“Cybersecurity for Critical National Infrastructure (CNI)”

Dr David E. Probert

VAZA International

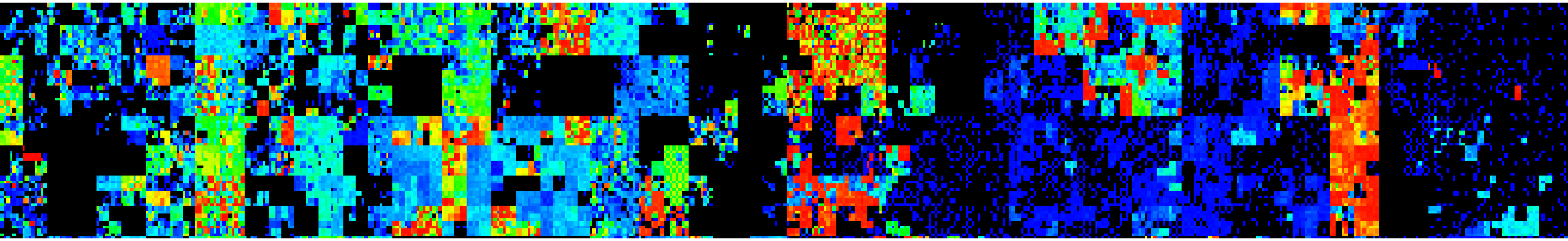
Dedicated to my Beloved Wife – Valentina

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 Critical National Infrastructure (CNI)

1 – The Strategic Importance of CNI	2 – Evolving Cyber Threats for CNI Sectors	3 –National & International CNI Plans
4 – 21stC Smart Systems – “Design Toolkit”	5 – Banking & Finance Sector – Analysis	6 – Energy & Transport Sectors - Analysis
7 – Civil and National Defence - Analysis	8 – CNI Security for “Internet of Things”	9 – Smart Security for YOUR Business!



Securing OUR *"21st Century Cyber World"*

- *Open World:* During the last 25 years we've evolved from the primitive Internet to the complex world of Web2.0, social, mobile & wireless applications

- *Criminals and Hackers* seek every opportunity to creatively penetrate wired, wireless, mobile devices, and social networking applications

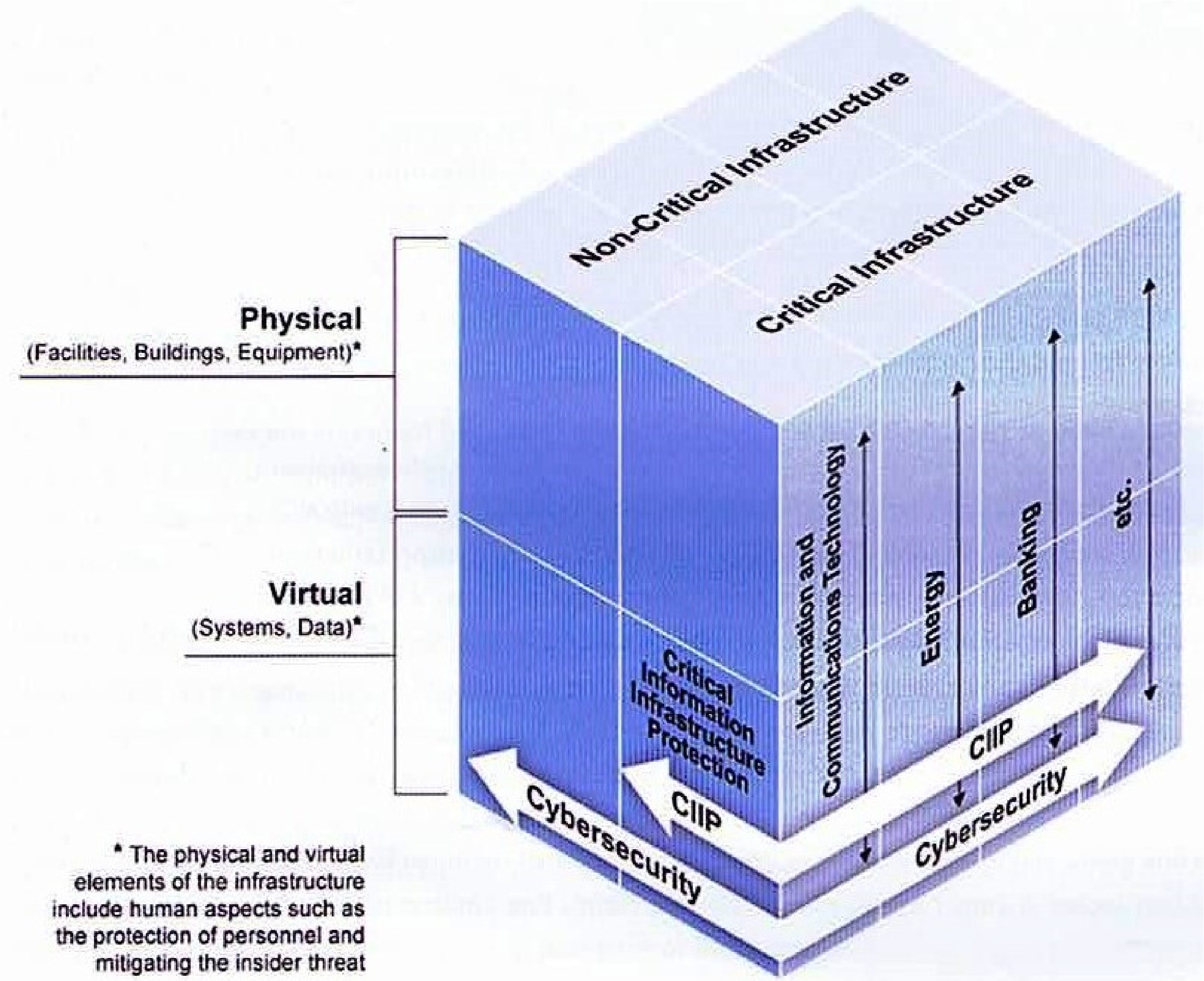
- *The war against cybercriminals* requires us to continuously create new cybersecurity solutions for every conceivable cyberattack

- *Standards, Architectures and Operational Security Policies* all ensure that the "business case for cybercriminals" is much less attractive

- *The DMZ Security Firewalls* of the mid-1990s are now only a partial solution to the protection of critical infrastructure for governments and business

…….In this presentation we explore the foundations of cybersecurity and the need to provide operational & systems integration with traditional physical security for **CNI**

Understanding Physical and Virtual *Critical National Infrastructure (CNI)*

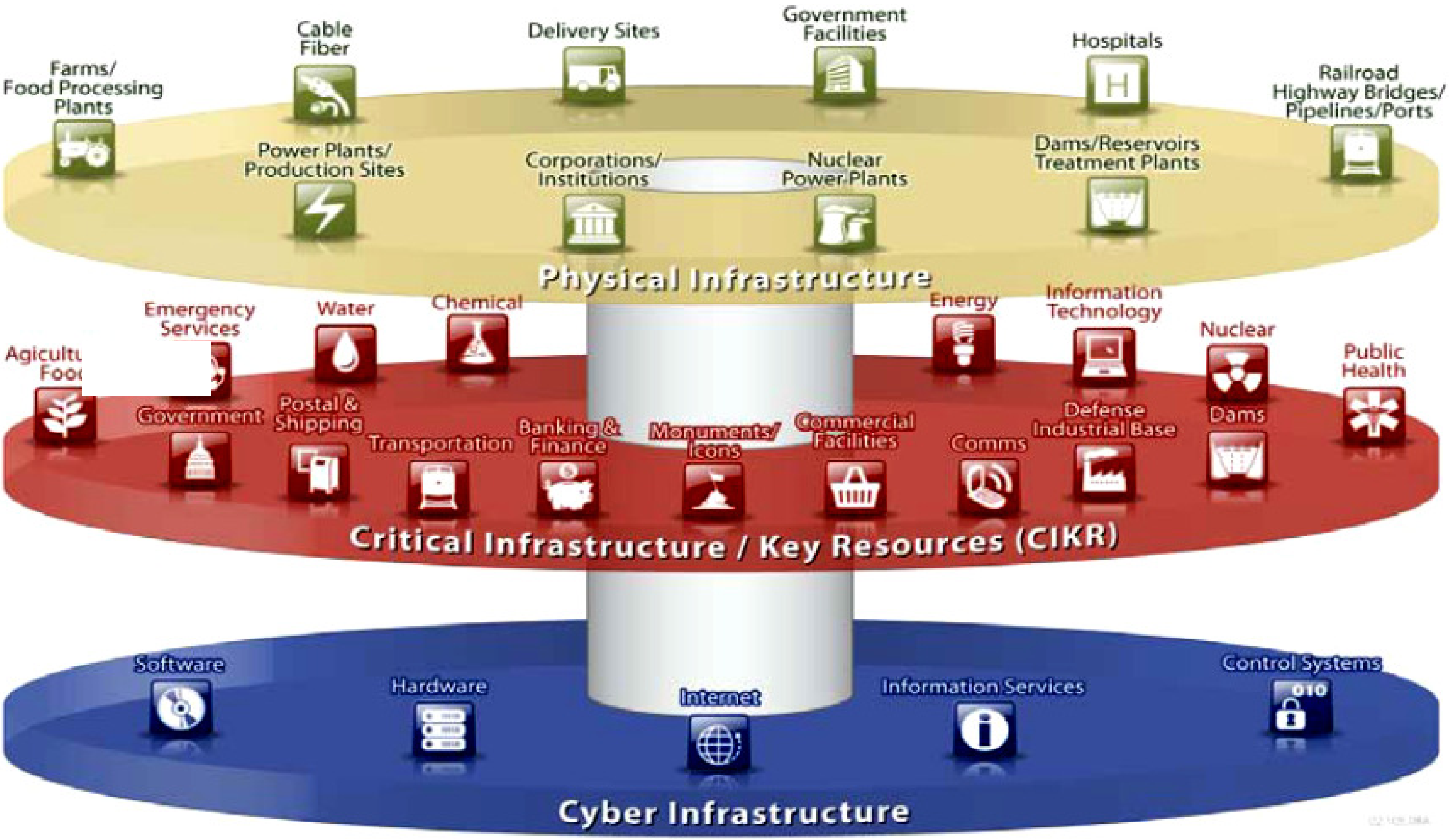

Physical
(Facilities, Buildings, Equipment)*
Virtual
(Systems, Data)*
Non-Critical Infrastructure
Critical Infrastructure
Information and Communications Technology
Energy
Banking
etc.
Critical Information Infrastructure Protection
CIIP
Cybersecurity
CIIP
Cybersecurity

* The physical and virtual elements of the infrastructure include human aspects such as the protection of personnel and mitigating the insider threat

A Short History of Cybersecurity for *CNI/CII*

- *Birth of CNI:* Early proposals appeared around 15 to 20 years ago, during the mid-1990s, after birth of commercial internet
- *International discussions* from G8, OECD and EU around 10 to 15 years ago with main focus upon physical CNI protection & less on cyber.
- *Early CNI/CII Plans:* More detailed National CNI/CII Plans started to be prepared and published from around 5 to 7 years ago
- *Cybersecurity for CNI:* Orchestrated cyberattacks on CNI for Estonia, Georgia and others from 2007 onwards led to major work on cyber CNI.
- *Major National Investment programmes* for Cybersecurity for CNI is now in place for USA, UK, Canada, Europe & Far East as previously discussed
- *Significant Cyber Focus* now for CNI in ALL major economic sectors such as Defence, Finance, Energy, Utilities, Transport, IT, Comms & Healthcare.

Critical Sectors and Infrastructure in *Cyberspace*



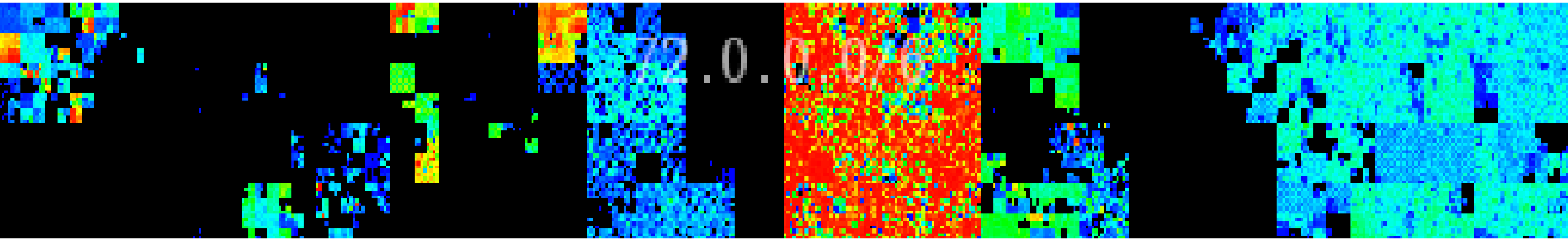
Cyber Crime against Critical Economic Sectors

- *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
- *Telecoms/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)

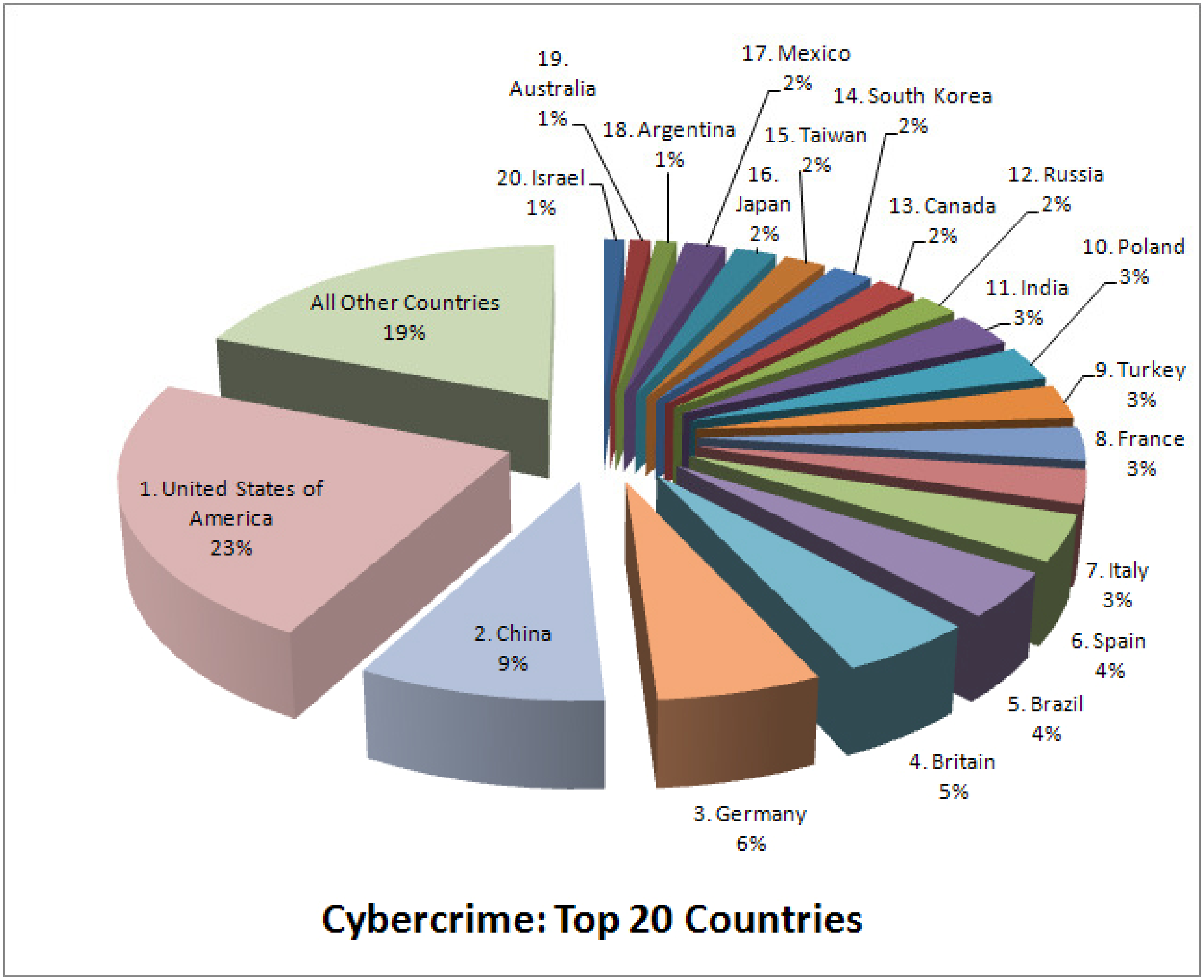
...Cybersecurity is a Critical National Issue that now requires a Global Response!

Cybersecurity for Critical National Infrastructure (CNI)

1 – The Strategic Importance of CNI	**2 – Evolving Cyber Threats for CNI Sectors**	3 – National & International CNI Plans
4 – 21stC Smart Systems – “Design Toolkit”	5 – Banking & Finance Sector – Analysis	6 – Energy & Transport Sectors - Analysis
7 – Civil and National Defence - Analysis	8 – CNI Security for “Internet of Things”	9 – Smart Security for YOUR Business!



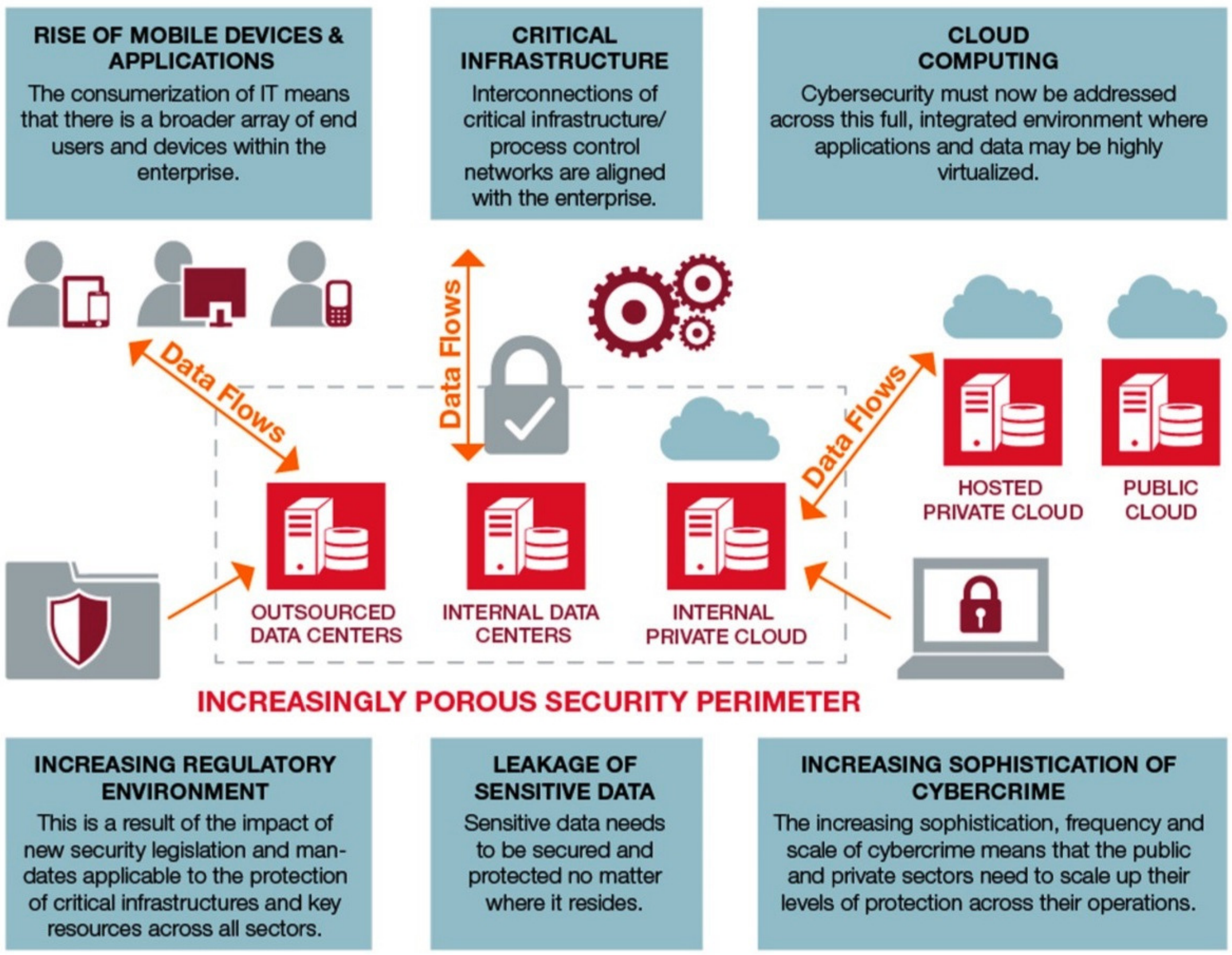
International CyberCrime: *Top 20 Countries*



Cybercrime: Top 20 Countries

Contemporary Cybersecurity Challenges

Cybersecurity Challenges and Interrelationships



RISE OF MOBILE DEVICES & APPLICATIONS

The consumerization of IT means that there is a broader array of end users and devices within the enterprise.

CRITICAL INFRASTRUCTURE

Interconnections of critical infrastructure/ process control networks are aligned with the enterprise.

CLOUD COMPUTING

Cybersecurity must now be addressed across this full, integrated environment where applications and data may be highly virtualized.

INCREASING REGULATORY ENVIRONMENT

This is a result of the impact of new security legislation and mandates applicable to the protection of critical infrastructures and key resources across all sectors.

LEAKAGE OF SENSITIVE DATA

Sensitive data needs to be secured and protected no matter where it resides.

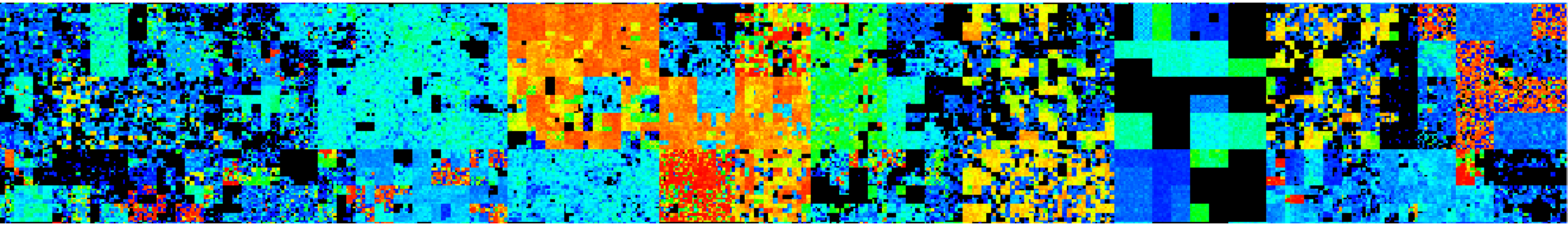
INCREASING SOPHISTICATION OF CYBERCRIME

The increasing sophistication, frequency and scale of cybercrime means that the public and private sectors need to scale up their levels of protection across their operations.

INCREASING SOPHISTICATION OF CYBERCRIME

Cybersecurity for Critical National Infrastructure (CNI)

1 – The Strategic Importance of CNI	2 – Evolving Cyber Threats for CNI Sectors	3 – National and International CNI Plans
4 – 21stC Smart Systems – "Design Toolkit"	5 – Banking & Finance Sector – Analysis	6 – Energy & Transport Sectors - Analysis
7 – Civil and National Defence - Analysis	8 –CNI Security for "Internet of Things"	9 – Smart Security for YOUR Business!



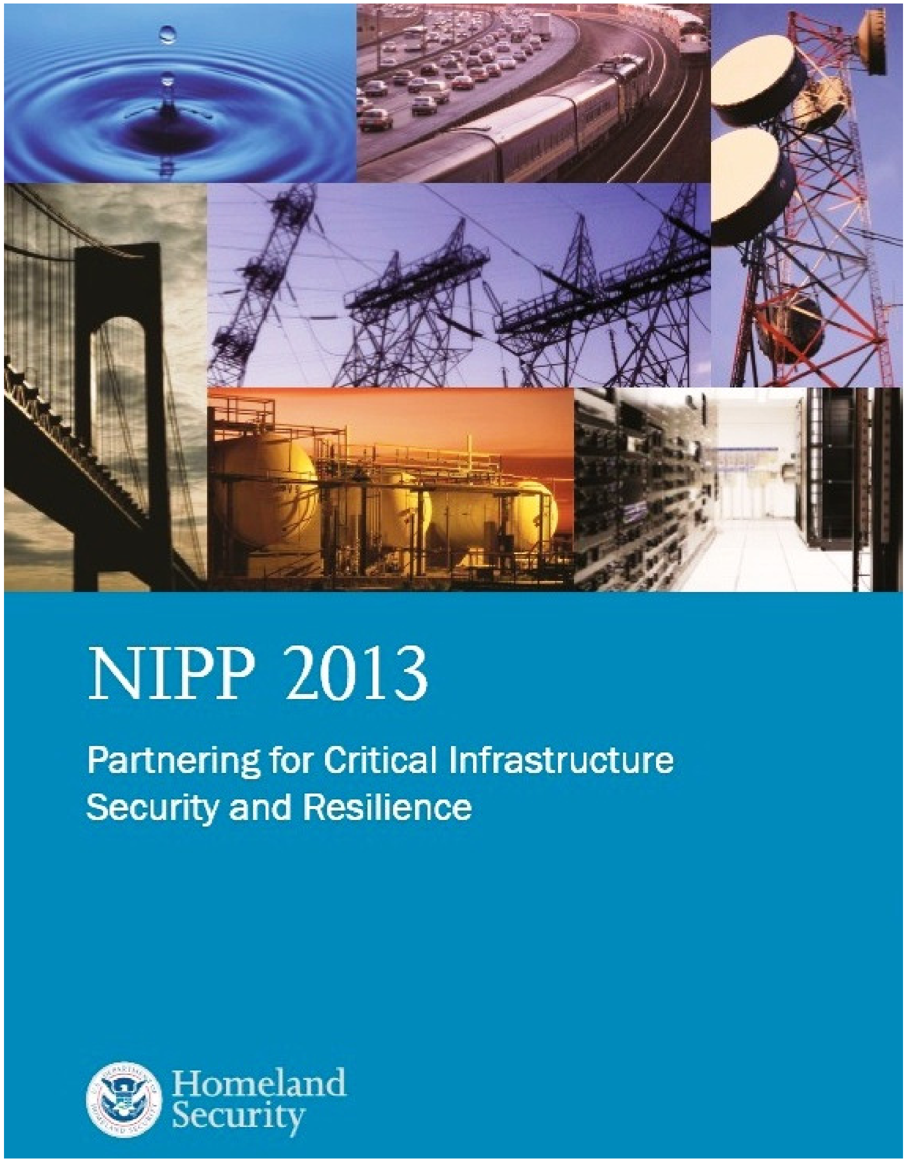
Some National & International *"CNI/CII"* Plans

- *USA:* NIPP 2013 – Partnering for Critical Infrastructure Security and Resilience
- *Canada:* National Strategy and Action Plan for Critical Infrastructure
- *UN/ITU:* Generic National Framework for CIIP
- *Joint Canada-USA* Action Plan for Critical Infrastructure
- *Australia:* National Guidelines for Protecting CNI from Terrorism
- *Germany:* CIP Implementation Plan of the National Plan for CIIP
- *UK - Cabinet Office:* Strategic Framework and Policy Statement on Improving the Resilience of CII . Also the "2013 Sector Resilience Plans"
- *Scotland:* Secure and Resilient – A Strategic CNI Framework for Scotland
- *OECD:* Recommendation of the Council on the Protection of CII

CNI: *Critical National Infrastructure*

CIIP: *Critical Information Infrastructure Protection*

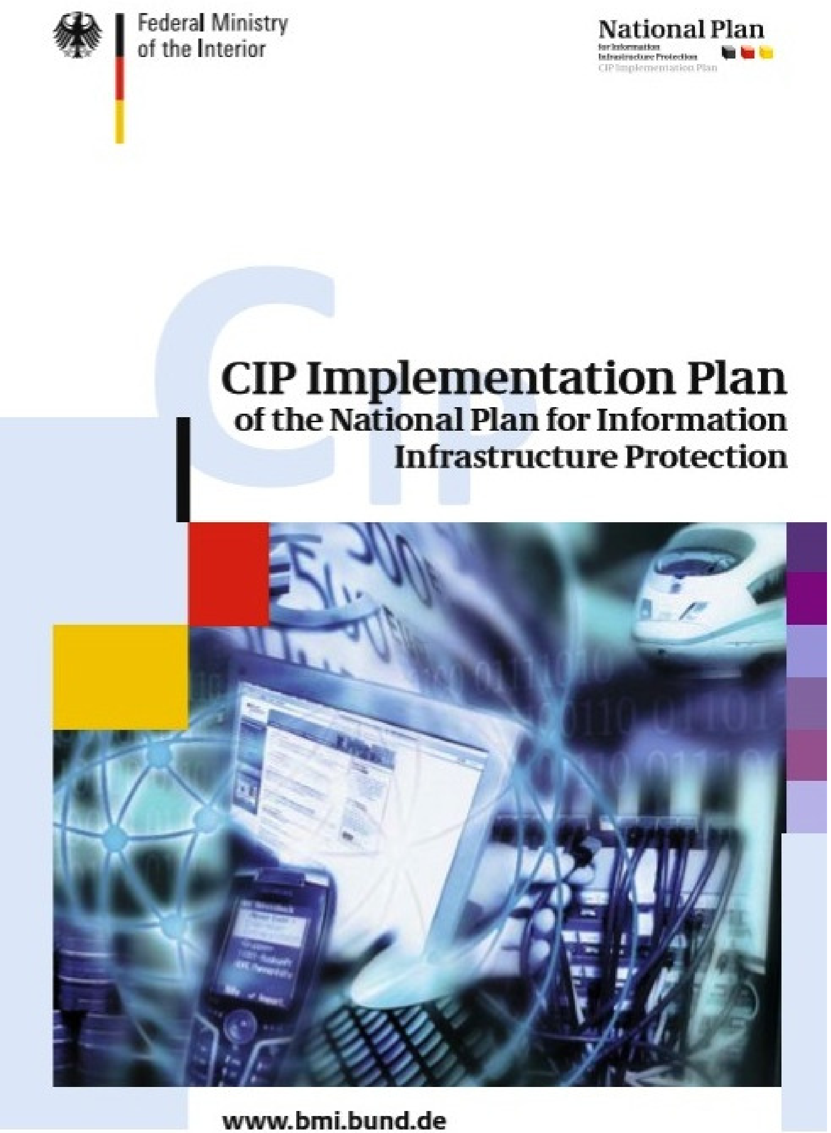
National Plans for CNIP/CIIP - Critical Information Infrastructure Protection: *USA and Germany*



