



# - CyberTerrorism (2) - *"Security in Cyberspace"*

Dr David E. Probert  
**VAZA International**

Dedicated to Richard Noble & Andy Green: "1<sup>st</sup> Supersonic Car - ThrustSSC"

**31<sup>st</sup> International East/West Security Conference**

**"CyberTerrorism(2): Security in Cyberspace"**

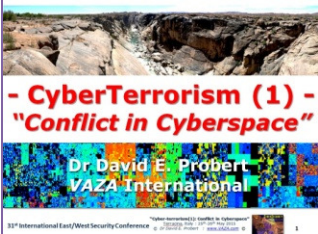
Terracina, Italy: 24<sup>th</sup> – 27<sup>th</sup> May 2015

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# CyberTerrorism – “Dual Themes”

## Theme (1)” *“Conflict in Cyberspace”* : The Players, Stakeholders & Emerging Trends



- The Colonisation of Cyberspace by the “Good Guys” & “Bad Guys”!
- Need for Integrated Physical-Cyber Security for 21<sup>st</sup> C Terrorist Defence
- Emergence of the “Internet of Things” as the Future Cyber Conflict Zone

*“Divergence: Chaotic Cyberspace Colonisation “*

**26<sup>th</sup> May: 09:00 – 09:45**

## Theme (2) – *“Security in Cyberspace”*: Operational Security Models for 21<sup>st</sup> Century



- Survey of Cybersecurity Strategies, Models & Frameworks
- Protection of Banking & Corporate Enterprises from Cyber Threats
- Developing YOUR Action Plans & Practical Cybersecurity Programme

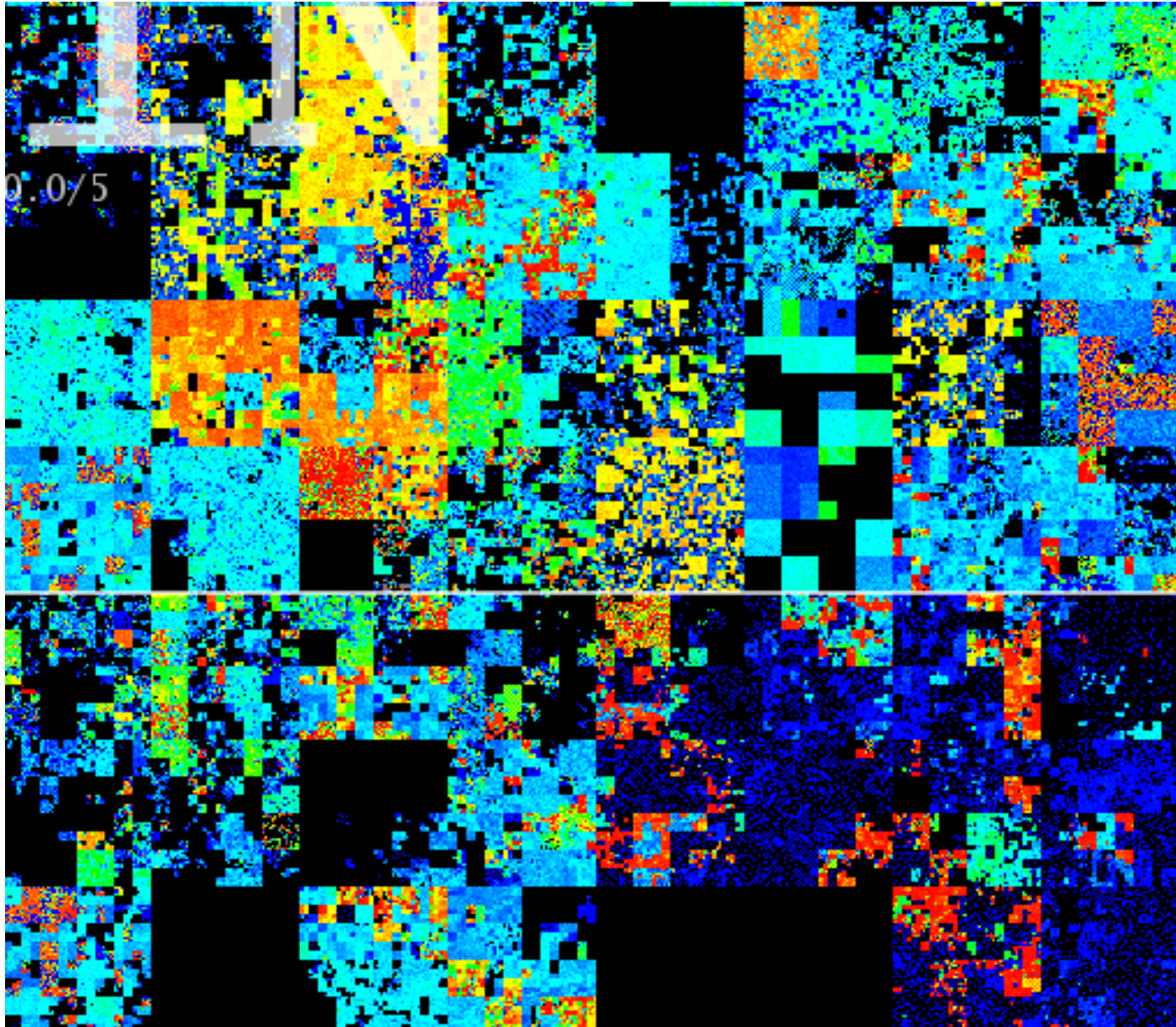
*“Convergence: Integrated Real-Time Defence”*

**26<sup>th</sup> May: 14:15 – 14:55**

**Download Slides: [www.valentina.net/East-West2015/](http://www.valentina.net/East-West2015/)**



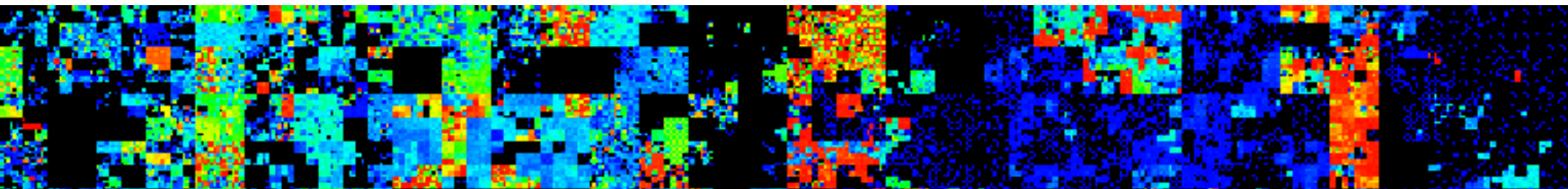
# *...or the Challenging Complexity of Securing Government & Business in **Cyberspace**!...*



# - CyberTerrorism (2) – “Security in Cyberspace”



1 – <i>Supersonic</i> “Real-Time” Cyber security	2 – Cybersecurity Models & Architectures	3 –Cyber <i>Emergency</i> Response Team: <i>CERT</i>
4 –Cybersecurity for Government & Defence	5 – Cybersecurity for Banking & Finance	6 – Securing Critical National Infrastructure
7 –Cyber Action Plans & <i>Tactical</i> Road Maps	8 – <i>OUR</i> Cyber Future : “ <i>Neural Society</i> ”	9 – Developing <i>YOUR</i> Cybersecurity Plans!





# Warning! : CyberTerror Travels @ “Light Speed”

О том, как  
мечта одного человека  
о преодолении сверхзвукового  
барьера могла бы содействовать  
успеху Вашего бизнеса



**Physical Terror = “Spatial”:** Attacks on Physical Infrastructure , Corporate Assets, Staff and Citizens

\*\*\* Sound Waves = 340metres/sec \*\*\*

**Cyber Terror = “Temporal”:** Anonymous Attacks on, Network Hubs, Servers, Databases & Social Media

\*\*\* Light Waves = 300,000,000 metres/sec \*\*\*



**Thrust SSC: - 1<sup>st</sup> Supersonic Car: 1995-1997**

Web Archive: [www.thrustssc.com](http://www.thrustssc.com)

31<sup>st</sup> International East/West Security Conference

“Cyber-terrorism(2): Security in Cyberspace”

Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



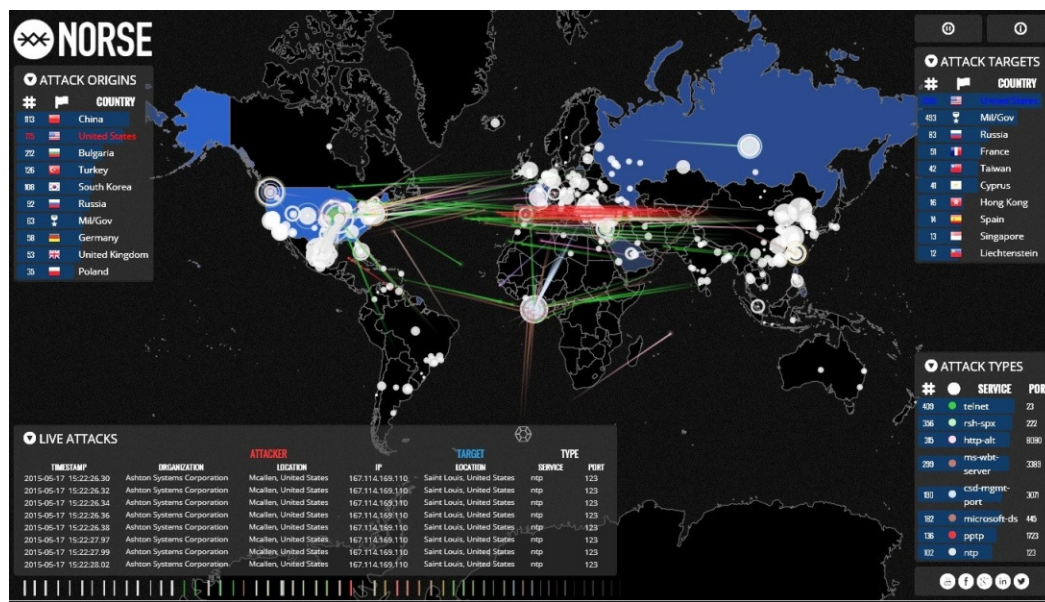
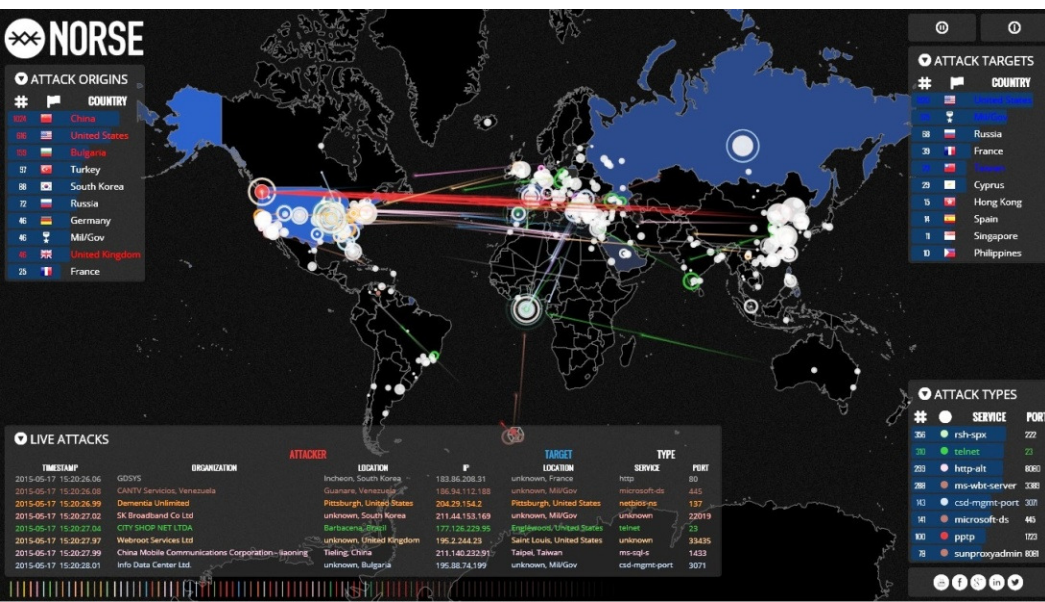
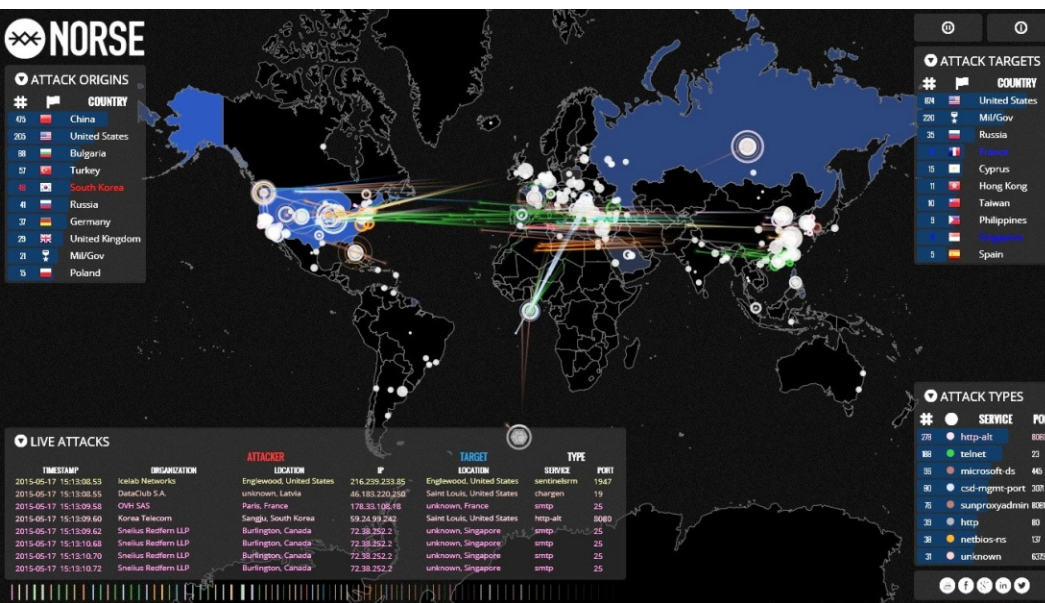
# Thrust SSC – “Breaking the Sound Barrier” \*

## Mach ONE - 1228km/h – October 1997 \*





# Successive “Real-Time” *DarkNet* CyberAttacks



Link: [map.ipviking.com](http://map.ipviking.com) - Norse Corporation

31<sup>st</sup> International East/West Security Conference

“Cyber-terrorism(2): Security in Cyberspace”

Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# “Real-Time” Cybersecurity for Business

- *“Massive \$\$\$ Losses”*: Increasing “Conflict, eCrime & Terrorism in Cyberspace” is costing Global Business an estimated \$450Billion/Year in financial losses.
- *“Cyber Light Speed”*: Cyber Threats & Attacks travel at “Light Speed” and require “Real-Time” Response!
- *“Rethink Security”*: Government & Business need to rethink “Security Strategy” to mitigate cyber threats

*....Now we present several practical Cybersecurity models that you may adapt to your Organisation or Business.*

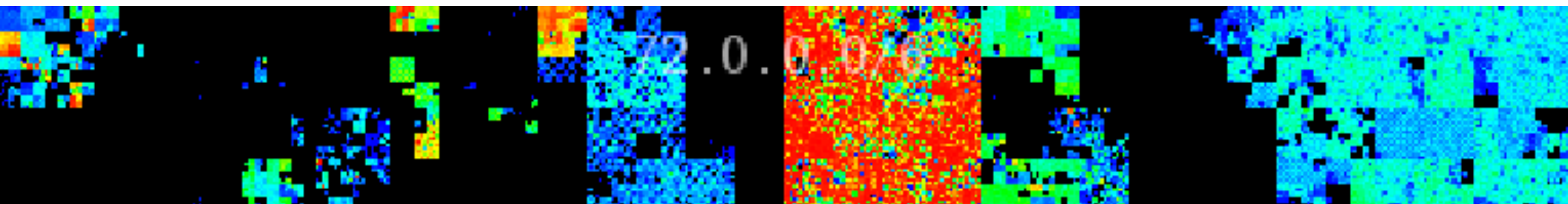




# - CyberTerrorism (2) – “Security in Cyberspace”



1 – <i>Supersonic</i> “Real-Time” Cybersecurity	2 – Cybersecurity Models & Architectures	3 –Cyber <i>Emergency</i> Response Team: <i>CERT</i>
4 –Cybersecurity for Government & Defence	5 – Cybersecurity for Banking & Finance	6 – Securing Critical National Infrastructure
7 –Cyber Action Plans & <i>Tactical</i> Road Maps	8 – <i>OUR</i> Cyber Future : “ <i>Neural Society</i> ”	9 – Developing <i>YOUR</i> Cybersecurity Plans!



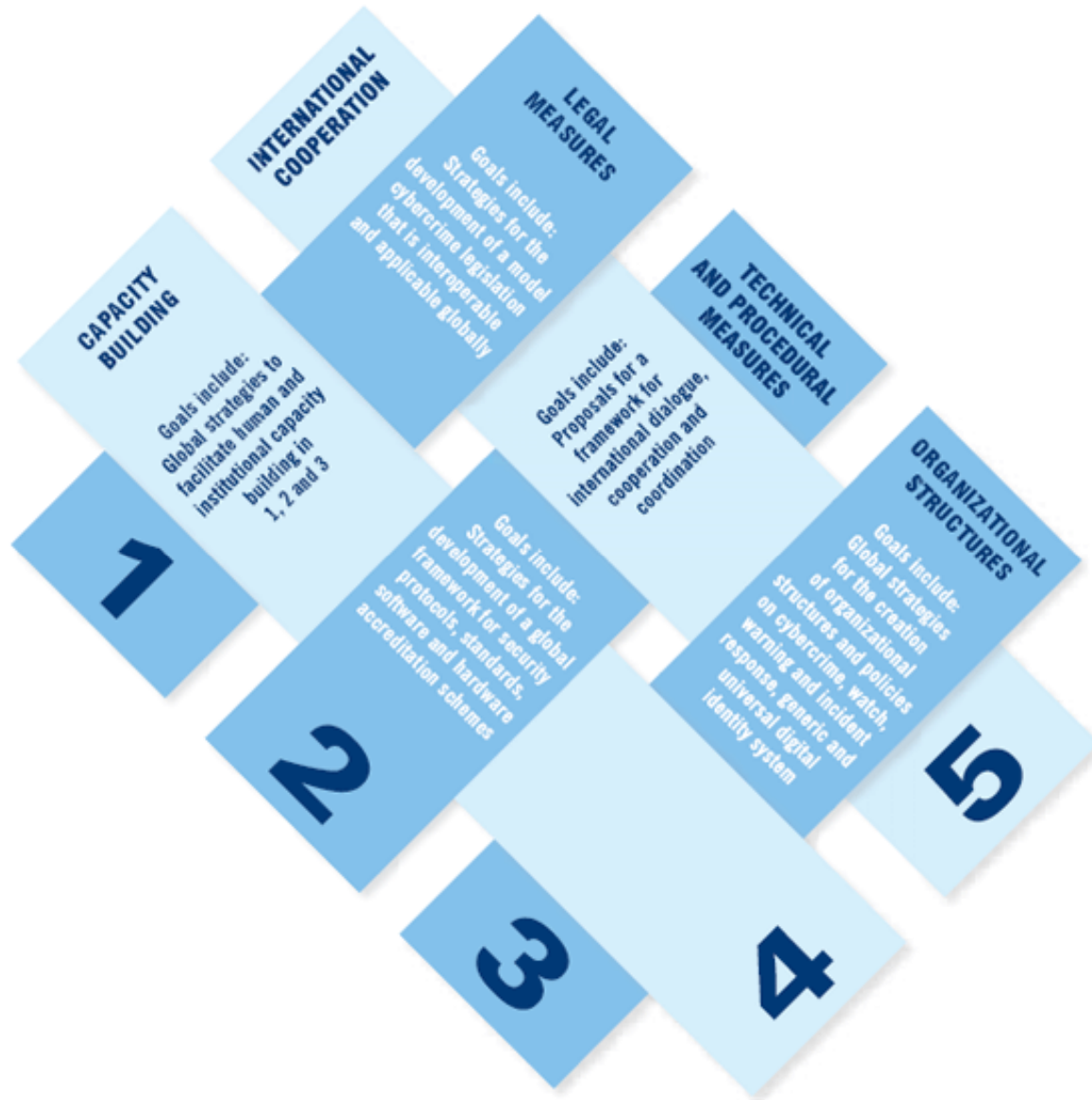
# Cybersecurity Models & Frameworks

- **UN/ITU:** Global CyberSecurity Agenda (GCA)
- **UK Contest:** Counter Terror Strategy: -  
*...Pursue, Prevent, Protect & Prepare*
- **NATO/CCDDOE:** National Cybersecurity Framework
- **EU/ENISA:** Info Security Agency – Cyber Good Practice Guide
- **OAS/CICTE:** Inter-American Committee against Terrorism
- **SANS Institute:** Critical Security Controls
- **ISF:** Information Security Forum: “Good Practice Standard”
- **ISO/IEC 27000 Series:** Information Security Standards
- **NIST :** Institute of Standards – Cybersecurity Framework





# UN/ITU:– *Global Cybersecurity Agenda (GCA)*



## The UN/ITU GCA - Global Cybersecurity Agenda:

- 1 – Legal Measures
- 2 – Technical Measures
- 3 – Organisational Measures
- 4 – Capacity Building
- 5 – International Cooperation

...The **UN/ITU** constitutes a **unique global forum** for partnership and the discussion of **cybersecurity**.



