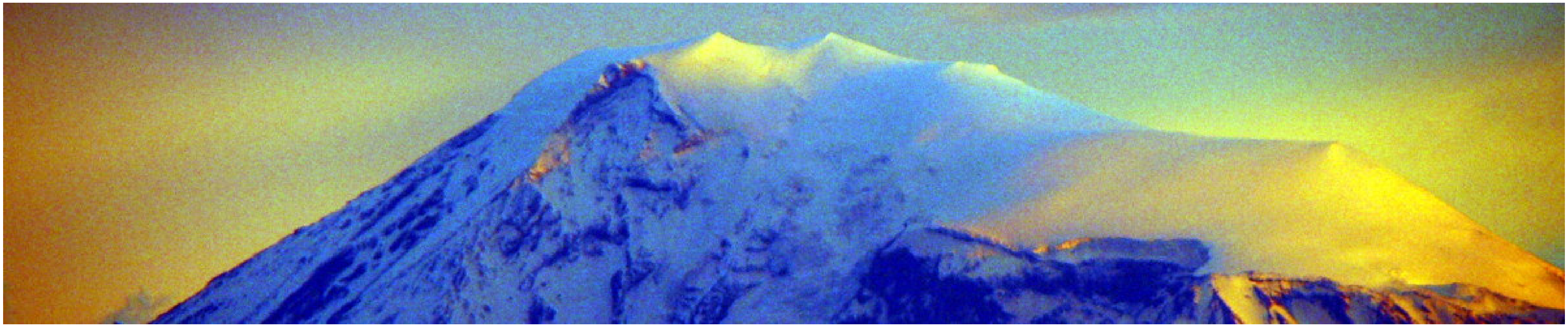
- ***National Strategies:*** Many countries & regions now consider the threat of cyber attacks to be high enough to build national cybersecurity strategies.

- ***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).

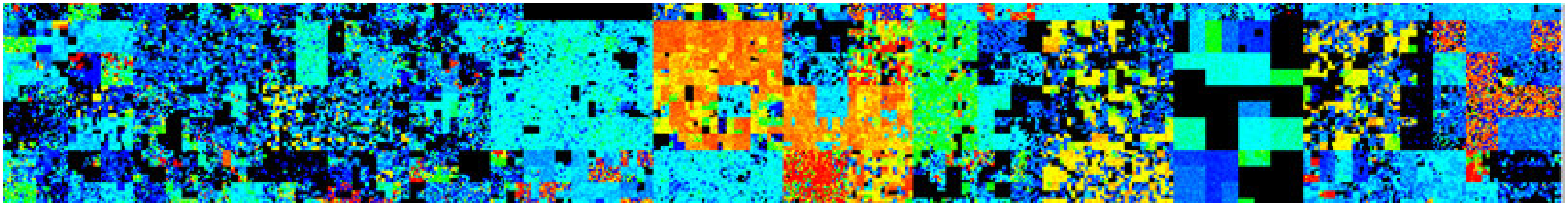
- ***Every Critical Service Sector*** should be considered in-depth:
  - Government (National & Regional)
  - Telecommunications/Mobile/ISPs
  - Banking/Financial Services
  - Transportation/Airports
  - Military/National Defence
  - Energy Power Grid & Utilities
  - Healthcare & Emergency Services
  - Police & Law Enforcement Agencies

...The National Cybersecurity Organisation will include ALL these stakeholders & the CERTs will respond to incidents & communicate across ALL sectors

Smart Sustainable Security for 21stC Armenia



1 – Background Perspectives	2 – Global Cybersecurity Challenge	3 – Cybersecurity Case Studies
4 – Transition to 21stC Sustainable Security	5 – Smart Security: Technology & Process	6 – Securing Critical National Infrastructure
7 – Integrating Cyber & Physical Security	8 – Towards Smart *"Neural Society"*	9 – Next Steps for Securing 21stC Armenia



- 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!