NIPP 2013

Partnering for Critical Infrastructure Security and Resilience

Homeland Security



Federal Ministry of the Interior

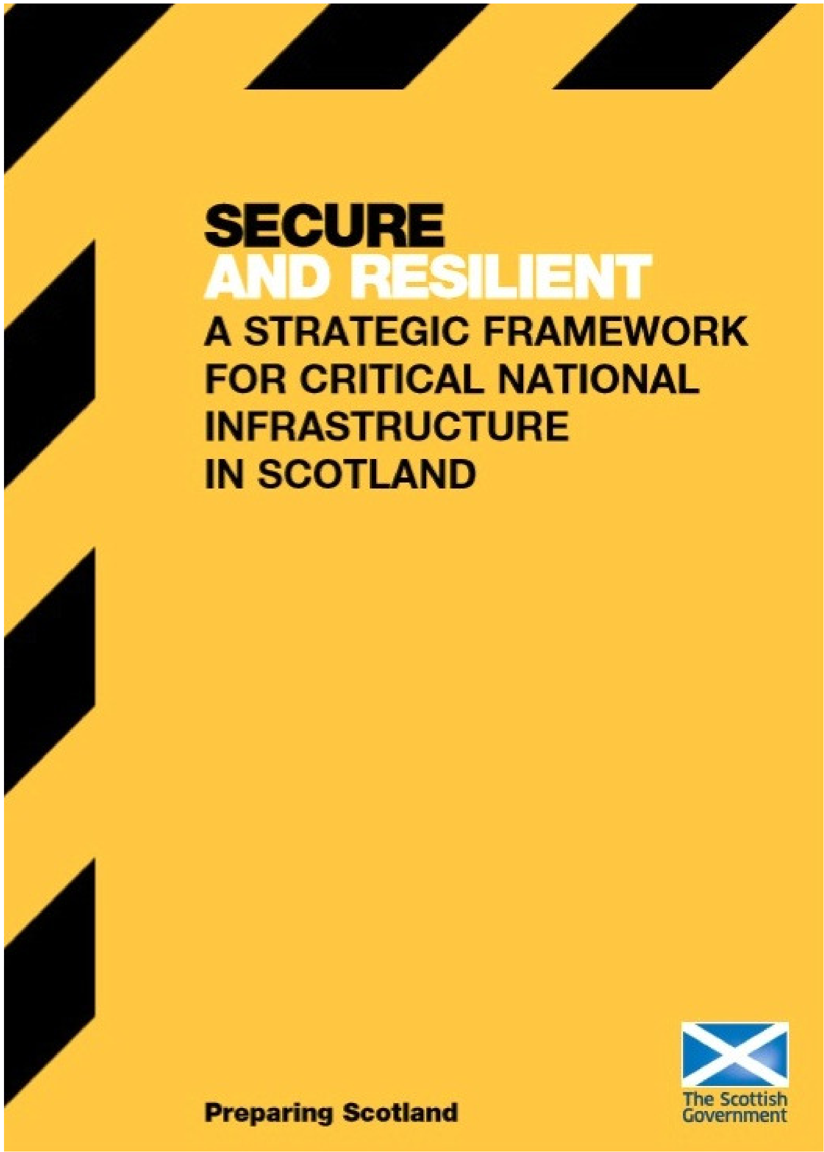
National Plan
for Information
Infrastructure Protection
CIP Implementation Plan

CIP Implementation Plan
of the National Plan for Information Infrastructure Protection

www.bmi.bund.de

Regional Strategic Plans for CNIP/CIIP:

Scotland, UK and Washington State, USA

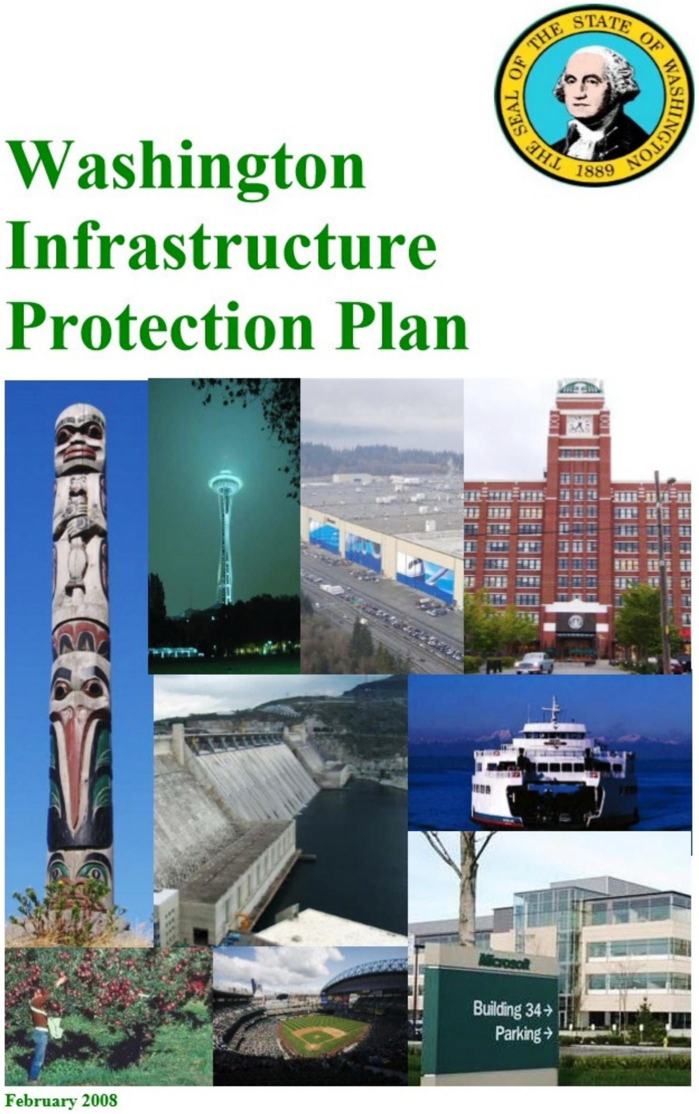


SECURE AND RESILIENT

A STRATEGIC FRAMEWORK FOR CRITICAL NATIONAL INFRASTRUCTURE IN SCOTLAND

Preparing Scotland

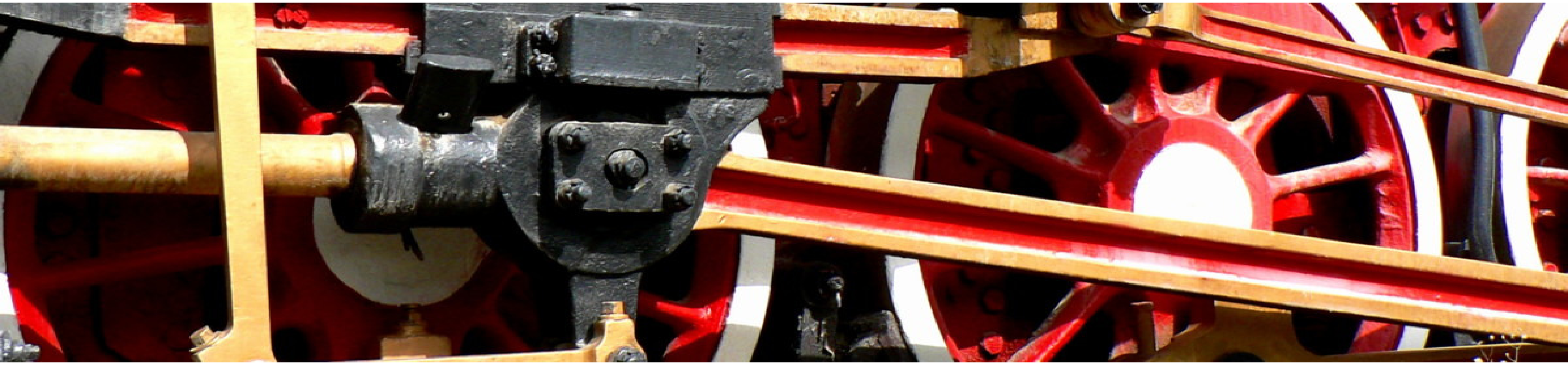
The Scottish Government



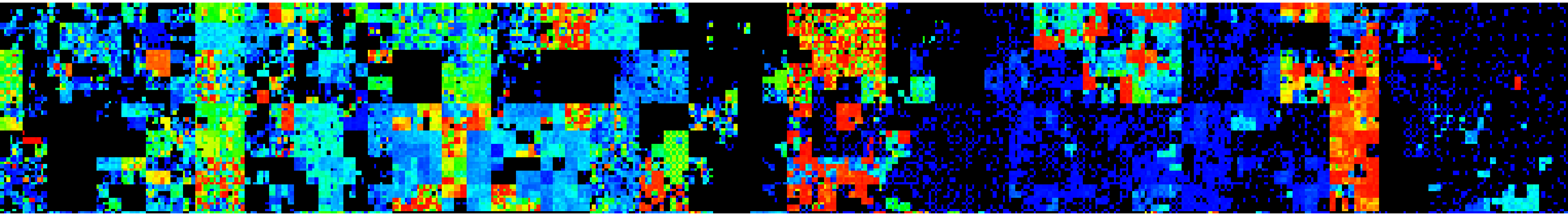
Washington Infrastructure Protection Plan

February 2008

Cybersecurity for Critical National Infrastructure (CNI)



1 – The Strategic Importance of CNI	2 – Evolving Cyber Threats for CNI Sectors	3 – National & International CNI Plans
4 – 21stC Smart Systems – “Design Toolkit”	5 – Banking & Finance Sector – Analysis	6 – Energy & Transport Sectors - Analysis
7 - Civil and National Defence - Analysis	8 – CNI Security for “Internet of Things”	9 – Smart Security for YOUR Business!



Basic Principles of Smart Security Solutions

- In the opening talk we provided some background theory and basic principles for Smart Systems which we summarise here:

……..Smart Security Solutions typically possess the following features:

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) ***Sustainability:*** Embedded Security – *Everywhere in the Network!*
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

………Now we'll consider the practical applications of these principles on the critical economic business sectors for most nations!....

Transition to *Smart Security Design* for Critical National Information Infrastructure

- In this talk we'll apply the practical "Smart Security Design Principles" to just a selection of national economic sectors:

  1) *Banking and Finance*
  2) *Energy, Utilities and Transportation*
  3) *National Civil and Military Defence*
  4) *Healthcare and Social Welfare*
  5) *Education and Research*
  6) *ICT, Mobile and Telecommunications*
  7) *Central and Regional Government*

- You'll then be able to easily extend these "Smart Principles" to the other key critical economic sectors such as Manufacturing

Building our Smart Security "Toolkit"

(1) 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!

Building our Smart Security "Toolkit"

(2) 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 => 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

Hybrid Organisation: *Hierarchical & Organic*

- ***Transition*** from 19thC/20thC to 21stC Business & Governance requires fundamental re-structuring of operations:
  - ***19thC /20thC Industrial Organisations:*** Hierarchical Bureaucracies (Pyramids) to process data/information.
  - ***21stC Intelligent Organisations:*** Networked Peer-to-Peer Business & Agencies with data processed in cyber clouds
- ***Living Systems***, such as mammals, use hybrid organisation of their extended nervous system (brain & body) to optimise real-time learning and environmental adaptation
- ***Smart Security Solutions*** will also require hybrid organisation to optimise real-time response to cyber & physical attacks.

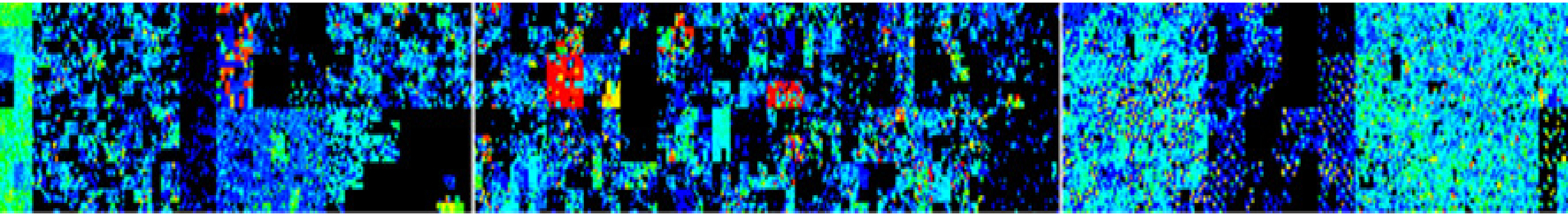
Smart Security – *"Design Toolkit"*

- The plan is now to apply the Smart Decision and Learning "Genes" as the transition design tools for these selected critical economic business sectors:
    - ***Smart Decision "D-Genes" :*** Spatial Geo-Location, Real-Time Operations, & Transforming Data to Decision through "Knowledge Lens"
    - ***Smart Learning "L-Genes":*** Adaptation, Self-Organisation, Scalable Architecture and Massive Memory & Data Storage
    - ***Smart Sustainability:*** Joint Operations for Cyber & Physical Security
    - ***Smart Governance:*** On-Line eGovernment Services together with new Laws, Legislation & Regulations for Cybercrime, eCommerce & Privacy

…..Together these Smart Principles form our "Design Toolkit"!

Cybersecurity for Critical National Infrastructure (CNI)

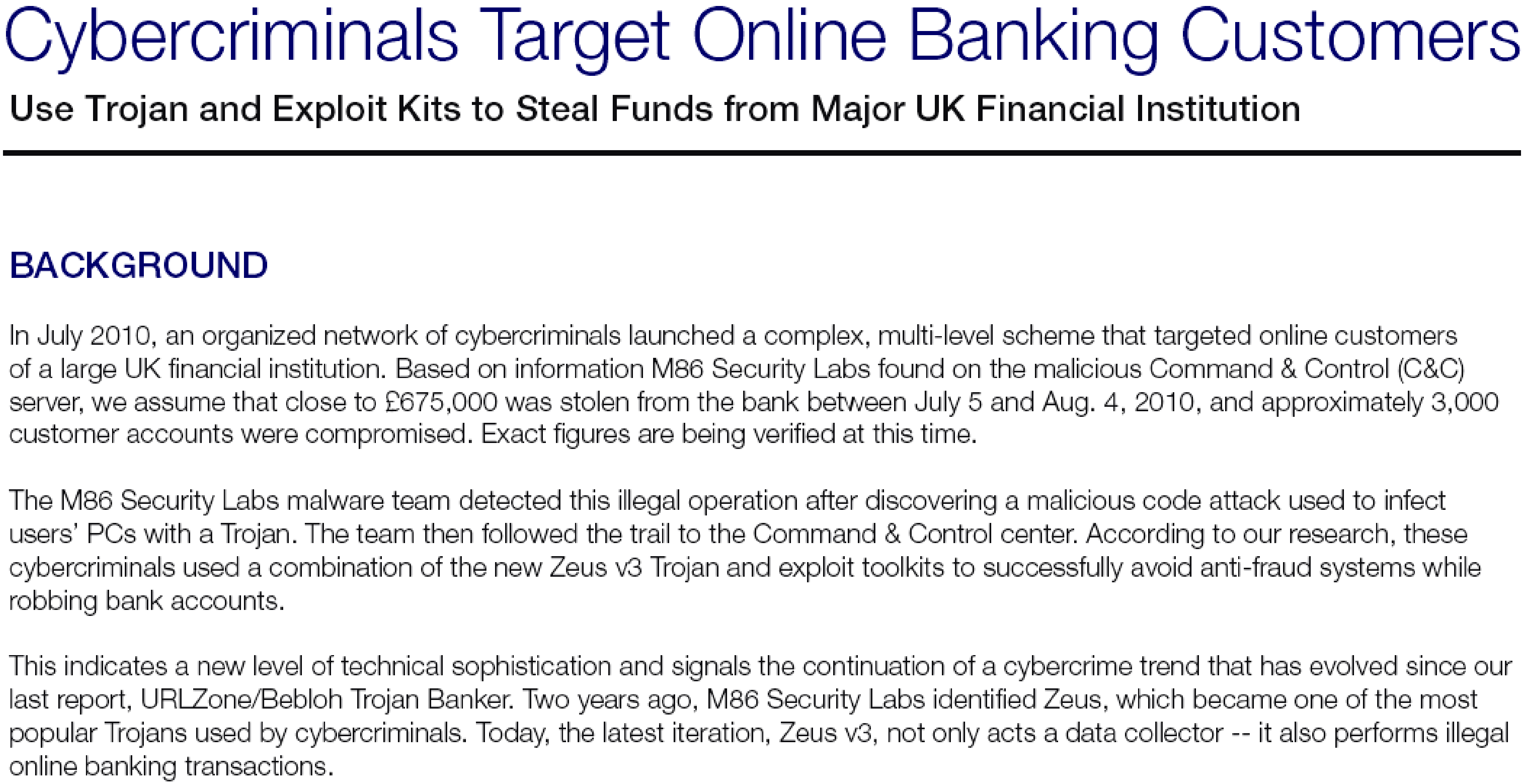
1 – The Strategic Importance of CNI	2 – Evolving Cyber Threats for CNI Sectors	3 – National & International CNI Plans
4 – 21stC Smart Systems – "Design Toolkit"	**5 – Banking and Finance Sector - Analysis**	6 – Energy & Transport Sectors - Analysis
7 – Civil and National Defence - Analysis	8 – CNI Security for "Internet of Things"	9 – Smart Security for YOUR Business!



“Smart Security” - *Banking and Finance*

- For each economic sector we’ll begin by analysing each of the critical sectors in the context of the Smart Genetic Design Principles of “Decisions” and “Learning”, and then discuss the implications for upgraded Smart Security and Governance:
  - ***Smart Decisions:***
    - *Geo-Location:* Smart Mobile Banking, with GPS Location to provide suggestions for shopping (based on profile), cafes, restaurants, nearby on-line friends…
    - *Real-Time:* Financial & Commodity Trading, on-line share dealing, maximise interest rates, foreign exchange dealing. Banking has really pioneered “real-time” financial trading & networking during last 30 years!
    - *Knowledge Lens:* Deep Data Mining, Business Intelligence2.0 and CRM (Customer Relationship Management for Banking & Investment Clients
  - ***Smart Learning:***
    - *Adaptation & Self-Organisation:* Investment Banks have pioneered applications of Smart Neural Network Apps, Adaptive Trading and Real-Time Risk Management.
    - *Massive Memory & Storage:* Secure Resilient Databases are Fundamental to Banking
    - *Scalable Architecture:* Banks are moving from “bricks & mortar” to global scalable networks, and most now provide mobile & home banking “apps” and highly secure on-line account services
  - ***Smart Sustainable Security*** Encryption, Portable Pin Pads, Biometrics, Cyber Risk Management
  - ***Smart Governance, Management and Operations :*** Data Integrity, Compliance & Audit, New Financial Regulations

Cybercriminals Target *Major UK Bank*



Cybercriminals Target Online Banking Customers

Use Trojan and Exploit Kits to Steal Funds from Major UK Financial Institution

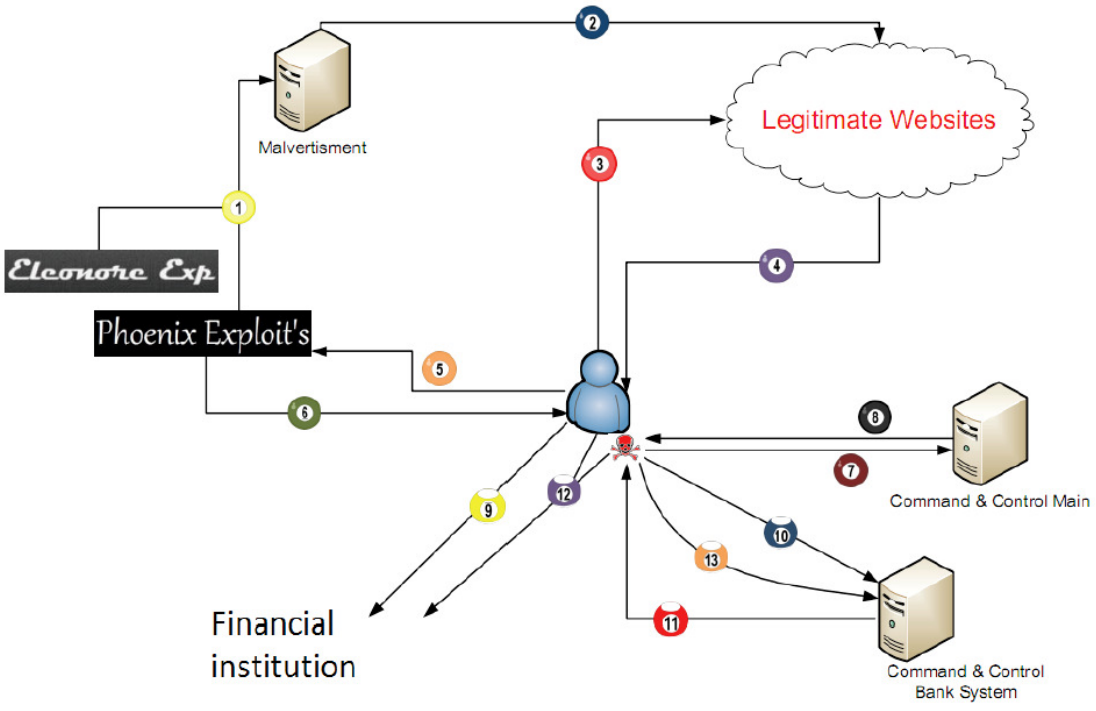
BACKGROUND

In July 2010, an organized network of cybercriminals launched a complex, multi-level scheme that targeted online customers of a large UK financial institution. Based on information M86 Security Labs found on the malicious Command & Control (C&C) server, we assume that close to £675,000 was stolen from the bank between July 5 and Aug. 4, 2010, and approximately 3,000 customer accounts were compromised. Exact figures are being verified at this time.

The M86 Security Labs malware team detected this illegal operation after discovering a malicious code attack used to infect users' PCs with a Trojan. The team then followed the trail to the Command & Control center. According to our research, these cybercriminals used a combination of the new Zeus v3 Trojan and exploit toolkits to successfully avoid anti-fraud systems while robbing bank accounts.

This indicates a new level of technical sophistication and signals the continuation of a cybercrime trend that has evolved since our last report, URLZone/Bebloh Trojan Banker. Two years ago, M86 Security Labs identified Zeus, which became one of the most popular Trojans used by cybercriminals. Today, the latest iteration, Zeus v3, not only acts a data collector -- it also performs illegal online banking transactions.

Process Flow of CyberCriminal Attack on Major UK *Financial Institution*: 2010



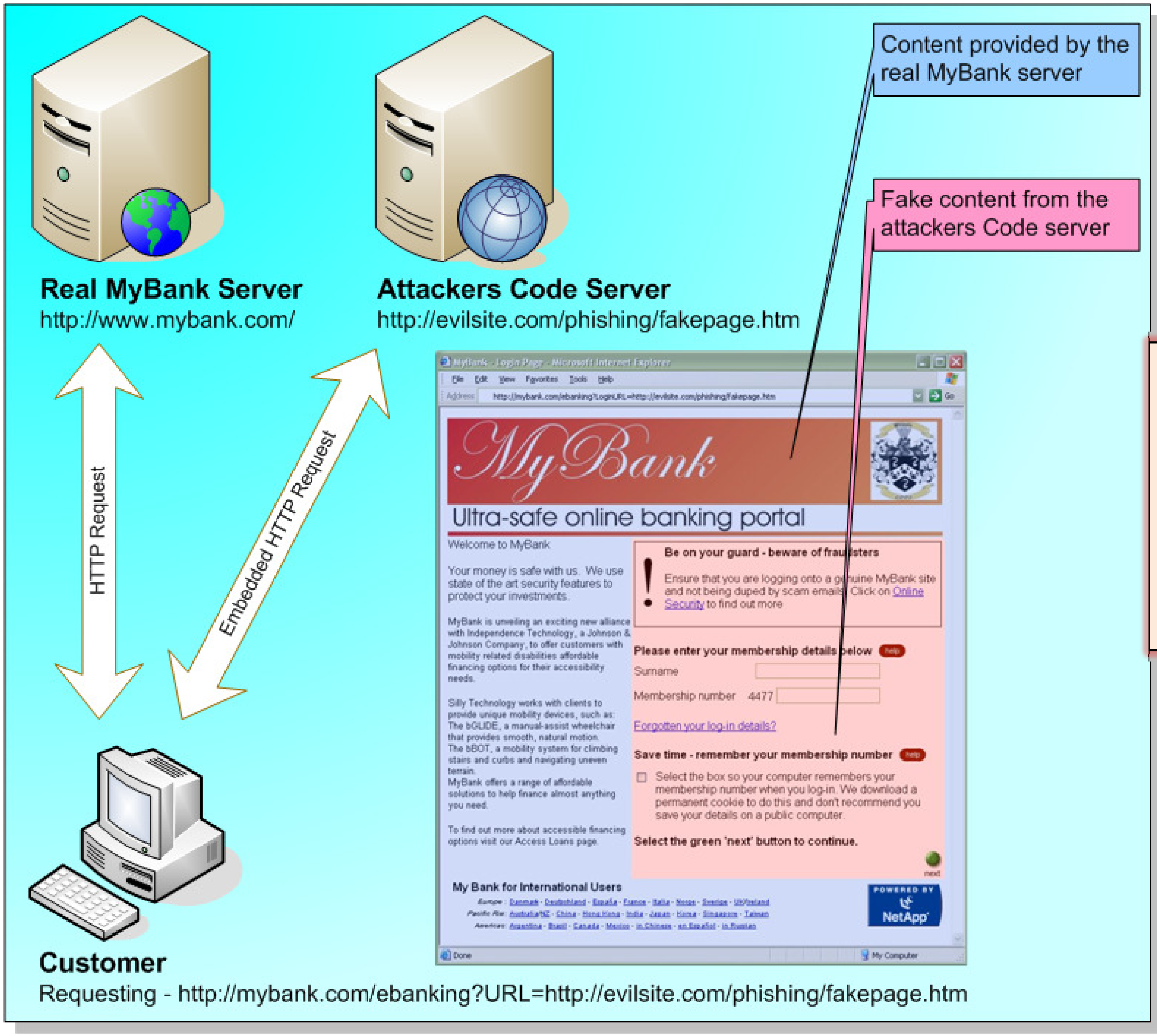
1. Uploads malicious advertisements to legitimate and fraud advertisements servers
2. The malicious advertisements published among the legitimate websites
3. User accesses to an infected website
4. The website content contains redirection to the malicious Exploit Kit
5. The user is redirected to the malicious Exploit Kit
6. The user's PC exploited, the payload was downloaded successfully
7. The Trojan reports for a new bot to the C&C
8. The C&C sends instruction to the Trojan
9. User access to financial institution
10. The Trojan reports for the user activities
11. The C&C sends commands to the Trojan to manipulate user bank transactions
12. Trojan manipulates User's bank transaction
13. Trojan reports the C&C about successful/failed transaction

Source: White Paper by M86 Security: Aug 2010

Such Cyber Attacks, with variations, take place regularly in *Banking & Financial Services*
... during Summer 2014 more than 83Million Accounts were "hacked" @ JP Morgan Chase

Financial Services Server - Cyber Attack:

Impact of XSS Cross-Site Scripting



Content provided by the real MyBank server

Fake content from the attackers Code server

Real MyBank Server
http://www.mybank.com/

Attackers Code Server
http://evilsite.com/phishing/fakepage.htm

MyBank - Login Page - Microsoft Internet Explorer

http://mybank.com/ebanking?LoginURL=http://evilsite.com/phishing/fakepage.htm

MyBank

Ultra-safe online banking portal

Welcome to MyBank

Your money is safe with us. We use state of the art security features to protect your investments.

MyBank is unveiling an exciting new alliance with Independence Technology, a Johnson & Johnson Company, to offer customers with mobility related disabilities affordable financing options for their accessibility needs.

Silly Technology works with clients to provide unique mobility devices, such as: The bGLIDE, a manual-assist wheelchair that provides smooth, natural motion. The bBOT, a mobility system for climbing stairs and curbs and navigating uneven terrain.
MyBank offers a range of affordable solutions to help finance almost anything you need.

To find out more about accessible financing options visit our Access Loans page.

Be on your guard - beware of fraudsters

Ensure that you are logging onto a genuine MyBank site and not being duped by scam emails. Click on Online Security to find out more

Please enter your membership details below help

Surname

Membership number 4477

Forgotten your log-in details?

Save time - remember your membership number help

☐ Select the box so your computer remembers your membership number when you log-in. We download a permanent cookie to do this and don't recommend you save your details on a public computer.

Select the green 'next' button to continue.

next

My Bank for International Users

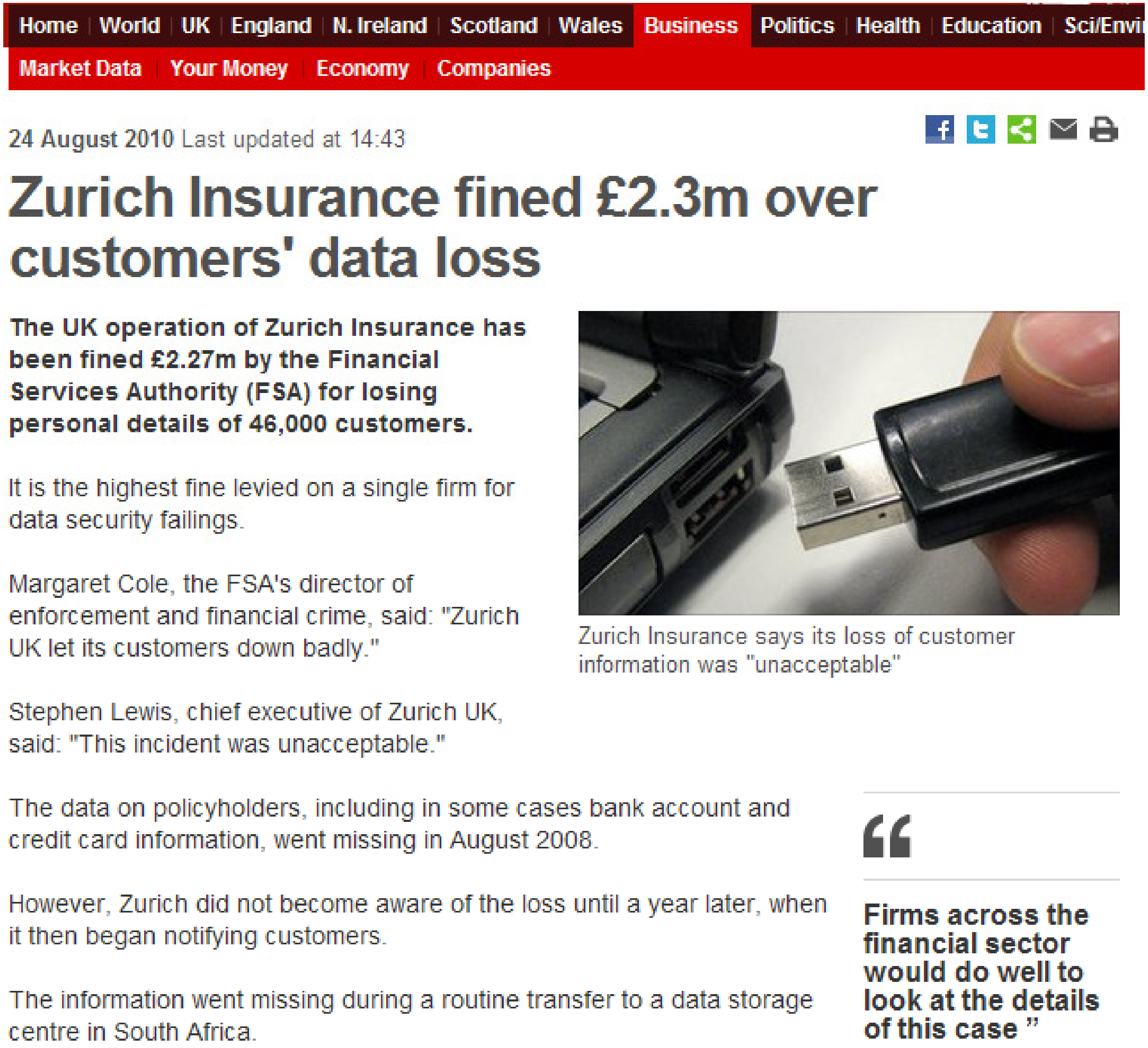
Europe: Danmark - Deutschland - España - France - Italia - Norge - Sverige - UK/Ireland
Pacific Rim: Australia/NZ - China - Hong Kong - India - Japan - Korea - Singapore - Taiwan
Americas: Argentina - Brasil - Canada - Mexico - in Chinese - en Español - in Russian

Customer
Requesting - http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm

Solution: Always check rigorously for data fields that allow user-input.