# Worldwide Security in *Cyberspace*!

- (4) – Capacity Building

- (1) –  
Legal Measures

- (2) –  
Technical  
&  
Procedural  
Measures

- (3) –  
Organisational  
Structures

- (5) – Regional and International Collaboration





# NATO *Cybersecurity* Framework Manual

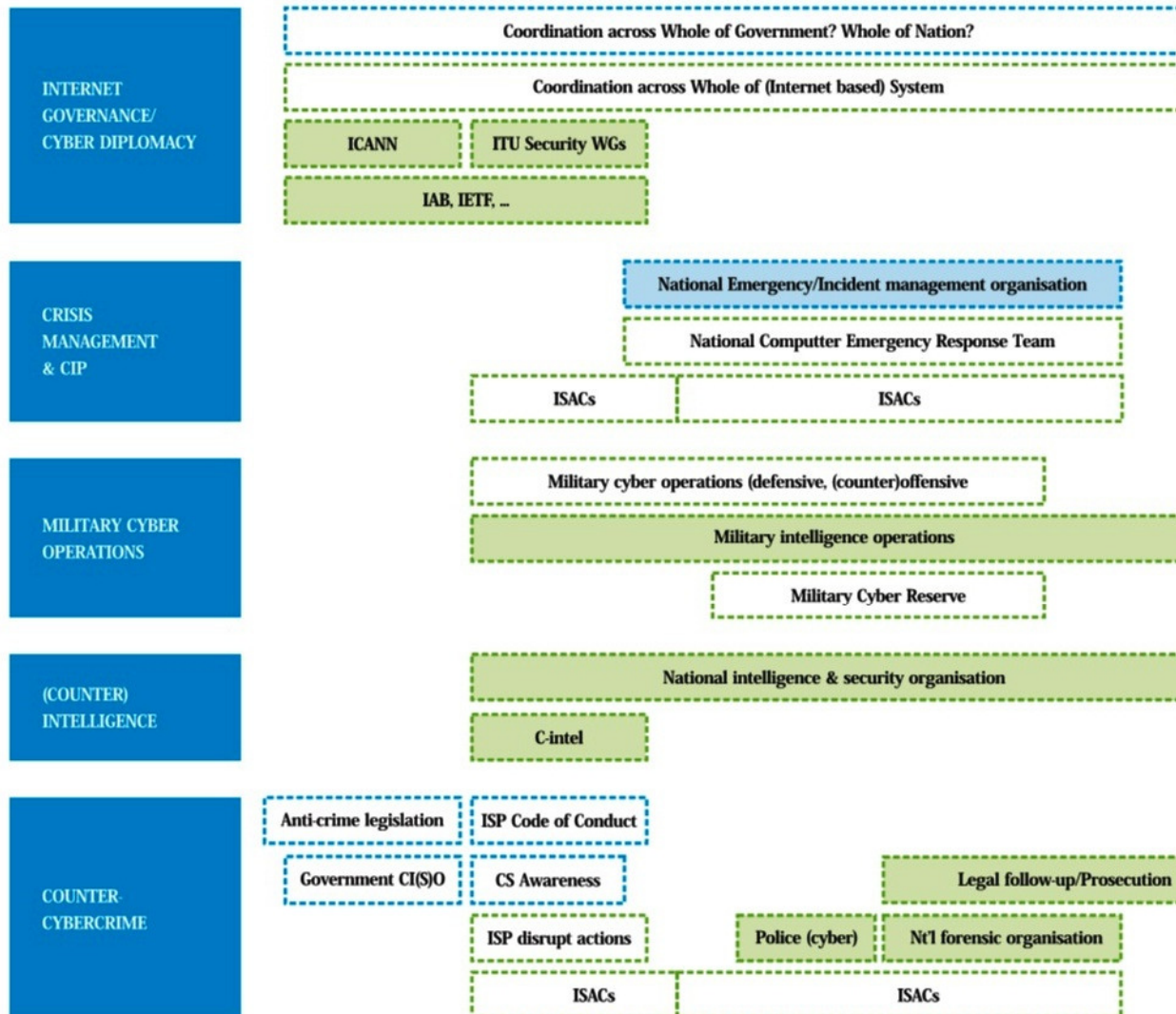
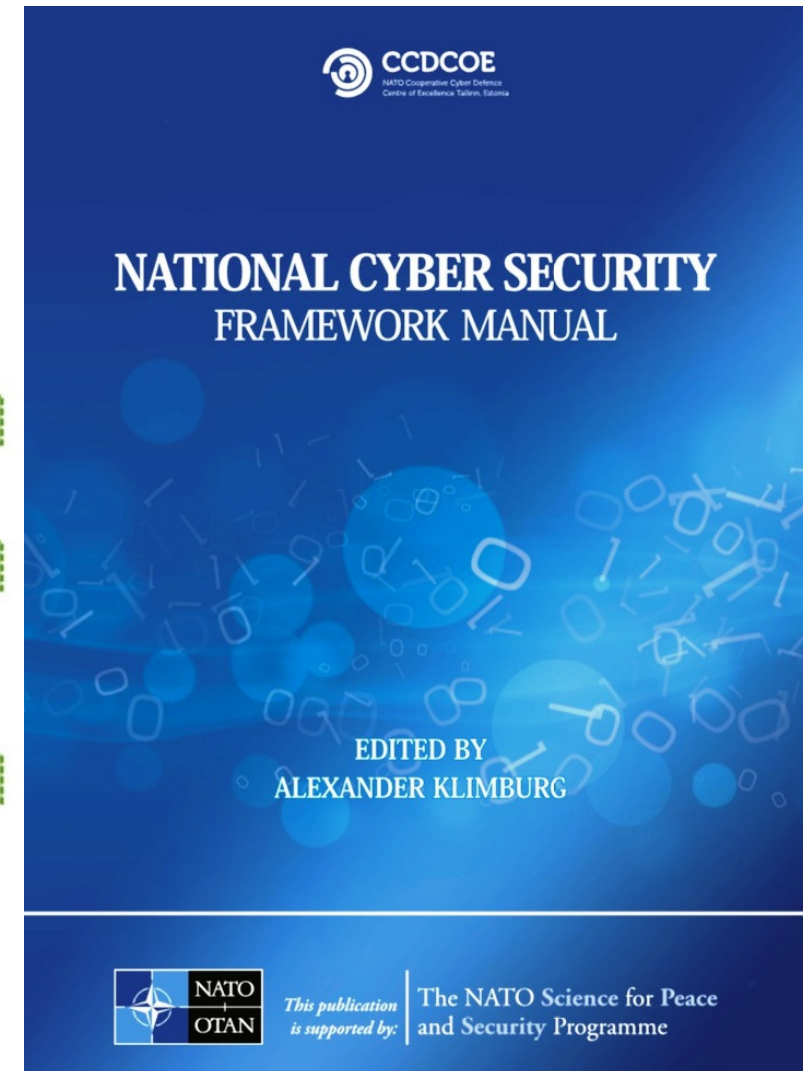


Figure 6: The Organisational Picture Across Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in



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





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



# NATO Cybersecurity Framework:

## - Organisational Architecture -

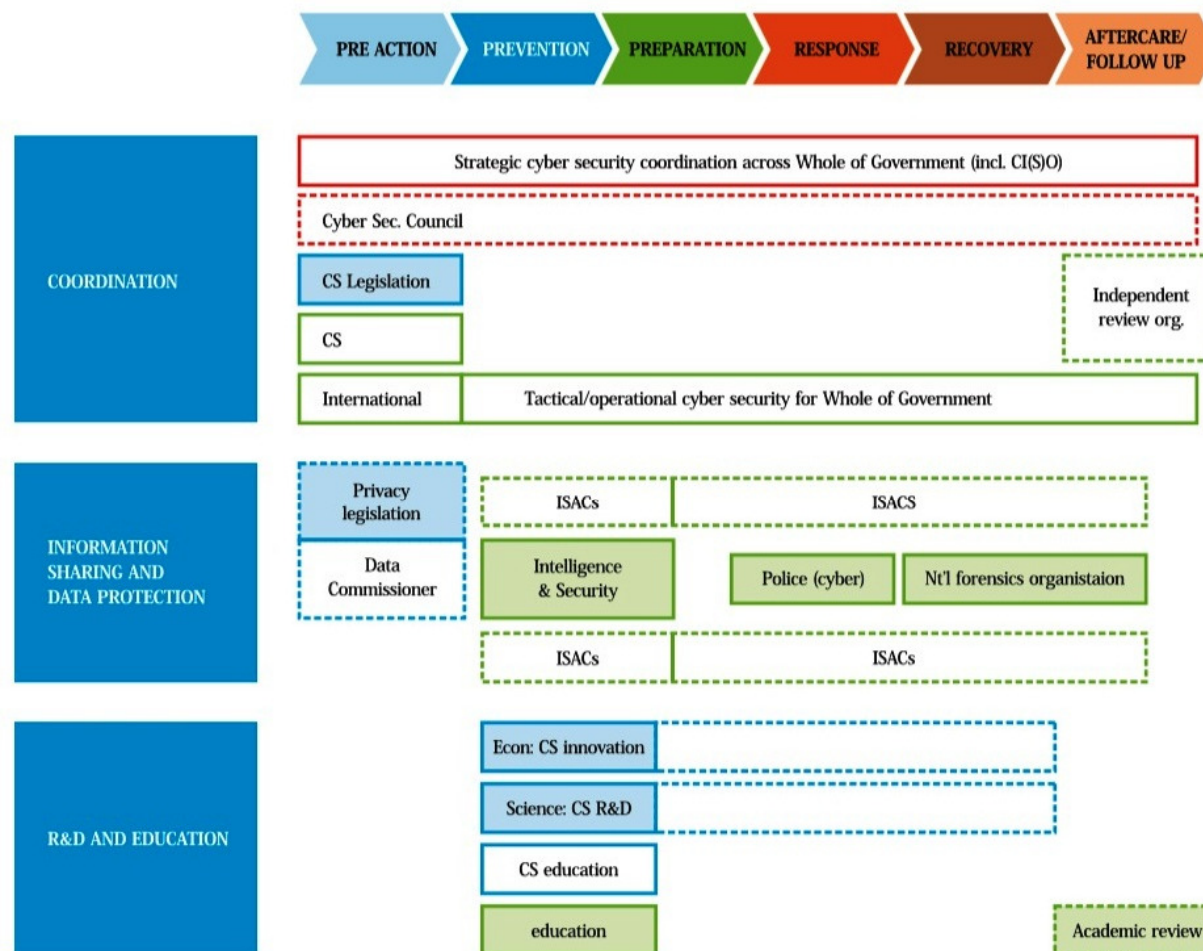
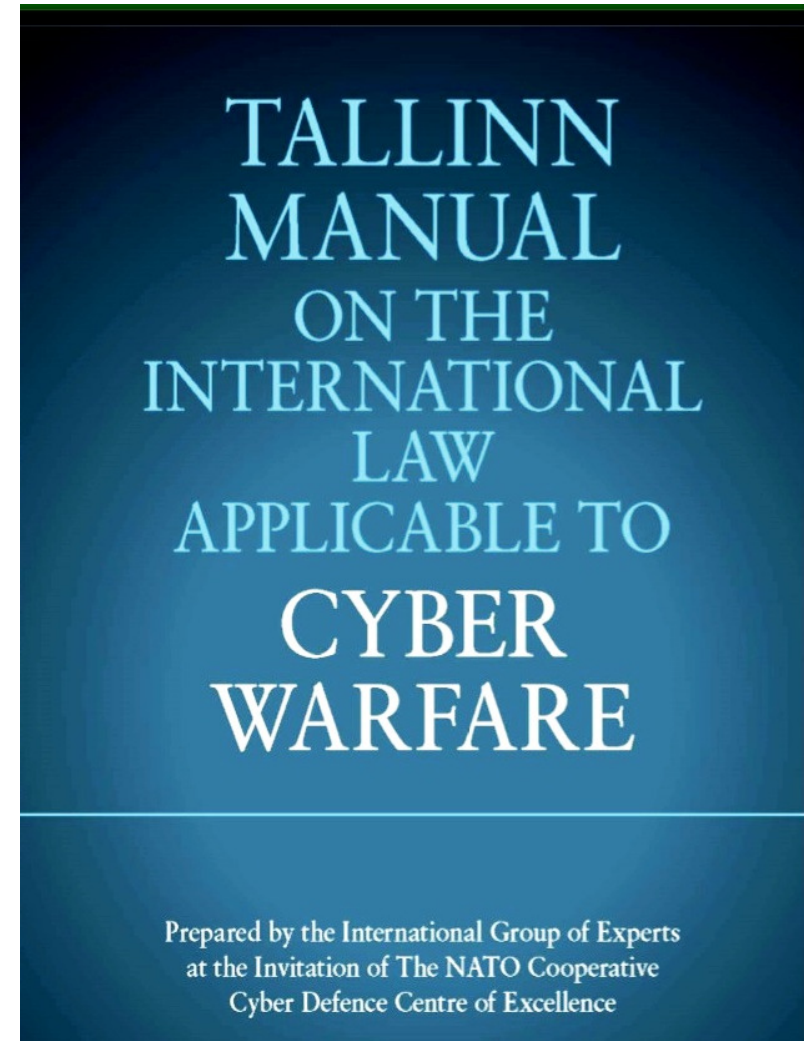
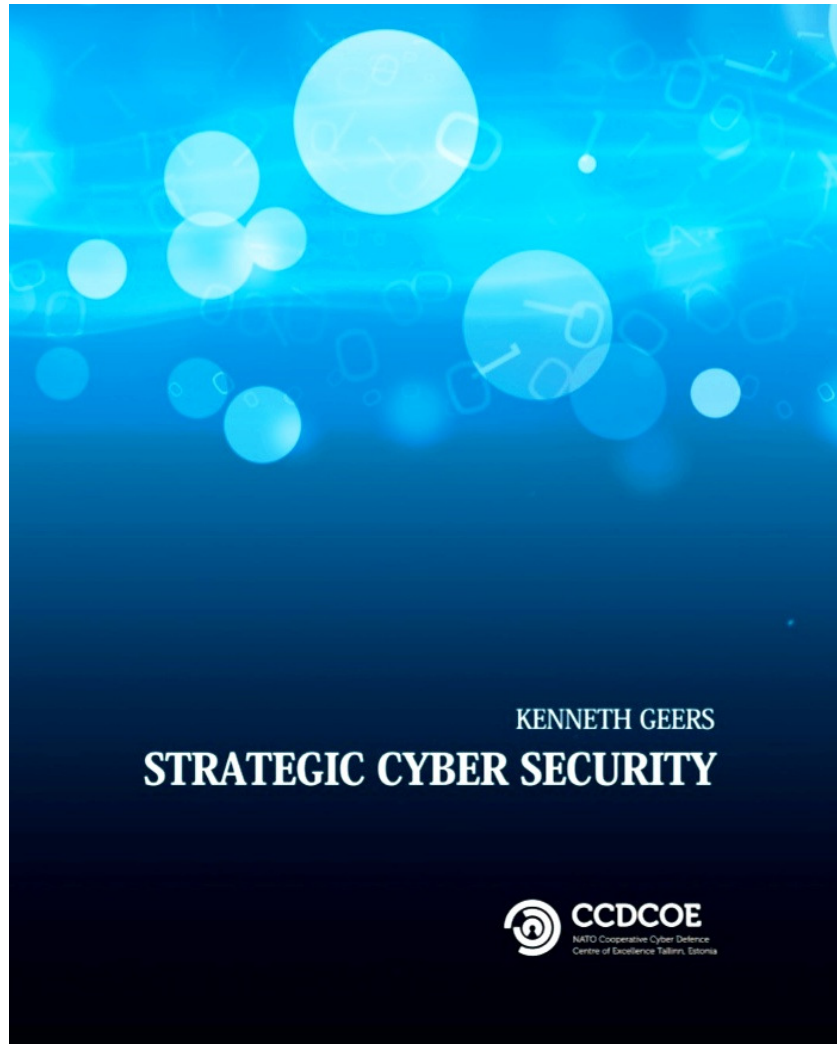


Figure 7: The Organisational Picture of the Cross-Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in existing organisation; dashed = option selected by some nations)



# **NATO** Cooperative Cyber Defence Centre of Excellence – **CCDCOE** - Estonia



Recommended Cyber Reference Books: from **NATO** - [ccdcoe.org/tallinn-manual.html](http://ccdcoe.org/tallinn-manual.html)