Cyber: Integrated Command & Control

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

“Cyber to Physical Attacks”

- The illegal penetration of ICT systems may allow criminals to secure information or “make deals” that facilities 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 & information infrastructure. Clearly it is important for countries to upgrade their national cybersecurity to minimise such risks

Physical: Integrated CCTV Surveillance

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

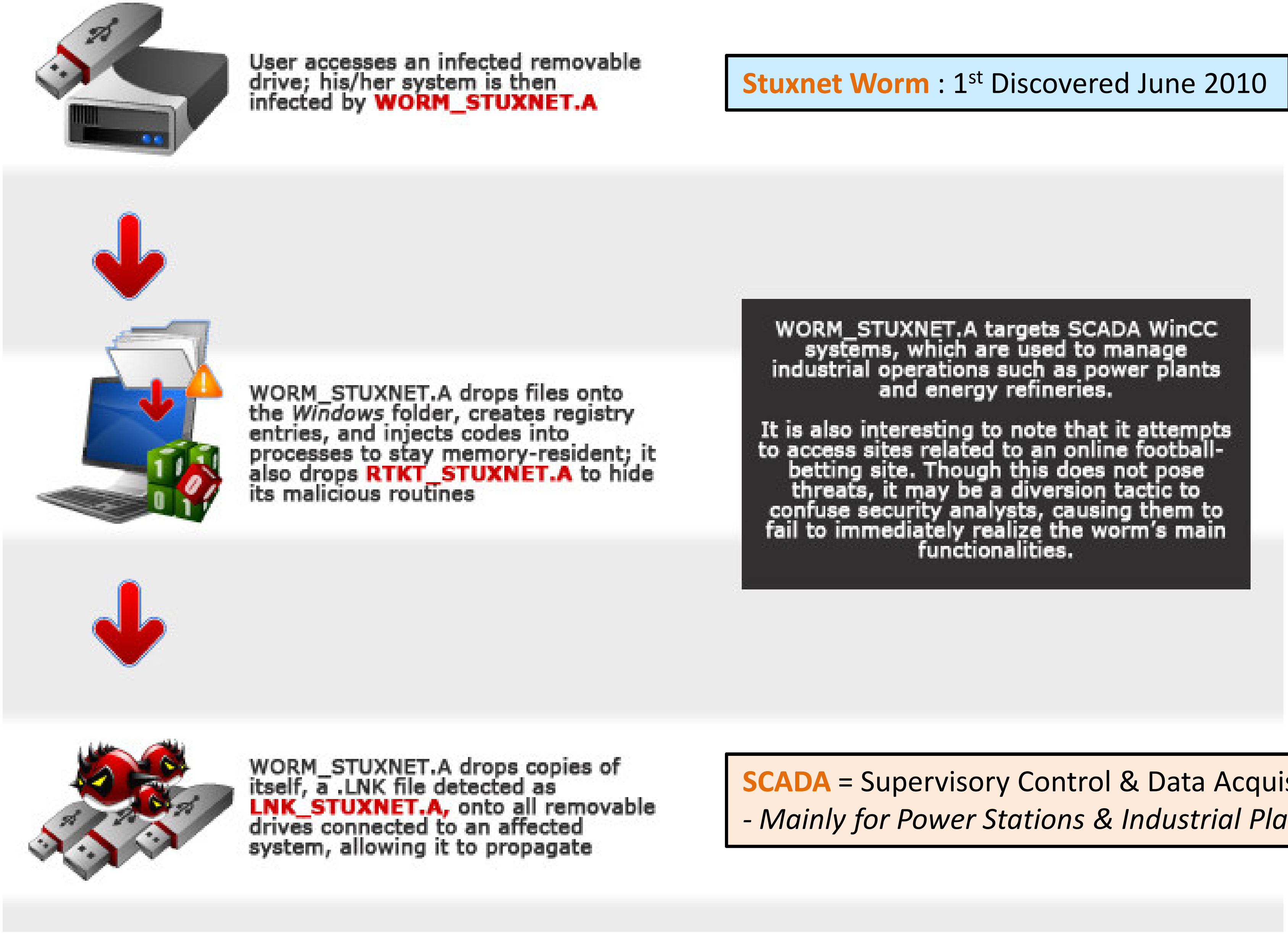
“Physical to Cyber Attacks”

- 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 key logger hardware devices or possibly extract information, plans and databases to USB memory chips, or steal DVDs!