Ensure that there is no possibility for User Script input to be executed in website coded "php" or "asp" pages

Financial Services: Personal Data Loss



24 August 2010 Last updated at 14:43

Zurich Insurance fined £2.3m over customers' data loss

The UK operation of Zurich Insurance has been fined £2.27m by the Financial Services Authority (FSA) for losing personal details of 46,000 customers.

Zurich Insurance says its loss of customer information was "unacceptable"

It is the highest fine levied on a single firm for data security failings.

Margaret Cole, the FSA's director of enforcement and financial crime, said: "Zurich UK let its customers down badly."

Stephen Lewis, chief executive of Zurich UK, said: "This incident was unacceptable."

The data on policyholders, including in some cases bank account and credit card information, went missing in August 2008.

However, Zurich did not become aware of the loss until a year later, when it then began notifying customers.

The information went missing during a routine transfer to a data storage centre in South Africa.

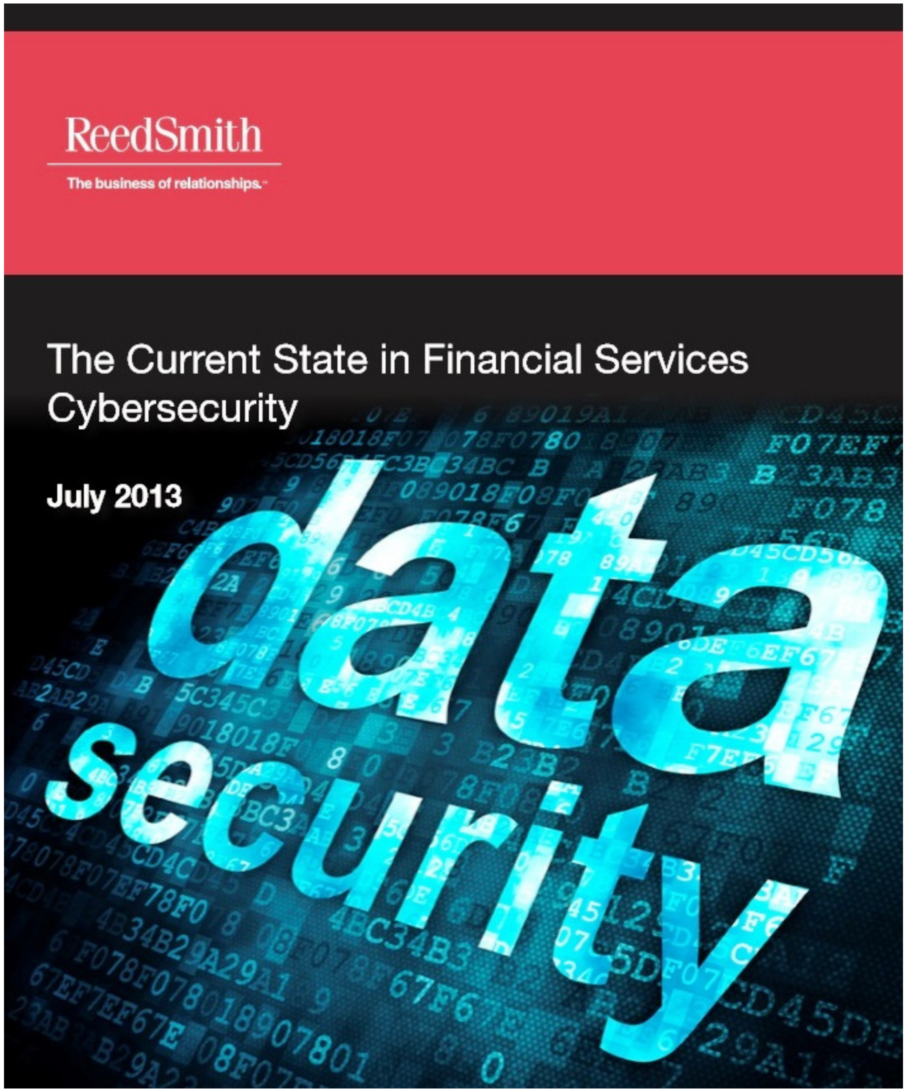
> **" Firms across the financial sector would do well to look at the details of this case "**

Cybersecurity for *Banking & Finance*

New York State

Department of Financial Services

Report on Cyber Security in the Banking Sector


ReedSmith

The business of relationships.

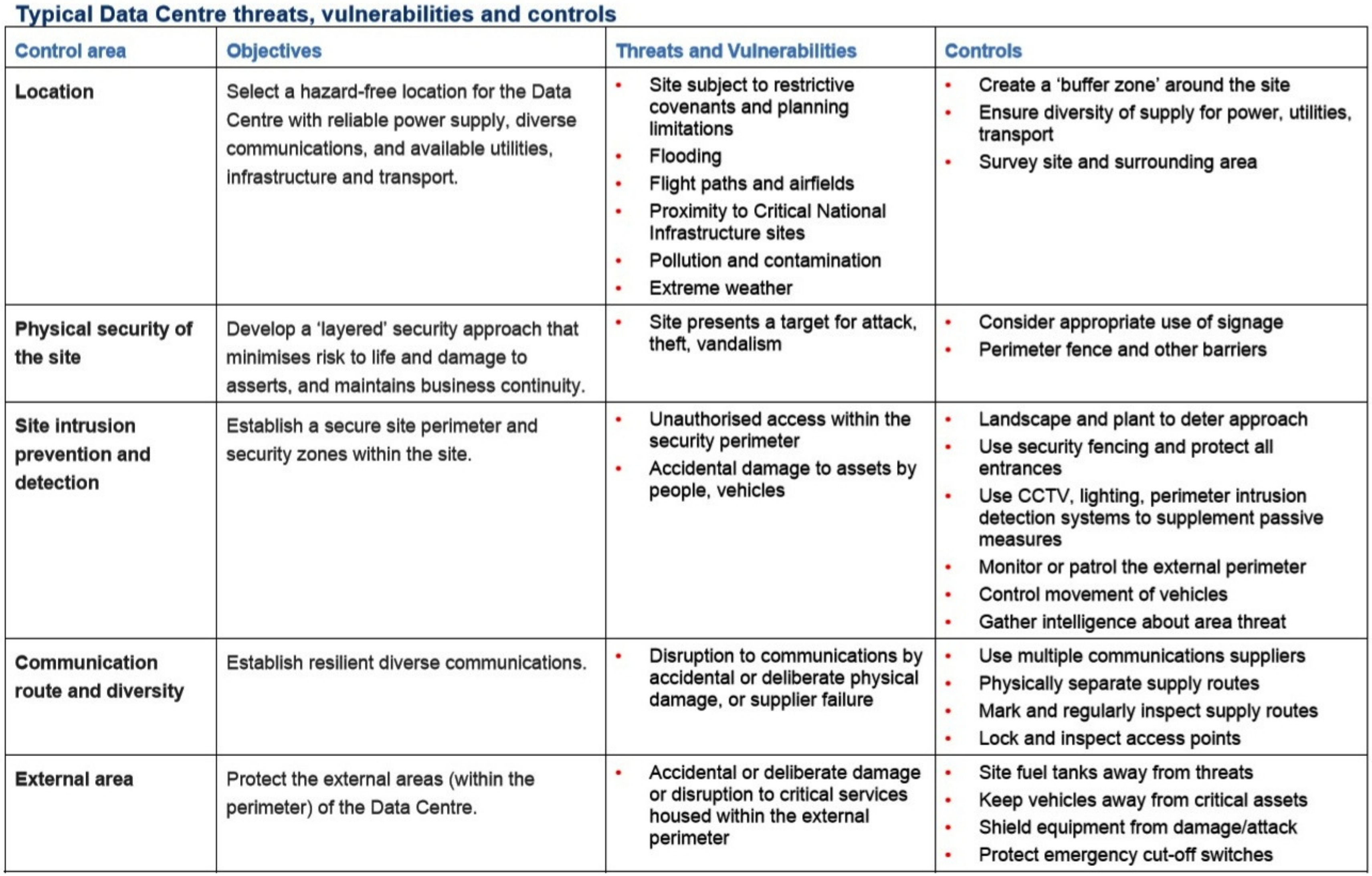
The Current State in Financial Services Cybersecurity

July 2013

Banking & Finance Sector: *Cybersecurity Threats*

- *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 cyber attacks 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

Typical Security Threats, Risks and Controls: *Financial Services Data Centre (1)*



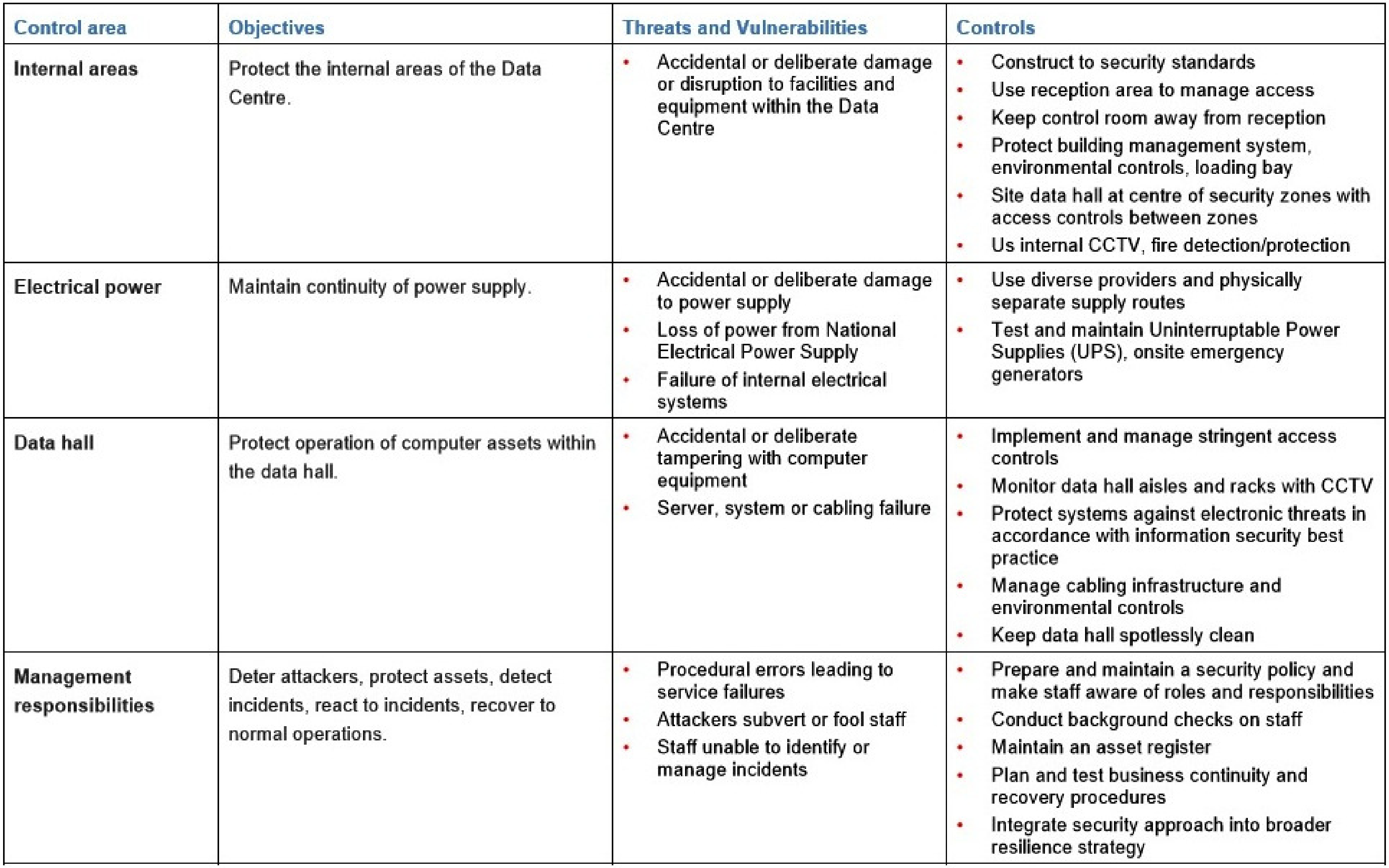
Typical Data Centre threats, vulnerabilities and controls

Control area	Objectives	Threats and Vulnerabilities	Controls
Location	Select a hazard-free location for the Data Centre with reliable power supply, diverse communications, and available utilities, infrastructure and transport.	• Site subject to restrictive covenants and planning limitations • Flooding • Flight paths and airfields • Proximity to Critical National Infrastructure sites • Pollution and contamination • Extreme weather	• Create a 'buffer zone' around the site • Ensure diversity of supply for power, utilities, transport • Survey site and surrounding area
Physical security of the site	Develop a 'layered' security approach that minimises risk to life and damage to asserts, and maintains business continuity.	• Site presents a target for attack, theft, vandalism	• Consider appropriate use of signage • Perimeter fence and other barriers
Site intrusion prevention and detection	Establish a secure site perimeter and security zones within the site.	• Unauthorised access within the security perimeter • Accidental damage to assets by people, vehicles	• Landscape and plant to deter approach • Use security fencing and protect all entrances • Use CCTV, lighting, perimeter intrusion detection systems to supplement passive measures • Monitor or patrol the external perimeter • Control movement of vehicles • Gather intelligence about area threat
Communication route and diversity	Establish resilient diverse communications.	• Disruption to communications by accidental or deliberate physical damage, or supplier failure	• Use multiple communications suppliers • Physically separate supply routes • Mark and regularly inspect supply routes • Lock and inspect access points
External area	Protect the external areas (within the perimeter) of the Data Centre.	• Accidental or deliberate damage or disruption to critical services housed within the external perimeter	• Site fuel tanks away from threats • Keep vehicles away from critical assets • Shield equipment from damage/attack • Protect emergency cut-off switches

Source: NY State Dept of Financial Services

Typical Security Threats, Risks and Controls:

Financial Services Data Centre (2)

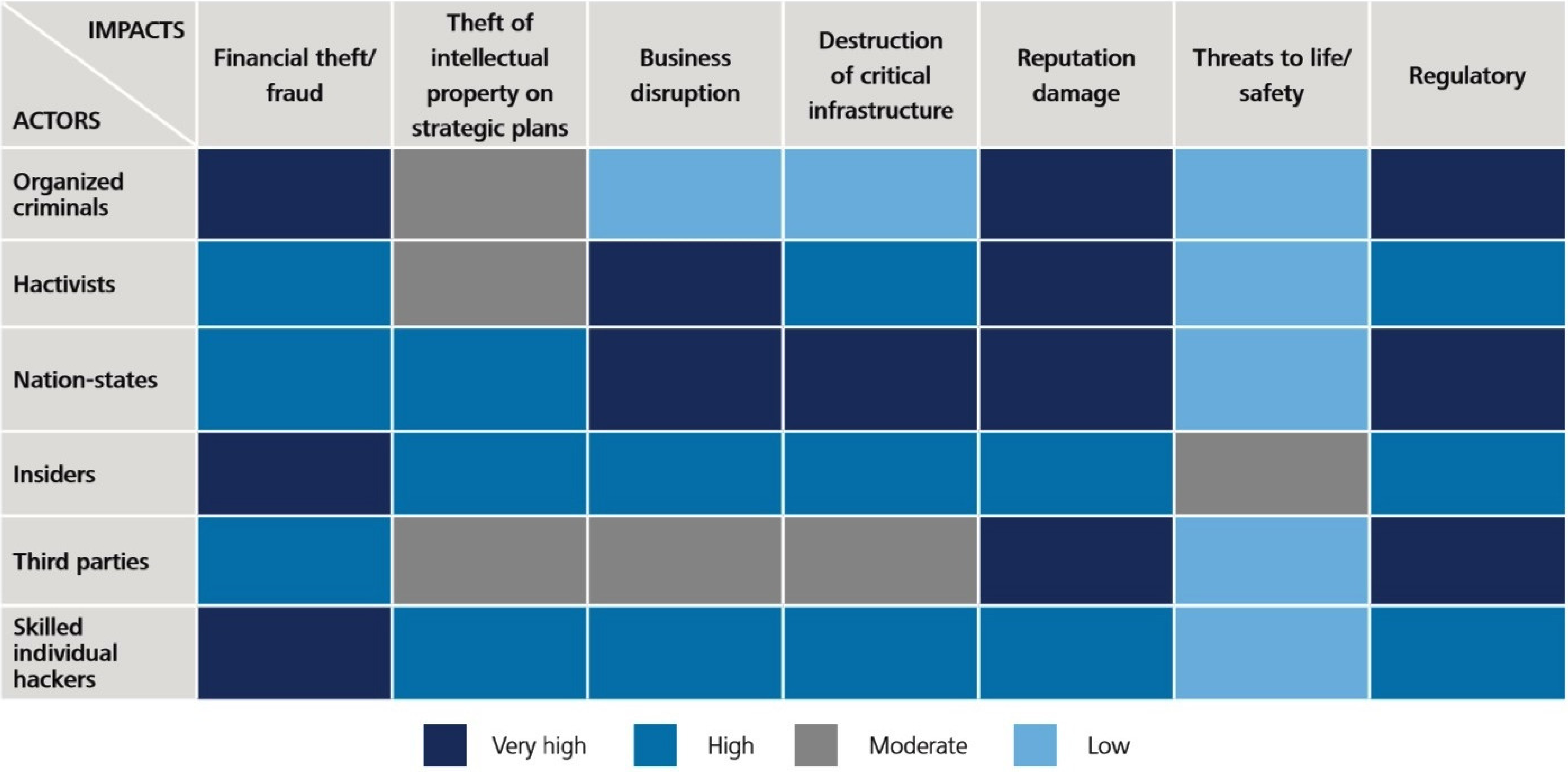


Control area	Objectives	Threats and Vulnerabilities	Controls
Internal areas	Protect the internal areas of the Data Centre.	• Accidental or deliberate damage or disruption to facilities and equipment within the Data Centre	• Construct to security standards • Use reception area to manage access • Keep control room away from reception • Protect building management system, environmental controls, loading bay • Site data hall at centre of security zones with access controls between zones • Us internal CCTV, fire detection/protection
Electrical power	Maintain continuity of power supply.	• Accidental or deliberate damage to power supply • Loss of power from National Electrical Power Supply • Failure of internal electrical systems	• Use diverse providers and physically separate supply routes • Test and maintain Uninterruptable Power Supplies (UPS), onsite emergency generators
Data hall	Protect operation of computer assets within the data hall.	• Accidental or deliberate tampering with computer equipment • Server, system or cabling failure	• Implement and manage stringent access controls • Monitor data hall aisles and racks with CCTV • Protect systems against electronic threats in accordance with information security best practice • Manage cabling infrastructure and environmental controls • Keep data hall spotlessly clean
Management responsibilities	Deter attackers, protect assets, detect incidents, react to incidents, recover to normal operations.	• Procedural errors leading to service failures • Attackers subvert or fool staff • Staff unable to identify or manage incidents	• Prepare and maintain a security policy and make staff aware of roles and responsibilities • Conduct background checks on staff • Maintain an asset register • Plan and test business continuity and recovery procedures • Integrate security approach into broader resilience strategy

Source: NY State Dept of Financial Services

Cybersecurity Threats & Risks for the Banking & Finance Sector

A typical cyber risk heat map for the banking sector



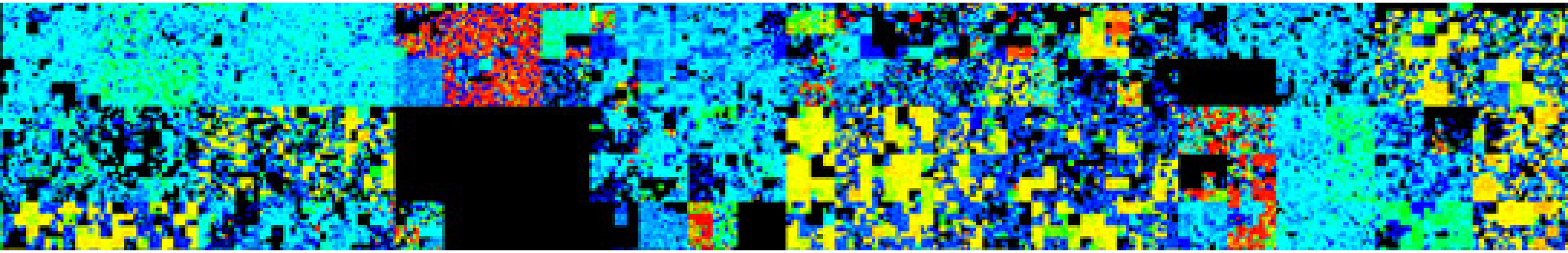
IMPACTS ACTORS	Financial theft/ fraud	Theft of intellectual property on strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life/ safety	Regulatory
Organized criminals	■	▨	□	□	■	□	■
Hactivists	🟦	▨	■	🟦	■	□	🟦
Nation-states	🟦	🟦	■	■	■	□	■
Insiders	■	🟦	🟦	🟦	🟦	▨	🟦
Third parties	🟦	▨	▨	▨	■	□	■
Skilled individual hackers	■	🟦	🟦	🟦	🟦	□	🟦

■ Very high 🟦 High ▨ Moderate □ Low

Source: Deloitte Center for Financial Services analysis

Cybersecurity for Critical National Infrastructure (CNI)

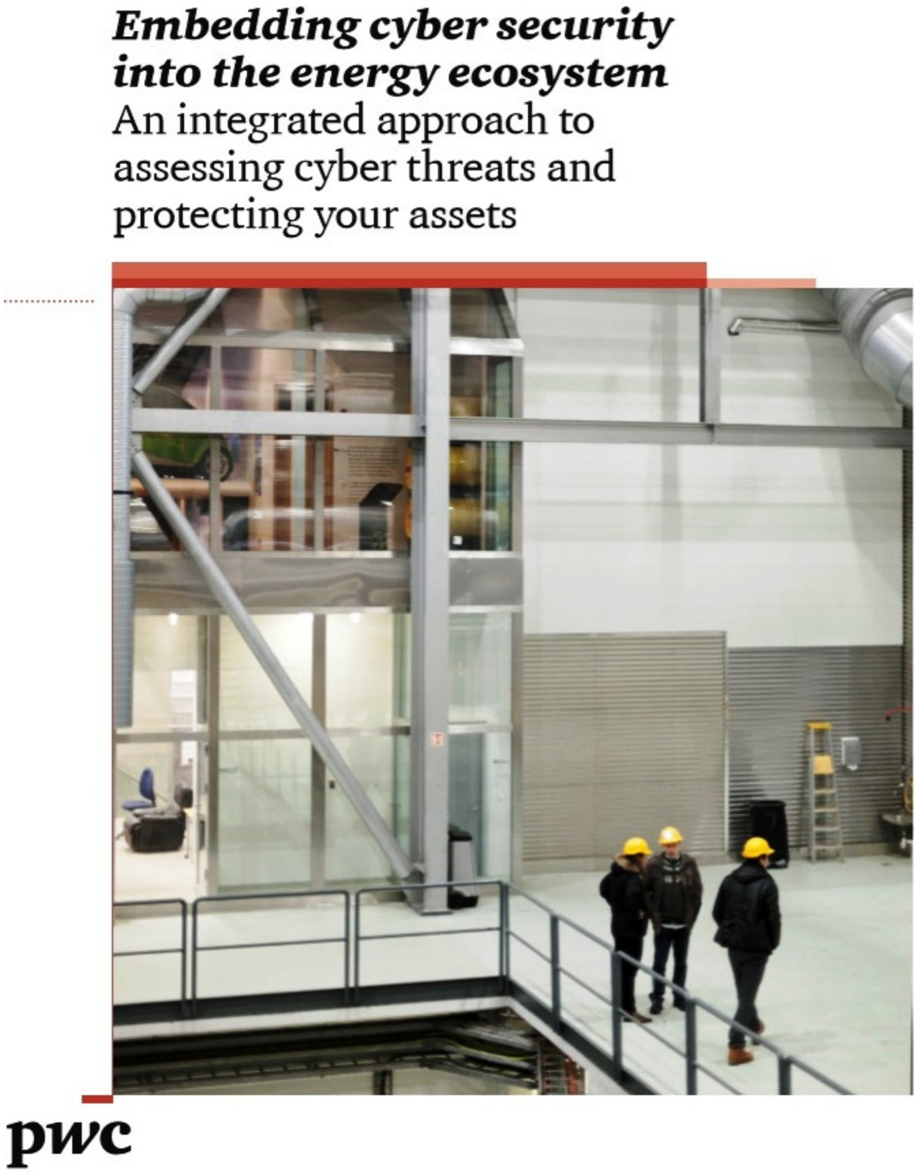
1 – The Strategic Importance of CNI	2 –Evolving Cyber Threats for CNI Sectors	3 – National & International CNI Plans
4 – 21stC Smart Systems – “Design Toolkit”	5 – Banking & Finance Sector – Analysis	**6 – Energy & Transport Sectors - Analysis**
7 – Civil and National Defence - Analysis	8 – CNI Security for “Internet of Things”	9 – Smart Security for YOUR Business!



"Smart Security" – *Energy & Utilities*

- ***Smart Decisions:***
  - *Geo-Location:* Managing & optimised local energy & utility needs within homes, apartments, offices, factories and public buildings.
  - *Real-Time:* Ensuring that key power plants & utilities, such as water supply, can meet regional requirements second-by-second.
  - *Knowledge Lens:* Forecasting future demand for oil, gas, electricity and water based upon historical usage & forecast economic growth/decline
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Adapting to local, regional & national energy demand through dynamic management control systems
  - *Massive Memory & Storage:* Consumer & Business Billing & Payment Databases
  - *Scalable Architecture:* Energy Grids are also scalable networks from local pipes and cables to the central coal, oil or nuclear plant
- ***Smart Security:*** Resilience to cyber attacks to SCADA control systems by sophisticated trojans such as Stuxnet, as well as physical plant protection
- ***Smart Governance:*** Regular physical inspections & audits to minimise risks from major incident such as power shutdown, radiation, chemical or water leaks

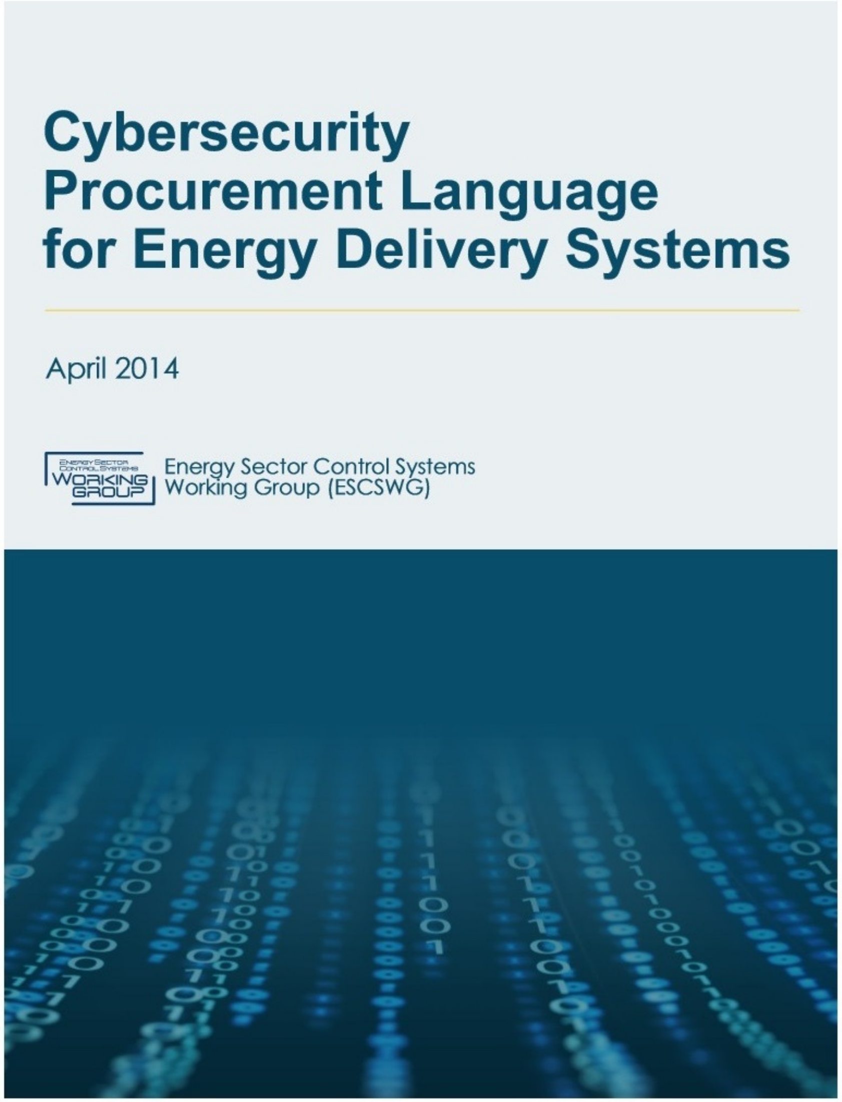
Recent Analysis & Policies for Cybersecurity in the *Energy Sector*



Embedding cyber security into the energy ecosystem

An integrated approach to assessing cyber threats and protecting your assets

pwc

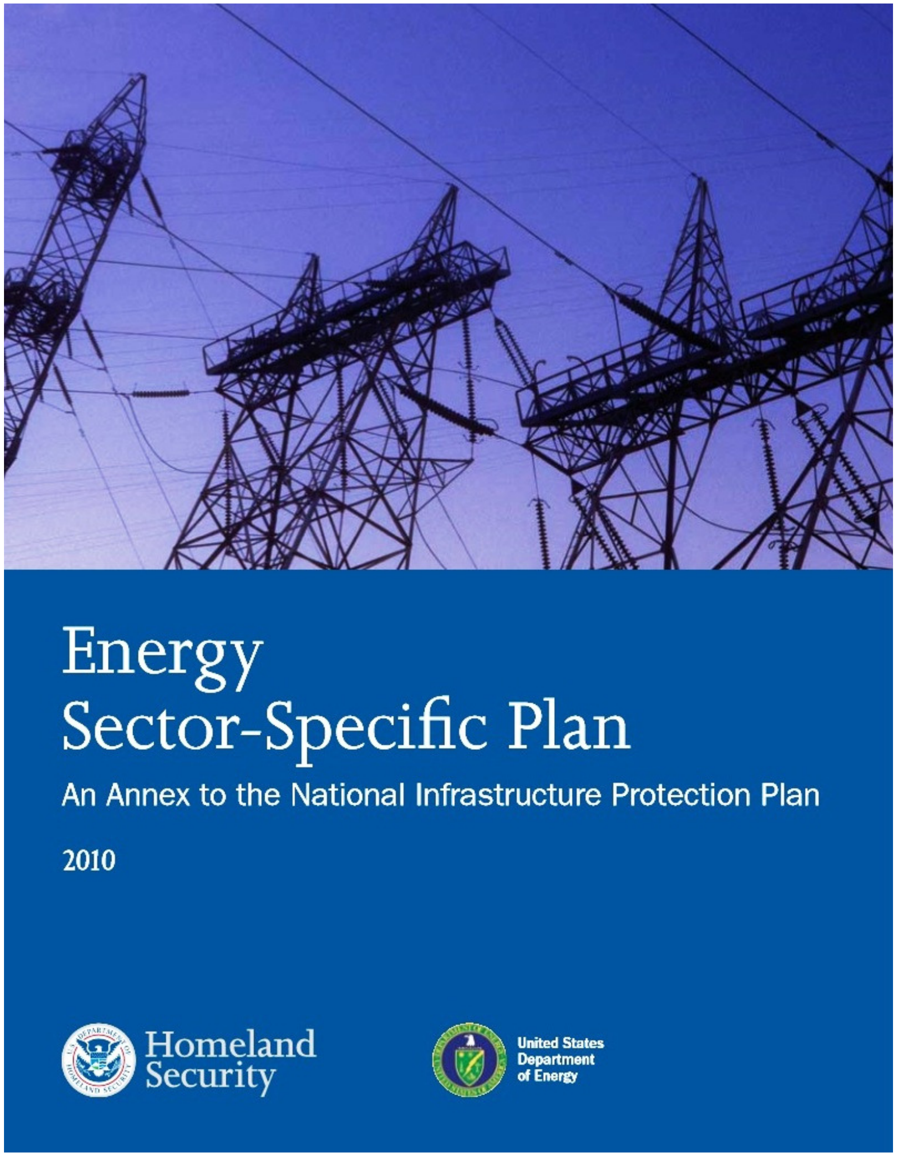


Cybersecurity Procurement Language for Energy Delivery Systems

April 2014

Energy Sector Control Systems Working Group (ESCSWG)