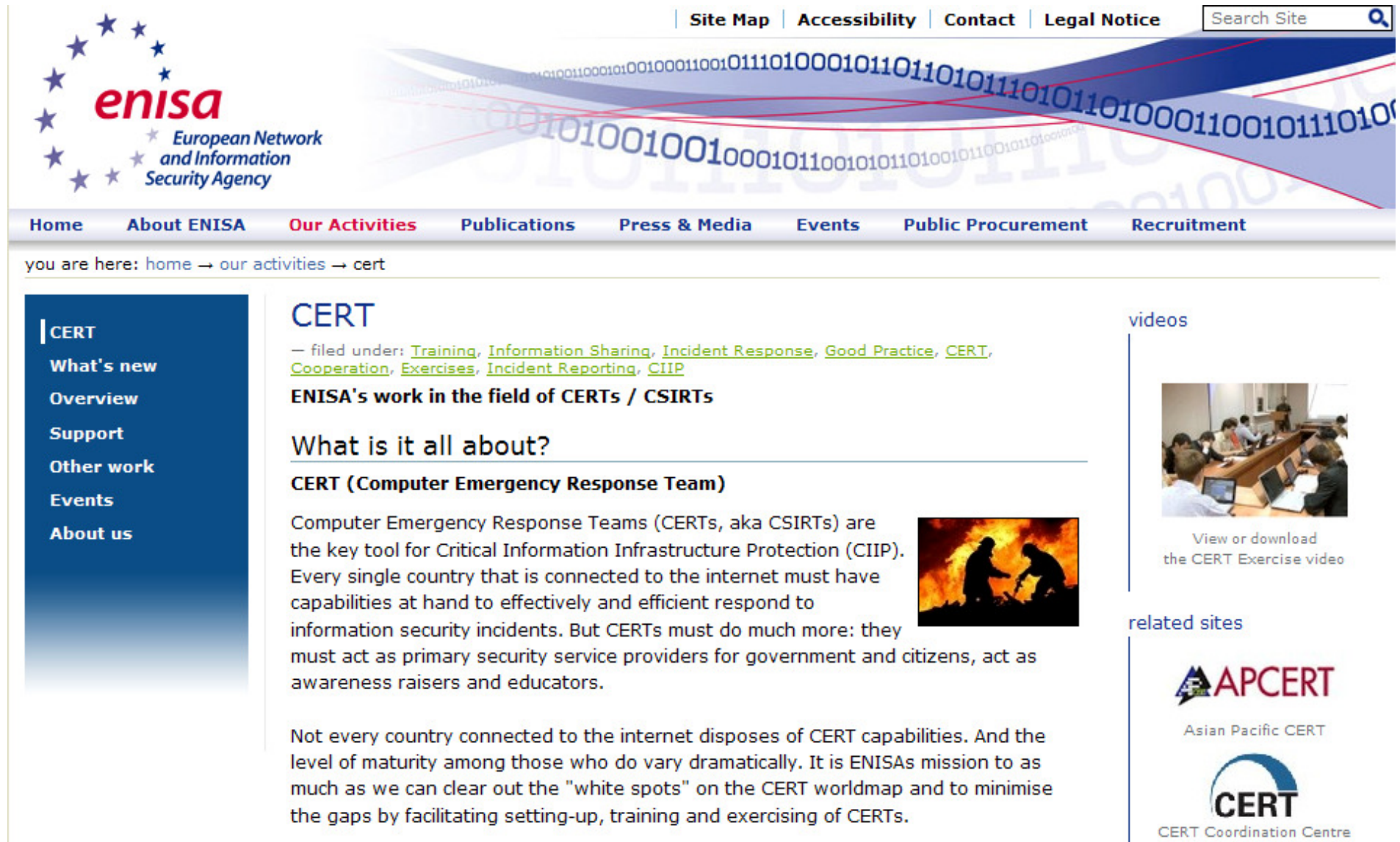
# International Cybersecurity Standards: *Players*

- *Multiple Players*: There are multiple international and national organisations that define and publish standards relating to physical and cyber security. In general these standards, recommendations and guidelines are complementary
- *UN/ITU*: We shall be focusing in this session of the technical security standards & recommendations published by the ITU as their X-Series as well as H-Series
- *Partnerships*: The ITU works closely in partnership with many other organisations, particularly for emerging Telecommunications. Multimedia, Mobile & IP Networking:
  - *ENISA* – European Network and Information Security Agency
  - *ISO* – International Standards Organisation
  - *IETF* – Internet Engineering Task Force
  - *ETSI* – European Telecommunications Standards Institute
  - *IEEE* – Institute of Electrical and Electronic Engineers
  - *ATIS* – Alliance for Telecommunications Industry Solutions
  - *3GPP* – 3<sup>rd</sup> Generation Partnership Project
  - *ANSI* – American National Standards Institute
  - *NIST* – National Institute of Standards and Technology
  - *ISF* – Information Security Forum





# European Network and Information Security Agency: *enisa*



The screenshot shows the ENISA website with a navigation bar at the top containing links for Site Map, Accessibility, Contact, Legal Notice, and a search box. The ENISA logo is on the left. Below the navigation bar is a secondary menu with links for Home, About ENISA, Our Activities, Publications, Press & Media, Events, Public Procurement, and Recruitment. A breadcrumb trail indicates the current location: home → our activities → cert.

**CERT**


— filed under: [Training](#), [Information Sharing](#), [Incident Response](#), [Good Practice](#), [CERT](#), [Cooperation](#), [Exercises](#), [Incident Reporting](#), [CIIP](#)

**ENISA's work in the field of CERTs / CSIRTs**

**What is it all about?**


**CERT (Computer Emergency Response Team)**

Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the internet must have capabilities at hand to effectively and efficiently respond to information security incidents. But CERTs must do much more: they must act as primary security service providers for government and citizens, act as awareness raisers and educators.




Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is ENISA's mission to as much as we can clear out the "white spots" on the CERT worldmap and to minimise the gaps by facilitating setting-up, training and exercising of CERTs.

**videos**




View or download the CERT Exercise video

**related sites**



Asian Pacific CERT



CERT Coordination Centre

# ISO/IEC 27000/2- *Info Security Management*

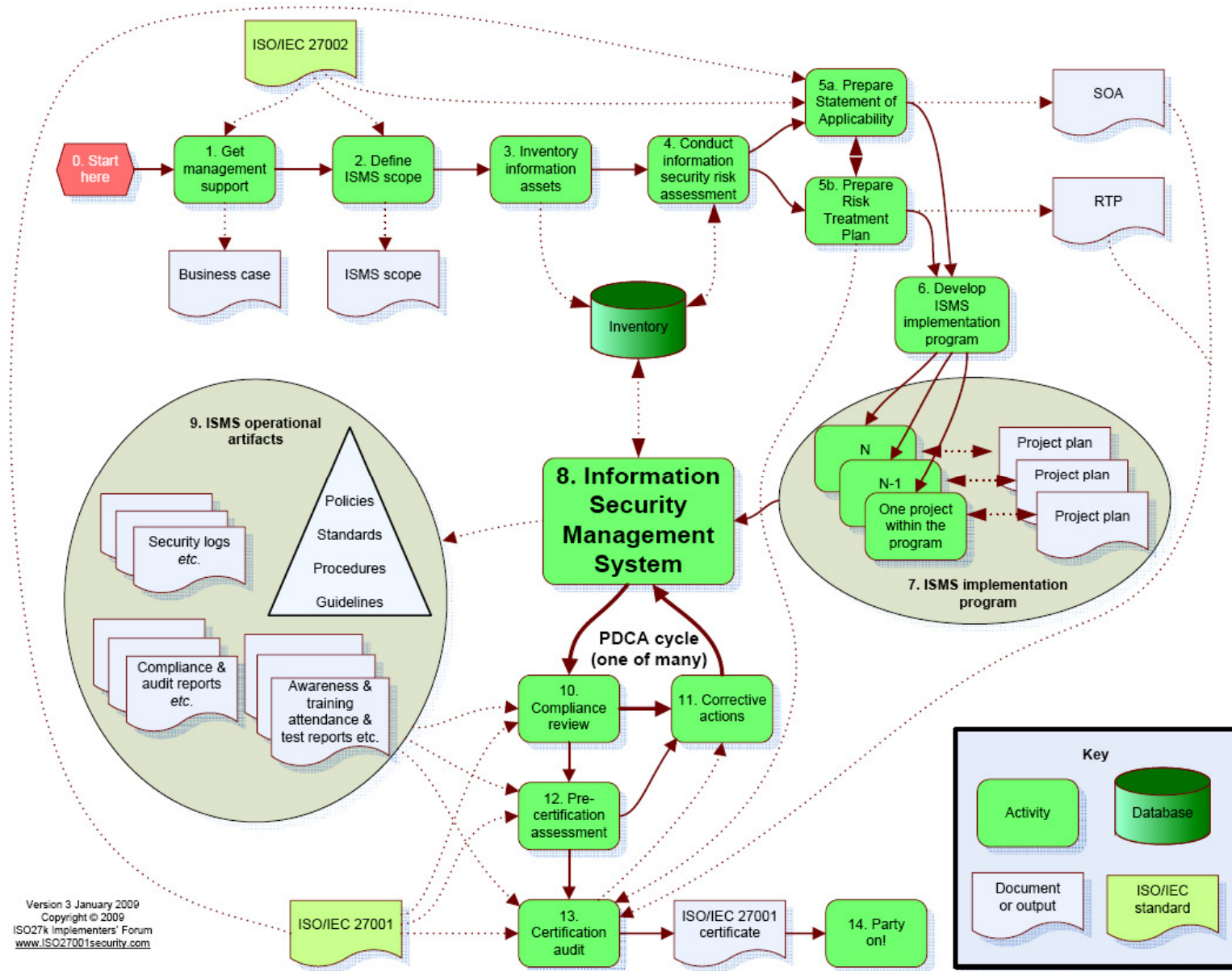
The ISO/IEC 27000-series numbering ("ISO27k") has been reserved for a family of information security management standards derived from British Standard [BS 7799](#). The following standards are either published (shown in red) or works in progress:

- [ISO/IEC 27000:2009](#) - provides an **overview/introduction** to the ISO27k standards as a whole plus the specialist **vocabulary** used in ISO27k.
- [ISO/IEC 27001:2005](#) is the **Information Security Management System (ISMS) requirements standard**, a specification for an ISMS against which thousands of organizations have been certified compliant.
- [ISO/IEC 27002:2005](#) is the **code of practice for information security management** describing a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.
- [ISO/IEC 27003](#) provides **implementation guidance** for ISO/IEC 27001.
- [ISO/IEC 27004](#) is an **information security management measurement** standard suggesting metrics to help improve the effectiveness of an ISMS.
- [ISO/IEC 27005:2008](#) is an **information security risk management** standard.
- [ISO/IEC 27006:2007](#) is a guide to the **certification or registration process** for accredited ISMS certification or registration bodies.
- [ISO/IEC 27007](#) will be a guideline for **auditing Information Security Management Systems**.
- [ISO/IEC 27008](#) will provide **guidance on auditing information security controls**.
- [ISO/IEC 27010](#) will provide guidance on **information security management for sector-to-sector communications**.
- [ISO/IEC 27011:2008](#) is the **information security management guideline for telecommunications organizations** (also known as ITU X.1051).

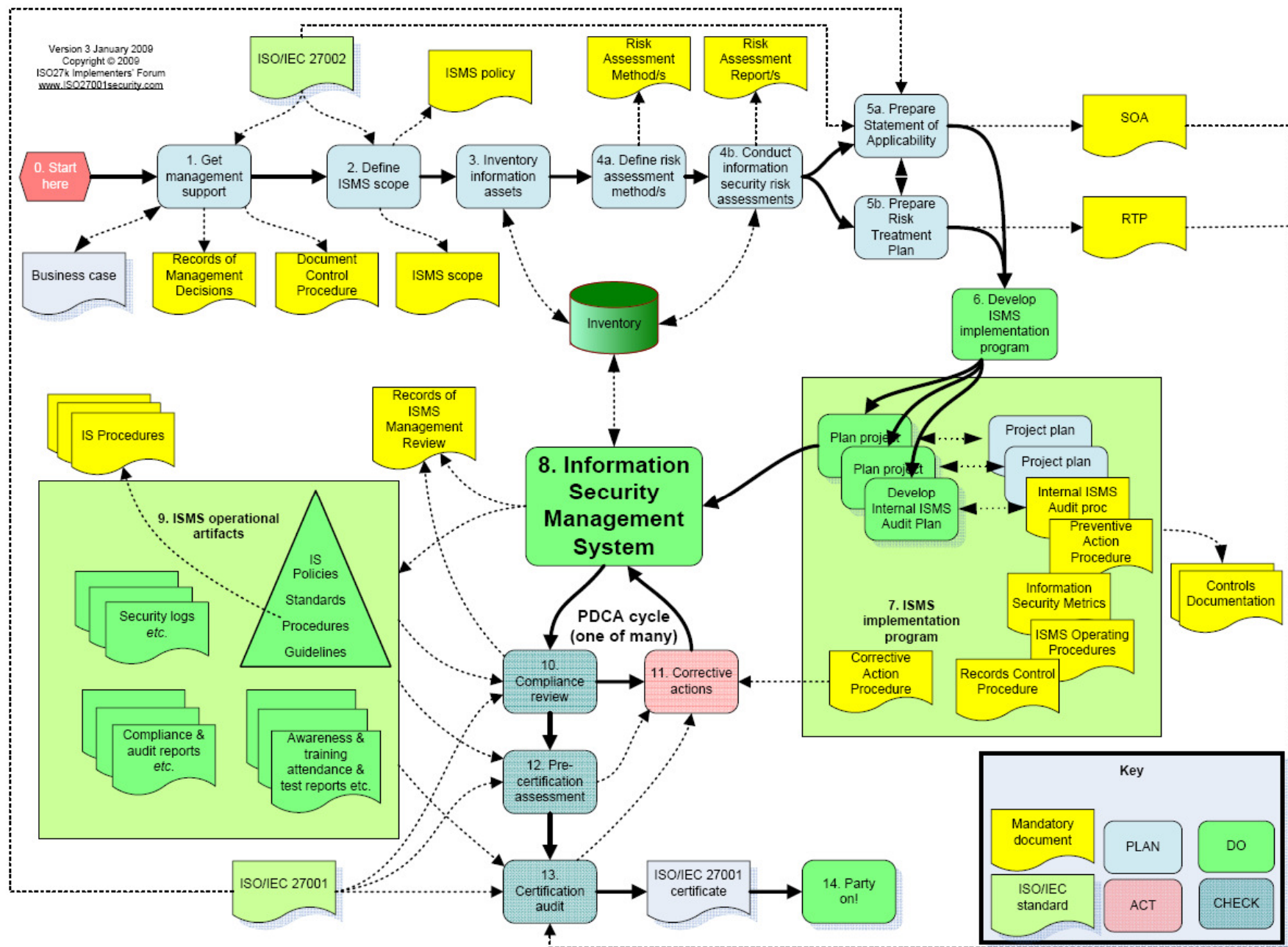




# Information Security Management System: *Implementation Process: ISO27001/2*



# Flow-Chart: Route to *ISO27001/2* Certification





# NIST Security Publications: “800 Series”

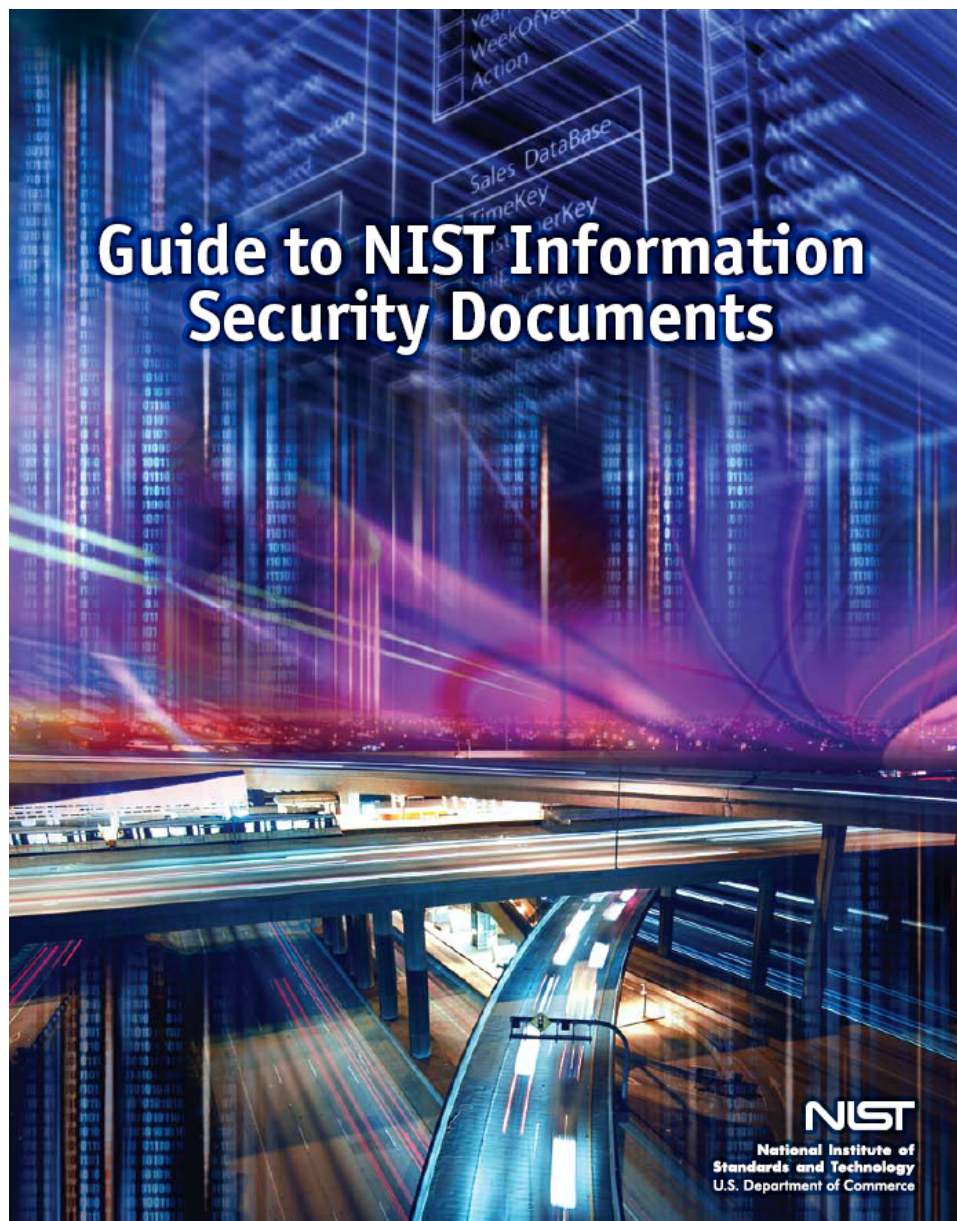


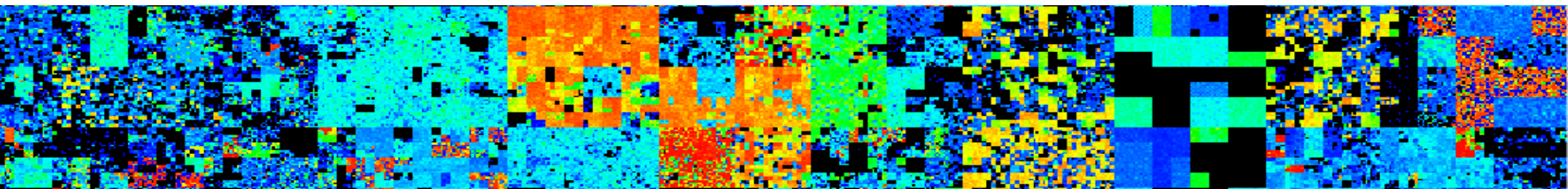
TABLE OF CONTENTS	
Introduction .....	1
<b>Topic Clusters .....</b>	<b>2</b>
Annual Reports .....	2
Audit & Accountability .....	2
Authentication .....	3
Awareness & Training .....	4
Biometrics .....	4
Certification & Accreditation (C&A) .....	5
Communications & Wireless .....	6
Contingency Planning .....	7
Cryptography .....	7
Digital Signatures .....	8
Forensics .....	9
General IT Security .....	9
Incident Response .....	10
Maintenance .....	11
Personal Identity Verification (PIV) .....	12
PKI .....	13
Planning .....	13
Research .....	16
Risk Assessment .....	16
Services & Acquisitions .....	17
Smart Cards .....	19
Viruses & Malware .....	19
Historical Archives .....	19
<b>Families .....</b>	<b>22</b>
Access Control .....	22
Awareness & Training .....	23
Audit & Accountability .....	23
Certification, Accreditation, & Security Assessments .....	23
Configuration Management .....	24
Contingency Planning .....	25
Identification and Authentication .....	26
Incident Response .....	27
Maintenance .....	27
Media Protection .....	27
Physical & Environmental Protection .....	28
Planning .....	28
Personnel Security .....	28
Risk Assessment .....	29
System & Services Acquisition .....	33
System & Communication Protection .....	30
System & Information Integrity .....	32
<b>Legal Requirements .....</b>	<b>35</b>
Federal Information Security Management Act of 2002 (FISMA) .....	35
OMB Circular A-130: Management of Federal Information Resources; Appendix III: Security of Federal Automated Information Resources .....	36
E-Government Act of 2002 .....	36
Homeland Security Presidential Directive-12 (HSPD-12), Common Identification Standard for Federal Employees and Contractors .....	36
OMB Circular A-11: Preparation, Submission, and Execution of the Budget .....	37
Health Insurance Portability and Accountability Act (HIPAA) .....	38
Homeland Security Presidential Directive-7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection .....	