Physical: Computer Automated Industrial Control & Safety Systems *(SCADA)*

Case Study: StuxNet Worm - *Industrial SCADA Systems*

Stuxnet Worm : 1st Discovered June 2010



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

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 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

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.

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

- Towards Smart Sustainable Security -

Integrating Physical & Cybersecurity Operations

- ***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.

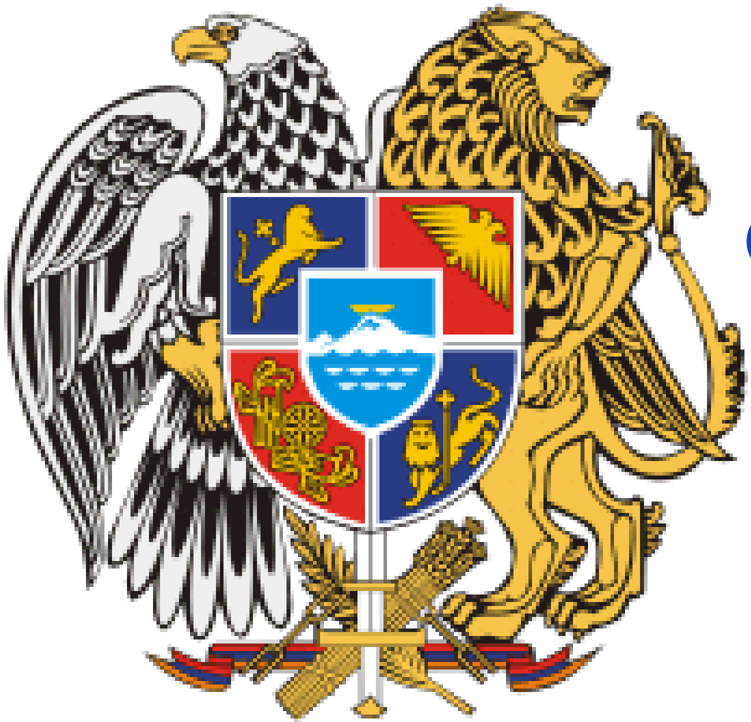
- ***Audit and Compliance :*** Investments in establishing and upgrading cybersecurity defences means that all physical security and associated operational staff should also be reviewed for compliance with government policies, & audited to international standards

- ***Smart Roadmap:*** I'd recommend developing a focused smart security action plan and roadmap (Physical & Cyber) for each critical sector across Government & Major Enterprises

Smart Sustainable Security: *Armenia's Coat of Arms*

Cyber World = Eagle

(Artaxiad & Arsacid)



Physical World= Lion

(Bagratuni & Rubenid)

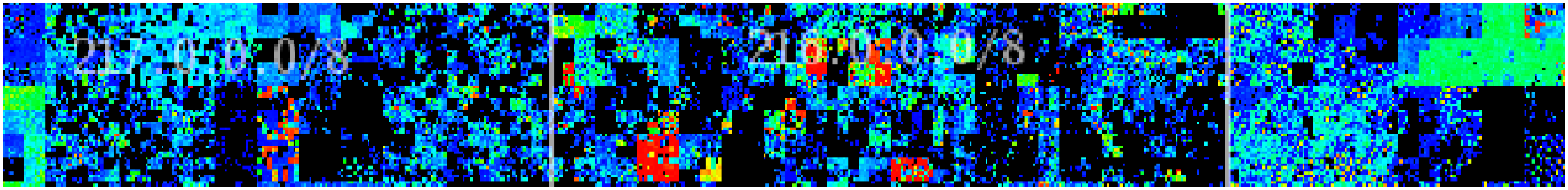
Five Vital Symbols:

Feather Pen (**Culture & Intelligence**), Broken Chain (**Freedom & Independence**), Wheat Flower (**Industry**), Sword (**Power & Strength**), Tri-Coloured Ribbon (**Armenian Flag**),