Cybersecurity for Critical Information Infrastructure of the *Energy Sector*



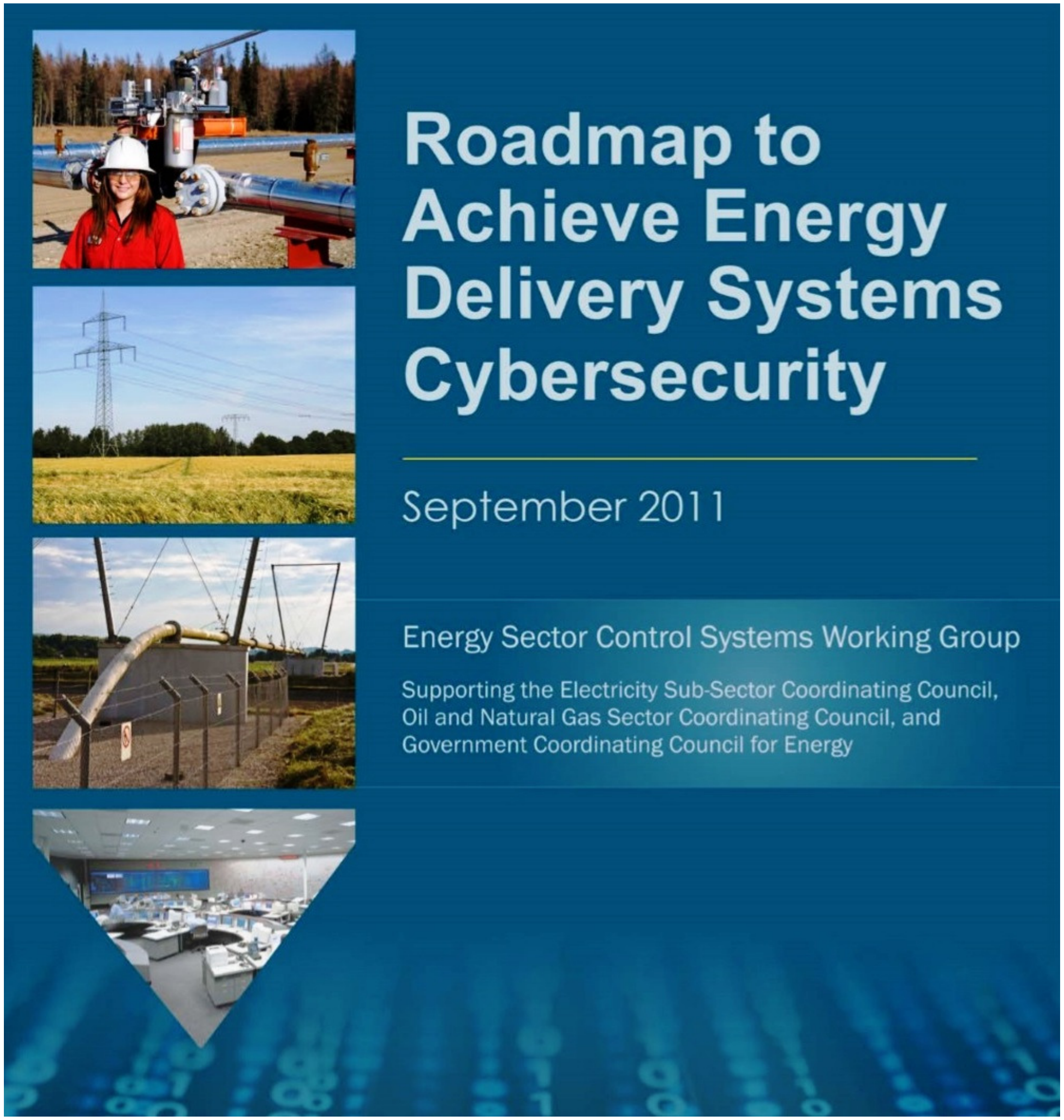
Energy
Sector-Specific Plan

An Annex to the National Infrastructure Protection Plan

2010

Homeland Security

United States Department of Energy



Roadmap to Achieve Energy Delivery Systems Cybersecurity

September 2011

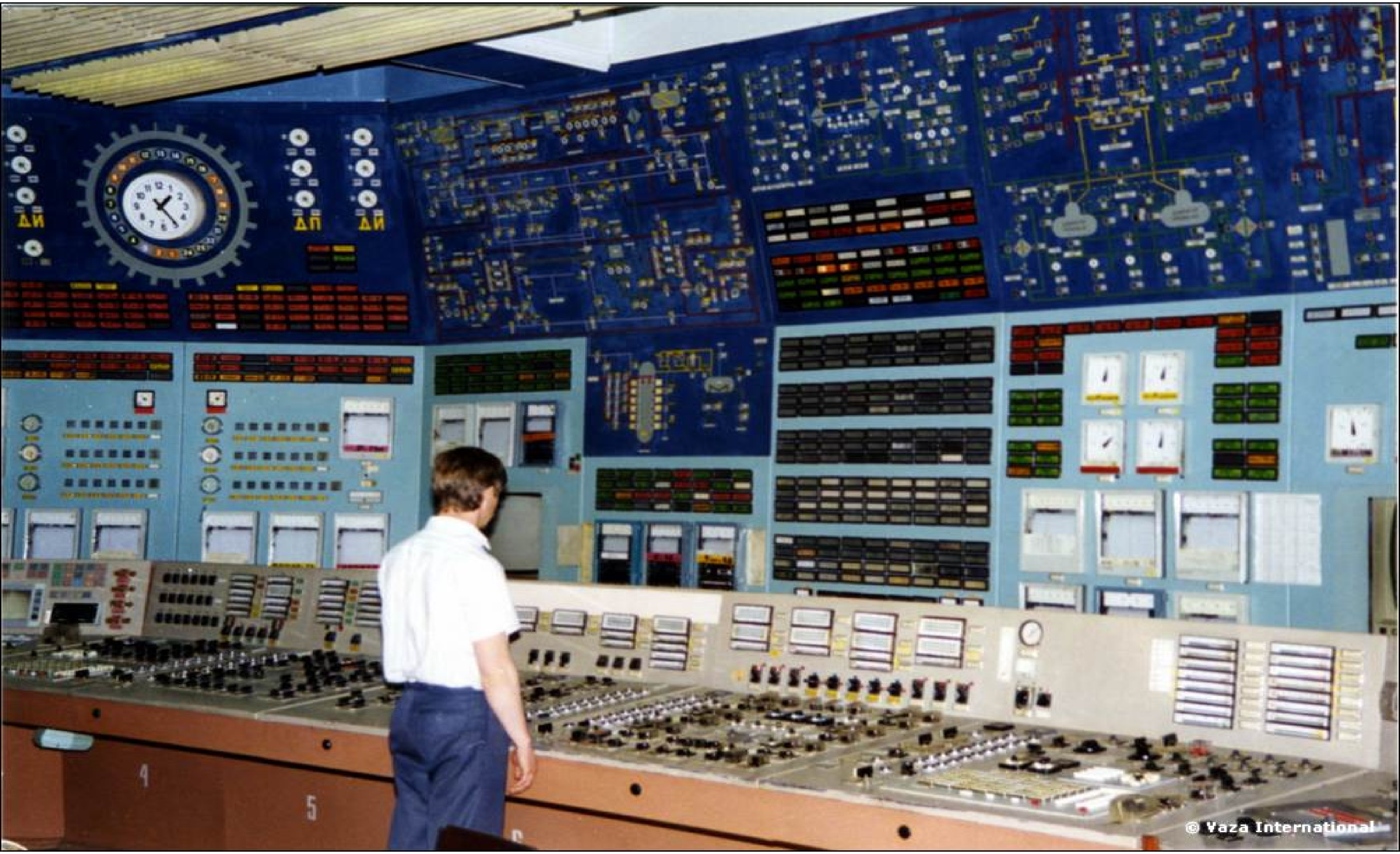
Energy Sector Control Systems Working Group

Supporting the Electricity Sub-Sector Coordinating Council, Oil and Natural Gas Sector Coordinating Council, and Government Coordinating Council for Energy

International "KolaNet" Project Team:

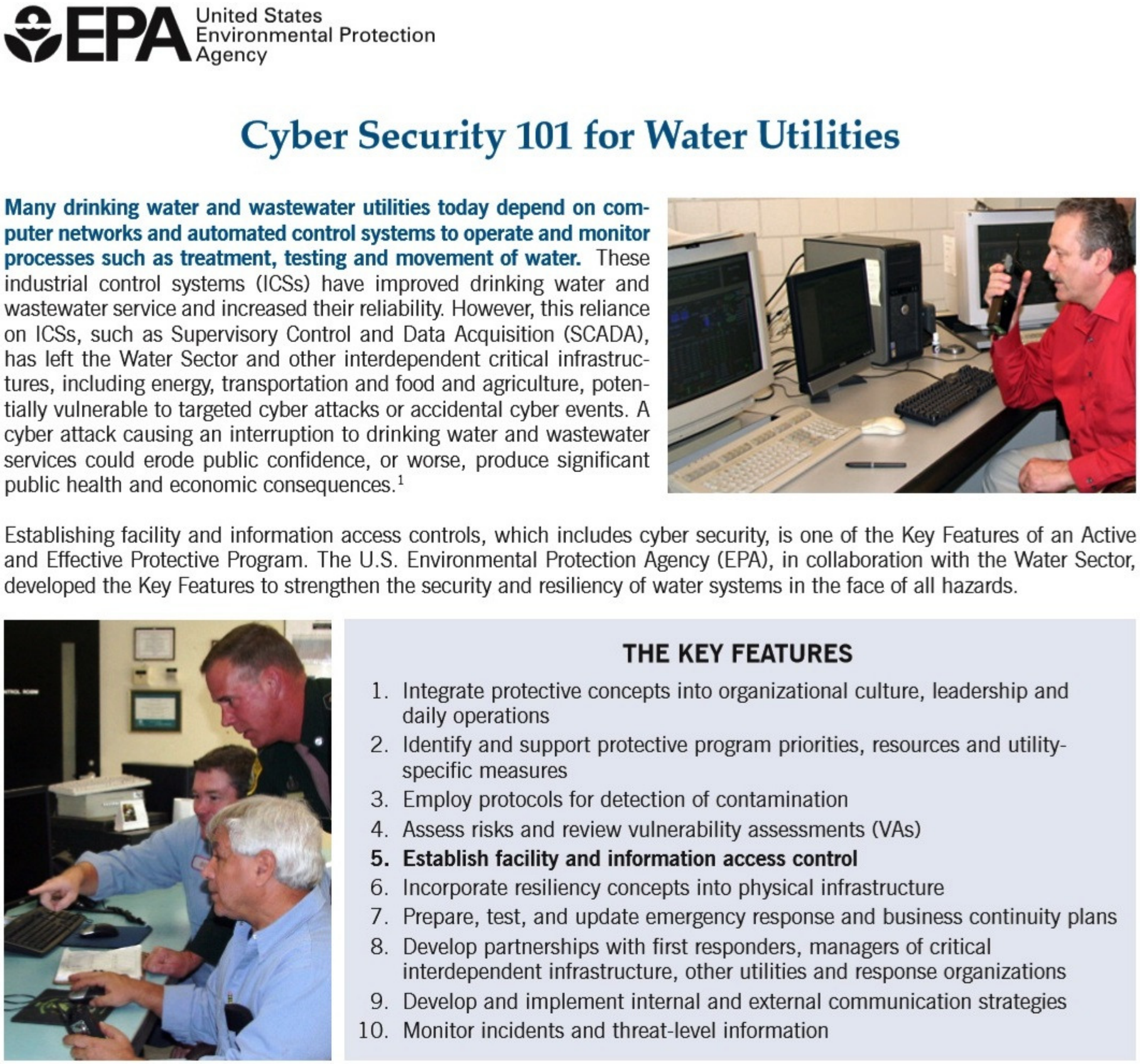
Regional Nuclear Safety & Security

Control Room - *Kola Nuclear Power Station* - Russia



KolaNet Project for *Nuclear Safety & Security* :1990s

Cybersecurity for the *Water Utilities*



United States Environmental Protection Agency

Cyber Security 101 for Water Utilities

Many drinking water and wastewater utilities today depend on computer networks and automated control systems to operate and monitor processes such as treatment, testing and movement of water. These industrial control systems (ICSs) have improved drinking water and wastewater service and increased their reliability. However, this reliance on ICSs, such as Supervisory Control and Data Acquisition (SCADA), has left the Water Sector and other interdependent critical infrastructures, including energy, transportation and food and agriculture, potentially vulnerable to targeted cyber attacks or accidental cyber events. A cyber attack causing an interruption to drinking water and wastewater services could erode public confidence, or worse, produce significant public health and economic consequences.[1]

Establishing facility and information access controls, which includes cyber security, is one of the Key Features of an Active and Effective Protective Program. The U.S. Environmental Protection Agency (EPA), in collaboration with the Water Sector, developed the Key Features to strengthen the security and resiliency of water systems in the face of all hazards.

THE KEY FEATURES

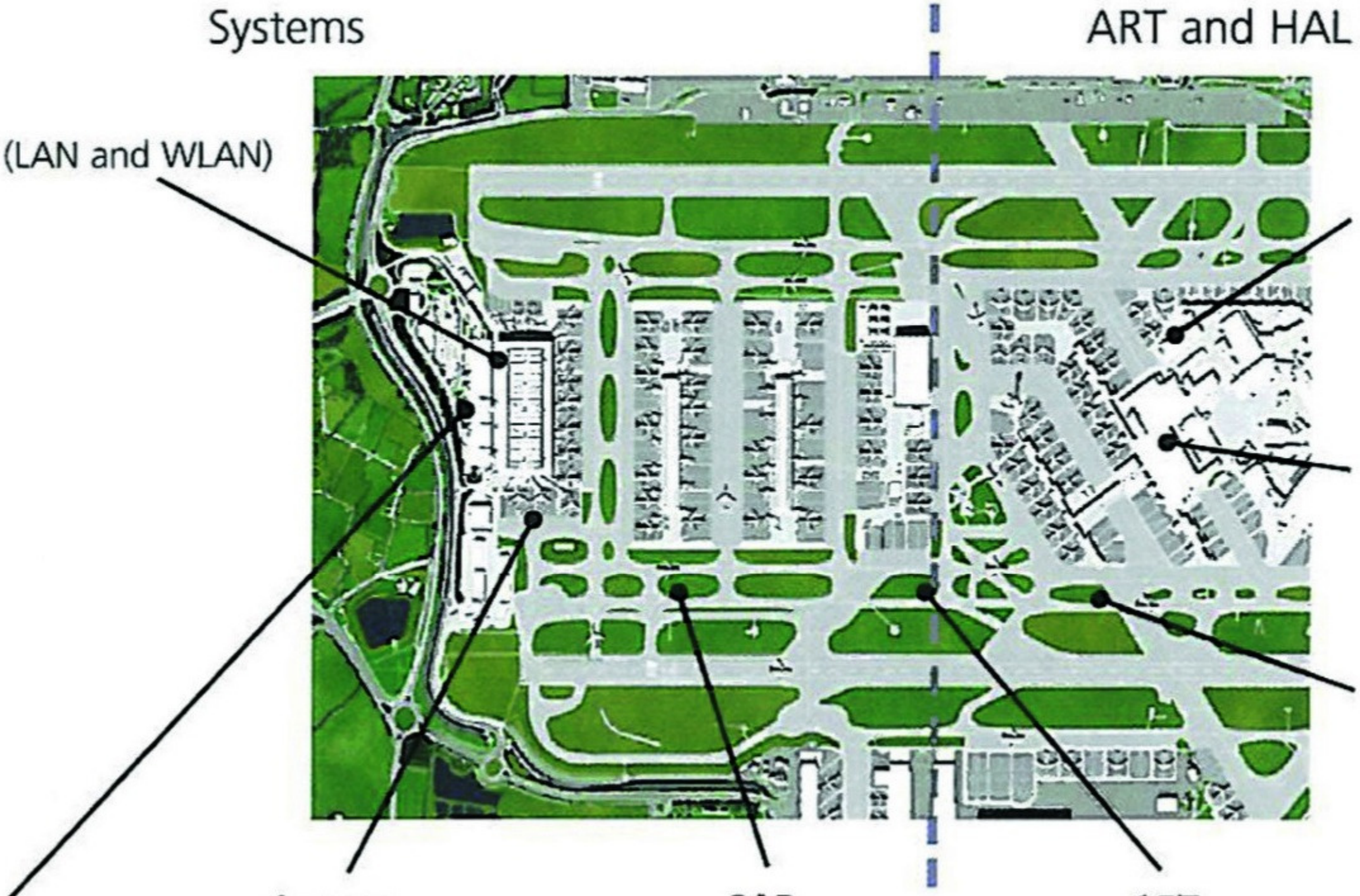
1. Integrate protective concepts into organizational culture, leadership and daily operations
2. Identify and support protective program priorities, resources and utility-specific measures
3. Employ protocols for detection of contamination
4. Assess risks and review vulnerability assessments (VAs)
5. **Establish facility and information access control**
6. Incorporate resiliency concepts into physical infrastructure
7. Prepare, test, and update emergency response and business continuity plans
8. Develop partnerships with first responders, managers of critical interdependent infrastructure, other utilities and response organizations
9. Develop and implement internal and external communication strategies
10. Monitor incidents and threat-level information

"Smart Security" – *Transportation*

- ***Smart Decisions:***
  - *Geo-Location:* Managing secure movements of traffic on the roads, rail, air and maritime using both wired, wireless and satellite communications
  - *Real-Time (RT) :* Ensure that all devices are connected and secured for real-time alerts, including continuous log streaming from aircraft, ships, cars and trains
  - *Knowledge Lens:* Forecasting future traffic movements in order to size growth in major transport hubs such as airports, train stations, motorways and ports
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Adapting to the dynamics of the traffic statistics, as well as the routing patterns, and the cargo/freight requirements
  - *Massive Memory & Storage:* In-Depth RT information on ALL vehicle movements
  - *Scalable Architecture:* Efficient, Flexible & Scaled Transportation Networks & Hubs
- ***Smart Security:*** Resilience to breakdowns, crashes, disasters that may be caused through accidents or deliberate acts of physical and cyber sabotage or attack
- ***Smart Governance:*** Regular physical inspections & audits or vehicles and transportation infrastructure to minimise risks of failure, disaster or attack (BCP/DR)

Cybersecurity: International Airports: LHR-T5

Systems | ART and HAL Integration



Buildings

- Networks (LAN and WLAN)
- Voice
- Radio
- Cellular
- TV
- CCTV
- ACS
- Search
- BSI
- AOS
- Displays

Star

- CCTV
- SCADA

IT

- Various

AOSU

- CCTV

Landside

- Comms
- Aerial Farms
- CCTV
- SCADA (HV & Water)

Aprons, Ancillary Areas

- Comms
- CCTV
- SCADA (Aprons Services & HV)

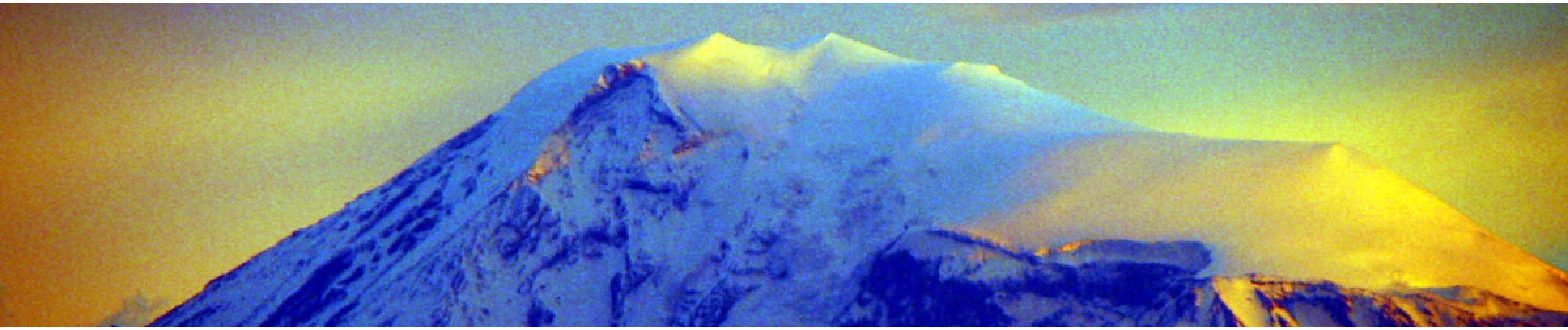
SAR

- Comms
- CCTV
- SCADA (Roads)

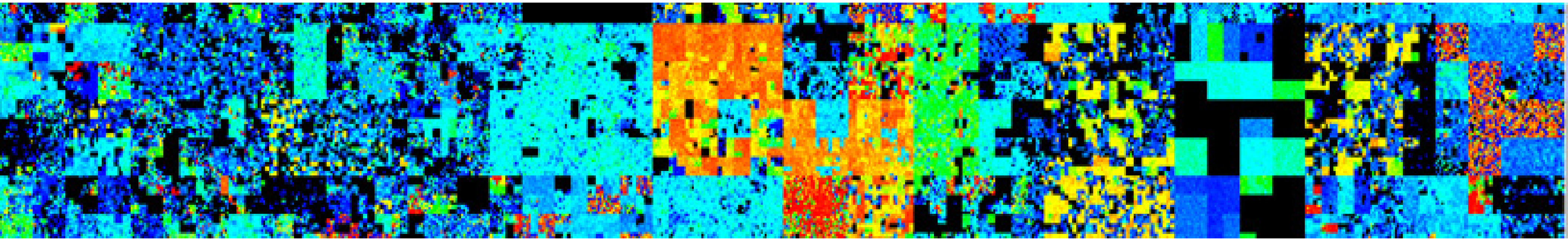
ART

- Comms
- CCTV
- SCADA (Roads)

Cybersecurity for Critical National Infrastructure (CNI)



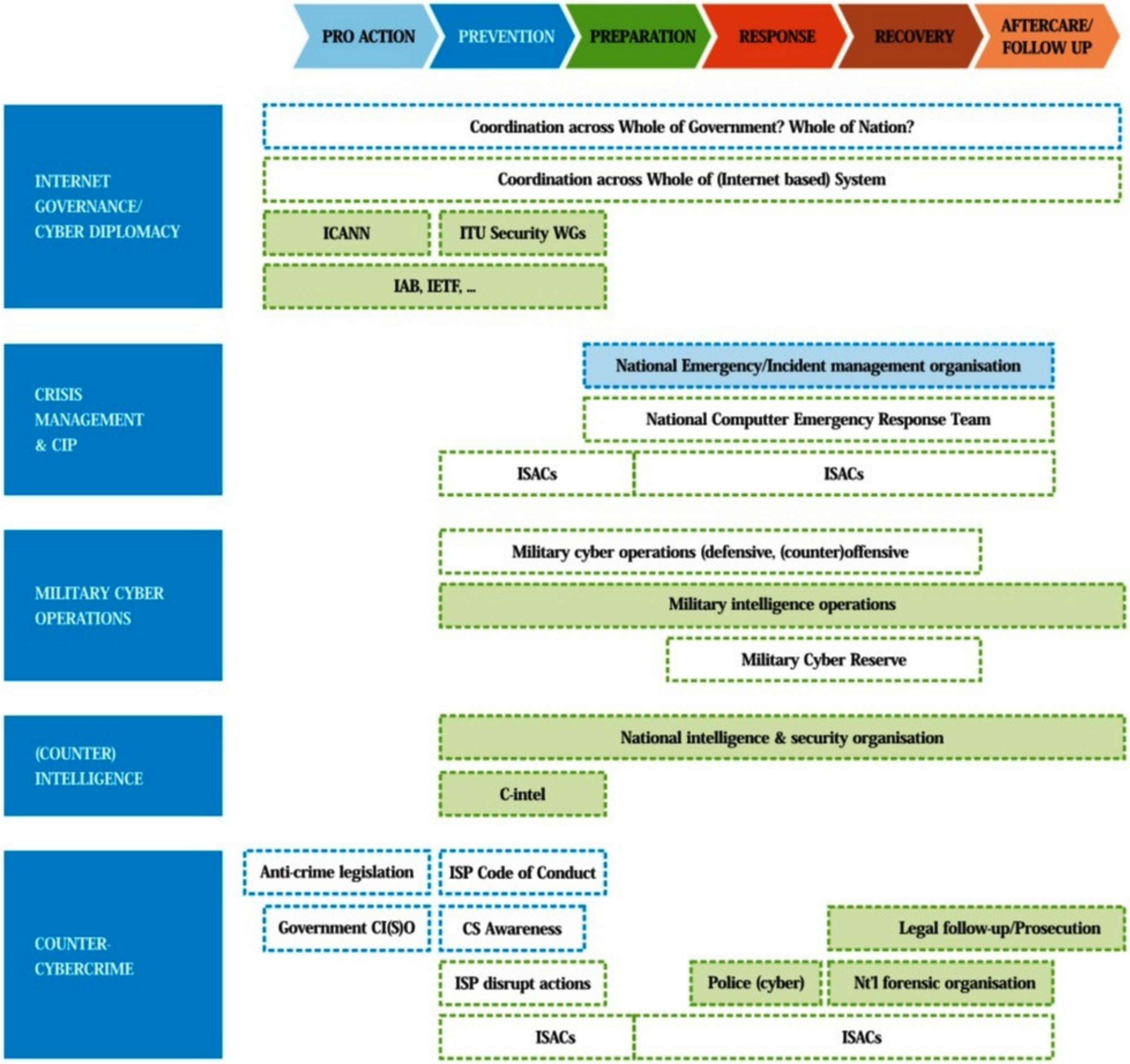
1 – The Strategic Importance of CNI	2 – Evolving Cyber Threats for CNI Sectors	3 – National & International CNI Plans
4 – 21stC Smart Systems – “Design Toolkit”	5 – Banking & Finance Sector – Analysis	6 – Energy & Transport Sectors - Analysis
7 – Civil and National Defence - Analysis	8 – CNI Security for “Internet of Things”	9 – Smart Security for YOUR Business!



“Smart Security” – *National Security & Defence*

- ***Smart Decisions:***
  - *Geo-Location:* For Civil Police & Military Security Assets, National Defence, Trans-Border Intelligence, Satellite Imagery & Mapping
  - *Real-Time:* Command & Control (C4ISR) for Civil Disturbance & Crisis and Regional Military Conflict, Virtual War Operations Room
  - *Knowledge Lens:* Filtering through real-time multimedia raw intelligence, images, audio, video to make informed decisions
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Hybrid Adaptive Organisation with Hierarchical C&C Coupled with networked cellular field operations
  - *Massive Memory & Storage:* Historical and Current National & Regional Intelligence, Alert & Security Database & Operations Net
  - *Scalable Architecture:* Resilient and Flexible Cellular C&C Network spanning all defence & military facilities and security assets
- ***Smart Security:*** Essential integrated physical & cybersecurity for the integrity & protection of Citizens, Government, Business & Financial Assets
- ***Smart Governance:*** 21stC State of the Art ***C4ISR*** – Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance

NATO *Cybersecurity* Framework Manual



PRO ACTION | PREVENTION | PREPARATION | RESPONSE | RECOVERY | AFTERCARE/ FOLLOW UP

INTERNET GOVERNANCE/ CYBER DIPLOMACY

Coordination across Whole of Government? Whole of Nation?

Coordination across Whole of (Internet based) System

ICANN

ITU Security WGs

IAB, IETF, ...