# - CyberTerrorism (2) – “Security in Cyberspace”



1 – <i>Supersonic</i> “Real-Time” Cybersecurity	2 – Cybersecurity Models & Architectures	3 – <i>Cyber Emergency Response Team: CERT</i>
4 – Cybersecurity for Government & Defence	5 – Cybersecurity for Banking & Finance	6 – Securing Critical National Infrastructure
7 – Cyber Action Plans & <i>Tactical</i> Road Maps	8 – <i>OUR</i> Cyber Future : “ <i>Neural Society</i> ”	9 – Developing <i>YOUR</i> Cybersecurity Plans!





# Cyber Analyst Teams: CERT/CSIRT

- **CERT** = Computer Emergency Response Team
- **CSIRT** = Computer Security Incident Response Team
- **CERT & CSIRT** refer to the professionally trained teams that manage real-time alerts & response
- ALL Businesses and Critical National Sectors (Energy, Banking, Transport, Defence.....) need to have access to a CERT/CSIRT Team to protect information assets!

*.....Now we briefly discuss the Role & Scope of CERTs*



# Professional *CERT/CSIRT* Organisations

- *Benefits:* Every national government, and major multi-site enterprise should consider the economic benefits of establishing a CERT/CSIRT.
- *Origins:* The original CERTs were established in the early 1990s following the arrival of the first computer viruses, worms & trojans.
- *CERT.org:* Carnegie Mellon University formed the 1<sup>st</sup> National CERT under contract from the US Government, and now runs [www.CERT.org](http://www.CERT.org) as a global partnership of national and regional CERTs.
- *ENISA:* Within European, the TERENA organisation (Trans-European Education and Research Networks Association) works with ENISA to manage the network of European CERTs, including skills training.



# *CERT/CSIRT* Operations Alert Centre

- *Alerts:* A Fundamental Process within any CERT is the management and classification of “incidents”, and their routing to provide a response
- *Triage:* Some “incidents” may actually be due to some unusual statistical traffic patterns rather than an actual alert, “hack” or cybercrime
- *Risk:* Once an incident is classified the CERT will need to assign staff responsibility to assess the event risk and potential impact & damage
- *Communicate:* The CERT will communicate their analysis with relevant stakeholders, that may include government agencies, business stakeholders, and those responsible for critical information infrastructure
- *Neutralise:* CERT will work with partners to minimise the disruptive risk & damage in order to neutralise the cyber attack and any future threat



# Computer Emergency Response Team (**CERT**)

## Reactive Services



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

## Proactive Services



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

## Security Quality Management Services

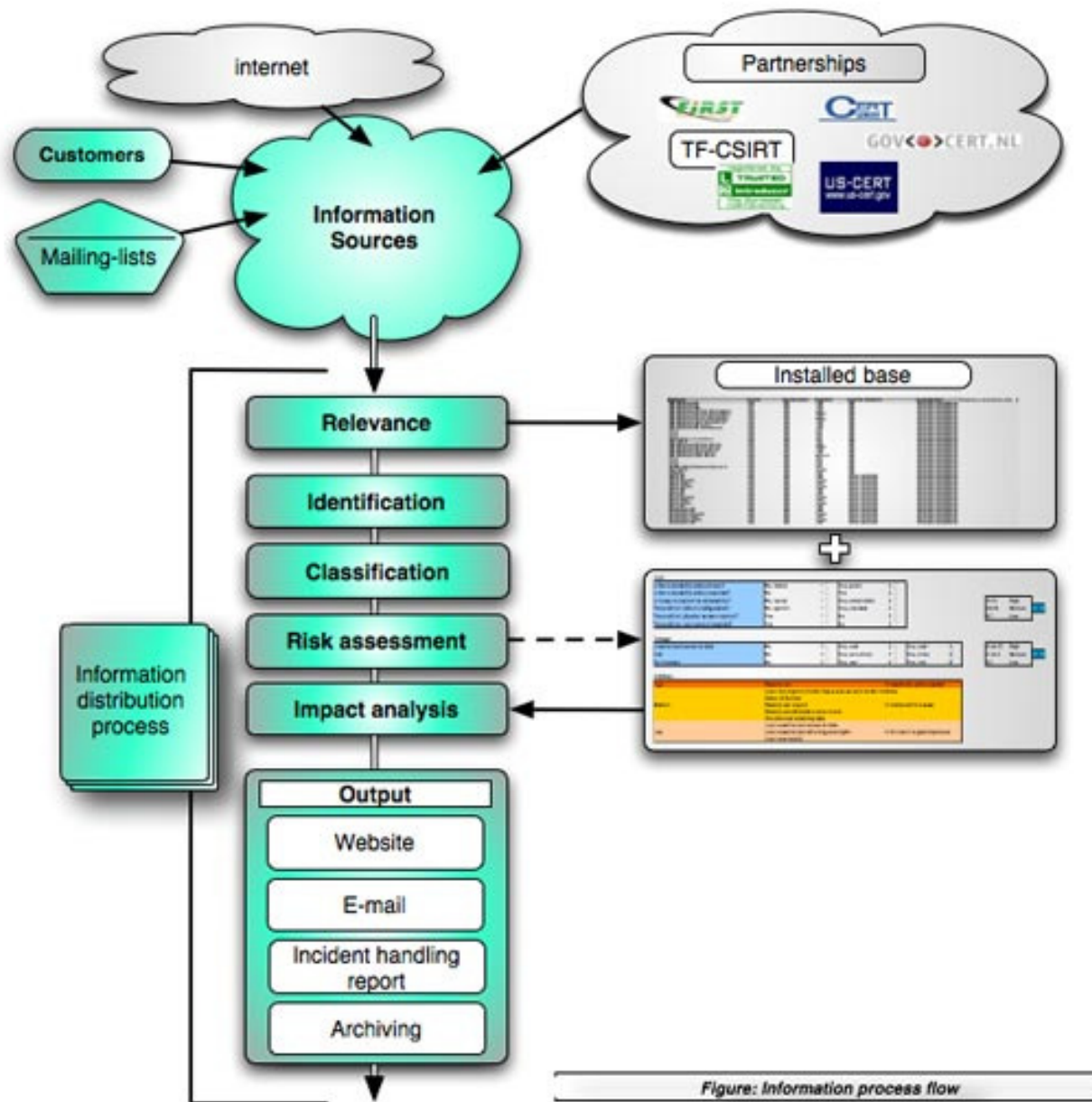


- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

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



# *CERT/CSIRT* – Information Process Flow



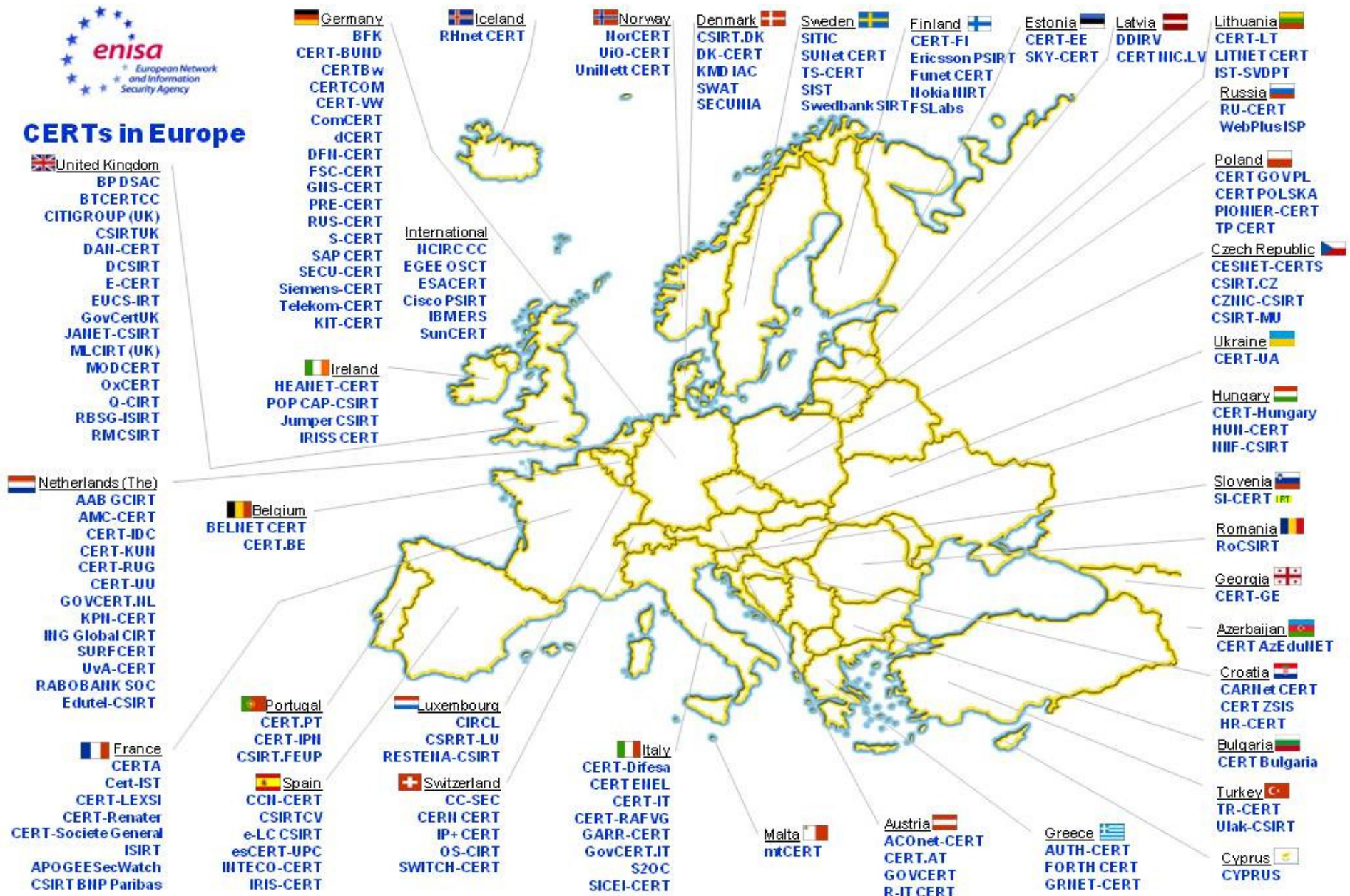
# *CERT/CSIRT* Roll-Out Action Plan

- Governments & Business may upgrade their CERT/CSIRT capability using the on-line guidebooks from Carnegie Mellon University (CMU) & the European EU/ENISA
- These step-by-step guides cover all aspects of the start-up action plan including:
  - *Business Case*: Development of the CERT/CSIRT Business Case
  - *Stakeholders*: Recruiting and Partnering with National Stakeholders
  - *Staff Training*: Recruitment and training of professional CERT staff
  - *Operations*: Establishing the Operational and Technical Procedures
  - *Incident Response*: Documented Process for classifying & responding to alerts
- Establishing a fully functional national CERT/CSIRT will probably take between 12 to 18 months depending on the scope of initial operations
- CERTs will need to continuously evolve, adapt and be trained to respond to new cyberthreats and potential attacks, and will to undergo annual compliance audits





# ENISA: European *CERT* Network



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

# ENISA: *CSIRT/CERT* Guidebook



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

Including examples and a checklist  
in form of a project plan

Deliverable WP2006/5.1(CERT-D1/D2)

### Index

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

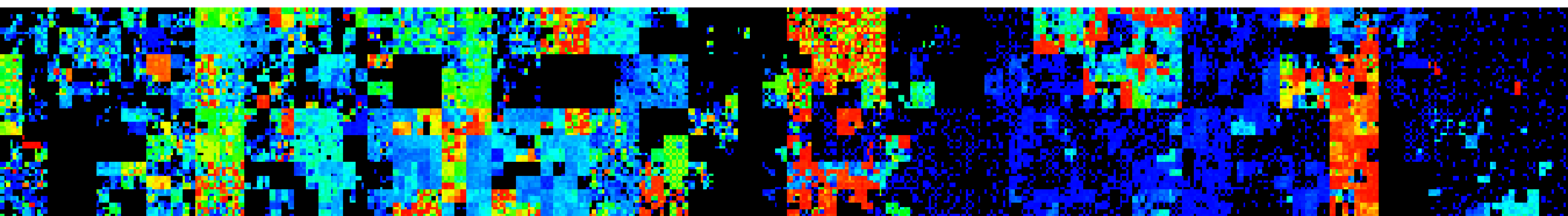




# - CyberTerrorism (2) – “Security in Cyberspace”



1 – <i>Supersonic</i> “Real-Time” Cybersecurity	2 – Cybersecurity Models & Architectures	3 –Cyber <i>Emergency</i> Response Team: <i>CERT</i>
4 –Cybersecurity for Government & Defence	5 – Cybersecurity for Banking & Finance	6 – Securing Critical National Infrastructure
7 –Cyber Action Plans & <i>Tactical</i> Road Maps	8 – <i>OUR</i> Cyber Future : “ <i>Neural Society</i> ”	9 – Developing <i>YOUR</i> Cybersecurity Plans!



# Government Cybersecurity Agencies: Common Roles

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

***...Next we review some examples of Governments that have implemented Cybersecurity during the last 5 to 7 years!...***



# UK Office of Cybersecurity – OCS & CSOC



## Cyber Security Strategy of the United Kingdom

safety, security and resilience in cyber space



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

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

# US Government : *Office of Cybersecurity* (CS&C)



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

## – *National Cyberspace Response System*

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

## – *Federal Network Security*

- Ensuring maximum security of executive civilian offices & agencies
- National *CDM* Cyber Program – Continuous Diagnostics & Mitigation

## – *Cyber-Risk Management Programmes*

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



*....The US Government DHS also has a National Cyber Security Center (NCSC) with the mission to protect the US Government's Communications Networks*

# KISA : Korea Internet & Security Agency

- **KISA(Korea Internet & Security Agency)** was established as the public corporation responsible for managing the Internet of Korea on July 23th, 2009, by merging three institutes NIDA, KISA, and KIICA.
  - NIDA(National Internet Development Agency of Korea)
  - KISA(Korean Information Security Agency)
  - KIICA(Korea IT International Cooperation Agency)
- **KISA** has the following roles:
  - Protects Internet infrastructure from hacking cyber-terror, spam and other malicious activities
  - Operates krCERT CC (Korea Computer Emergency Response Team Coordination Center) to improve Internet security in Korea
  - Supporting international organizations such as ITU and OECD and assisting Korean IT companies
  - Specifically, KISA manages the Internet address resources such as IP address and .kr domain name as the national NIC (Network Information Center), and also researches for the next generation Internet address resources of Korea.





# Malaysian Government: *MOSTi*

The screenshot shows the CyberSecurity Malaysia website, an agency under MOSTi. The header includes the CyberSecurity Malaysia logo, the MOSTi logo (Ministry of Science, Technology and Innovation), and a search bar. The date 15 August 2010 13:58:32 is displayed. The navigation menu includes links for HOME, ABOUT US, OUR SERVICES, EVENTS, KNOWLEDGE BANK, COMMUNITY, MEDIA CENTRE, and CONTACT US.

The main content area features a large graphic on the left with the text "Securing Our Cyberspace" and a grid of orange blocks. Below this is the Malaysian coat of arms and the MOSTi logo. The right side of the main content area is titled "Welcome To CyberSecurity Malaysia" and contains several service tiles:

- Upcoming Event:** csm-ace 2010 (Cyber Security Malaysia Awareness Conference & Exhibition)
- Financial Assistance:** Click here to Apply (mycc logo)
- Training:** TRAINING PROGRAMS (silhouettes of people)
- Cyber999:** Cyber999 is a service offered by CyberSecurity Malaysia to handle incidents faced by computer/Internet user.
- Registration:** Malaysia Information Security Professional (Register now! button)
- Online Survey:** National Strategy for Cyber Security Acculturation and Capacity Building Program
- Media:** CyberSecurity Malaysia Corporate Video (Click here to view our introduction video (30 seconds))
- Media:** Cyber Security Song (click here to listen)
- CyberSAFE Ambassador:** Join Us CyberSAFE Ambassador Program

At the bottom, there is a "News Coverage" section with a microphone icon and a list of news items:

- 06/08/2010: Critical Agencies Told To Get ISMS Certification To Face Cyber Threat
- 06/08/2010: X-MAYA 3: BENCHMARKING THE NATIONAL CYBER CRISIS MANAGEMENT PLAN
- 06/08/2010: Protecting Agencies From Cyber Attacks

A "MORE ..." link is available at the bottom right of the news section. Social media icons for Facebook and Twitter are located at the bottom left.

# Cybersecurity Mitigation Strategies

## - Australian Govt: Department of Defence -





# National Cybersecurity for Latin America & Caribbean:


## - CITELE/CICTE/OAS -

- Within Latin America & Caribbean, CITELE, CICTE and the OAS are working together on Regional Cybersecurity Strategy, Plans & Programmes with UN/ITU support:

- **CITELE** = Inter-American Telecommunications Commission
- **CICTE** = Inter-American Committee against Terrorism
- **OAS** = Organisation of American States



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

 [Antigua and Barbuda](#)

 [Costa Rica](#)

 [Haiti](#)

 [Saint Lucia](#)

 [Argentina](#)

 [Cuba](#)<sup>1</sup>

 [Honduras](#)<sup>2</sup>

 [Saint Vincent and the Grenadines](#)

 [Barbados](#)

 [Dominica](#)  
(Commonwealth of)

 [Jamaica](#)

 [Suriname](#)

 [Belize](#)

 [Dominican Republic](#)

 [Mexico](#)


 [The Bahamas](#)  
(Commonwealth of)


 [Bolivia](#)

 [Ecuador](#)

 [Nicaragua](#)

 [Trinidad and Tobago](#)

 [Brazil](#)

 [El Salvador](#)

 [Panama](#)

 [United States of America](#)

 [Canada](#)

 [Grenada](#)

 [Paraguay](#)

 [Uruguay](#)

 [Chile](#)

 [Guatemala](#)

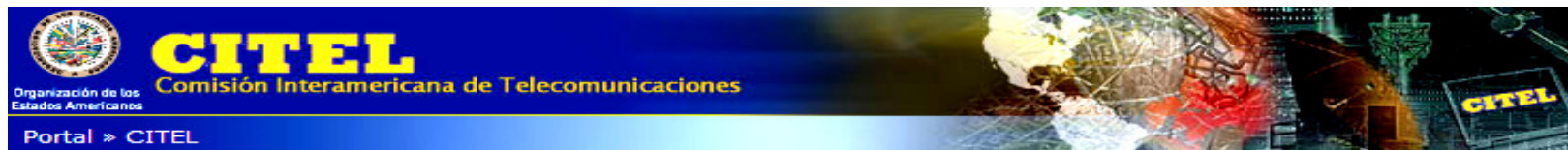
 [Peru](#)

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

 [Colombia](#)

 [Guyana](#)

 [Saint Kitts and Nevis](#)





# ITU: Cybersecurity Training – UTECH, Kingston, JAMAICA

## *Government, Central Bank, Energy & Telecoms Sectors*





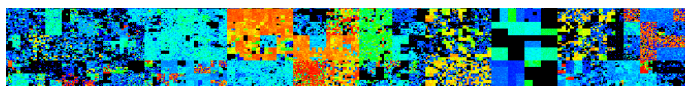
# Case Study: White Paper: 21<sup>st</sup> C Georgia – “Cyber-Vardzia”

\* Cyber-Vardzia: Integrated Cyber & Physical Security Systems for 21<sup>st</sup>C Georgia \*

...“21stC Georgia”...