Smart Security = *Eagle AND Lion Jointly Protecting Armenia!*

Smart Sustainable Security for 21stC Armenia

1 – Background Perspectives	2 – Global Cybersecurity Challenge	3 – Cybersecurity Case Studies
4 – Transition to 21stC Sustainable Security	5 – Smart Security: Technology & Process	6 – Securing Critical National Infrastructure
7 – Integrating Cyber & Physical Security	**8 – Towards Smart *"Neural Society"***	9 – Next Steps for Securing 21stC Armenia

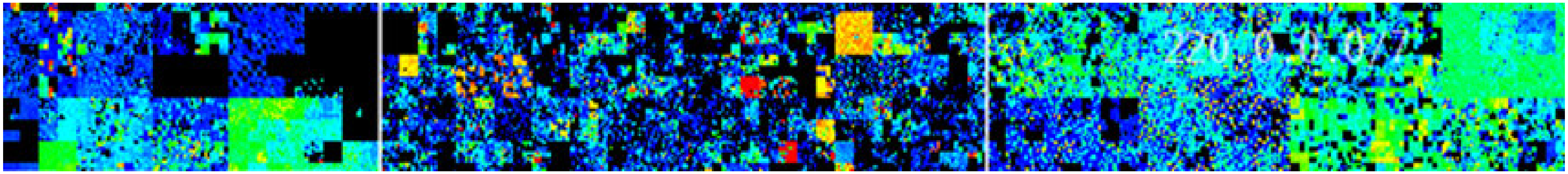


The Future: *Towards Smart "Neural Society"*

- ***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 & Immersive 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 Simulation & 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
- ***Smart Security Architectures:***
  - Effective integrated security requires management through hybrid hierarchical and "peer-to-peer" organisational architectures. Living organic systems also exploit hybrid architectures for optimal command & control as in the "*Mammalian Nervous System"*

Smart Sustainable Security for 21stC Armenia

1 – Background Perspectives	**2 – Global Cybersecurity Challenge**	**3 – Cybersecurity Case Studies**
4 – Transition to 21stC Sustainable Security	**5 – Smart Security: Technology & Process**	**6 – Securing Critical National Infrastructure**
7 – Integrating Cyber & Physical Security	**8 – Towards Smart *"Neural Society"***	**9 – Next Steps for Securing 21stC Armenia**



Smart Security: *“Next Steps for 21stC Armenia”*

1) ***National Cybersecurity Agency:*** Establishment of a National Armenian CERT & Government Cybersecurity Agency within the organisation of Armenian Government Ministries & Agencies
2) ***CIIP:*** Critical Information Infrastructure Protection (CIIP) for *ALL* Critical Economic Sectors
3) ***System Upgrades:*** Phased Technical Infrastructure ICT Upgrades using “ Smart Solutions” including Hardware, Software, Secure Network Links, Virtualised Servers & Cloud Storage
4) ***Back-Up:*** Disaster Recovery, Business Continuity, Crisis Management and Back-Up Systems
5) ***Physical :*** Physical Security Applications – CCTV, Alarms, Control Centre, RFID Asset Tracking
6) ***Awareness Campaign:*** Government Campaign for National Cybersecurity Awareness
7) ***Training:*** National Cybersecurity Skills & Professional Training Programme with Industry & Colleges
8) ***Encryption:*** National User & Systems PKI Authentication, ID & eSignature Programme
9) ***Laws:*** Programme for Drafting and Enforcing new 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”

“Smart Sustainable Security” for 21stC Armenia!

21stC Armenia : “Smart Economy”

DigiTec Business Forum – Yerevan, Armenia

Thank-You!...

Presentation Slides:

www.Valentina.net/DigiTec2012/

Presentation Slides:
www.Valentina.net/DigiTec2012/

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.

- ***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 55 professional engineers & a diverse portfolio of hi-tech security products.

- ***Republic of Georgia*** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament.

- ***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: 2007-2012 Editions.

21stC Armenia : "Smart Security"

DigiTec Business Forum – Yerevan, Armenia

BACK-UP SLIDES