CRISIS MANAGEMENT & CIP

National Emergency/Incident management organisation

National Computter Emergency Response Team

ISACs

ISACs

MILITARY CYBER OPERATIONS

Military cyber operations (defensive, (counter)offensive

Military intelligence operations

Military Cyber Reserve

(COUNTER) INTELLIGENCE

National intelligence & security organisation

C-intel

COUNTER-CYBERCRIME

Anti-crime legislation

ISP Code of Conduct

Government CI(S)O

CS Awareness

Legal follow-up/Prosecution

ISP disrupt actions

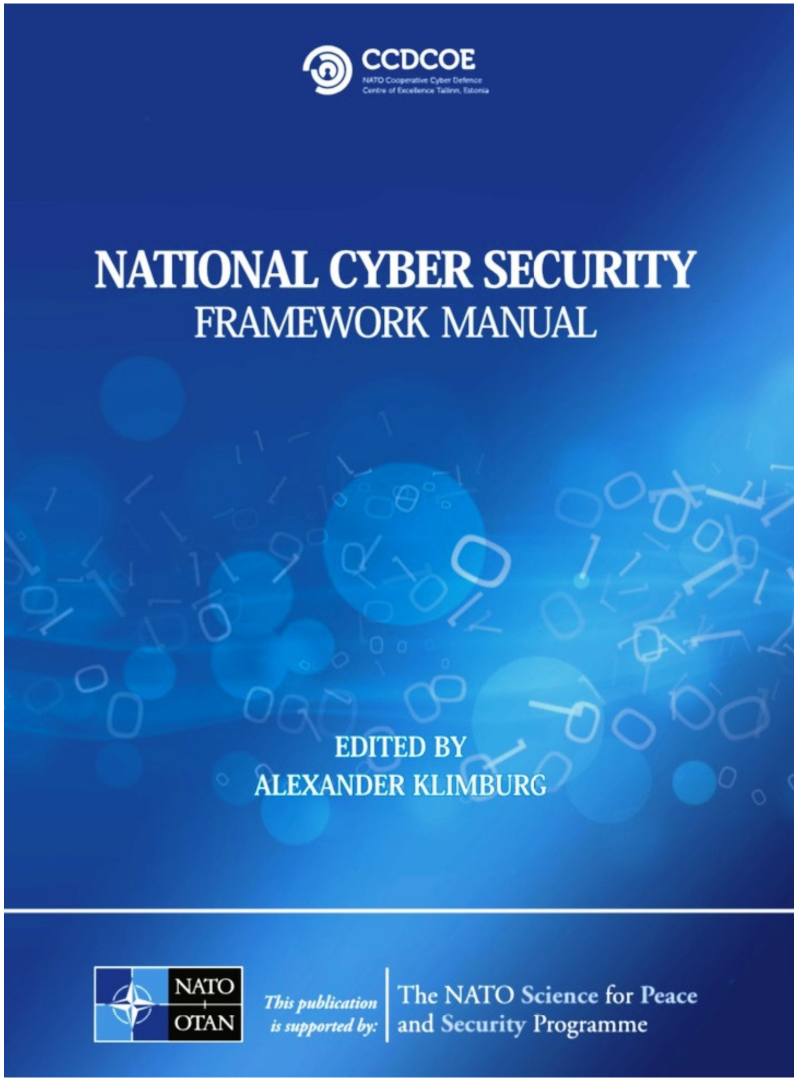
Police (cyber)

Nt'l forensic organisation

ISACs

ISACs

Figure 6: The Organisational Picture Across Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in



CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

NATIONAL CYBER SECURITY

FRAMEWORK MANUAL

EDITED BY

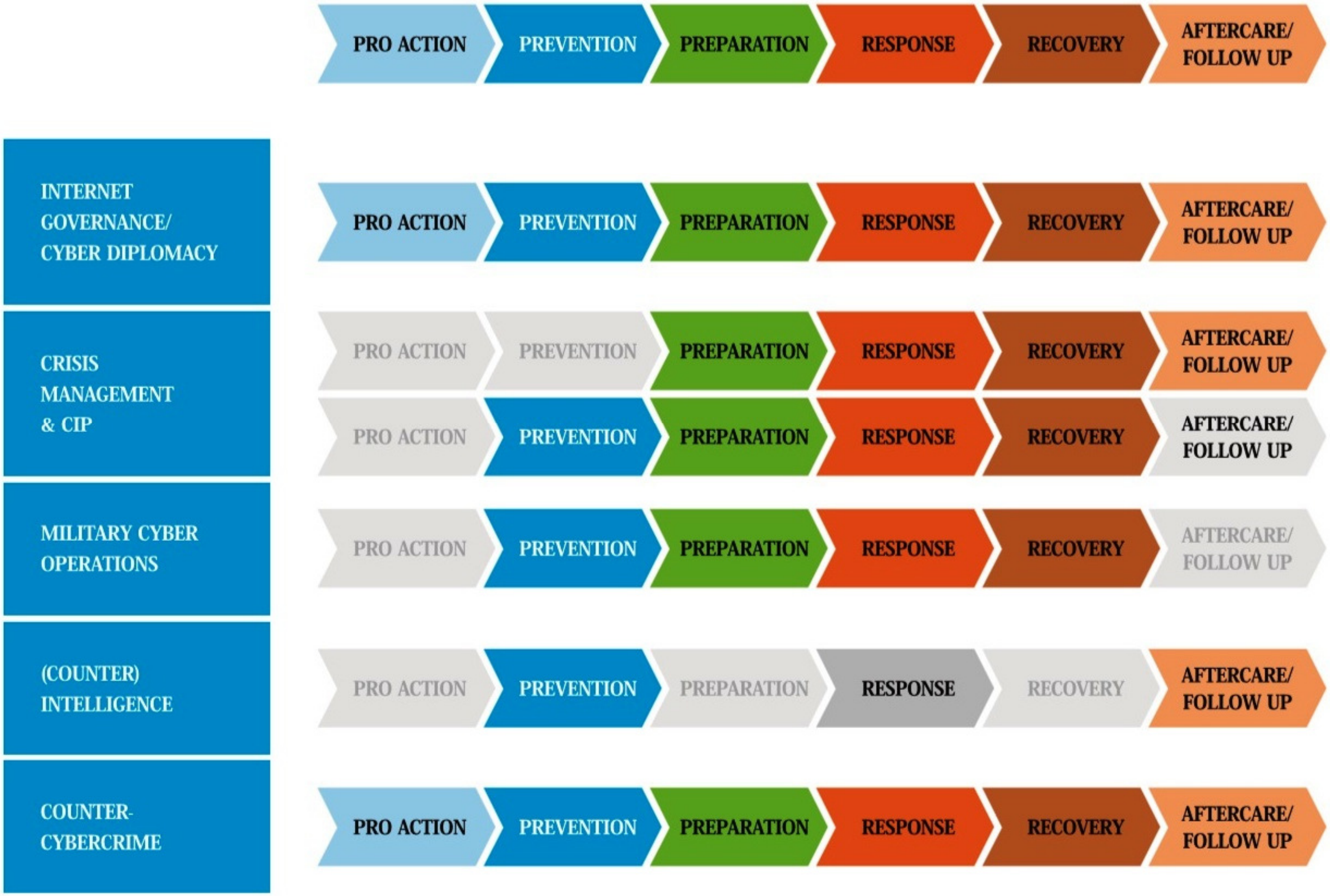
ALEXANDER KLIMBURG

NATO OTAN

This publication is supported by:

The NATO Science for Peace and Security Programme

NATO Framework: *The Five Mandates and Six Elements of the Cybersecurity Cycle*



	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
INTERNET GOVERNANCE/ CYBER DIPLOMACY	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
CRISIS MANAGEMENT & CIP	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
MILITARY CYBER OPERATIONS	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
(COUNTER) INTELLIGENCE	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
COUNTER-CYBERCRIME	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP

NATO Cybersecurity Framework:
- Organisational Architecture -

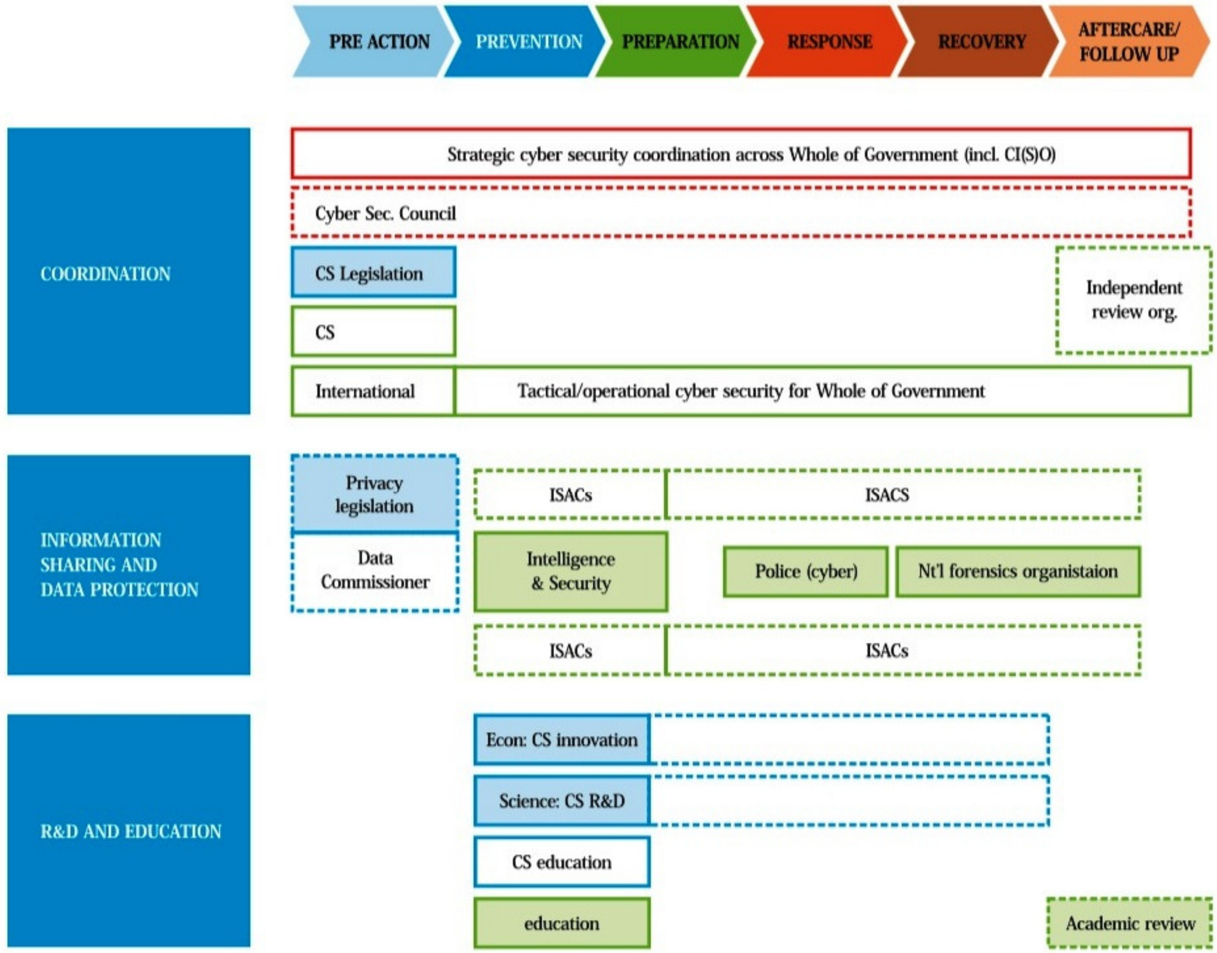
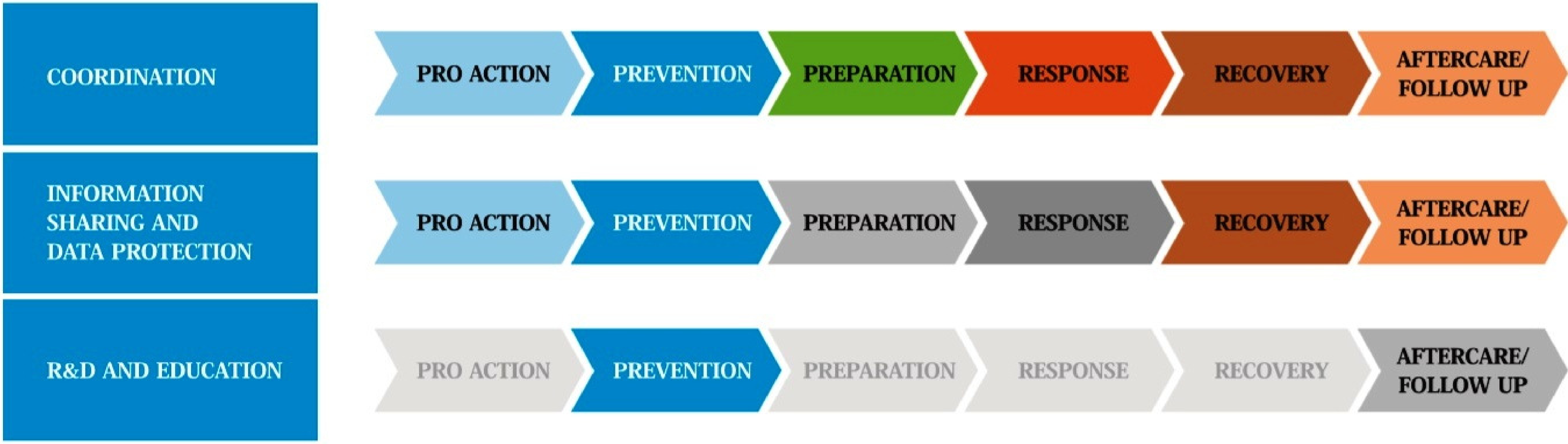


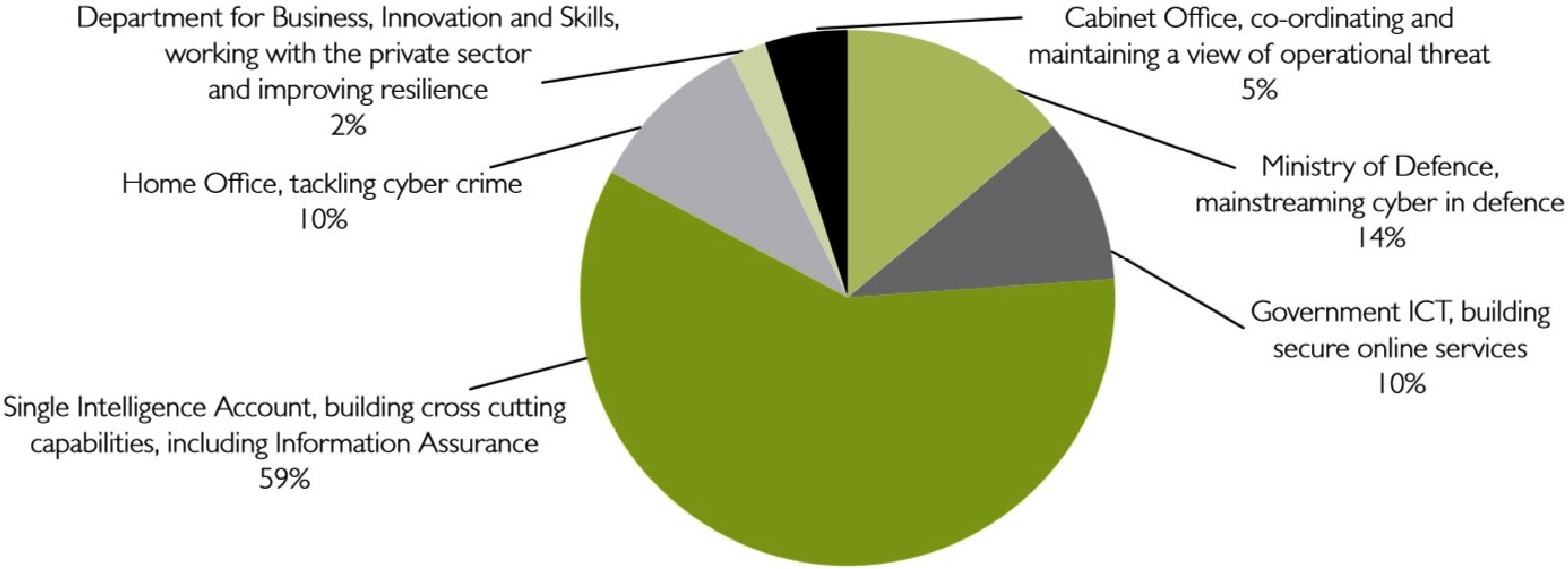
Figure 7: The Organisational Picture of the Cross-Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in existing organisation; dashed = option selected by some nations)

NATO Framework: *The Cybersecurity Incident Model with 3 Cross-Mandates*



COORDINATION	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
INFORMATION SHARING AND DATA PROTECTION	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
R&D AND EDUCATION	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP

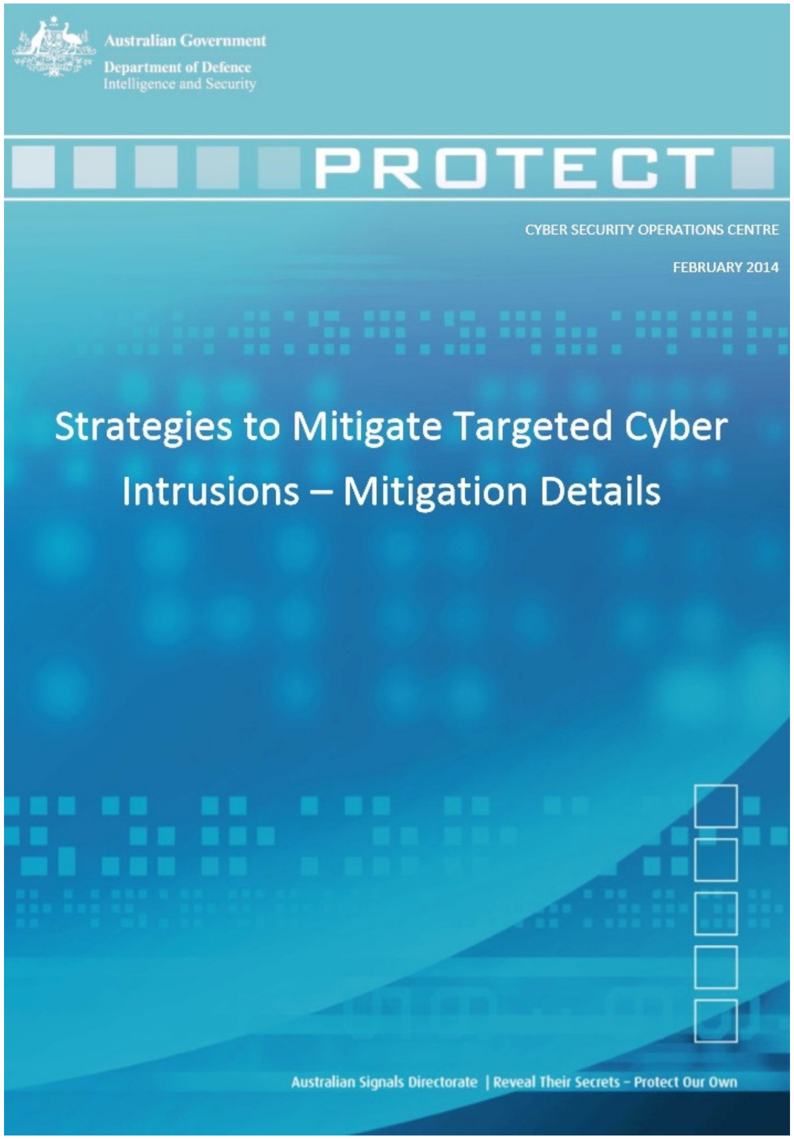
UK National *Cybersecurity* Budget (2011-2015)



UK 2010 Strategic Defence and Security Review: **£650m** – ***4 Year Cybersecurity Programme***

Cybersecurity Mitigation Strategies

- Australian Govt: Department of Defence -



Australian Government
Department of Defence
Intelligence and Security

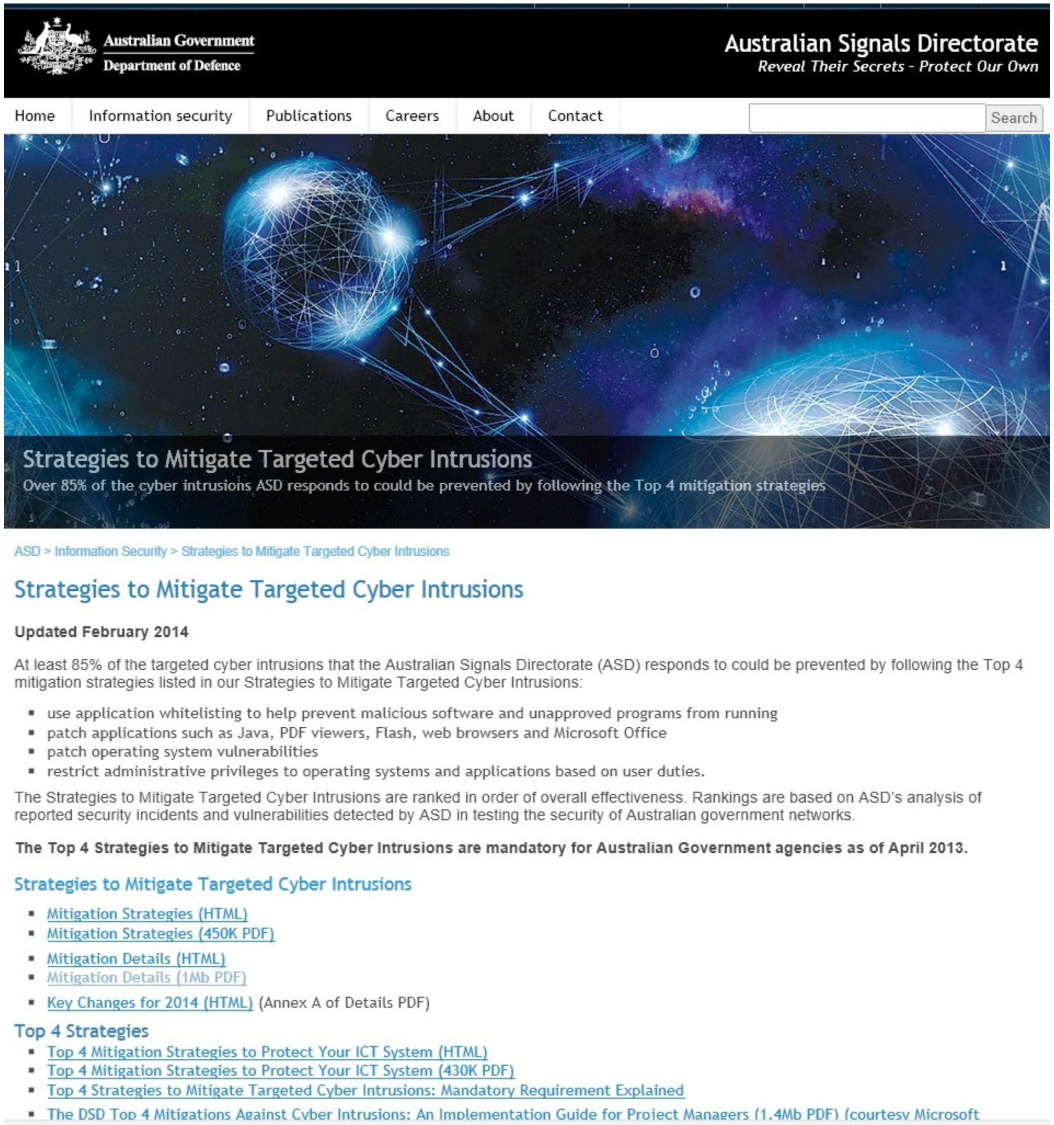
PROTECT

CYBER SECURITY OPERATIONS CENTRE

FEBRUARY 2014

Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details

Australian Signals Directorate | Reveal Their Secrets – Protect Our Own



Strategies to Mitigate Targeted Cyber Intrusions

Over 85% of the cyber intrusions ASD responds to could be prevented by following the Top 4 mitigation strategies

ASD > Information Security > Strategies to Mitigate Targeted Cyber Intrusions

Strategies to Mitigate Targeted Cyber Intrusions

Updated February 2014

At least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following the Top 4 mitigation strategies listed in our Strategies to Mitigate Targeted Cyber Intrusions:

- use application whitelisting to help prevent malicious software and unapproved programs from running
- patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office
- patch operating system vulnerabilities
- restrict administrative privileges to operating systems and applications based on user duties.

The Strategies to Mitigate Targeted Cyber Intrusions are ranked in order of overall effectiveness. Rankings are based on ASD's analysis of reported security incidents and vulnerabilities detected by ASD in testing the security of Australian government networks.

The Top 4 Strategies to Mitigate Targeted Cyber Intrusions are mandatory for Australian Government agencies as of April 2013.

Strategies to Mitigate Targeted Cyber Intrusions

- Mitigation Strategies (HTML)
- Mitigation Strategies (450K PDF)
- Mitigation Details (HTML)
- Mitigation Details (1Mb PDF)
- Key Changes for 2014 (HTML) (Annex A of Details PDF)

Top 4 Strategies

- Top 4 Mitigation Strategies to Protect Your ICT System (HTML)
- Top 4 Mitigation Strategies to Protect Your ICT System (430K PDF)
- Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained
- The DSD Top 4 Mitigations Against Cyber Intrusions: An Implementation Guide for Project Managers (1.4Mb PDF) (courtesy Microsoft

Smart Sustainable Security will extend to ALL our *National Economic Sectors*

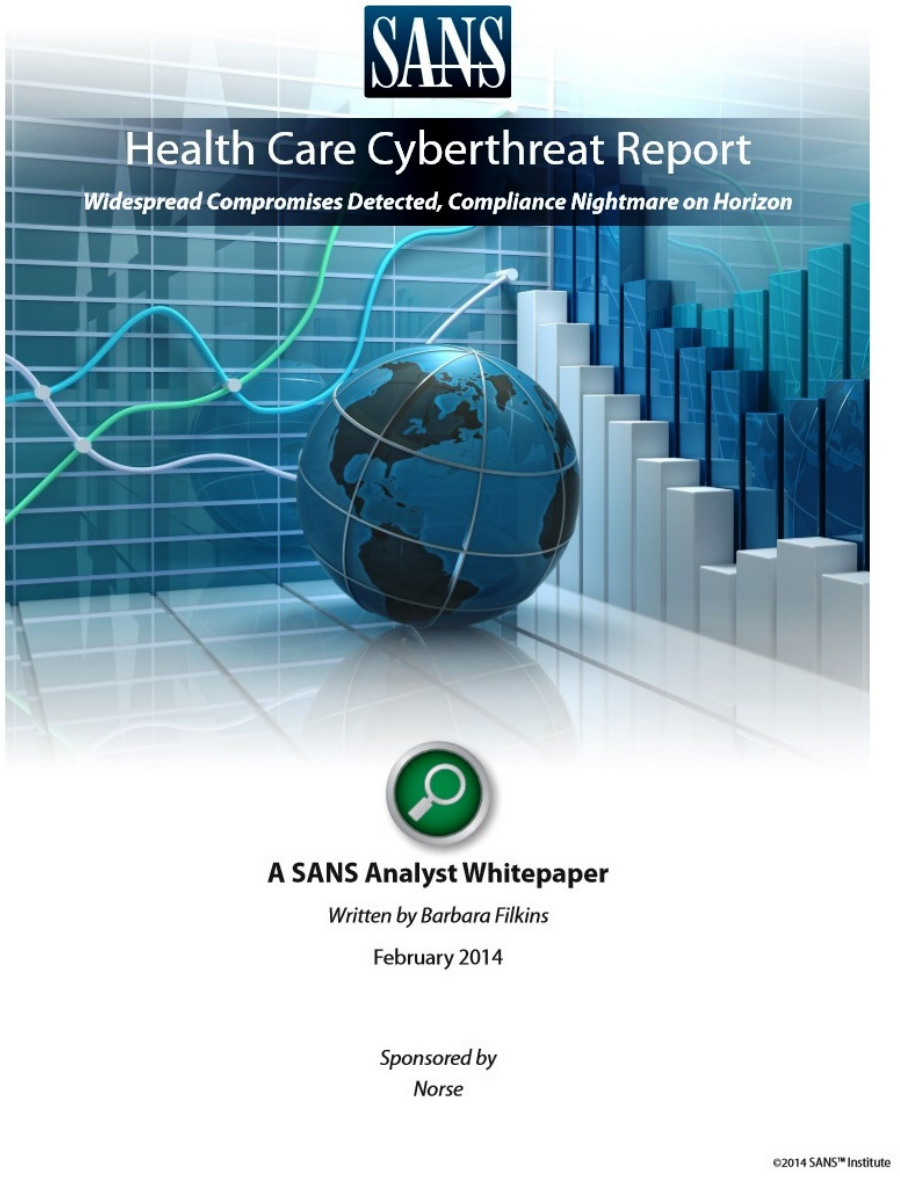
(1) Healthcare and Social Welfare
(2) ICT, Mobile and Telecommunications
(3) Education and Research
(4) Manufacturing & Logistics
(5) Retail and Distribution
(6) Central & Regional Government

.....ALL Economic Sectors will eventually require embedded “”smart security” in order to provide real-time resilience to simultaneous physical and cyber attacks or sabotage

"Smart Security" – *Healthcare & Social Welfare*

- ***Smart Decisions:***
  - *Geo-Location:* GPS Location for Medical Emergencies, Patient Images, Crisis Management, Ambulance Routing, Regional Social Support
  - *Real-Time:* On-Line Telemedicine Consultation & Preliminary Diagnosis. Also Smart Support during Intensive Hospital Surgery
  - *Knowledge Lens:* Filtering & Analysing Complex 3D Medical Scan Images, as well as future Data Mining for On-Line Patient Records
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Challenging Medical Research in New Treatments for Cancer & Neural Diseases through Global Partnerships
  - *Massive Memory & Storage:* Design, Analysis and extensive Patient Trials of New Pharmaceutical Drugs, including new "Smart Drugs"
  - *Scalable Architecture:* National professional support network for both social welfare as well as citizen health, diagnosis and treatments
- ***Smart Security:*** Cybersecurity & Personal Privacy for Patient Records, as well as integrated security for hospitals, medical assets, drugs & social welfare facilities
- ***Smart Governance:*** Professional Government Support, Management & Funding for National Medical & Social Welfare Services

Cybersecurity for the *Healthcare Sector*



SANS

Health Care Cyberthreat Report

Widespread Compromises Detected, Compliance Nightmare on Horizon

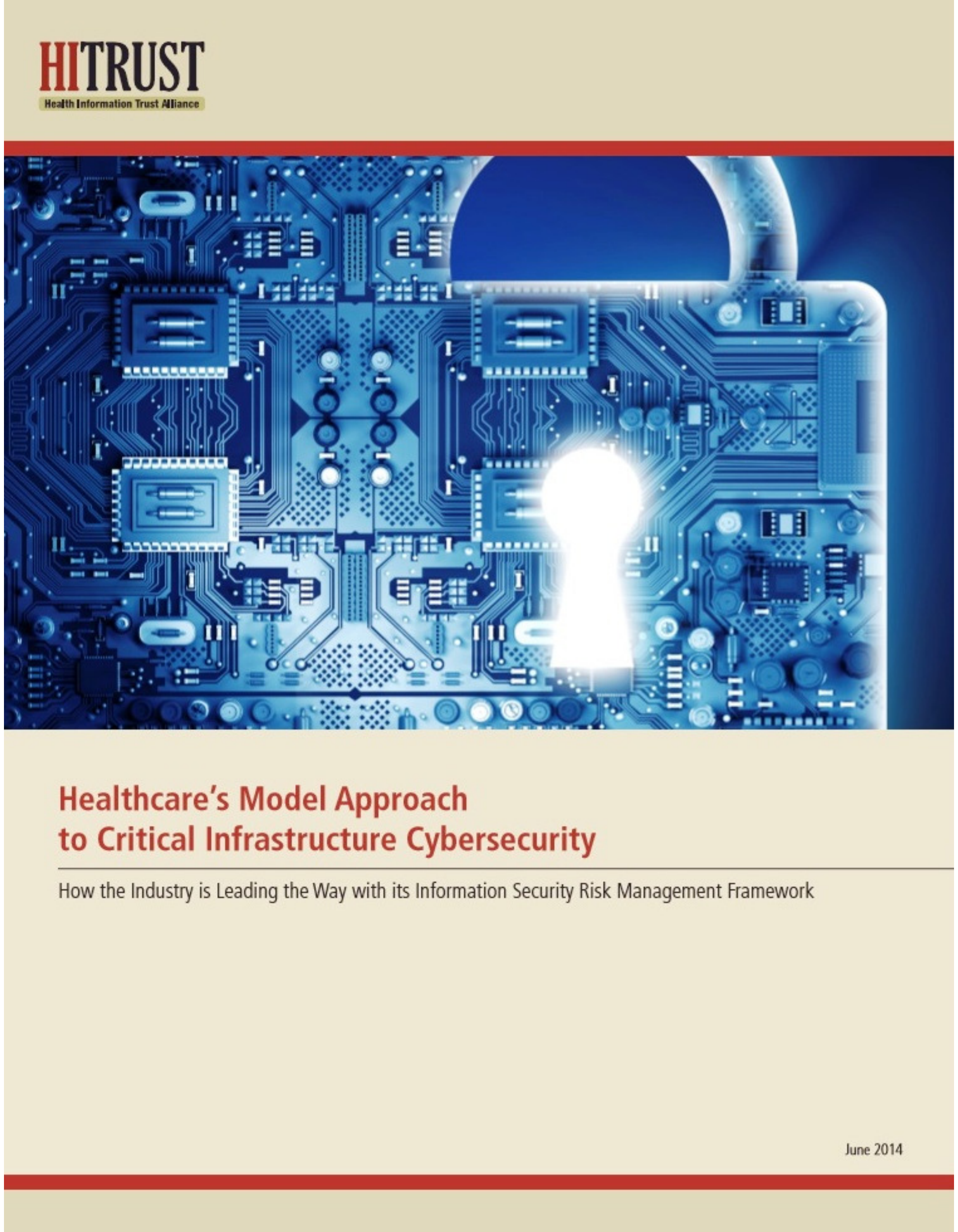
A SANS Analyst Whitepaper

Written by Barbara Filkins

February 2014

Sponsored by
Norse

©2014 SANS™ Institute



HITRUST
Health Information Trust Alliance

Healthcare's Model Approach
to Critical Infrastructure Cybersecurity

How the Industry is Leading the Way with its Information Security Risk Management Framework