...“Cyber-Vardzia”...



“Integrated Cyber & Physical Security”

\*\*\* for \*\*\*

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

Author: Dr David E Probert – VAZA International

\* Cyber-Vardzia: Integrated Cyber & Physical Security Systems for 21<sup>st</sup>C Georgia \*



\* Integrated Cyber & Physical Security Systems for 21<sup>st</sup>C Georgia \*

Author: Dr David E Probert – VAZA International

## (0) Executive Summary

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

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

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

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

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

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

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

Web Link : [www.Valentina.net/vardzia/Georgia2010.pdf](http://www.Valentina.net/vardzia/Georgia2010.pdf)



# Cybersecurity for the *Georgian Parliament*



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



# National Cybersecurity Strategy : ***“The Shopping List”***

## ***Smart Security for Business & Government is a Multi-Year Programme!***

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

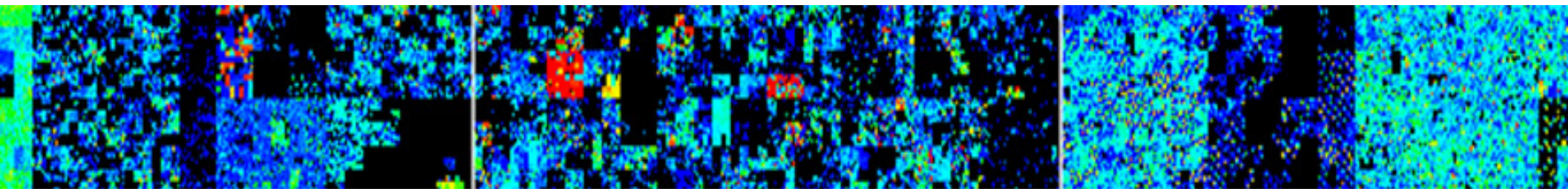
*.....It is also important to develop an in-depth economic **“Cost-Benefit”** analysis and Business Case in order to evaluate the **“Return on Investment”** for Smart Security*



# - CyberTerrorism (2) – “Security in Cyberspace”



1 – <i>Supersonic</i> “Real-Time” Cybersecurity	2 –Cybersecurity Models & Architectures	3 –Cyber <i>Emergency</i> Response Team: <i>CERT</i>
4 –Cybersecurity for Government & Defence	<b>5 – Cybersecurity for Banking &amp; Finance</b>	6 – Securing Critical National Infrastructure
7 –Cyber Action Plans & <i>Tactical</i> Road Maps	8 – <i>OUR</i> Cyber Future : “ <i>Neural Society</i> ”	9 – Developing <i>YOUR</i> Cybersecurity Plans!



# Cybersecurity for Banking & Finance

- CyberTerrorism is now accepted as a Mission Critical Threat to ALL Financial Institutions
- CyberCrime & CyberTerrorism are closely related with dual motives of *“Profit & Power”*

.....Recent massive cyber attacks indicate the urgency of securing YOUR financial info assets!





# Banking & Finance Sector: *Cybersecurity Threats*

- *Banks & Financial Institutions* are prime targets for Cybercriminals & Cyberterrorists since they are at the heart of ALL National Economies!
- *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



# Cybercriminals Target *Major UK Bank*

## Cybercriminals Target Online Banking Customers

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

---

### BACKGROUND

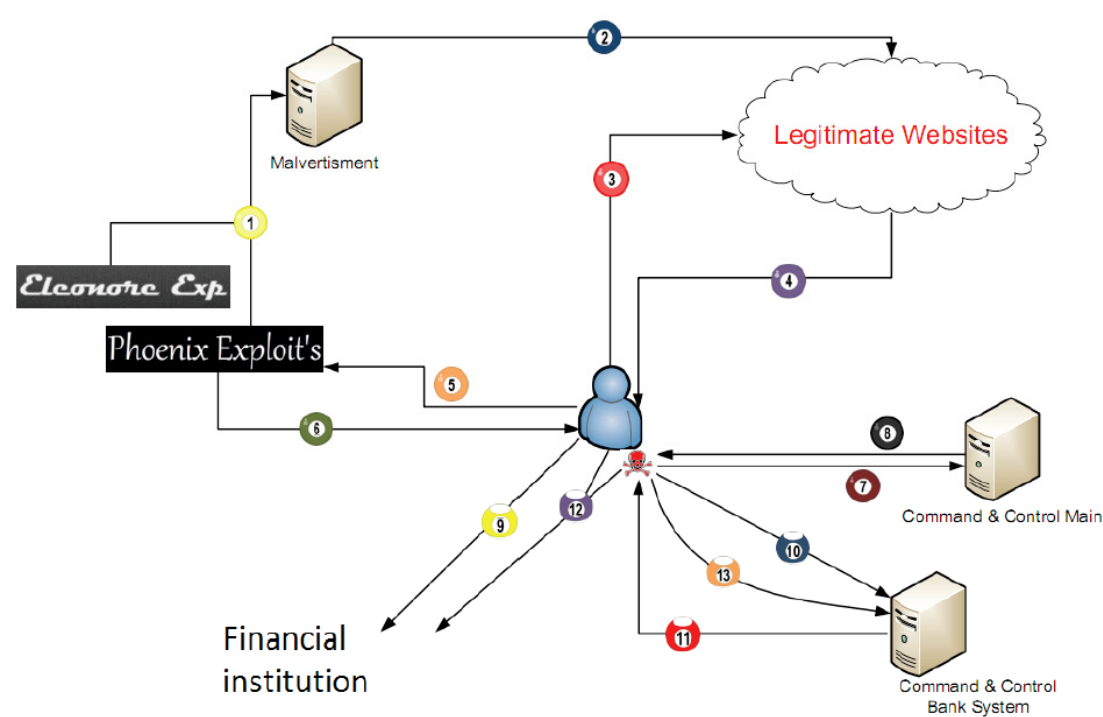
In July 2010, an organized network of cybercriminals launched a complex, multi-level scheme that targeted online customers of a large UK financial institution. Based on information M86 Security Labs found on the malicious Command & Control (C&C) server, we assume that close to £675,000 was stolen from 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

**M86**  
SECURITY

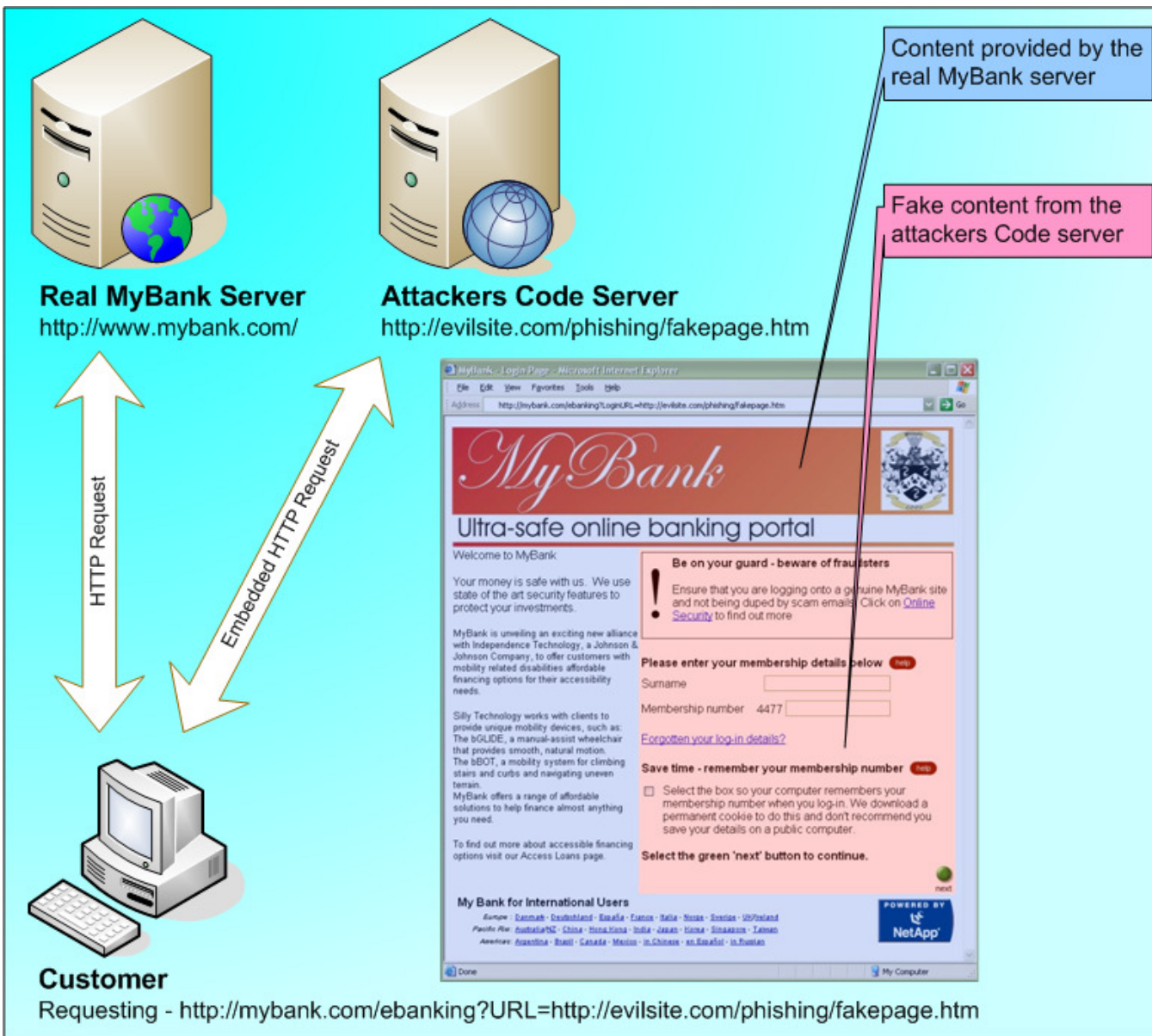
Such Cyber Attacks, with variations, take place regularly in *Banking & Financial Services*. During *Summer 2014* more than *83 Million Accounts* were "hacked" @ *JP Morgan Chase* -

- It is estimated that more than *\$450 Billion/Year* is lost through CyberCrime -



# Financial Services Server - Cyber Attack:

## *Impact of XSS Cross-Site Scripting*



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

Home | World | UK | England | N. Ireland | Scotland | Wales | **Business** | Politics | Health | Education | Sci/Env  
Market Data | Your Money | Economy | Companies

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.

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.



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

“

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



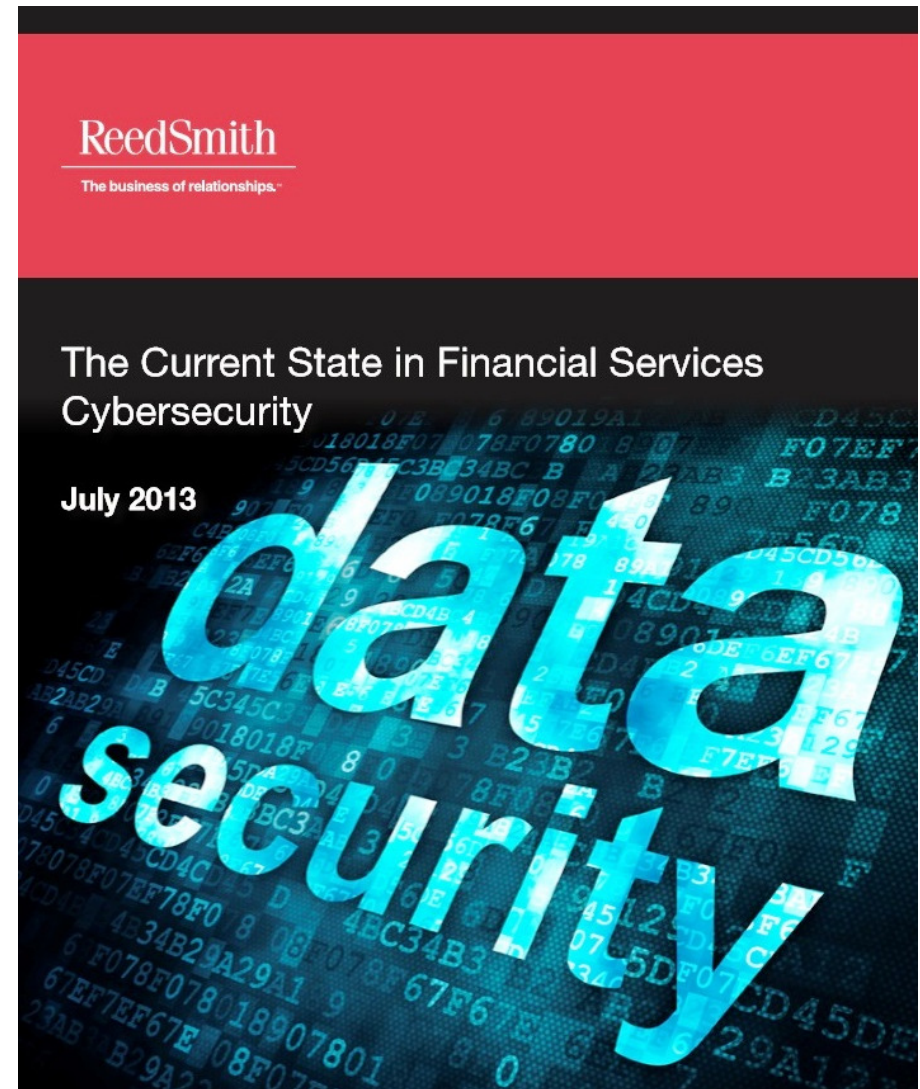
# Cybersecurity for *Banking & Finance*



**New York State**

**Department of Financial Services**

*Report on Cyber Security in the Banking Sector*



**31<sup>st</sup> International East/West Security Conference**

**"Cyber-terrorism(2): Security in Cyberspace"**

Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# 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
<b>Location</b>	Select a hazard-free location for the Data Centre with reliable power supply, diverse communications, and available utilities, infrastructure and transport.	<ul style="list-style-type: none"> <li>• Site subject to restrictive covenants and planning limitations</li> <li>• Flooding</li> <li>• Flight paths and airfields</li> <li>• Proximity to Critical National Infrastructure sites</li> <li>• Pollution and contamination</li> <li>• Extreme weather</li> </ul>	<ul style="list-style-type: none"> <li>• Create a 'buffer zone' around the site</li> <li>• Ensure diversity of supply for power, utilities, transport</li> <li>• Survey site and surrounding area</li> </ul>
<b>Physical security of the site</b>	Develop a 'layered' security approach that minimises risk to life and damage to assets, and maintains business continuity.	<ul style="list-style-type: none"> <li>• Site presents a target for attack, theft, vandalism</li> </ul>	<ul style="list-style-type: none"> <li>• Consider appropriate use of signage</li> <li>• Perimeter fence and other barriers</li> </ul>
<b>Site intrusion prevention and detection</b>	Establish a secure site perimeter and security zones within the site.	<ul style="list-style-type: none"> <li>• Unauthorised access within the security perimeter</li> <li>• Accidental damage to assets by people, vehicles</li> </ul>	<ul style="list-style-type: none"> <li>• Landscape and plant to deter approach</li> <li>• Use security fencing and protect all entrances</li> <li>• Use CCTV, lighting, perimeter intrusion detection systems to supplement passive measures</li> <li>• Monitor or patrol the external perimeter</li> <li>• Control movement of vehicles</li> <li>• Gather intelligence about area threat</li> </ul>
<b>Communication route and diversity</b>	Establish resilient diverse communications.	<ul style="list-style-type: none"> <li>• Disruption to communications by accidental or deliberate physical damage, or supplier failure</li> </ul>	<ul style="list-style-type: none"> <li>• Use multiple communications suppliers</li> <li>• Physically separate supply routes</li> <li>• Mark and regularly inspect supply routes</li> <li>• Lock and inspect access points</li> </ul>
<b>External area</b>	Protect the external areas (within the perimeter) of the Data Centre.	<ul style="list-style-type: none"> <li>• Accidental or deliberate damage or disruption to critical services housed within the external perimeter</li> </ul>	<ul style="list-style-type: none"> <li>• Site fuel tanks away from threats</li> <li>• Keep vehicles away from critical assets</li> <li>• Shield equipment from damage/attack</li> <li>• Protect emergency cut-off switches</li> </ul>