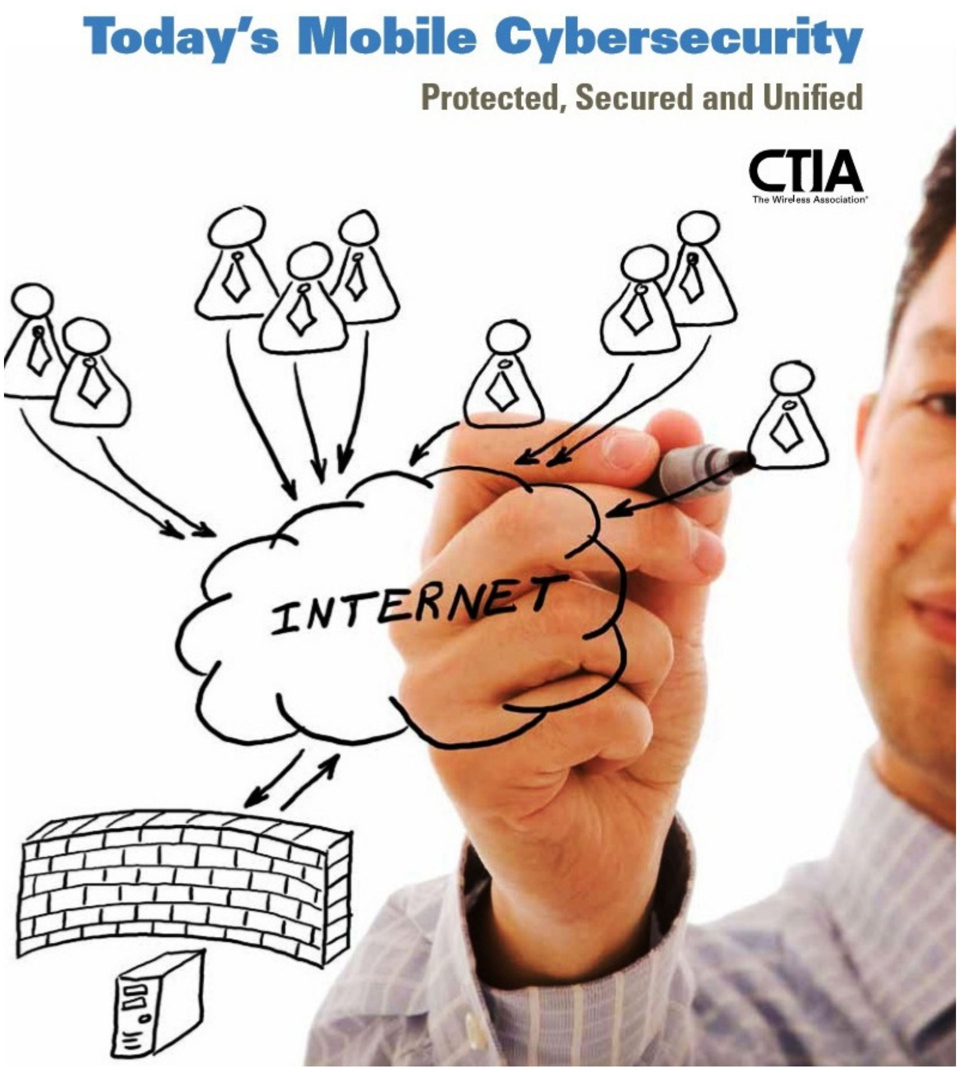
June 2014

Healthcare in the Russian Arctic – *Kola Peninsula*

"Smart Security" - *ICT, Mobile & Telecommunications*

- ***Smart Decisions:***
  - *Geo-Location:* Local Mobile Information – Maps, Satellite Imagery, Climate, Geology, History, On-Line Persons on Smart Devices.
  - *Real-Time:* Financial Transactions, ePayments, eGovernment Services, IM, Social Media, MMORG and Immersive Virtual Worlds
  - *Knowledge Lens:* Global Data & Information can be filtered and focused for Local Decisions with ICT enabled "Knowledge Lens"
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Mobile, Wireless & Cellular Ad-Hoc Networks use adaptive routing & roaming protocols
  - *Massive Memory & Storage:* ICT provides the essential Smart Storage & Processing Tools including System Virtualisation & Cloud Computing
  - *Scalable Architecture:* Fundamental for smart ICT systems that already scale from nano machines to global search & social media "apps"
- ***Smart Security:*** Cybersecurity needs to be embedded EVERYWHERE!
- ***Smart Governance:*** ICT requires new laws, regulations & governance

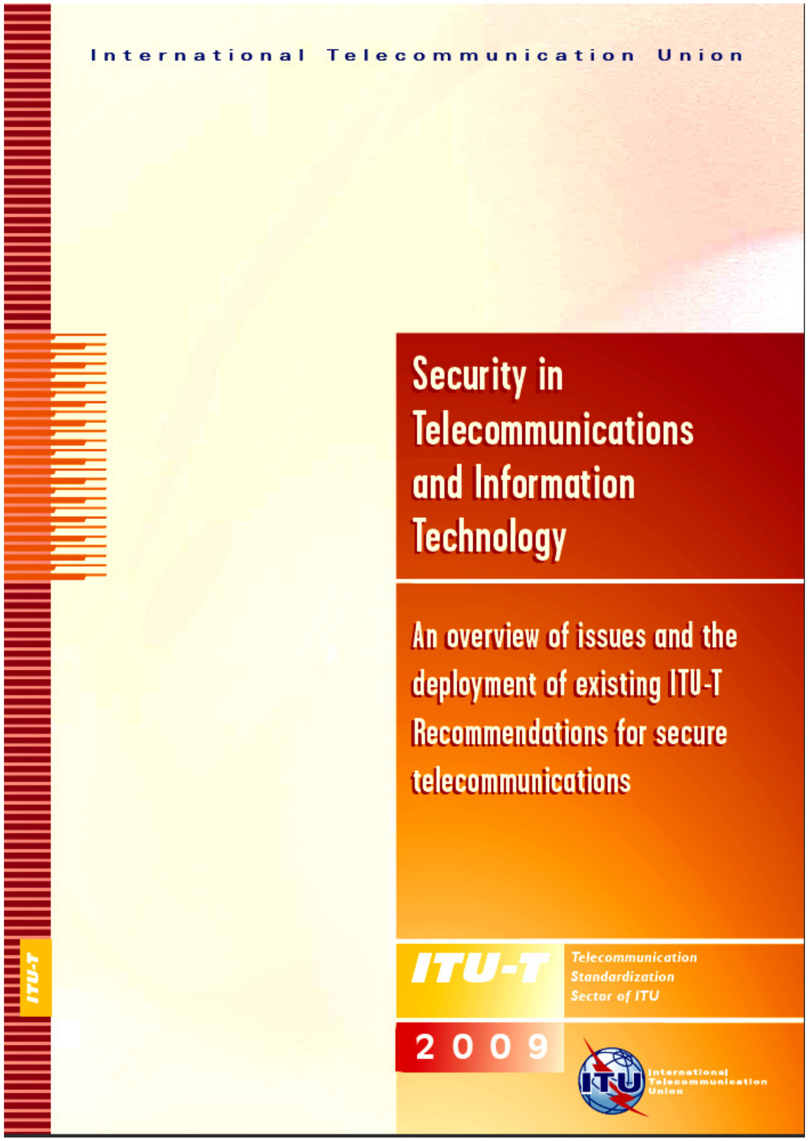
Cybersecurity for ICT, Mobile & Telecommunications



Today's Mobile Cybersecurity

Protected, Secured and Unified

CTIA
The Wireless Association®



International Telecommunication Union

Security in Telecommunications and Information Technology

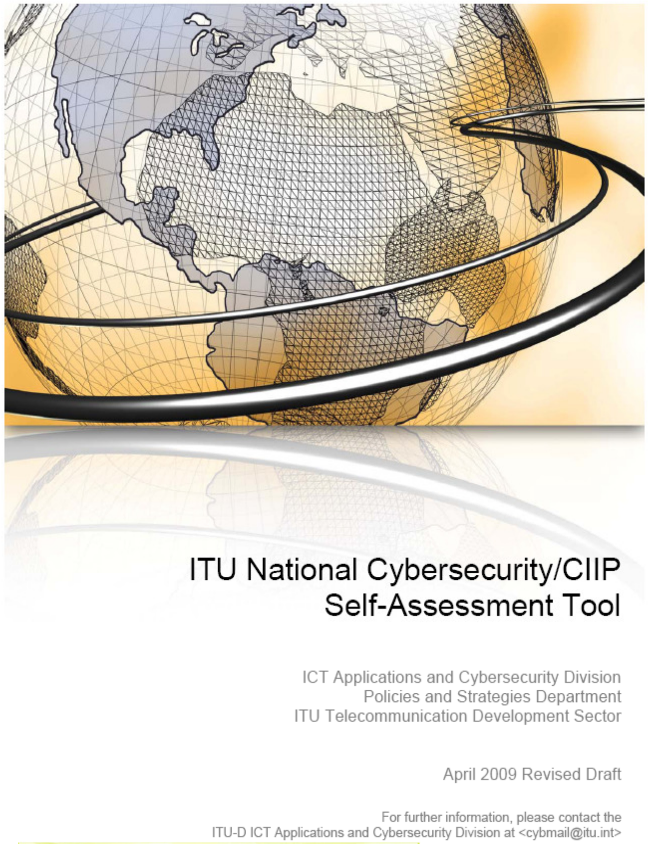
An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications

ITU-T
Telecommunication Standardization Sector of ITU

2009

ITU
International Telecommunication Union

UN/ITU *Cybersecurity* Guides & Toolkits

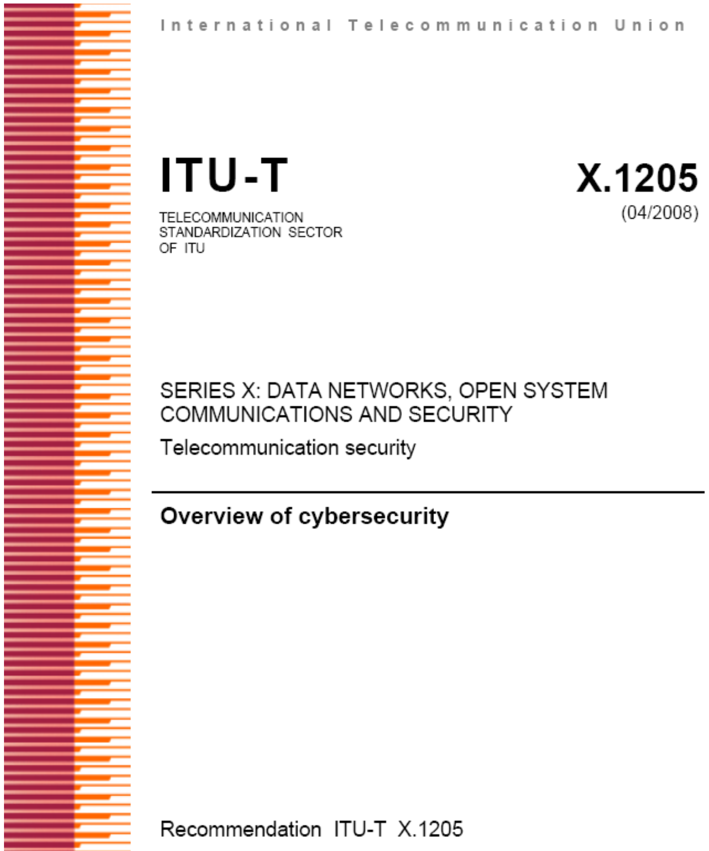


ITU National Cybersecurity/CIIP Self-Assessment Tool

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

April 2009 Revised Draft

For further information, please contact the
ITU-D ICT Applications and Cybersecurity Division at <cybmail@itu.int>



International Telecommunication Union

ITU-T
TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1205
(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY
Telecommunication security

Overview of cybersecurity

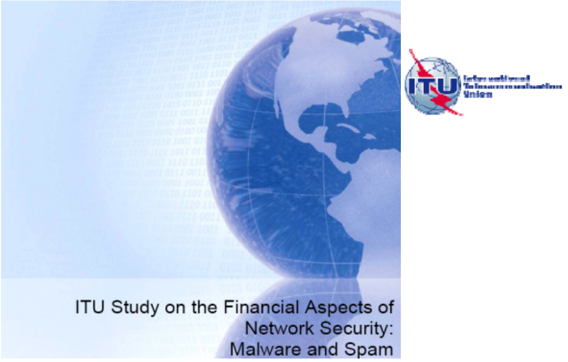
Recommendation ITU-T X.1205

ITU Botnet Mitigation Toolkit
Background Information

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

January 2008

ICTs for e-Environment
Guidelines for Developing Countries,
with a Focus on Climate Change



ITU Study on the Financial Aspects of Network Security:
Malware and Spam

Cybersecurity Guide
for Developing Countries

“Smart Security” - *Education & Research*

- ***Smart Decisions:***
  - *Geo-Location:* Mobile Education, Navigation & Mapping, Augmented & Immersive Reality based on Geo-Location with Mobile Devices & Headsets
  - *Real-Time:* Networked Laboratories for Synchronised Parallel Research in Genetics, High-Energy Physics, Optical & Radio-Astronomy
  - *Knowledge Lens:* Smart Grid Computing with In-Depth Data Mining in search for New Particles in CERN LHC Collider.
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Virtual On-Line Colleges for remote students. Collaborative academic & commercial Techno Parks & Labs
  - *Massive Memory & Storage:* Crowd Sourced Volunteer PC Research as in the SETI Project (BOINC – Berkeley Open Net Computing)
  - *Scalable Architecture:* Business Opportunities for Global Niche College for minority study & research themes. Study courses on mobile “apps”!
- ***Smart Security:*** College Campus & Laboratory Cyber & Physical Security
- ***Smart Governance:*** Rigorous Educational Data Audit & Compliance Regime

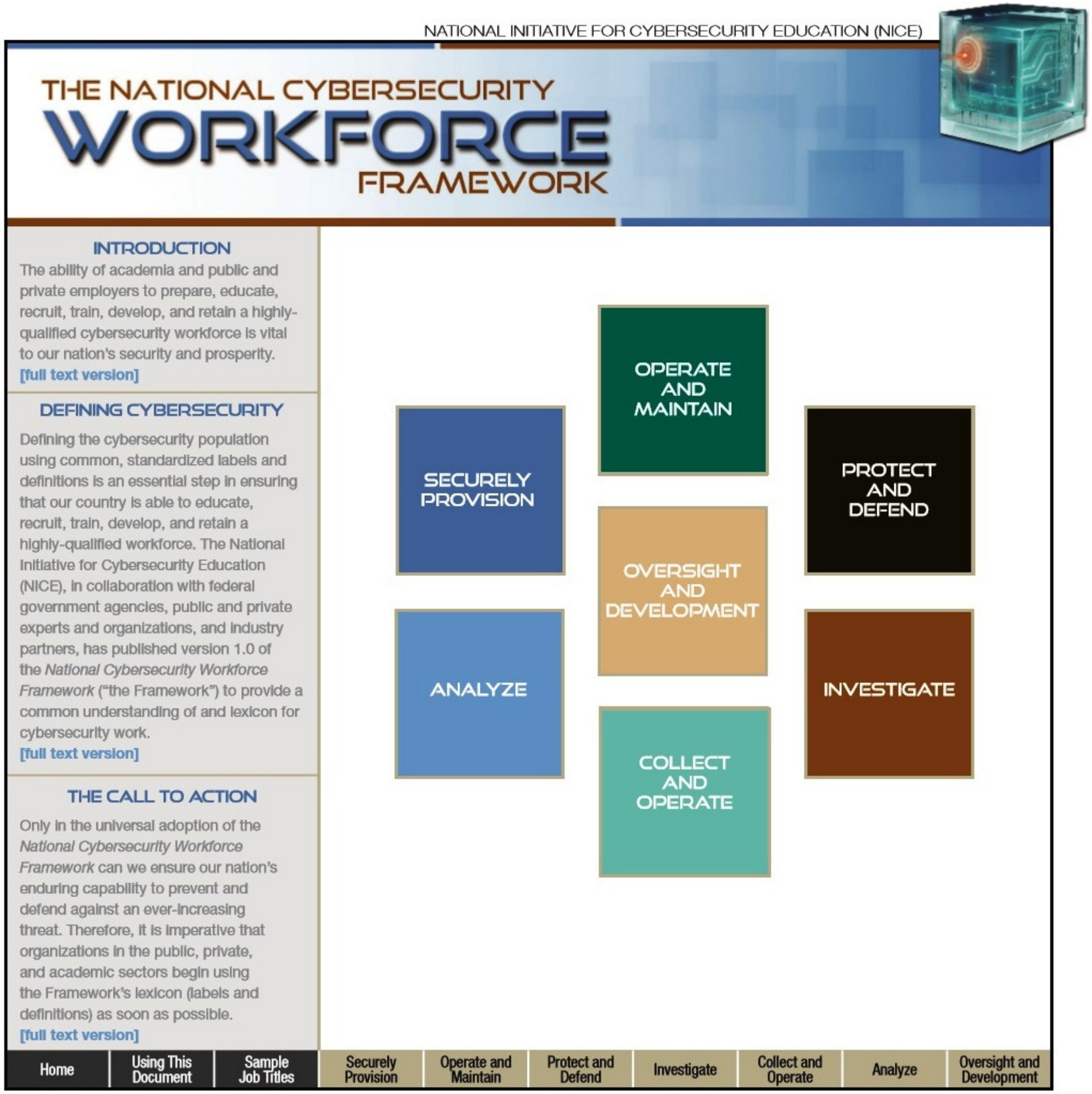
National Initiative for Cybersecurity Education *(NICE)*

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

STRATEGIC PLAN

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION



NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INTRODUCTION

The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a highly-qualified cybersecurity workforce is vital to our nation's security and prosperity.
[full text version]

DEFINING CYBERSECURITY

Defining the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The National Initiative for Cybersecurity Education (NICE), in collaboration with federal government agencies, public and private experts and organizations, and industry partners, has published version 1.0 of the *National Cybersecurity Workforce Framework* ("the Framework") to provide a common understanding of and lexicon for cybersecurity work.
[full text version]

THE CALL TO ACTION

Only in the universal adoption of the *National Cybersecurity Workforce Framework* can we ensure our nation's enduring capability to prevent and defend against an ever-increasing threat. Therefore, it is imperative that organizations in the public, private, and academic sectors begin using the Framework's lexicon (labels and definitions) as soon as possible.
[full text version]

"Smart Security" - *Government*

- ***Smart Decisions:***
  - *Geo-Location:* Tracking all government assets, physical & electronic documents and devices to reduce loss or corruption of information
  - *Real-Time:* Ensure that the government ALWAYS has complete real-time info on its resources, staff and financial & political affairs
  - *Knowledge Lens:* "In-Depth" Smart Data Mining to link Government Databases relating to ALL Government Ministries & Agencies
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Flexible Networked Government Organisations and Operations to respond to evolving national & international events, policies & overall business & political environment
  - *Massive Memory & Storage:* Ability to store and analyse PetaBytes of Government Data relating to Programmes, Policies & Governance
  - *Scalable Architecture*: Efficient networked operational framework for the transparent management of national, region and local citizen programmes
- ***Smart Security:*** Implementation of integrated Physical and Cyber Security Operations according to International Standards – ISO/ITU
- ***Smart Governance:*** Provision of Open eGovernment Portal supporting ALL major Ministries, Agencies and Partners for On-Line Transaction Processing & Analysis

Smart Security: *Government*

- *Cyber Agencies:* Governments such as UK, USA, Canada, Malaysia, South Korea , Australia and many other nations 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 physical & cyber 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

.......Eventually ALL UN Member States will find it necessary to implement, regulate, audit and manage Cybersecurity through some form of dedicated *National Cybersecurity Agency* (*Smart Security*)

Cybersecurity Benefits: *Government*

- Improved cybersecurity provides significant economic & political 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 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 control systems
  - ***Telecommunications:*** Top security of government communications with alternative routings, encryption & protection against cyber attacks both internet & external to the nation state.

UN/ITU - *Georgian Cyber Mission* Objectives & Outcomes

- Stakeholders: Interview the key stakeholders including the major civil Government Ministries, Parliament, Georgian CERT (GRENA) & Critical Infrastructure Sectors (Telecommunications, ISPs, National & Commercial Banks)

- UN/ITU - GCA: Follow the 5 GCA Pillars: Legal, Technology, Organisation, Capacity Building & Partnerships and develop detailed recommended *Action Plan* & *Rolling Project Road-Map* for the Georgian Government

- General Outcomes:

  - National Cybersecurity Agency(NCA) : Recommendation to establish an NCA with authority and budget to manage the national cybersecurity strategy & programmes - The Data Exchange Agency (DEA) within Georgian Ministry of Justice manages National Cybersecurity Programmes.

  - Georgian CERTs: Key players with professional skills that can be leveraged to build up capacity across both the Public and Private Sector working with International Partners

  - Critical Infrastructure: Recommendation to Review, Audit and then Upgrade Critical Infrastructure to International Technical & Operational Security Standards (ITU/ISO)

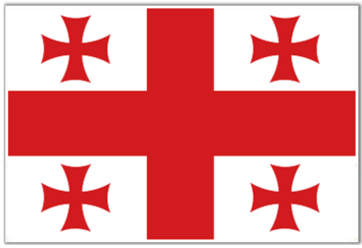
……*Long-Term Success will be dependant upon developing professional cybersecurity skills through public-private partnerships that leverage all skills & knowledge*

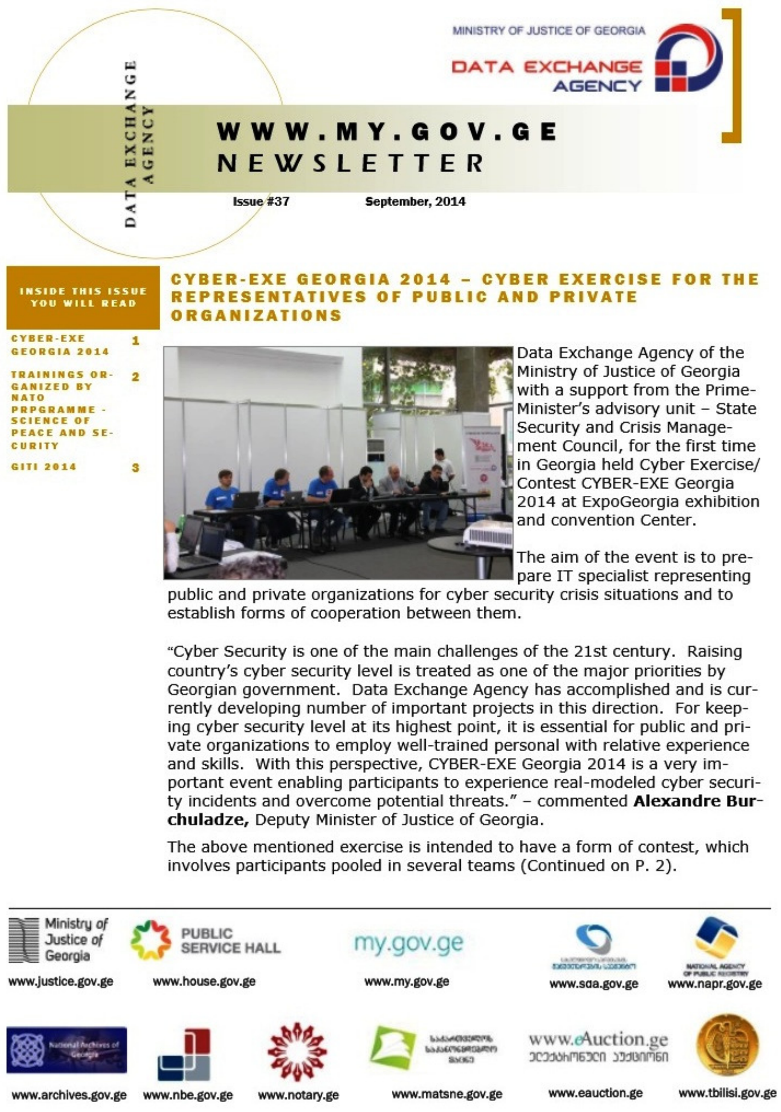
Cybersecurity for the *Georgian Parliament*

…..Critical Infrastructure Analysis during the UN/ITU Cybersecurity Mission included Georgian Parliament

Georgia: Data Exchange Agency (DEA)

- Cybersecurity and eGovernance -





MINISTRY OF JUSTICE OF GEORGIA

DATA EXCHANGE AGENCY

DATA EXCHANGE AGENCY

WWW.MY.GOV.GE

NEWSLETTER

Issue #37 September, 2014

INSIDE THIS ISSUE YOU WILL READ

CYBER-EXE GEORGIA 2014 – CYBER EXERCISE FOR THE REPRESENTATIVES OF PUBLIC AND PRIVATE ORGANIZATIONS

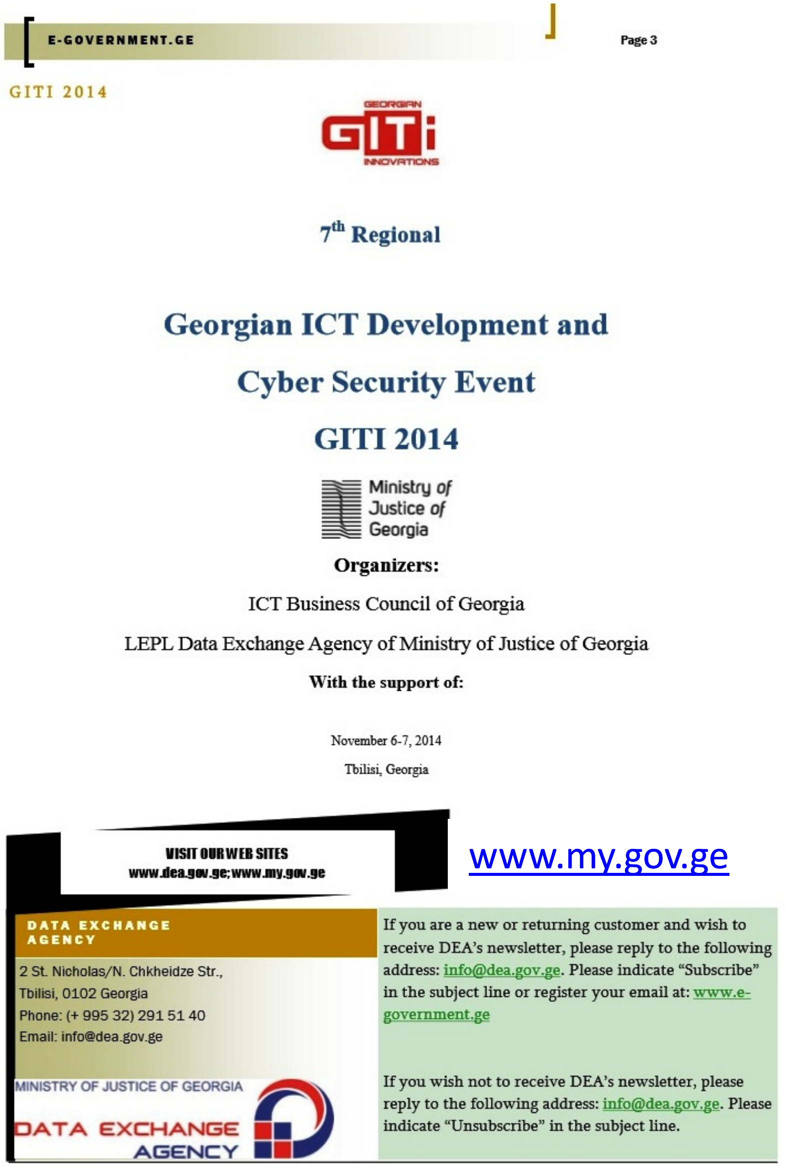
Data Exchange Agency of the Ministry of Justice of Georgia with a support from the Prime-Minister's advisory unit – State Security and Crisis Management Council, for the first time in Georgia held Cyber Exercise/ Contest CYBER-EXE Georgia 2014 at ExpoGeorgia exhibition and convention Center.

The aim of the event is to prepare IT specialist representing public and private organizations for cyber security crisis situations and to establish forms of cooperation between them.

"Cyber Security is one of the main challenges of the 21st century. Raising country's cyber security level is treated as one of the major priorities by Georgian government. Data Exchange Agency has accomplished and is currently developing number of important projects in this direction. For keeping cyber security level at its highest point, it is essential for public and private organizations to employ well-trained personal with relative experience and skills. With this perspective, CYBER-EXE Georgia 2014 is a very important event enabling participants to experience real-modeled cyber security incidents and overcome potential threats." – commented **Alexandre Burchuladze,** Deputy Minister of Justice of Georgia.

The above mentioned exercise is intended to have a form of contest, which involves participants pooled in several teams (Continued on P. 2).

Ministry of Justice of Georgia www.justice.gov.ge
PUBLIC SERVICE HALL www.house.gov.ge
my.gov.ge www.my.gov.ge
www.sda.gov.ge
NATIONAL AGENCY OF PUBLIC REGISTRY www.napr.gov.ge
National Archives of Georgia www.archives.gov.ge
www.nbe.gov.ge
www.notary.ge
www.matsne.gov.ge
www.eAuction.ge www.eauction.ge
www.tbilisi.gov.ge



E-GOVERNMENT.GE

Page 3

GITI 2014

GEORGIAN GITI INNOVATIONS

7th Regional

Georgian ICT Development and

Cyber Security Event

GITI 2014

Ministry of Justice of Georgia

Organizers:

ICT Business Council of Georgia

LEPL Data Exchange Agency of Ministry of Justice of Georgia

With the support of:

November 6-7, 2014

Tbilisi, Georgia

VISIT OUR WEB SITES
www.dea.gov.ge;www.my.gov.ge

DATA EXCHANGE AGENCY

2 St. Nicholas/N. Chkheidze Str.,
Tbilisi, 0102 Georgia
Phone: (+ 995 32) 291 51 40
Email: info@dea.gov.ge

MINISTRY OF JUSTICE OF GEORGIA
DATA EXCHANGE AGENCY

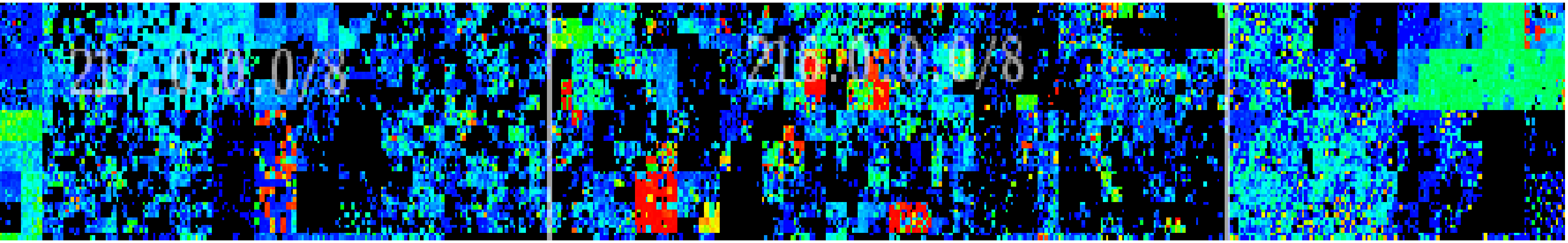
If you are a new or returning customer and wish to receive DEA's newsletter, please reply to the following address: info@dea.gov.ge. Please indicate "Subscribe" in the subject line or register your email at: www.e-government.ge

If you wish not to receive DEA's newsletter, please reply to the following address: info@dea.gov.ge. Please indicate "Unsubscribe" in the subject line.

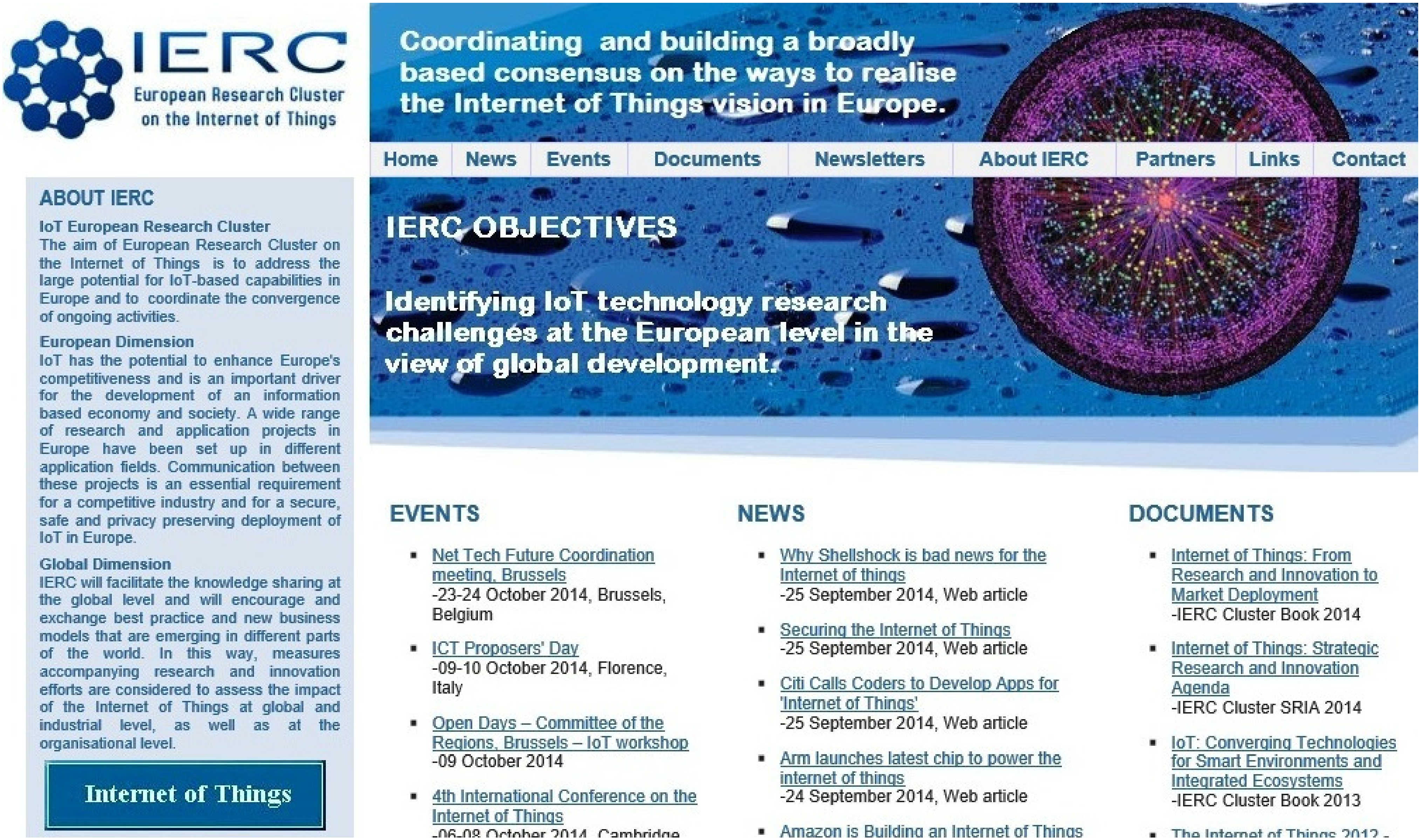
www.my.gov.ge

Cybersecurity for Critical National Infrastructure (CNI)

1 – The Strategic Importance of CNI	2 – Evolving Cyber Threats for CNI Sectors	3 – National & International CNI Plans
4 – 21stC Smart Systems – "Design Toolkit"	5 – Banking & Finance Sector – Analysis	6 – Energy & Transport Sectors - Analysis
7 – Civil and National Defence - Analysis	8 – CNI Security for "Internet of Things"	9 – Smart Security for YOUR Business!



European Research Cluster: *Internet of Things*



IERC
European Research Cluster on the Internet of Things

Coordinating and building a broadly based consensus on the ways to realise the Internet of Things vision in Europe.

ABOUT IERC

IoT European Research Cluster
The aim of European Research Cluster on the Internet of Things is to address the large potential for IoT-based capabilities in Europe and to coordinate the convergence of ongoing activities.

European Dimension
IoT has the potential to enhance Europe's competitiveness and is an important driver for the development of an information based economy and society. A wide range of research and application projects in Europe have been set up in different application fields. Communication between these projects is an essential requirement for a competitive industry and for a secure, safe and privacy preserving deployment of IoT in Europe.

Global Dimension
IERC will facilitate the knowledge sharing at the global level and will encourage and exchange best practice and new business models that are emerging in different parts of the world. In this way, measures accompanying research and innovation efforts are considered to assess the impact of the Internet of Things at global and industrial level, as well as at the organisational level.

Internet of Things

IERC OBJECTIVES

Identifying IoT technology research challenges at the European level in the view of global development.

EVENTS

- Net Tech Future Coordination meeting, Brussels
  -23-24 October 2014, Brussels, Belgium
- ICT Proposers' Day
  -09-10 October 2014, Florence, Italy
- Open Days – Committee of the Regions, Brussels – IoT workshop
  -09 October 2014
- 4th International Conference on the Internet of Things
  -06-08 October 2014, Cambridge

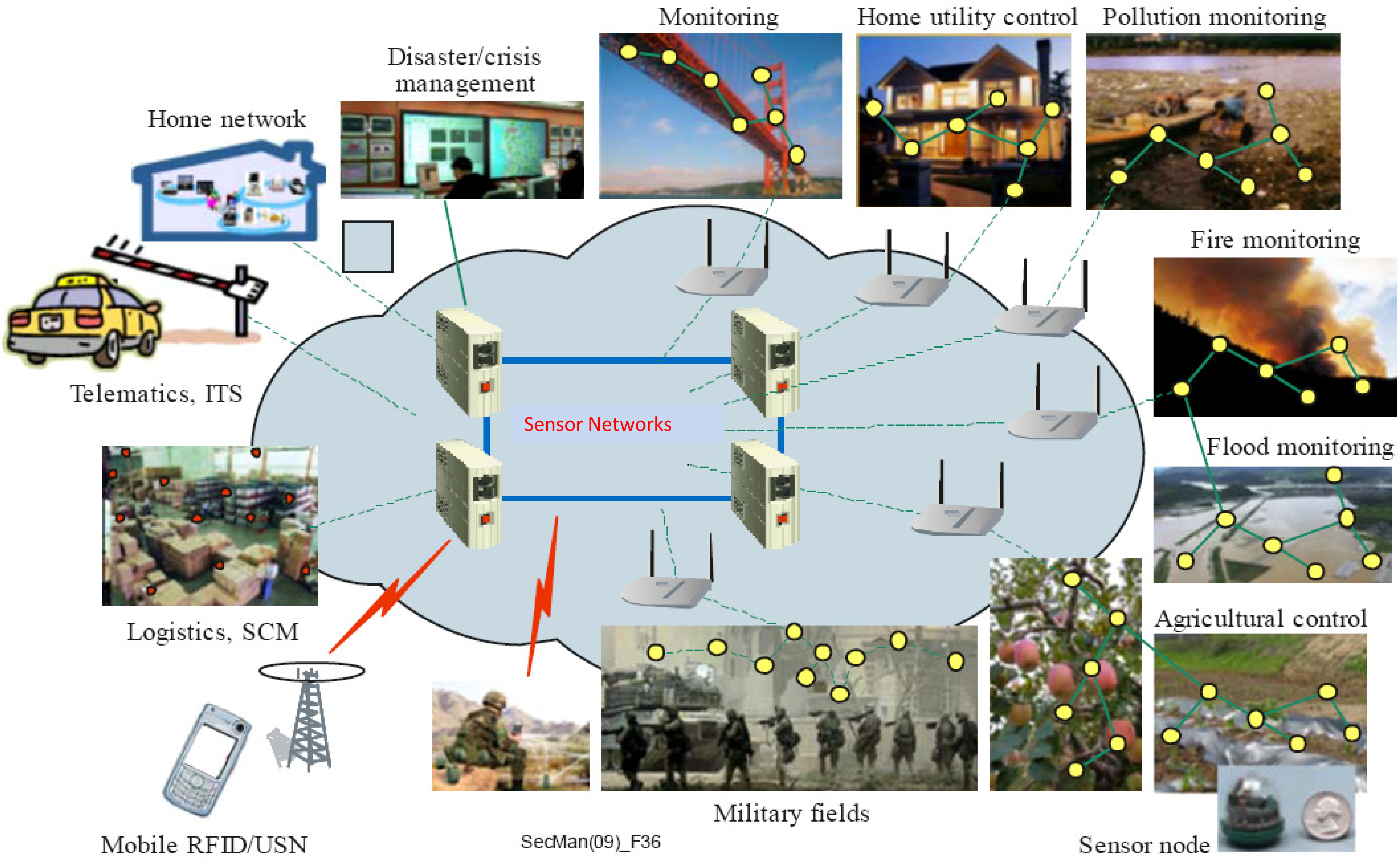
NEWS

- Why Shellshock is bad news for the Internet of things
  -25 September 2014, Web article
- Securing the Internet of Things
  -25 September 2014, Web article
- Citi Calls Coders to Develop Apps for 'Internet of Things'
  -25 September 2014, Web article
- Arm launches latest chip to power the internet of things
  -24 September 2014, Web article
- Amazon is Building an Internet of Things

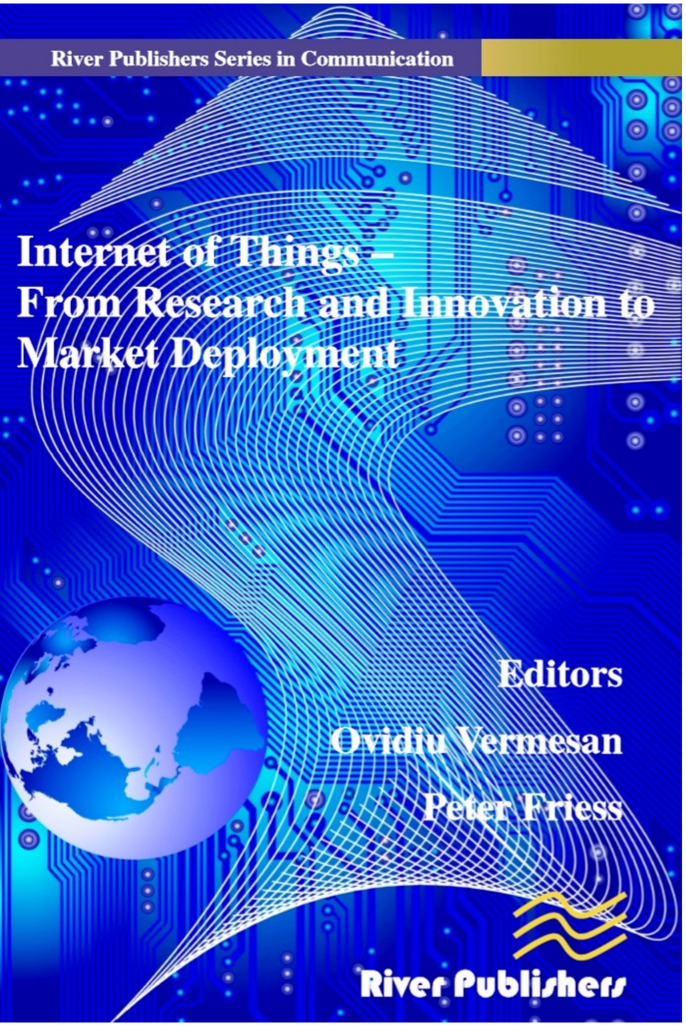
DOCUMENTS

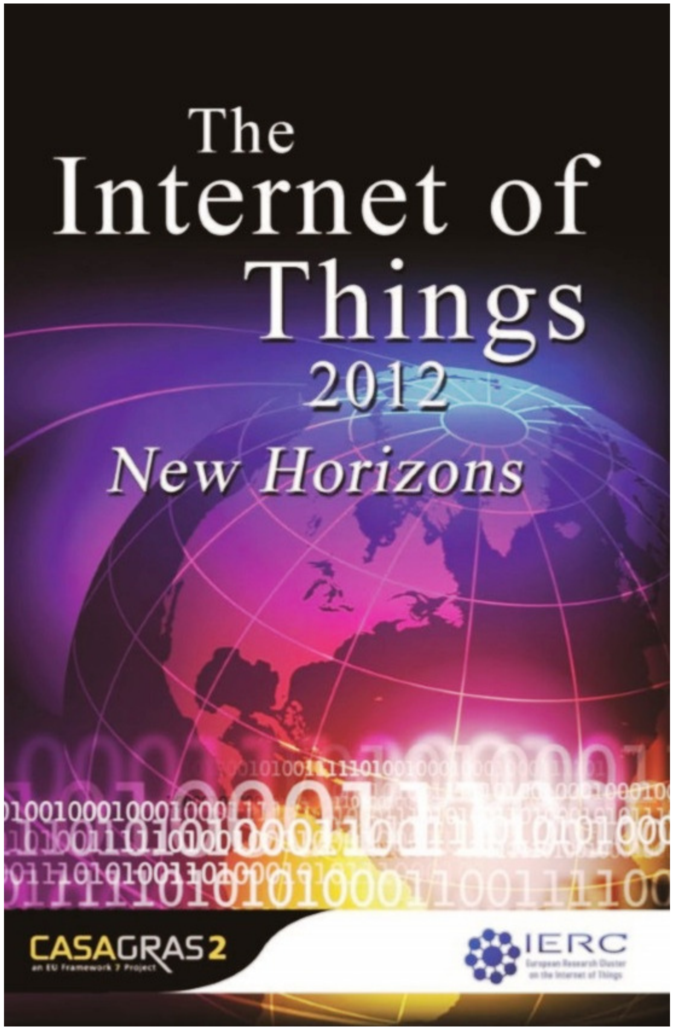
- Internet of Things: From Research and Innovation to Market Deployment
  -IERC Cluster Book 2014
- Internet of Things: Strategic Research and Innovation Agenda
  -IERC Cluster SRIA 2014
- IoT: Converging Technologies for Smart Environments and Integrated Ecosystems
  -IERC Cluster Book 2013
- The Internet of Things 2012 -

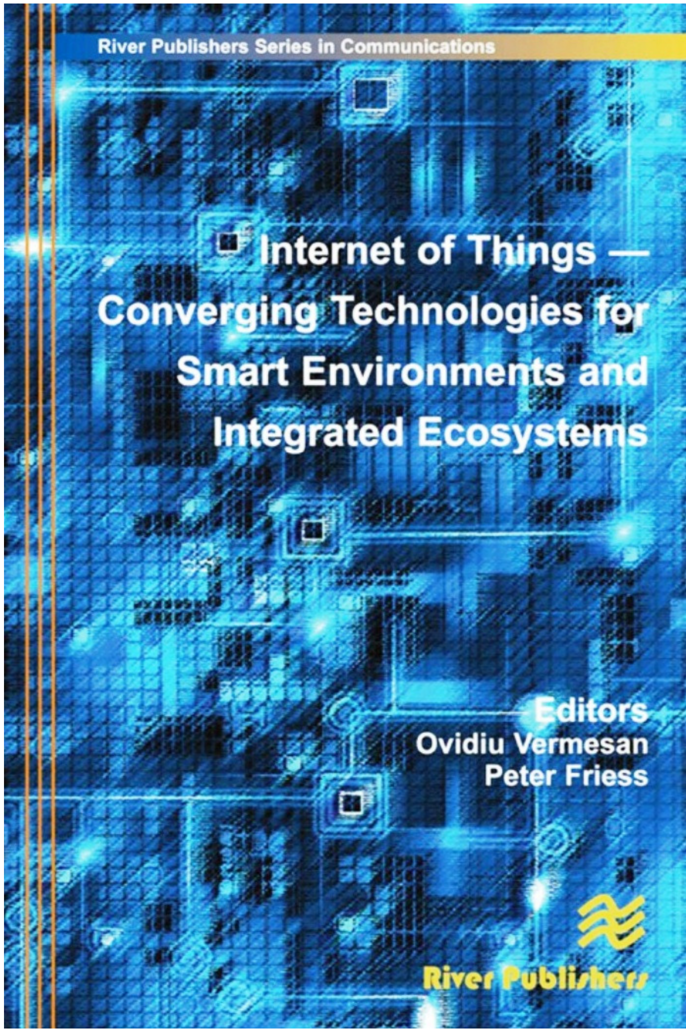
Cybersecurity for Critical Sector Environmental Networks: *"Internet of Things"*



IERC – Research Cluster Reports on *"Smart Systems" & the Internet of Things*

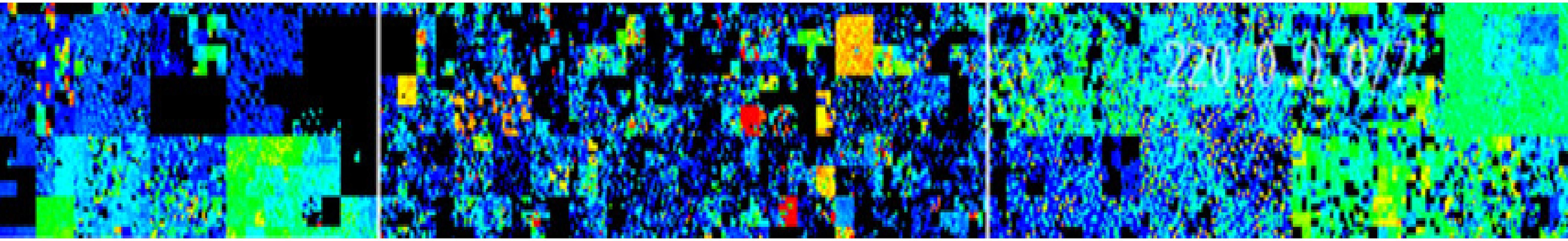

River Publishers Series in Communication
Internet of Things – From Research and Innovation to Market Deployment
Editors
Ovidiu Vermesan
Peter Friess
River Publishers


The Internet of Things 2012
New Horizons
CASAGRAS2
an EU Framework 7 Project
IERC
European Research Cluster on the Internet of Things


River Publishers Series in Communications
Internet of Things — Converging Technologies for Smart Environments and Integrated Ecosystems
Editors
Ovidiu Vermesan
Peter Friess
River Publishers

Cybersecurity for Critical National Infrastructure (CNI)

1 – The Strategic Importance of CNI	2 – Evolving Cyber Threats for CNI Sectors	3 – National & International CNI Plans
4 – 21stC Smart Systems – "Design Toolkit"	5 – Banking & Finance Sector – Analysis	6 – Energy & Transport Sectors - Analysis
7 – Civil and National Defence - Analysis	8 – CNI Security for "Internet of Things"	**9 – Smart Security for YOUR Business!**



"Smart Security" for Critical Sectors:
YOUR Shopping and To Do List!

- *Security Audit:* In-Depth Security Audit and Action Report - Spanning BOTH Physical and Cybersecurity Operations, Assets and Technologies
- *International Standards:* Understand and Implement Security Policies and Programmes to International Standards – ISO/IEC, UN/ITU, IEEE, NIST, ASIS, ISF
- *Training:* Professional Training: Form strategic partnerships with leading educational & research institutions to develop pipeline of professional graduations in cybersecurity & integrated security technologies
- *CERT/CSIRTs:* Understand the critical role of Cybersecurity CERTs and link their alerts and operational processes within your overall security policies
- *Security Associations*: Join Security Associations and follow emerging developments in Cybersecurity for *"Smart Systems"* & *"Internet of Things"*

- *.......YOUR Top Priority is Professional Cybersecurity Training & Certification with regular course "Top-Ups" since the field is moving at supersonic speed!*

Traditional *"Physical Security"* Programmes in the context of *"Cybersecurity"* for *"Critical Sectors"*

- *Audit & 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 within each prioritised critical economic sector

- *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 3 to 5 years.

- *Training:* Investment in Programme of Cross Training and Awareness such that Cybersecurity Specialists have good knowledge and understanding of physical security and vice versa

- *Roadmap:* I'd recommend developing a focused *total* security action plan and roadmap (Physical & Cyber) for each critical sector within YOUR National Economy & Enterprise Zones following the *UN/ITU GCA Framework*

....Ensure that these *Actions* are also all listed in your *"Shopping and To Do List"!*

Engineering Cybersecurity for CNI: *Cyber Skills Strategy*

- ***National and Sector-Based CERTs:*** Each country needs to build cybersecurity skills within the context of its national cybersecurity plan, led by the National CERT /CSIRT

- ***Stakeholders:*** The skills development programme will be an on-going multi-year programme and should be undertaken by the government in partnership with key public & private security stakeholders including:

  - Academic & Research Institutions such as major Universities & Colleges
  - Awareness Programmes with High Schools through competitions such as the UK and US Government "Cyber Challenge" Programmes , and Global Cyber Forensics Challenge
  - ICT Market Sector, including the major Telecommunications, ISP & Mobile Players
  - Critical Service Sector Businesses including Energy, Financial & Transportation
  - Strong focus on training for Law Enforcement Professional & Civilian Agencies

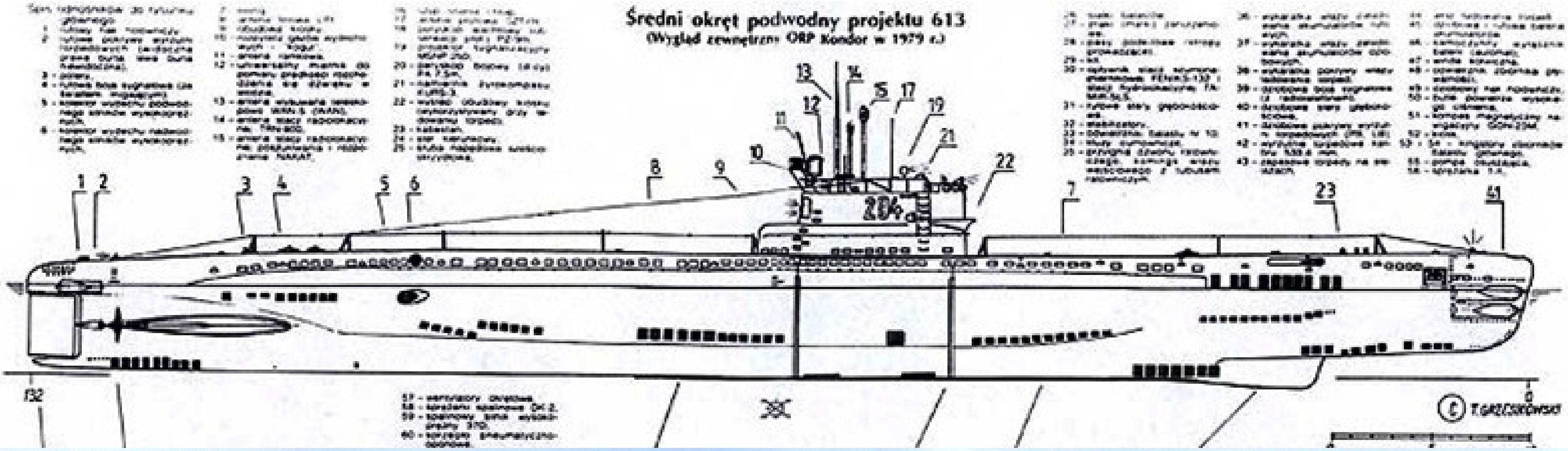
- ***Support:*** The Government should provide some financial support to "kick-start" the programme which should initially run for 3 to 5 years, with the aim to train-up professionally certified cybersecurity specialists at major educational institutions. *UK's GCHQ has recently launched High-Level MSc Cybersecurity Training through university affiliates that are audited and then certified.*

*….**People** are both the most important asset, but also often the weakest link!*

Internet Training Course: *Kola Academy of Sciences*

Whiskey 137 Class – Soviet Submarines (Project 613)

*Proposed Barter Deal in 1992 for **Training Centre** Network (**СПИИРАН**)*



Średni okręt podwodny projektu 613
(Wygląd zewnętrzny ORP Kondor w 1979 r.)
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
17
19
21
22
23
41
132
204
T. GRZEGORZEWSKI

Санкт-Петербургский институт информатики и автоматизации РАН

Cybersecurity Skills & Capacity Building

- Critical Cyber Skills Shortage: Professional Cybersecurity Skills are currently in extremely short supply even in developed countries & regions such as USA, UK and Europe!

A Human Capital Crisis in Cybersecurity

Technical Proficiency Matters

A White Paper of the
CSIS Commission on Cybersecurity for the 44th Presidency

- US Cyber Skills Report: The US Centre for Strategic and International Studies published a report in July 2010 recommending ways to overcome the skills crisis

- UK Cyber Challenge: The UK Government launched the Cybersecurity Challenge – 2010
- GCHQ launched Partnership Programme for Cybersecurity Master Degrees (MSc) with several UK Universities including Oxford, Edinburgh, Lancaster & London – August 2014

Annual International *Digital Forensics* Challenge

Winning Team 2009 : *from* South Korea

CYBER CRIME CENTER

SANS

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

CYBER SECURITY CHALLENGE.ORG.UK

JOHNS HOPKINS CAREY BUSINESS SCHOOL
Where business is taught with humanity in mind.

EC-Council

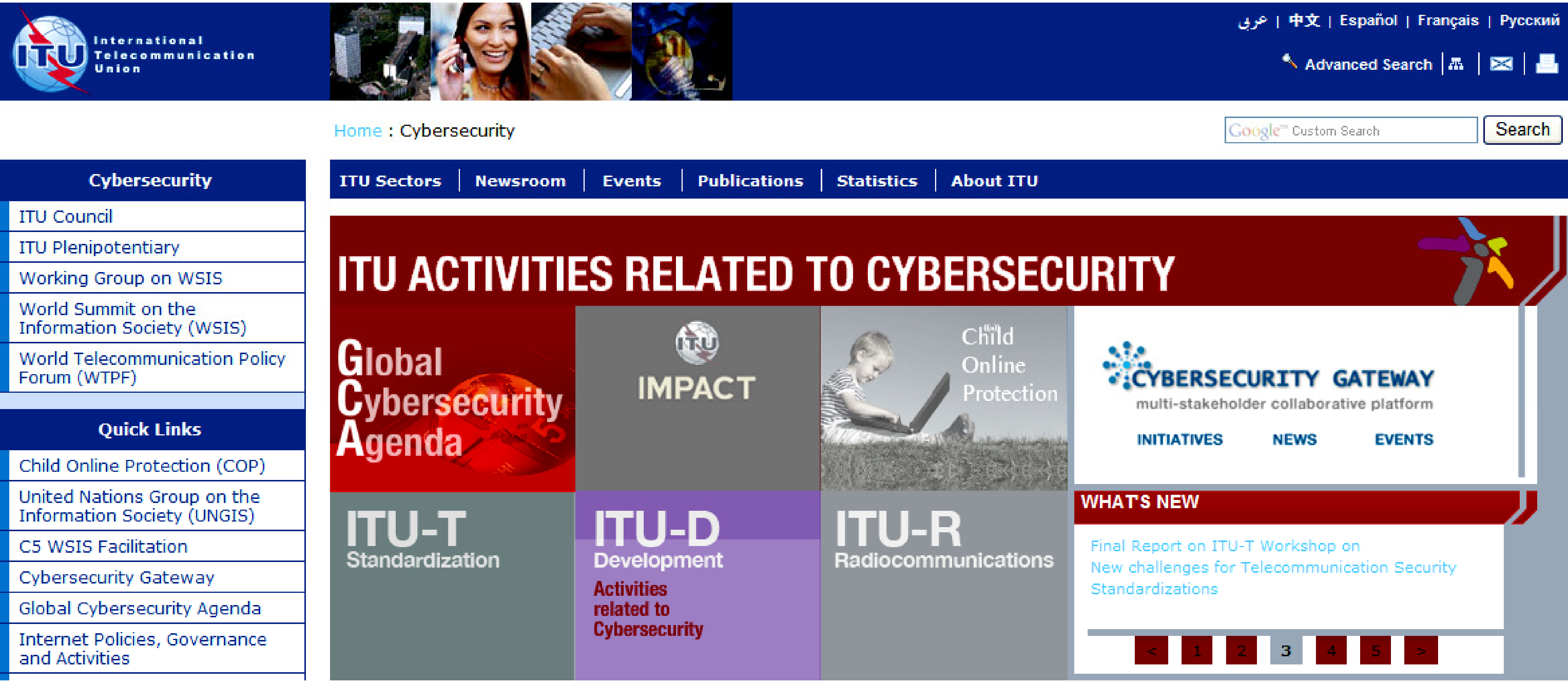
Some Professional *Cybersecurity* Roles

1) Chief Information Security Officer (CSO/CISO)
2) Systems Operations & Maintenance Personnel
3) Network Security Specialists
4) Digital Forensics & Incident Response Analysts
5) Information Security Assessor
6) Information Systems Security Officer
7) Security Architect
8) Vulnerability Analyst
9) Information Security Systems & Software Development

Critical Cybersecurity Skills Needs

Management	Information Assurance	Technical
• Cybersecurity business case formulation • IT Base skills • Staff Management skills/ Leadership skills • Personnel Security • Multi-Disciplinary skills (technology, people etc) • Communication skills • Cyber-Criminal Psychology • Cyber-Ethics Skills • Data ownership	• Cybersecurity Policies, Standards and Procedures • Risk Management • System Accreditation • Compliance Checking • Audit and Monitoring • User Rights and Responsibilities • Incident Management Process Design • Assurance, trust and confidence mechanisms	• IT technical skills (security management) • IT technical skills (IT defences deployment) • Security Design Principles e.g. zoning • Resilient Infrastructure • Data Protection/ System administration • Cryptographic and Applied Crypto Skills • Data custodianship • Operational Security • Incident Management

UN/ITU: Global Cybersecurity Programmes



International Telecommunication Union

عربي | 中文 | Español | Français | Русский

Advanced Search

Home : Cybersecurity

Google™ Custom Search | Search

Cybersecurity

- ITU Council
- ITU Plenipotentiary
- Working Group on WSIS
- World Summit on the Information Society (WSIS)
- World Telecommunication Policy Forum (WTPF)

Quick Links

- Child Online Protection (COP)
- United Nations Group on the Information Society (UNGIS)
- C5 WSIS Facilitation
- Cybersecurity Gateway
- Global Cybersecurity Agenda
- Internet Policies, Governance and Activities

ITU Sectors | Newsroom | Events | Publications | Statistics | About ITU

ITU ACTIVITIES RELATED TO CYBERSECURITY

Global Cybersecurity Agenda

IMPACT

Child Online Protection

CYBERSECURITY GATEWAY
multi-stakeholder collaborative platform

INITIATIVES NEWS EVENTS

ITU-T Standardization

ITU-D Development
Activities related to Cybersecurity

ITU-R Radiocommunications

WHAT'S NEW

Final Report on ITU-T Workshop on New challenges for Telecommunication Security Standardizations

< 1 2 3 4 5 >

Multiple ITU Programmes that contribute to National Cybersecurity Skills Building!