Source: NY State Dept of Financial Services

# Typical Security Threats, Risks and Controls:

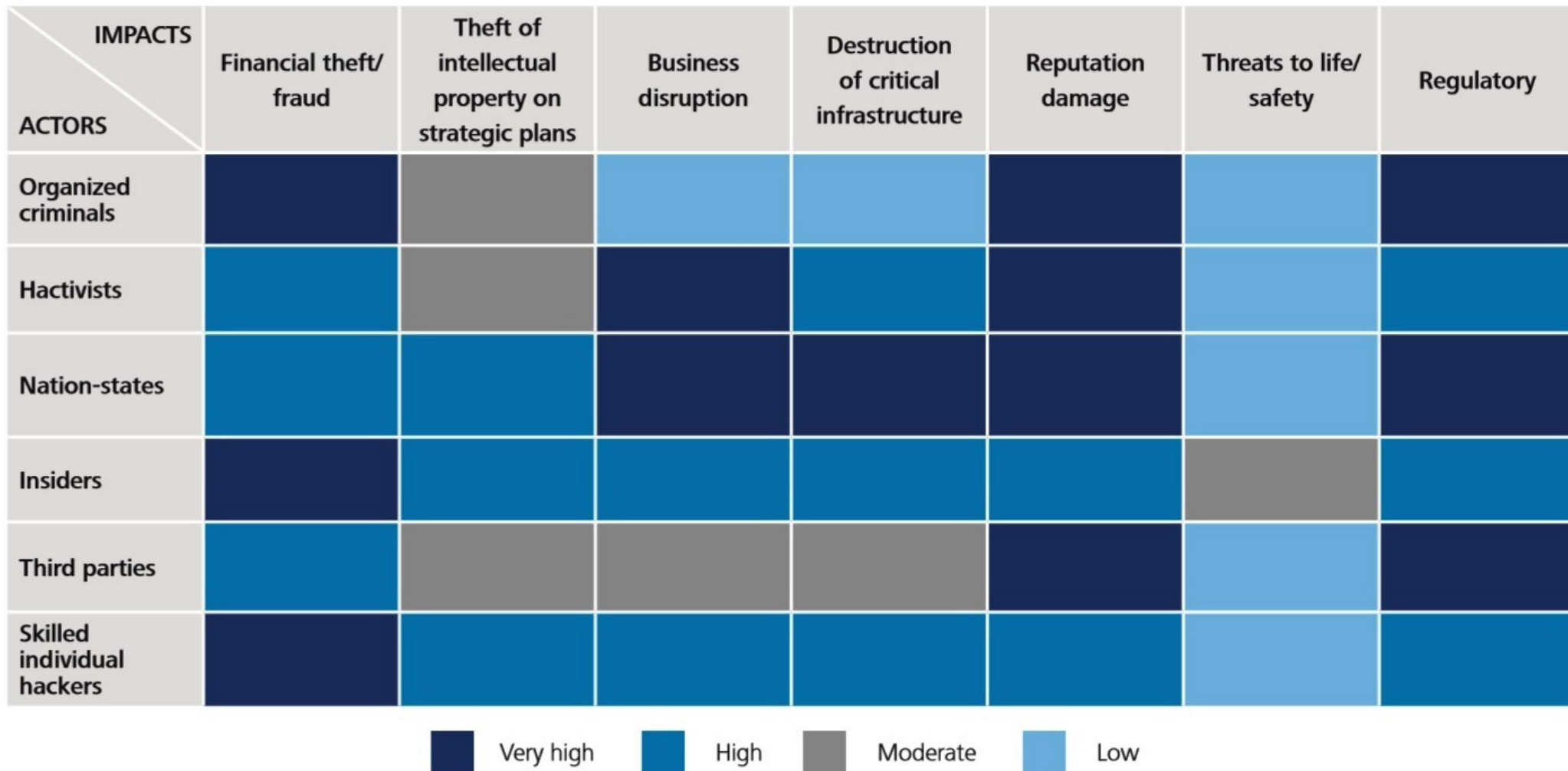
## *Financial Services Data Centre (2)*

Control area	Objectives	Threats and Vulnerabilities	Controls
Internal areas	Protect the internal areas of the Data Centre.	<ul style="list-style-type: none"> <li>Accidental or deliberate damage or disruption to facilities and equipment within the Data Centre</li> </ul>	<ul style="list-style-type: none"> <li>Construct to security standards</li> <li>Use reception area to manage access</li> <li>Keep control room away from reception</li> <li>Protect building management system, environmental controls, loading bay</li> <li>Site data hall at centre of security zones with access controls between zones</li> <li>Use internal CCTV, fire detection/protection</li> </ul>
Electrical power	Maintain continuity of power supply.	<ul style="list-style-type: none"> <li>Accidental or deliberate damage to power supply</li> <li>Loss of power from National Electrical Power Supply</li> <li>Failure of internal electrical systems</li> </ul>	<ul style="list-style-type: none"> <li>Use diverse providers and physically separate supply routes</li> <li>Test and maintain Uninterruptable Power Supplies (UPS), onsite emergency generators</li> </ul>
Data hall	Protect operation of computer assets within the data hall.	<ul style="list-style-type: none"> <li>Accidental or deliberate tampering with computer equipment</li> <li>Server, system or cabling failure</li> </ul>	<ul style="list-style-type: none"> <li>Implement and manage stringent access controls</li> <li>Monitor data hall aisles and racks with CCTV</li> <li>Protect systems against electronic threats in accordance with information security best practice</li> <li>Manage cabling infrastructure and environmental controls</li> <li>Keep data hall spotlessly clean</li> </ul>
Management responsibilities	Deter attackers, protect assets, detect incidents, react to incidents, recover to normal operations.	<ul style="list-style-type: none"> <li>Procedural errors leading to service failures</li> <li>Attackers subvert or fool staff</li> <li>Staff unable to identify or manage incidents</li> </ul>	<ul style="list-style-type: none"> <li>Prepare and maintain a security policy and make staff aware of roles and responsibilities</li> <li>Conduct background checks on staff</li> <li>Maintain an asset register</li> <li>Plan and test business continuity and recovery procedures</li> <li>Integrate security approach into broader resilience strategy</li> </ul>

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



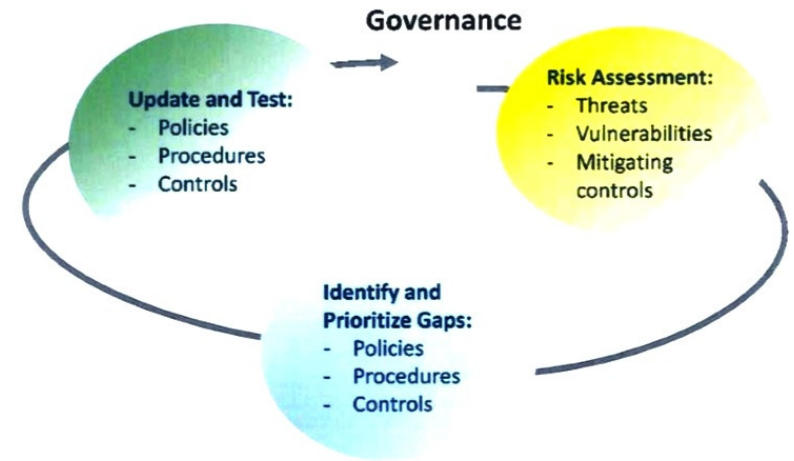
Source: Deloitte Center for Financial Services analysis



# Cybersecurity “101” for Bank Executives



A Resource Guide for **BANK EXECUTIVES**  
Executive Leadership of Cybersecurity



**01**

**IDENTIFY**  
internal and external cyber risks.



**02**

**PROTECT**  
organizational systems, assets, and data.



**03**

**DETECT**  
system intrusions, data breaches, and unauthorized access.



**04**

**Respond**  
to a potential cybersecurity event.



**05**

**RECOVER**  
from a cybersecurity event by restoring normal operations and services.

Web Link: [www.csbs.org](http://www.csbs.org)

31<sup>st</sup> International East/West Security Conference

“Cyber-terrorism(2): Security in Cyberspace”

Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# Cybersecurity Applications & Benefits for *Financial Institutions*

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

Source: **UN/ITU Cybersecurity Strategy Guide**  
**31<sup>st</sup> International East/West Security Conference**

**"Cyber-terrorism(2): Security in Cyberspace"**  
 Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015  
 © Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# 10 Steps To Cyber Security



Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

**Network Security**  
Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

**Malware Protection**  
Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

**Monitoring**  
Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

**Maintain the Board's engagement with the cyber risk.**

**Incident Management**  
Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

**Establish an effective governance structure and determine your risk appetite.**

**Information Risk Management Regime**

**Produce supporting information risk management policies.**

**User Education and Awareness**  
Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

**Home and Mobile Working**  
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

**Secure Configuration**  
Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

**Removable Media Controls**  
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

**Managing User Privileges**  
Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.



**Incident Management**  
Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Link: [www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility](http://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility)

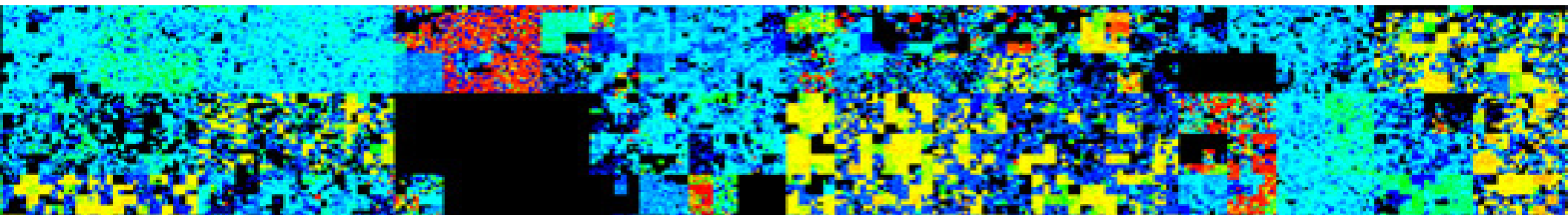




# - CyberTerrorism (2) – “Security in Cyberspace”



1 – <i>Supersonic</i> “Real-Time” Cybersecurity	2 –Cybersecurity Models & Architectures	3 –Cyber <i>Emergency</i> Response Team: <i>CERT</i>
4 –Cybersecurity for Government & Defence	5 – Cybersecurity for Banking & Finance	<b>6 – Securing Critical National Infrastructure</b>
7 –Cyber Action Plans & <i>Tactical</i> Road Maps	8 – <i>OUR</i> Cyber Future : “ <i>Neural Society</i> ”	9 – Developing <i>YOUR</i> Cybersecurity Plans!

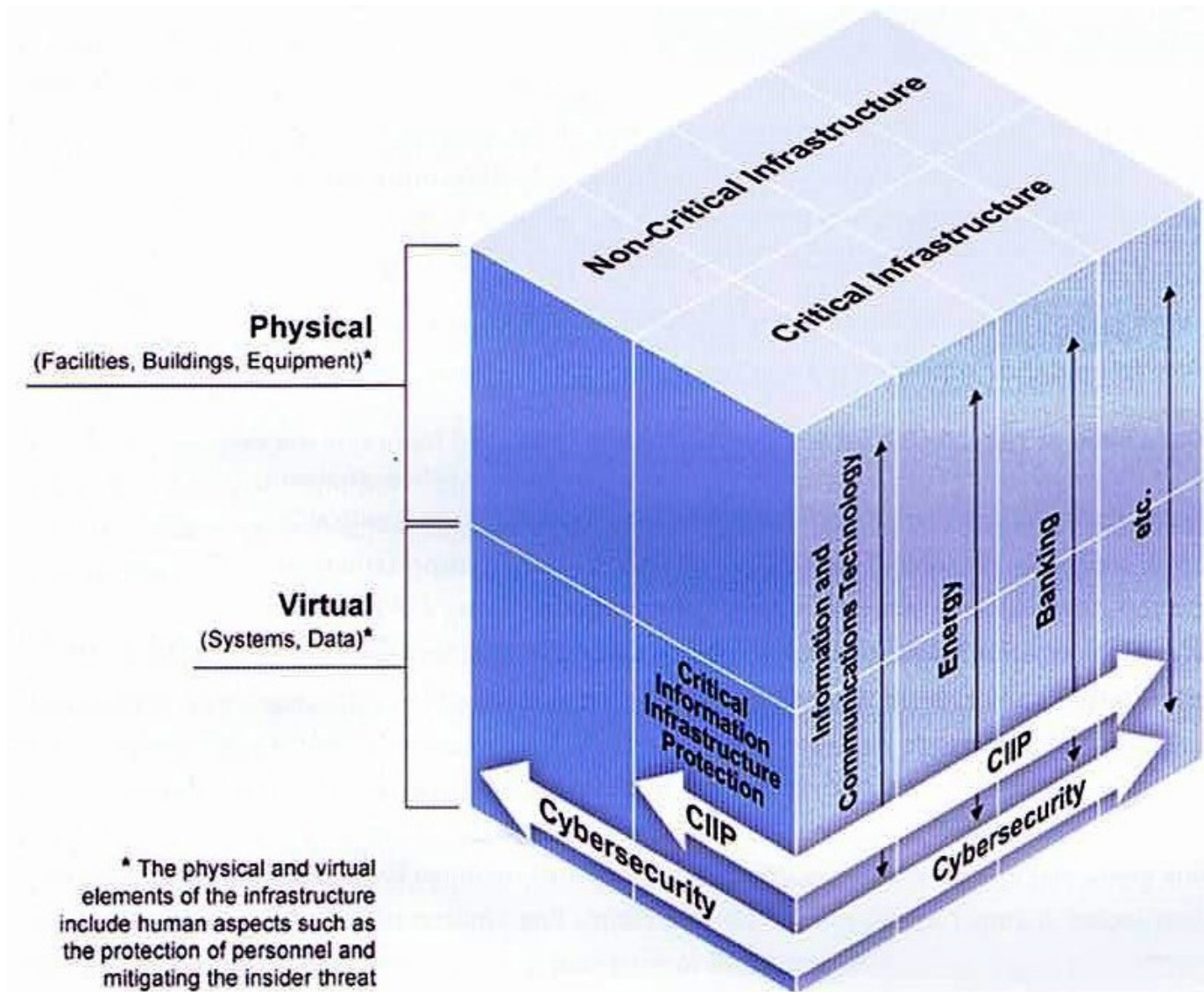


# Critical National Infrastructure: CNI

- *Economy Disruption:* CyberTerrorists will deliberately target CNI to seriously disrupt national economies.
- *Hybrid CNI Attacks:* CNI attacks will often combine both physical & cyber terror threats to maximise national & regional economic disruption
- *Critical Economic Sectors:* Typical CNI Targets will include Energy Grids, Transport Hubs, Retail Malls & Uni Campuses, Financial Institutions, Government Ministries, Defence Agencies and Military Bases.

*....We now briefly explore CyberSecurity for CNI Sectors*

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

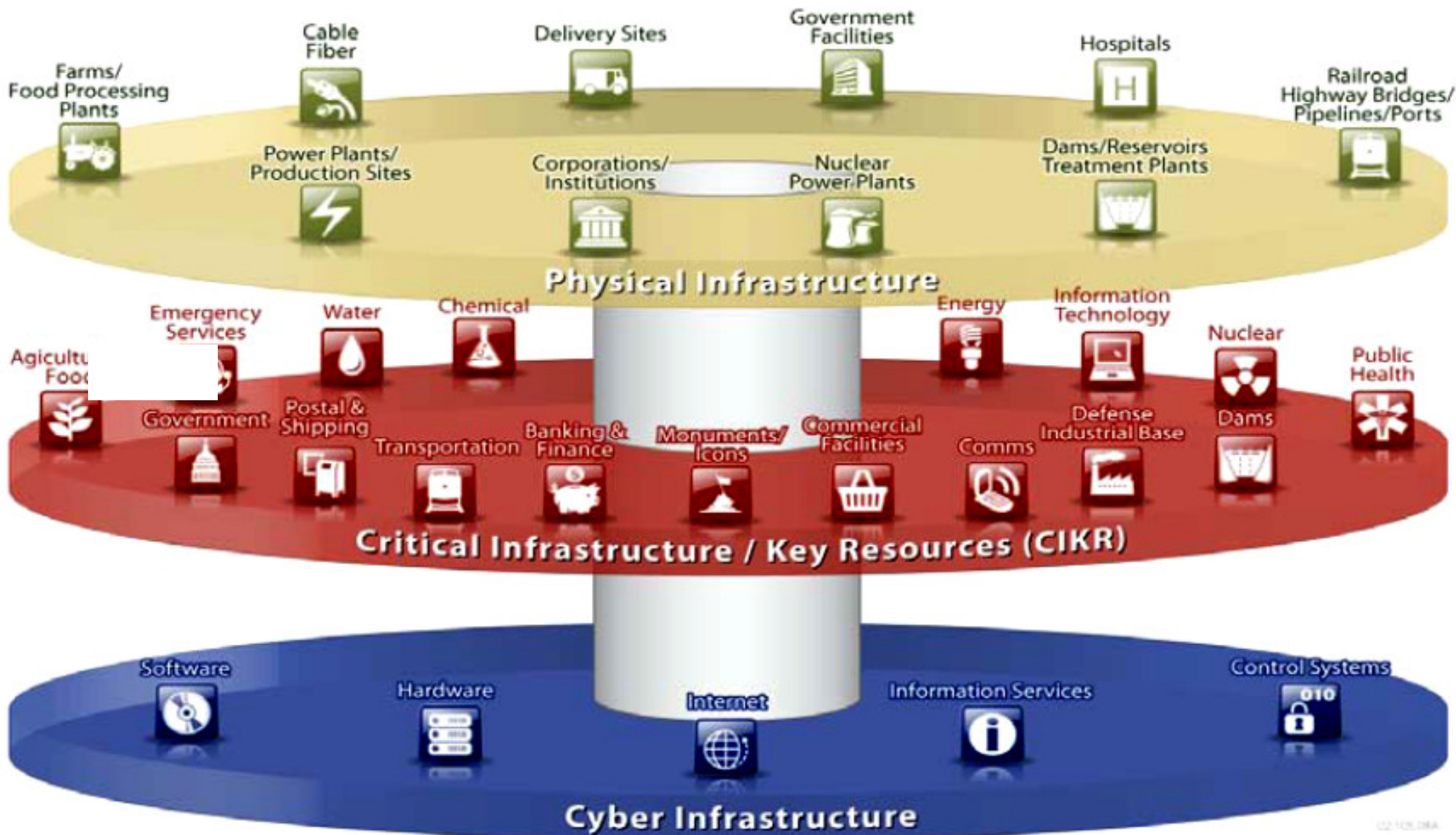




# A Short History of Cybersecurity for *CNI/CII*

- *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 Terrorism* against Critical Sectors

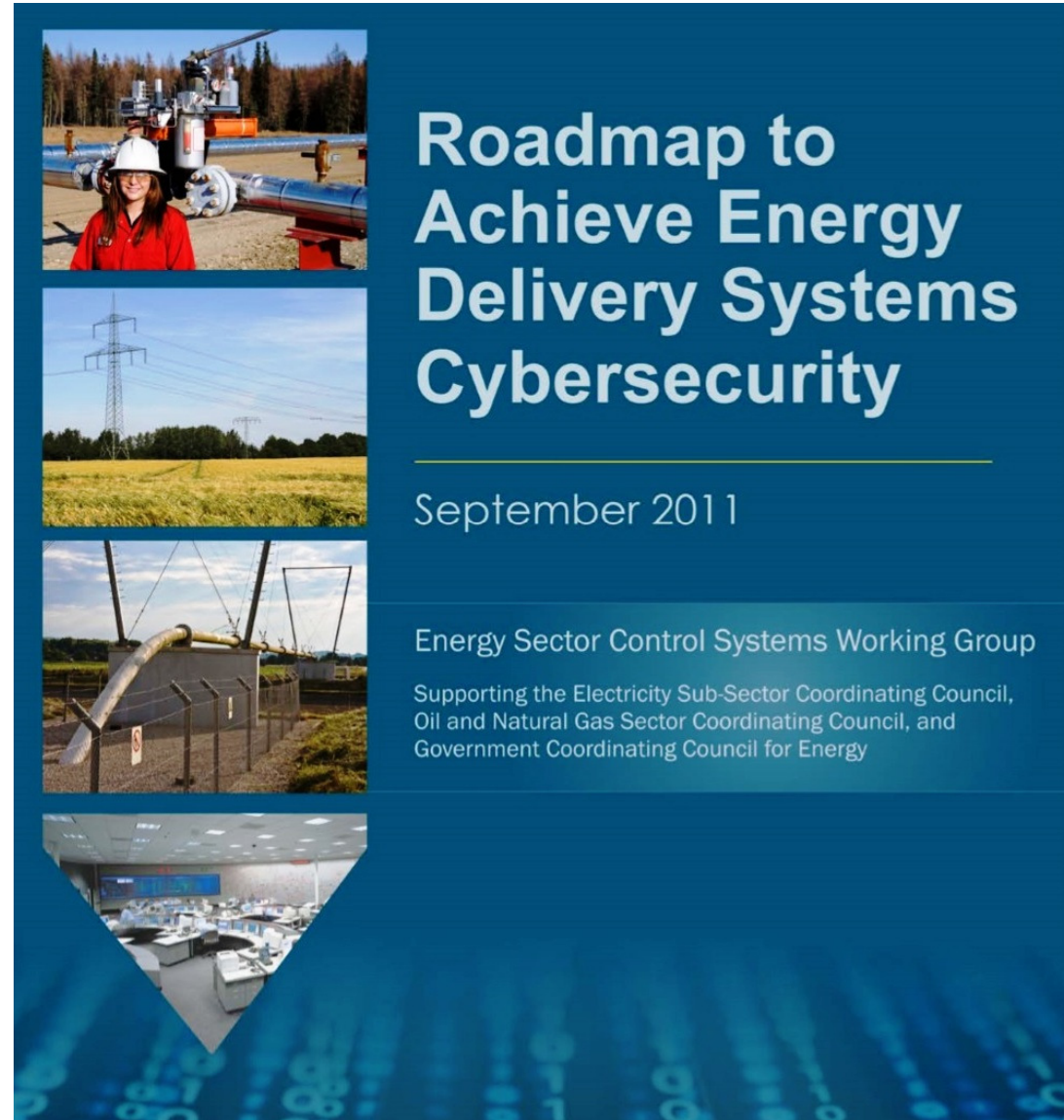
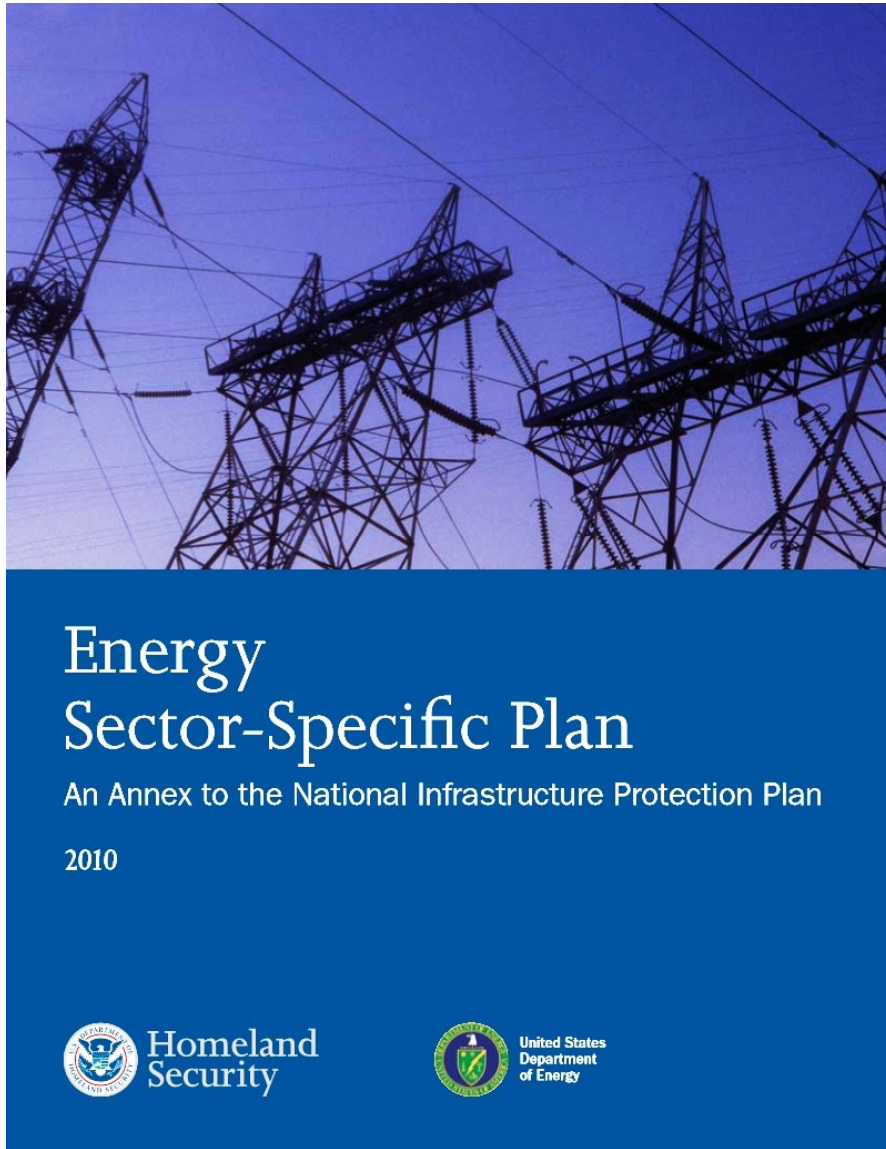
- *Government/Defence:*
  - Theft of secret intelligence, manipulation of documents, and illegal access to confidential citizen databases & national records
- *Banking/Finance:*
  - Denial of Service attacks against clearing bank network, phishing attacks against bank account & credit cards, money laundering
- *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!*

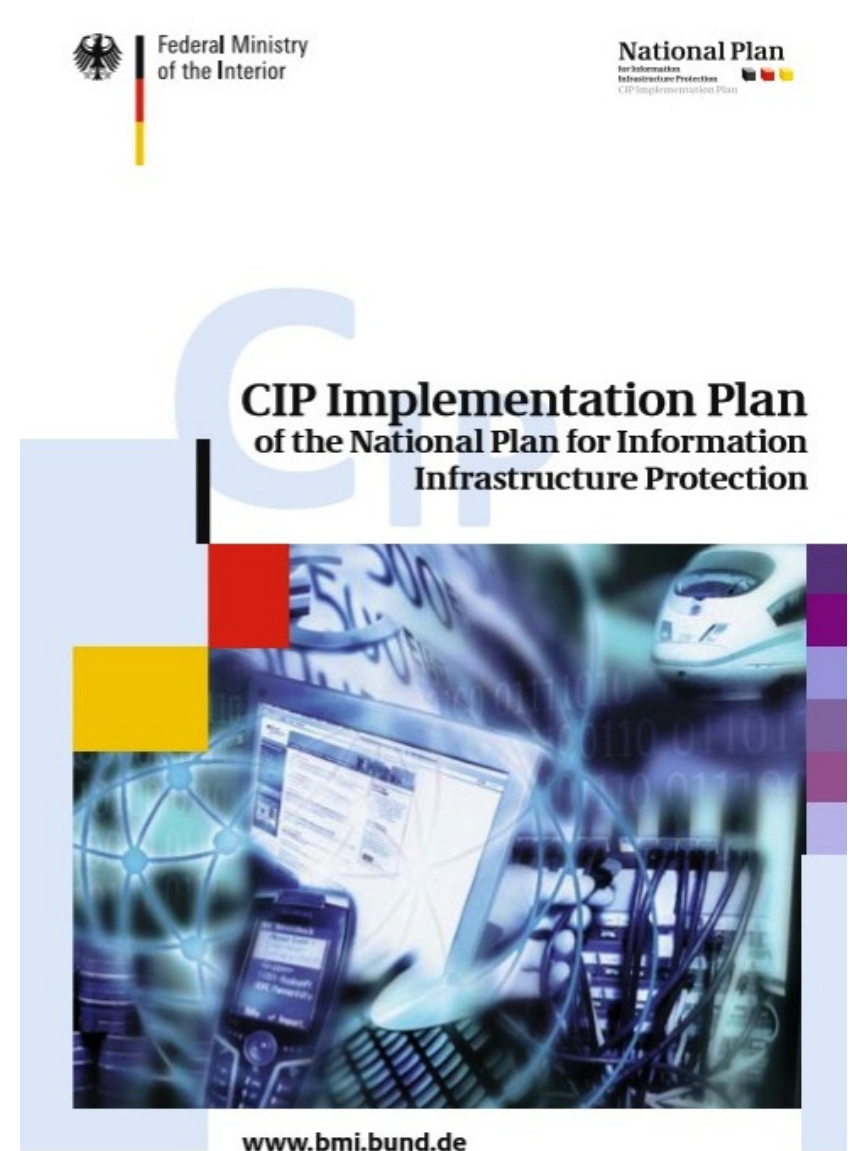
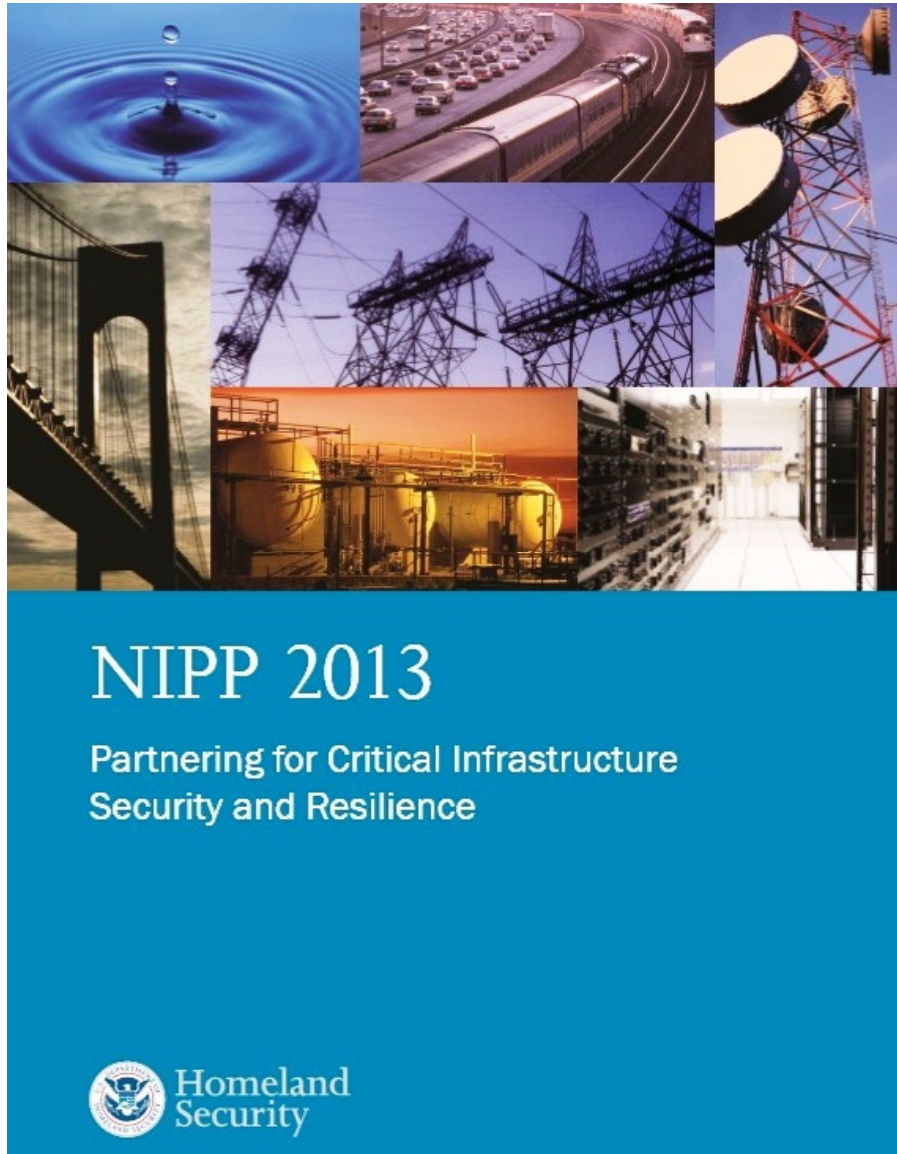




# *Cybersecurity* for Critical Information Infrastructure of the *Energy Sector*



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





# Cybersecurity for the *Healthcare Sector*



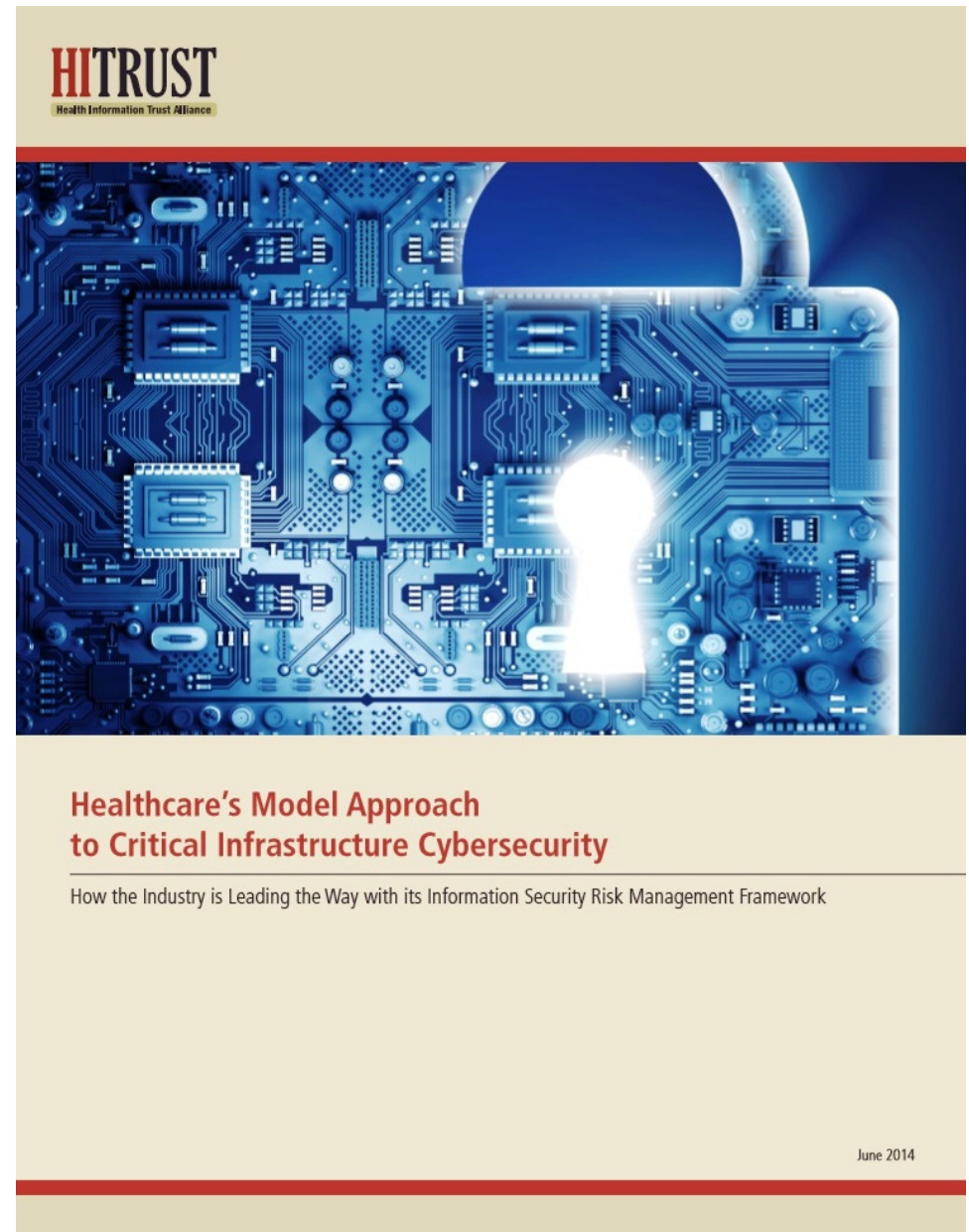
**A SANS Analyst Whitepaper**

*Written by Barbara Filkins*

February 2014

*Sponsored by  
Norse*

©2014 SANS™ Institute



June 2014

**31<sup>st</sup> International East/West Security Conference**

**"Cyber-terrorism(2): Security in Cyberspace"**

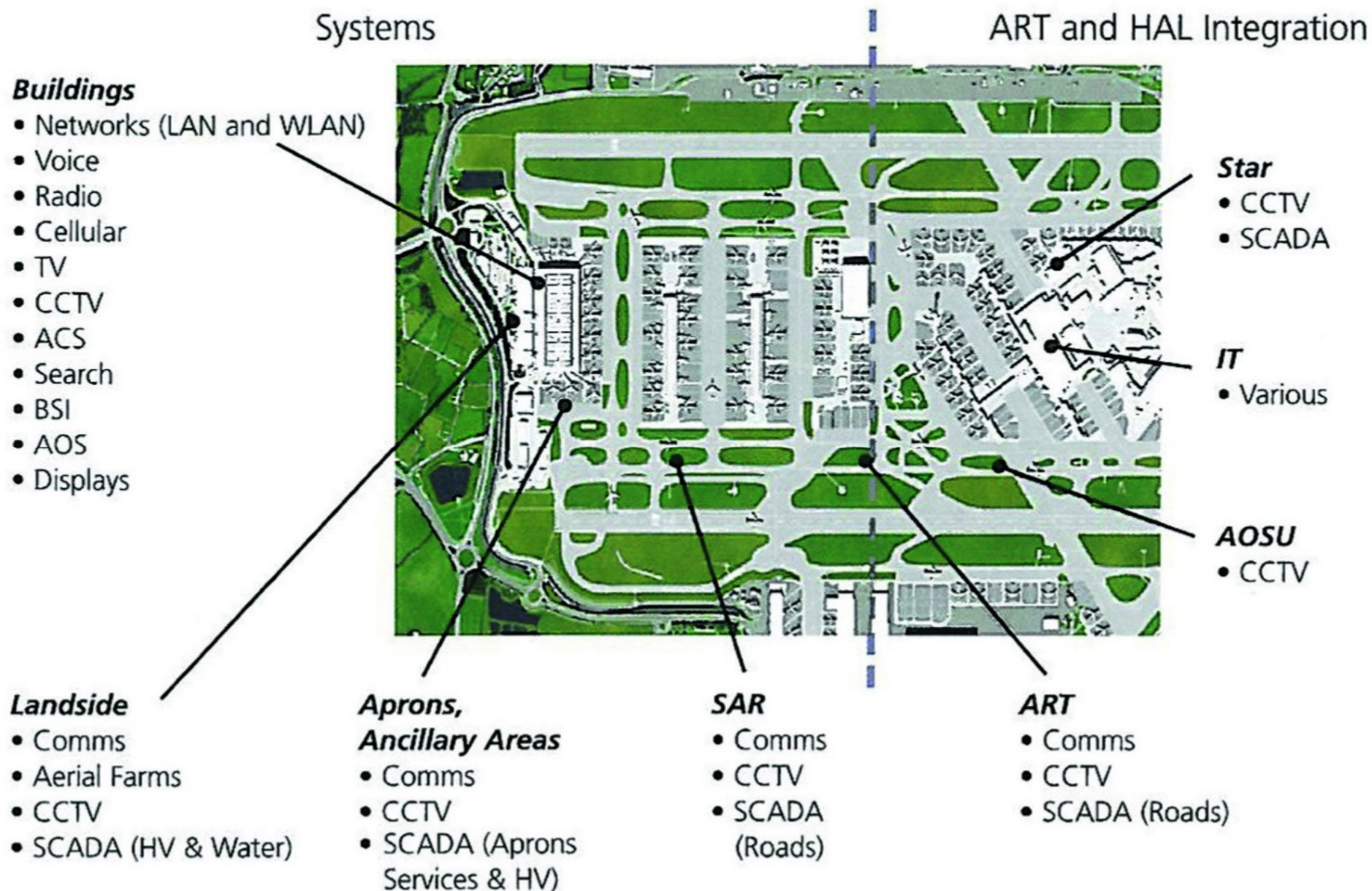
Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Cybersecurity: International Airports: LHR-T5



# Cybersecurity Benefits: *Critical Business Sectors*

- Improved cybersecurity provides significant benefits to the Government & Critical National Sectors & Commercial Enterprises 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
  - *Defence*: Early warning, alerts and defences against cyberattacks through national CERT (Computer Emergency Response Centre)
  - *Cybercrime*: Investigate, Digital Forensics and Prosecution of cybercrimes such ID & Financial Theft, “Computer Misuse, Laundering, On-Line Drug Trafficking & Pornographic Materials
  - *Cyberterrorism*: Ability to assess, predict and prevent potential major cyber terrorist attacks, and to minimise damage during events
  - *Power & Water Utilities*: Prevent malicious damage to control systems
  - *Telecommunications*: Top security of government communications with alternative routings, encryption & protection against cyberattack

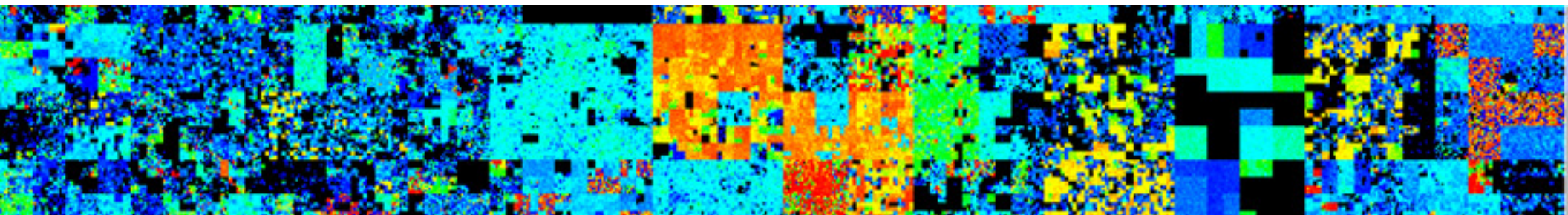




# - CyberTerrorism (2) – “Security in Cyberspace”



1 – <i>Supersonic</i> “Real-Time” Cybersecurity	2 –Cybersecurity Models & Architectures	3 –Cyber <i>Emergency</i> Response Team: <i>CERT</i>
4 –Cybersecurity for Government & Defence	5 – Cybersecurity for Banking & Finance	6 – Securing Critical National Infrastructure
7 –Cyber Action Plans & <i>Tactical</i> Road Maps	8 – <i>OUR</i> Cyber Future : “ <i>Neural Society</i> ”	9 – Developing <i>YOUR</i> Cybersecurity Plans!