UN/ITU: Global Cybersecurity Agenda: *Training Resources*

Legal Measures

ITU Toolkit for Cybercrime Legislation

ITU Publication on Understanding Cybercrime: A Guide for Developing Countries

Technical and Procedural Measures

ITU Standardization Work
ICT Security Standards Roadmap
ITU-R Security Activities

ITU-T Study Group 17
ITU-T Study Group 2

Organizational Structures

ITU-IMPACT Collaboration
National CIRT establishment

International Cooperation

ITU High Level Expert Group (HLEG)
ITU-IMPACT Collaboration
ITU Cybersecurity Gateway
ITU’s Child Online Protection (COP)

Capacity Building

ITU National Cybersecurity/CIIP Self-Assessment Tool
ITU Toolkit for Promoting a Culture of Cybersecurity
ITU Botnet Mitigation Toolkit and pilot projects

IMPACT Training and Skills Development Centre
IMPACT Research Division

CISSP Certification – International Cyber Qualification

- The CISSP – Certified Information Systems Security Professional is one of the highest international qualifications from the (ISC)² , and is based upon the core tenets of *Confidentiality, Integrity & Availability:*

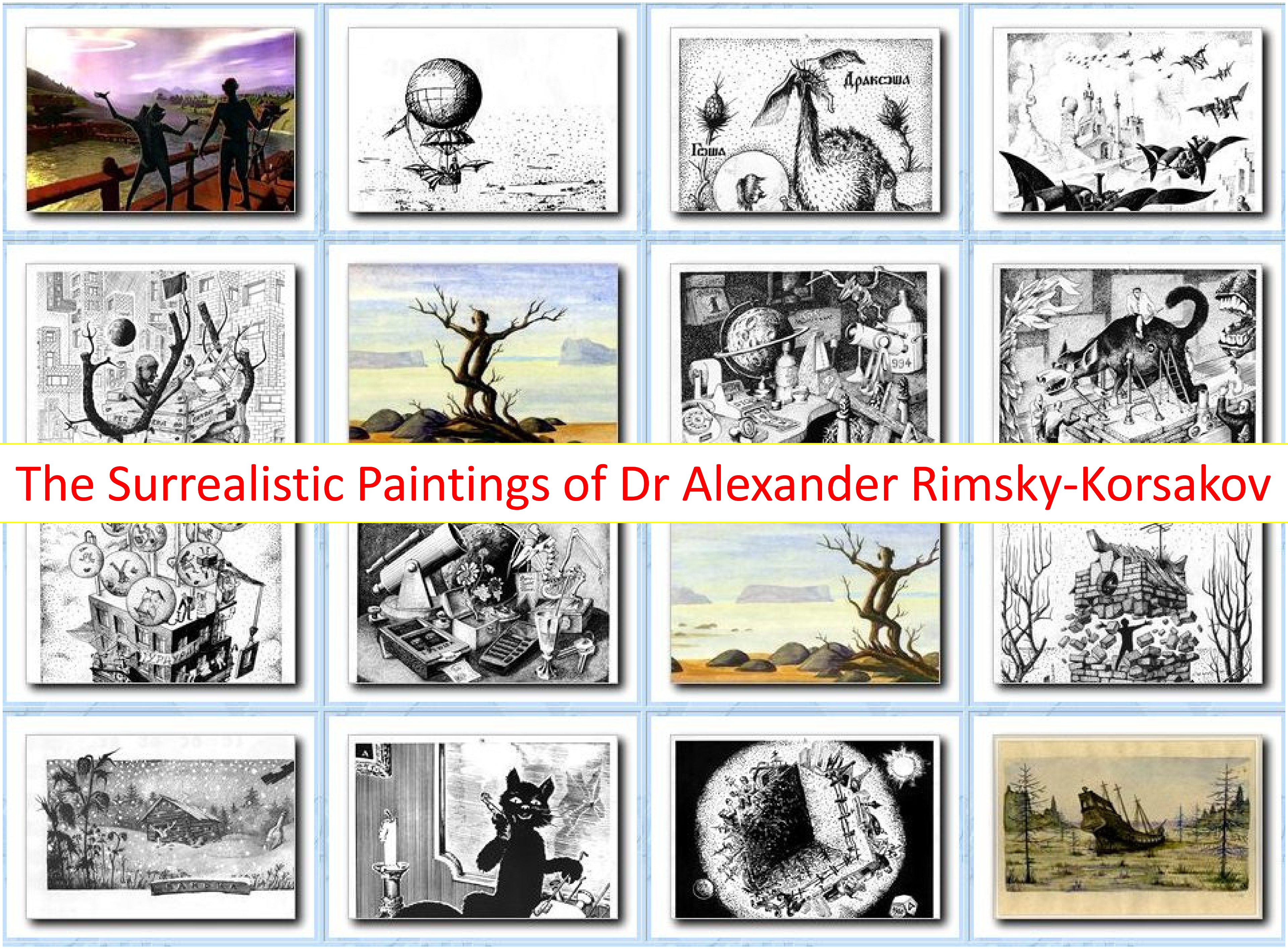
1) Access Control
2) Application Security
3) Business Continuity and Disaster Recovery
4) Cryptography
5) Information Security and Risk Management
6) Legal, Regulations, Compliance and Investigations
7) Operations Security
8) Physical (Environmental) Security
9) Security Architecture and Design
10) Telecommunications and Network Security

- *An in-depth study of all these security topics would fill an intensive 3 month training schedule, but I hope that my "trilogy" of presentations has provided the foundations!*

Striving for *Cybersecurity* Resilience!

Painting Courtesy of - *Dr Alexander Rimsky-Korsakov* - Great Grandson of the Russian Composer

The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov

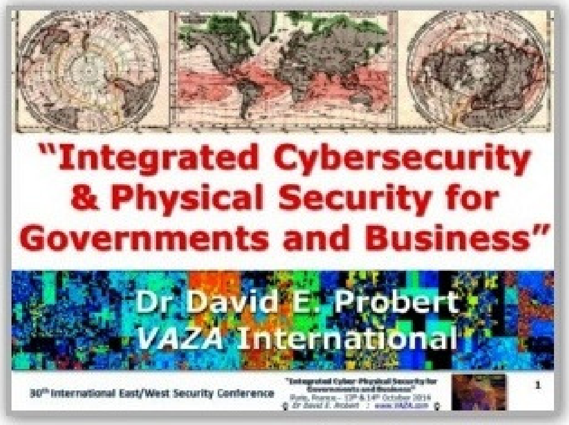


Web Link: www.valentina.net/ARK3/ark2.html

East-West Security Conference – Paris 2014

- *Cybersecurity Presentation Slides (PDF)* -

Smart Sustainable Security - "Theme Trilogy"

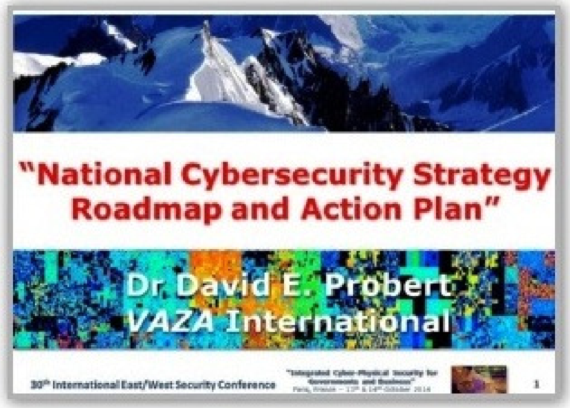


"Integrated Cybersecurity & Physical Security for Governments and Business"

Dr David E. Probert
VAZA International

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 © 1

(1) Smart Security

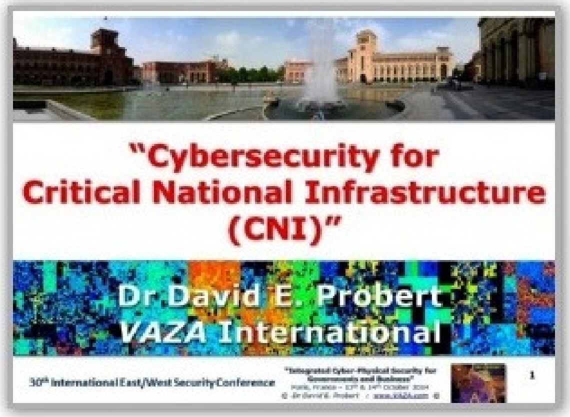


"National Cybersecurity Strategy Roadmap and Action Plan"

Dr David E. Probert
VAZA International

30th International East/West Security Conference "Integrated Cyber-Physical Security for Governments and Business" Paris, France – 13th & 14th October 2014 1

(2) National Security



"Cybersecurity for Critical National Infrastructure (CNI)"

Dr David E. Probert
VAZA International

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 © 1

(3) Critical Security

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

"Cybersecurity for Critical National Infrastructure"

30th East-West Security Conference – Paris, France

Thank-You!...

Presentation Slides:

www.Valentina.net/East-West2014/

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.

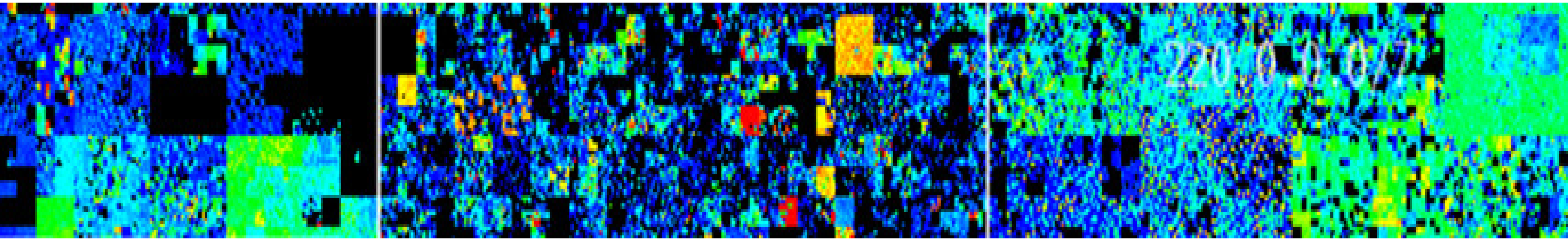
Presentation Slides:
www.Valentina.net/East-West2014/

Thank you for your time!

“Cybersecurity for Critical National Infrastructure”

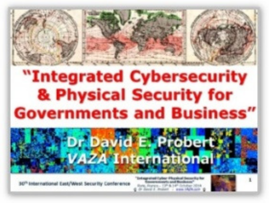
30th East/West Security Conference – Paris, France

BACK-UP SLIDES



Smart Sustainable Security – *"Theme Trilogy"*

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

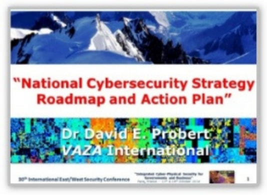

"Integrated Cybersecurity & Physical Security for Governments and Business"

Dr David E. Probert
VAZA International

- *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*

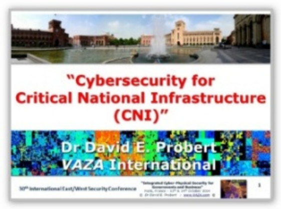

"National Cybersecurity Strategy Roadmap and Action Plan"

Dr David E. Probert
VAZA International

- *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*


"Cybersecurity for Critical National Infrastructure (CNI)"

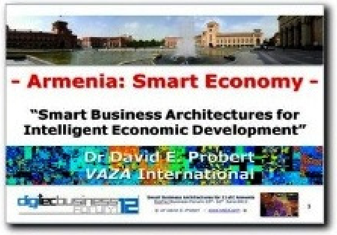
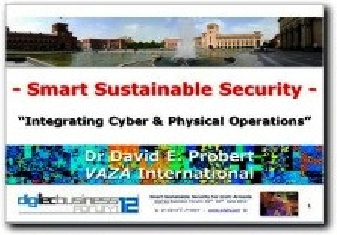
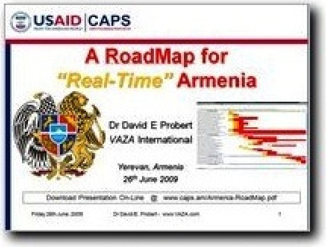
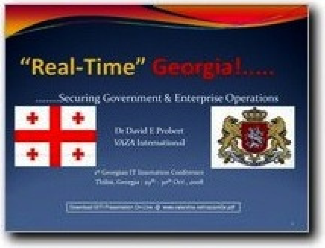
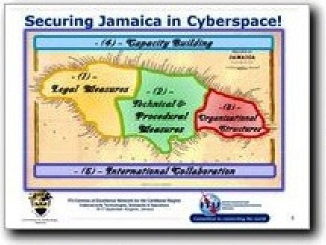
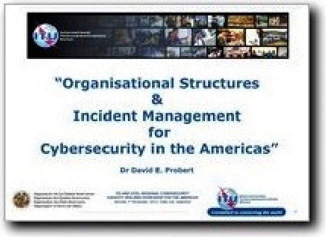
Dr David E. Probert
VAZA International

- *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/

Additional *Cybersecurity* Resources

 Smart Solutions: "Master Class" – Part 1 - Defining Smart Solutions & Business Architectures - Dr David E. Probert VAZA International	 Smart Solutions: "Master Class" – Part 3 - Designing & Engineering Smart Solutions - Dr David E. Probert VAZA International	 - Armenia: Smart Economy - "Smart Business Architectures for Intelligent Economic Development" Dr David E. Probert VAZA International	 - Smart Sustainable Security - "Integrating Cyber & Physical Operations" Dr David E. Probert VAZA International	 - Smart Governance - "Stimulating Innovation & Economic Growth" Dr David E. Probert VAZA International
"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" "Securing Government & Financial Enterprise Operations"	 "Real-Time" ARMENIA!... ...Securing Government & Financial Enterprise Operations Dr David E Probert VAZA International	 "Awesome Armenia!" Photos and Panoramas Armenia Spring - 2009 Armenia Summer 2009 Armenian Panoramas Summer - 2009	 "Roadmap for Real-Time Armenia" "E-Government, E-Commerce and E-Security" USAID | CAPS	 USAID | CAPS A RoadMap for "Real-Time" Armenia Dr David E Probert VAZA International Yerevan, Armenia 26th June 2009
"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!..... ...Securing Government & Enterprise Operations Dr David E Probert VAZA International	 "Real-Time Georgia" "Securing Government & Enterprise Operations"	 "Republic of Georgia" Photos and Panoramas Georgian Panoramas Autumn 2007 Caucasus Aerial Panoramas Georgian Panoramas Autumn 2008 Georgia 2008	 ..."21stC Georgia"... ..."Cyber-Vardzia"...	 21stC Georgia – "Cyber Vardzia" "Integrated Cyber & Physical Security" for e-Government & e-Georgia Dr David E. Probert VAZA International GITI
"Real-Time Georgia" - GITI 2008 Slides	"Real-Time Georgia" - GITI 2008 Paper	Gorgeous Georgia: In Photos	21stC Georgia: "CyberVardzia" - Paper	21stC Georgia - "CyberVardzia" - Slides
 Securing Jamaica in Cyberspace! - (4) - Capacity Building - (1) - Legal Measures - (2) - Technical & Procedural Measures - (3) - Organisational Structures - (5) - International Collaboration	 * ITU Cybersecurity Strategy * "3-Day Workshop Overview" Workshop Presentations Group Tasks & Discussions Workshop Presentations Group Tasks & Discussions	 Dr. David E PROBERT (Executive Director, VAZA International)	 "Organisational Structures & Incident Management for Cybersecurity in the Americas" Dr David E. Probert	 "Cybersecurity Capacity Building & International Collaboration " Dr David E. Probert
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

21stC Technology Foundations for *Smart Systems*

- *Smart Systems* require a wide diversity of functions & features just like “living organic cells”. Advanced ICT technologies now provides many existing & emerging smart options:
  - ***Networks:*** High-Speed Giga Byte Networking: Physical, Mobile & Wi-Fi
  - ***Virtualisation:*** Multi-Threaded Processors & System Virtualisation
  - ***Massive Storage:*** Internal, External & “Cloud” Storage, with Data Mining
  - ***Semantic Web:*** Led by W3C – “Smart Web” with linguistic understanding
  - ***Cybersecurity:*** Real-Time Security for O/S & Applications Software
  - ***Architecture :*** Scalable Architecture Solutions for Software Platform
  - ***Interface:*** Intelligent User Interface: Touch & Body Control
  - ***Standards:*** Conformance to International Standards (ISO/IEEE)
  - ***Location:*** Location Aware (GPS) & Environmental Sensors/Feedback
  - ***Immersive Media:*** Augmented Reality (AR) for Immersive Real/Virtual Worlds
  - ***Social Media & Search:*** Both are now generic global ICT service capabilities
  - ***Smart Mobile Media:*** At the heart of new Business Models & Architectures

- *Internet Protocol – TCP/IP (1975 – Vint Cerf & Robert Kahn) - is itself an adaptive networking protocol with dynamic routing, transmission and congestion control*

“Master Class”: Armenia - *DigiTec2012*

- Smart Security, Economy & Governance -

Smart Solutions: “Master Class” – Part 1

- Defining Smart Solutions & Business Architectures -

Dr David E. Probert
VAZA International

"Master Class - Smart Theory"

Smart Solutions: “Master Class” – Part 2

- Smart Solutions in Practice for 21stC Armenia -

Dr David E. Probert
VAZA International

"Master Class - Smart Practice"

Smart Solutions: “Master Class” – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

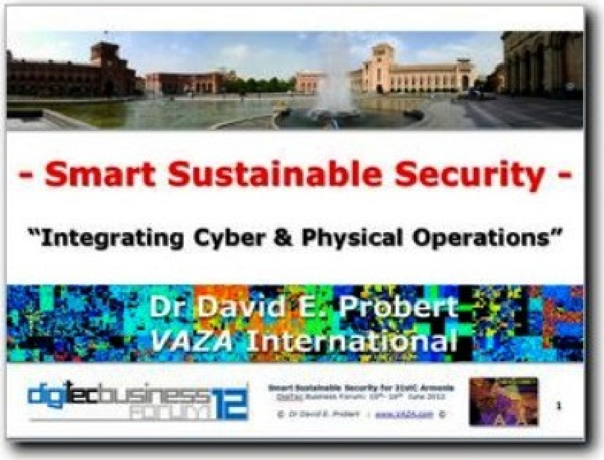
"Master Class - Smart Design"

- Armenia: Smart Economy -

“Smart Business Architectures for Intelligent Economic Development”

Dr David E. Probert
VAZA International

"Armenia: Smart Economy"



- Smart Sustainable Security -

“Integrating Cyber & Physical Operations”

Dr David E. Probert
VAZA International

"Armenia: Smart Sustainable Security"

- Smart Governance -

“Stimulating Innovation & Economic Growth”

Dr David E. Probert
VAZA International

"Armenia: Smart Governance"

Cyber Attack on *Personal Laptop:* 3rd Oct 2014

(1) Sequence and Symptoms of Cyber Attack

- Downloaded Express Thumbnail Creator (Shareware) from Tucows.com for Web Page
- Chose Advanced Option not to install alternative Browser Tabs or new Search Software
- Installation Software took much longer than expected and started to install "Potentially Unwanted Programs" (PUPs) = Malware
- Malware downloaded included unwanted *StormWatch, RocketTab* and *Groovorio*
- McAfee Real-Time Applications Checker quarantined multiple *Artemis Trojan Apps*!
- Stopped Software Download & Installation prematurely since clearly something wrong!
- Discovered Internet Explorer had new Proxy Server Setting and could not connect to Internet
- Rebooted computer and received unusual blank command Prompt Screen on start-up sequence
- Both Windows and McAfee Firewalls *disabled*

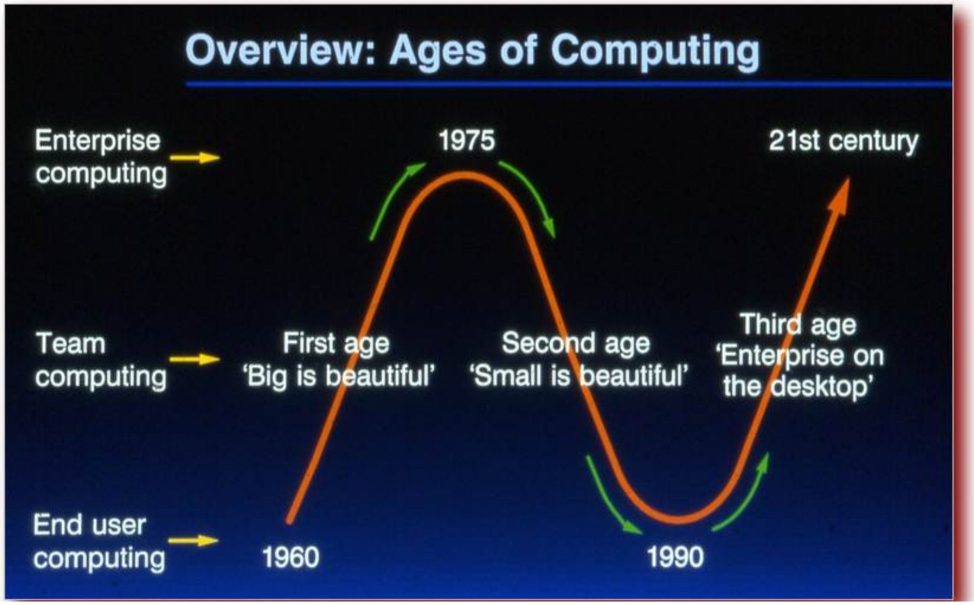
- *Result was PC wide open to hacker attacks via open firewall and internet routed through criminal proxy server for theft of personal ID*

(2) Steps to Discover and Delete Malware

- System Restore failed with Corrupt Files Error
- Reset Firefox, IE and Chrome to Factory Settings
- Full Virus Check with *McAfee* Total Protection
- Use *sfc/scannow* to repair some files but error shows remaining windows OS corruption
- Used *CheckDisk* on all drives to fix corruption
- Finally used *DISM* for On-Line *HealthCheck* and *RestoreHealth* for Windows OS 8.1 for repairs
- Edited Start Menu to delete unwanted malware
- Installed and scanned using *MalwareBytes.org* which found several dangerous malware files
- Installed *Hitman_x64* as second opinion scanner which discovered further client.exe startup file for the RocketTab Malware as well as numerous ad cookies.
- Used *McAfee Virtual Technican* to check on Anti-Virus Installation. Still failed some checks so fully re-installed Mcafee on-line for maximum security

- ***Time to Fix Malware Attack = 5+ Hours!***

Ages of Computing, Networking & Intelligence: *1960 - 21stC*



Overview: Ages of Computing

Enterprise computing →

Team computing →

End user computing →

1960

1975

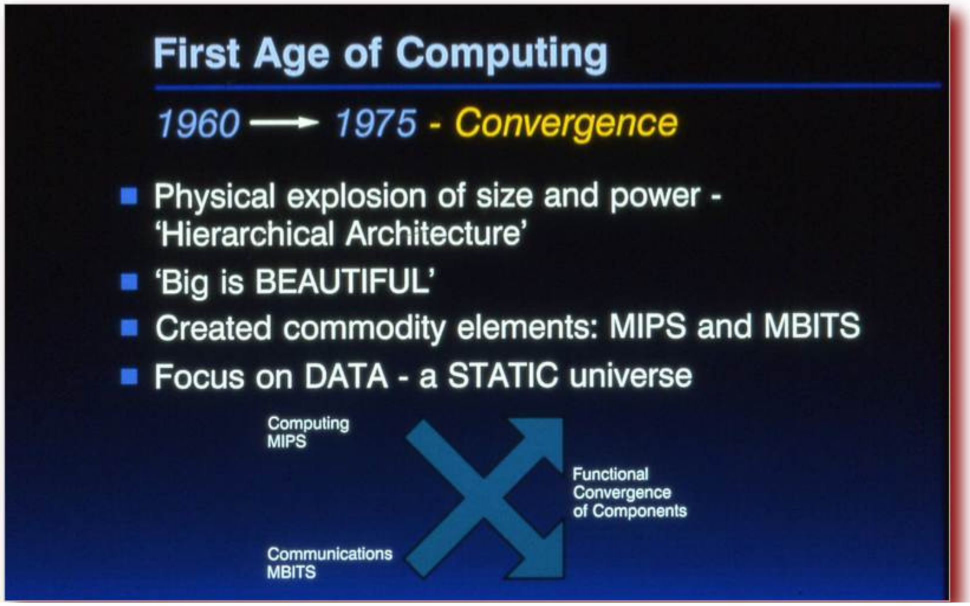
1990

21st century

First age
'Big is beautiful'

Second age
'Small is beautiful'

Third age
'Enterprise on the desktop'



First Age of Computing

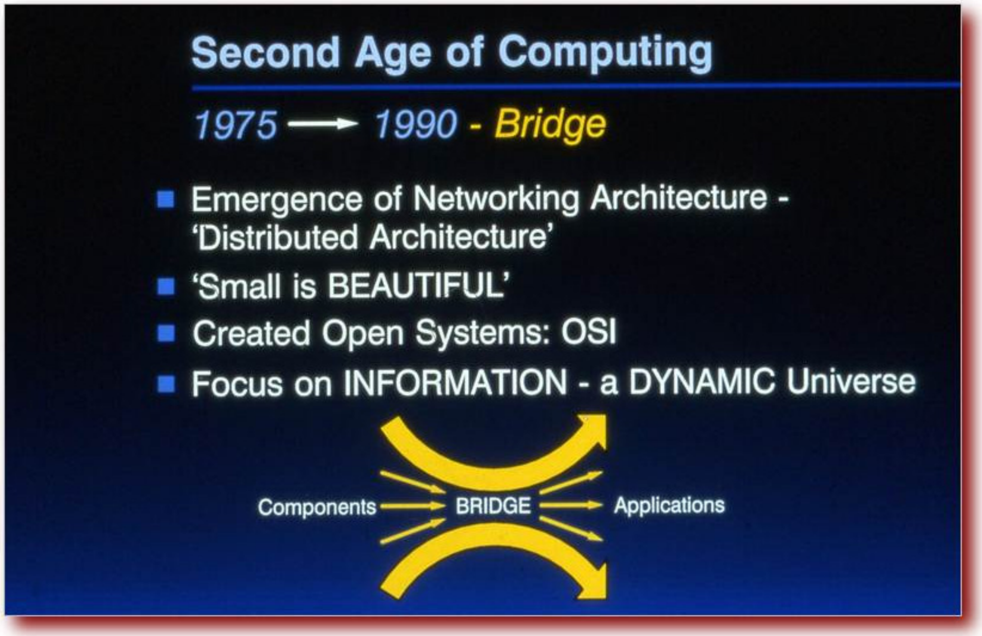
1960 → 1975 - Convergence

- Physical explosion of size and power - 'Hierarchical Architecture'
- 'Big is BEAUTIFUL'
- Created commodity elements: MIPS and MBITS
- Focus on DATA - a STATIC universe

Computing MIPS

Communications MBITS

Functional Convergence of Components

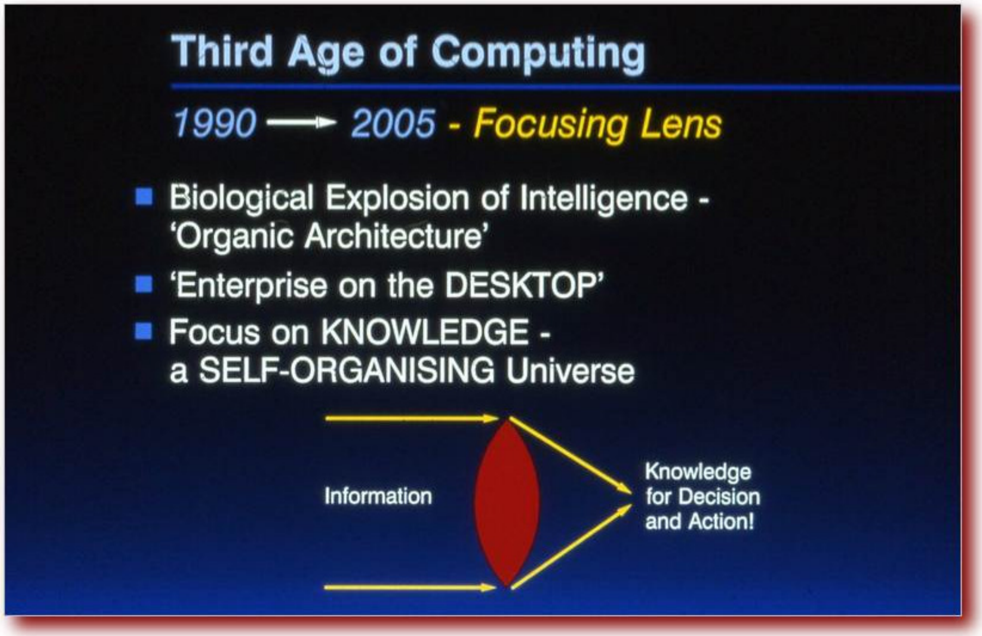


Second Age of Computing

1975 → 1990 - Bridge

- Emergence of Networking Architecture - 'Distributed Architecture'
- 'Small is BEAUTIFUL'
- Created Open Systems: OSI
- Focus on INFORMATION - a DYNAMIC Universe

Components → BRIDGE → Applications



Third Age of Computing

1990 → 2005 - Focusing Lens

- Biological Explosion of Intelligence - 'Organic Architecture'
- 'Enterprise on the DESKTOP'
- Focus on KNOWLEDGE - a SELF-ORGANISING Universe

Information

Knowledge for Decision and Action!

Ages of Computing, Networking & Intelligence: *1960 – 2020+*

- ***1960 to 1980 (Computing Big Bang –*** *Physical Data* ***):*** "Big is Beautiful" – Era of Massive Mainframe Computing with Minimal Networking

- ***1980 to 2000 (Network Architecture –*** *Fluid Information* ***):*** "Small is Beautiful" – Evolution of Networking (Ethernet, Token-Ring, and TCP/IP: '75 – Vint Cerf & Robert Kahn), PCs, Web1.0: '92-'94 & Mobile Phones

- ***2000 to 2020+ (Intelligent Systems –*** *Cellular Knowledge* ***):*** "Smart Solutions"- Web2.0, Social Media, Smart Phones & Intelligent Apps.

- ***Summary:*** The Evolution of ICT mirrors the Evolution of the Physical Universe, DNA/RNA Bio-Architecture, Intelligent Organisms & Life.