# Cyber Action Plans & *Tactical* Road Maps

- *Action Plan*: 21<sup>st</sup> C “Conflict in Cyberspace” demands swift action and the extension of *YOUR* Business-Wide Security to defend against CyberThreats & Attacks.
- *CSO Team*: Physical Security and CyberSecurity need to be managed through a dedicated Team led by qualified “Board Level” - Chief Security Officer (CSO)
- *Road Map*: Successful CyberSecurity requires an in-depth Business Investment Plan coupled with a *Tactical* Multi-Year Operational Programme & Cyber RoadMap

.....Each **Critical Economic Sector** such as Banking & Finance, Government & Defence, Telecommunications, Transportation & Energy will require its own Cyber Strategy, Risk Assessment, Roadmap & Action Plan!



# Cybersecurity Teams: *Operational Budgets*

- *CSO Operations & Investment Plan*: Managing Cybersecurity for *YOUR* Organisation is an ongoing task with a continuous need for systems upgrades, professional staff training, compliance audits, standards certifications and CERT Team response to emergency cyber events.
- *Annual Operational Security Budgets* will need to include allowances for:
  - Staff salaries & operational costs for your Professional Cybersecurity Team
  - Costs for tackling Cybercrime & Cyberterrorism throughout your business
  - Costs of required annual security audits to ensure ongoing regulatory compliance
  - Professional training courses at leading Universities & Educational Institutions
  - Costs for maintaining “Best Practice” Cybersecurity within each organisational unit
  - Regular Systems, Computing & Communications reviews & upgrades to ensure that all networked servers, databases and computing devices are secure against CyberAttack!

*...YOUR CSO led Team will need to develop Action Plans and Tactical Road Maps in order to Professionally Programme Manage the Multi-Year Implementation of CyberSecurity!*



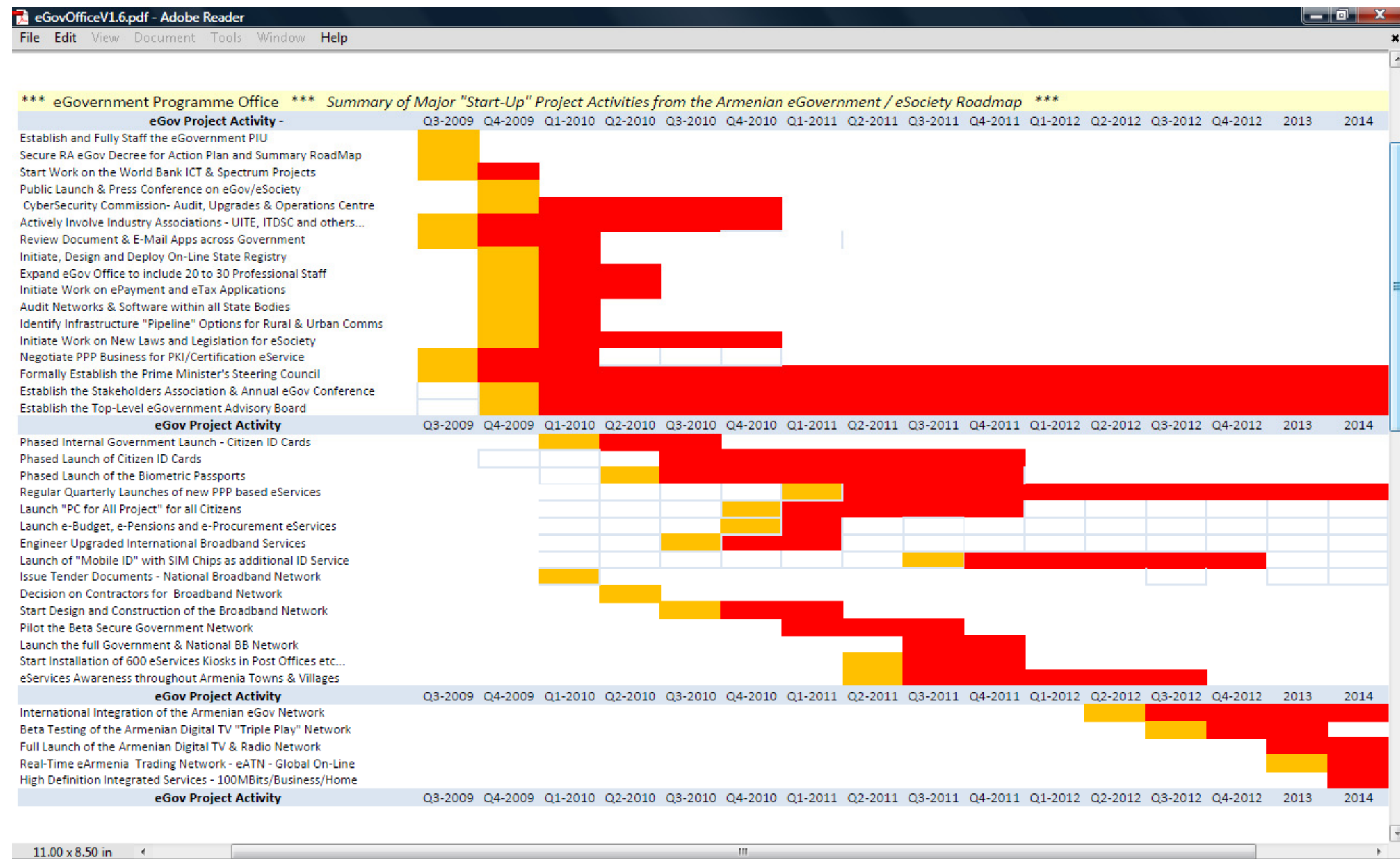
# Typical Cybersecurity Programme RoadMap:

## *Spanning the UN/ITU Cybersecurity Agenda (GCA)*

Cybersecurity Project Activity - Phase 1 - Jan/Feb/March 2011														
	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q1 Project Activity -(1)-														
Q1 Project Activity -(2)-														
Q1 Project Activity -(3)-														
Q1 Project Activity -(4)-														
Q1 Project Activity -(5)-														
Q1 Project Activity -(6)-														
Q1 Project Activity -(7)-														
Q1 Project Activity -(8)-														
Q1 Project Activity -(9)-														
Q1 Project Activity -(10)-														
Cybersecurity Project Activity - Phase 2 - April/May/June 2011														
	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q2 Project Activity -(1)-														
Q2 Project Activity -(2)-														
Q2 Project Activity -(3)-														
Q2 Project Activity -(4)-														
Q2 Project Activity -(5)-														
Q2 Project Activity -(6)-														
Q2 Project Activity -(7)-														
Q2 Project Activity -(8)-														
Q2 Project Activity -(9)-														
Q2 Project Activity -(10)-														
Cybersecurity Project Activity - Phase 3 - July/Aug/Sept 2011														
	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q3 Project Activity -(1)-														
Q3 Project Activity -(2)-														
Q3 Project Activity -(3)-														
Q3 Project Activity -(4)-														
Q3 Project Activity -(5)-														
Q3 Project Activity -(6)-														
Q3 Project Activity -(7)-														
Q3 Project Activity -(8)-														
Q3 Project Activity -(9)-														
Q3 Project Activity -(10)-														
Cybersecurity Project Activity-Phase 4-Oct/Nov/Dec 2011-2012														
	Jan-11	Feb-11	Mar-11	Apr-11	May-11	Jun-11	Jul-11	Aug-11	Sep-11	Oct-11	Nov-11	Dec-11	Q1-2012	Q2-2012
Q4 Project Activity -(1)-														
Q4 Project Activity -(2)-														
Q4 Project Activity -(3)-														
Q4 Project Activity -(4)-														
Q4 Project Activity -(5)-														
Q4 Project Activity -(6)-														
Q4 Project Activity -(7)-														
Q4 Project Activity -(8)-														
Q4 Project Activity -(9)-														
Q4 Project Activity -(10)-														



# eGovernance/eSecurity Road Map – 2009 to 2014 -



# CISSP Certification – International Cyber Qualification

- The **CISSP** – Certified Information Systems Security Professional is one of the highest international qualifications from the (ISC)<sup>2</sup>, 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

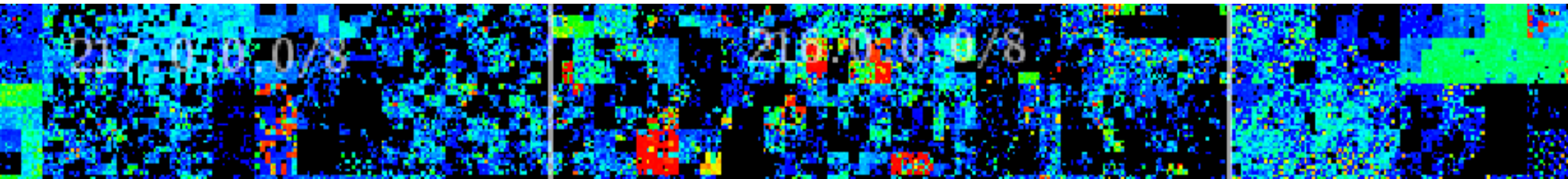


- An in-depth study of all these security topics would fill an intensive 3 month training schedule, but I hope that these 2 presentations have provided the foundations!*

# - CyberTerrorism (2) – “Security in Cyberspace”



1 – <i>Supersonic</i> “Real-Time” Cybersecurity	2 –Cybersecurity Models & Architectures	3 –Cyber <i>Emergency</i> Response Team: <i>CERT</i>
4 –Cybersecurity for Government & Defence	5 – Cybersecurity for Banking & Finance	6 – Securing Critical National Infrastructure
7 –Cyber Action Plans & <i>Tactical</i> Road Maps	8 – <i>OUR</i> Cyber Future : “ <i>Neural Society</i> ”	9 – Developing <i>YOUR</i> Cybersecurity Plans!





# 1995 – 2015 – 2035: *Next 20 Years*

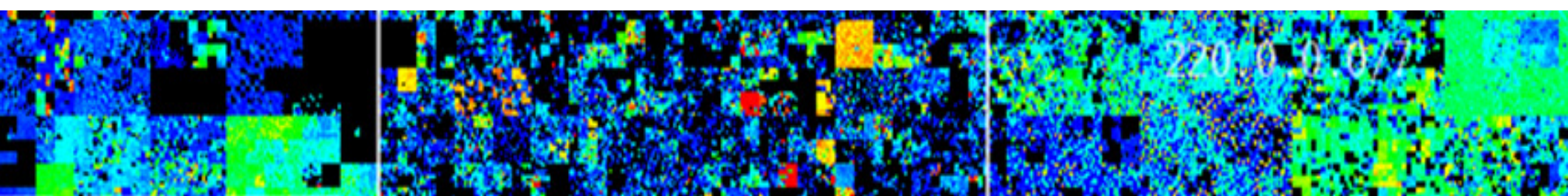
- *IoT*: Global Connected “Internet of Things” – All On-Line Intelligent Devices across most sectors & geographies.
- *“The Bad Cyber Guys”* : Professionally Trained Cyber Criminals and Cyber Terrorists operating WorldWide!
- *Augmented Reality*: Emergence of 4D Immersive Virtual Augmented Reality (*a la Matrix Movies*)
- *Universally Embedded Security*: Need for Cybersecurity in ALL intelligent devices, servers, data & network nodes
- *On-Line CyberPolice*: CyberBot Avatars patrolling as Virtual CyberPolice Force across “Internet of Things”



# - CyberTerrorism (2) – “Security in Cyberspace”



1 – <i>Supersonic</i> “Real-Time” Cybersecurity	2 –Cybersecurity Models & Architectures	3 –Cyber <i>Emergency</i> Response Team: <i>CERT</i>
4 –Cybersecurity for Government & Defence	5 – Cybersecurity for Banking & Finance	6 – Securing Critical National Infrastructure
7 –Cyber Action Plans & <i>Tactical</i> Road Maps	8 – <i>OUR</i> Cyber Future : “ <i>Neural Society</i> ”	9 – Developing <b>YOUR</b> Cybersecurity Plans!



# YOUR Cybersecurity *Action Plan*!...

- **Phase 1:** Define your cybersecurity STRATEGY and OBJECTIVES
- **Phase 2:** Establish, resource & train your CSO led Cybersecurity ORGANISATION
- **Phase 3:** Agree and communicate Technical & Operational standards & Cyber Policy
- **Phase 4:** Review, Audit and Upgrade CyberSecurity according to *YOUR* Action Plan
- **Phase 5:** On-Going Operational Management by CSO, including regular compliance audits and technical upgrades to newly researched Cyber Threats , Events & Alerts.

.....In summary, the implementation of **CyberSecurity** for **YOUR** Enterprise will have a significant impact on reducing losses from **Cybercrime**, & mitigate the risk of damaging **CyberTerror** Attacks across your Business Operations



# Developing **YOUR** Cyber Action Plans!

- Immediate 3 Day Cyber Security Info Asset Audit
- 30 Day Programme – Review Top 10 CSO Actions
- 300 Day/1 Year Cyber Implementation Plan (Suggest using the UN/ITU – Global Cybersecurity Agenda)
- Long Term Investment – 3 to 5 Year Road Map (Recruit, Train and Implement YOUR CyberSecurity Plan!)

*.....Be Prepared for “Real-Time” alerts & response to Cyber Attacks and Terrorism – **They strike without warning at the “Speed of Light” across Global Information Networks !***



# CyberTerrorism: *Wrap-Up & Summary*

- 1) *New Disruptive Force*: CyberTerrorism is already a real disruptive & expensive threat to Business, Government and National Economies
- 2) *Rethinking 21stC Security*: Business & Government need to radically rethink their strategy, tactics and implementation of Integrated Physical-Cybersecurity for the 21<sup>st</sup> Century to mitigate the risks
- 3) *Practical Plans*: We recommend that CSO-Led Teams develop in-depth action Plans and Road Maps for their business organisations
- 4) *CERT/CSIRT*: One key task for Critical Business Sectors such as Banking & Finance is the implementation of a dedicated CERT/CSIRT
- 5) *Cyber Training*: Cybersecurity Training, Certification and Membership of Professional Security Associations are also recommended
- 6) *Security Standards*: Finally we recommend that your business adopts International Standards for CyberSecurity such as ISO27000 Series with suggested annual independent audits for full compliance.



# “CyberTerrorist”: *Woland (Воланд)*

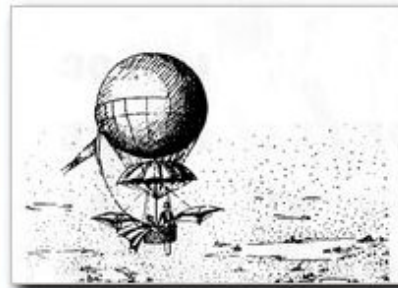
Prepare for CyberTerror Attacks  
through *your* CERT & Real-Time Alerts!

Don't be taken by surprise by **Woland**  
- **The Satanic Terrorist Cat** - from  
Bulgakov's : “*The Master & Margarita*”

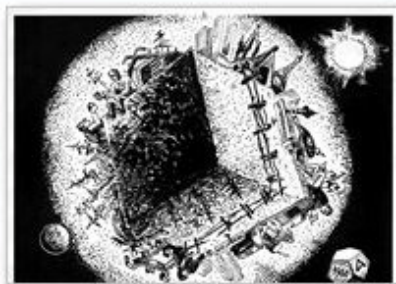
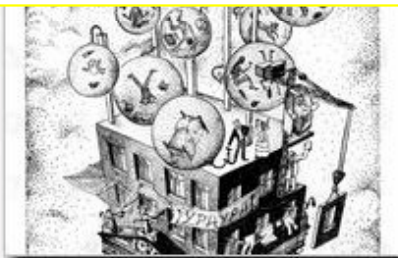
*Graphic Print (1972) courtesy of :  
Dr Alexander Rimski-Korsakov  
Great Grandson of the Composer*







## The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov





# CyberTerrorist Invasion @ *“Light Speed!”*

**Prepare for CyberTerror Invasion  
through your Real-Time CERT !**

*Graphic Print (1981) courtesy of :  
Dr Alexander Rimski-Korsakov  
Great Grandson of the Composer*

***Light travels almost 1million times  
faster than the Speed of Sound!***



# \* Final Warning!: *CyberTerror* Strikes @ “*Light Speed*” in Global Networks!





# East-West Security Conference – Italy 2015

## - *CyberTerrorism Presentation Slides (PDF)* -



### - **CyberTerrorism (1)** - - *"Conflict in Cyberspace"* -



31<sup>st</sup> International East/West Security Conference  
"Cyber-terrorism(1): Conflict in Cyberspace"  
Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



1

Theme (1) – "Conflict in Cyberspace"



### - **CyberTerrorism (2)** - - *"Security in Cyberspace"* -



31<sup>st</sup> International East/West Security Conference  
"CyberTerrorism(2): Security in Cyberspace"  
Terracina, Italy: 24<sup>th</sup> – 27<sup>th</sup> May 2015  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



1

Theme (2) – "Security in Cyberspace"

Download Link: [www.valentina.net/East-West2015/](http://www.valentina.net/East-West2015/)

31<sup>st</sup> International East/West Security Conference

"Cyber-terrorism(2): Security in Cyberspace"  
Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



86



# CyberTerrorism (2): “Security in Cyberspace”

International East-West Security Conference: Terracina, Italy

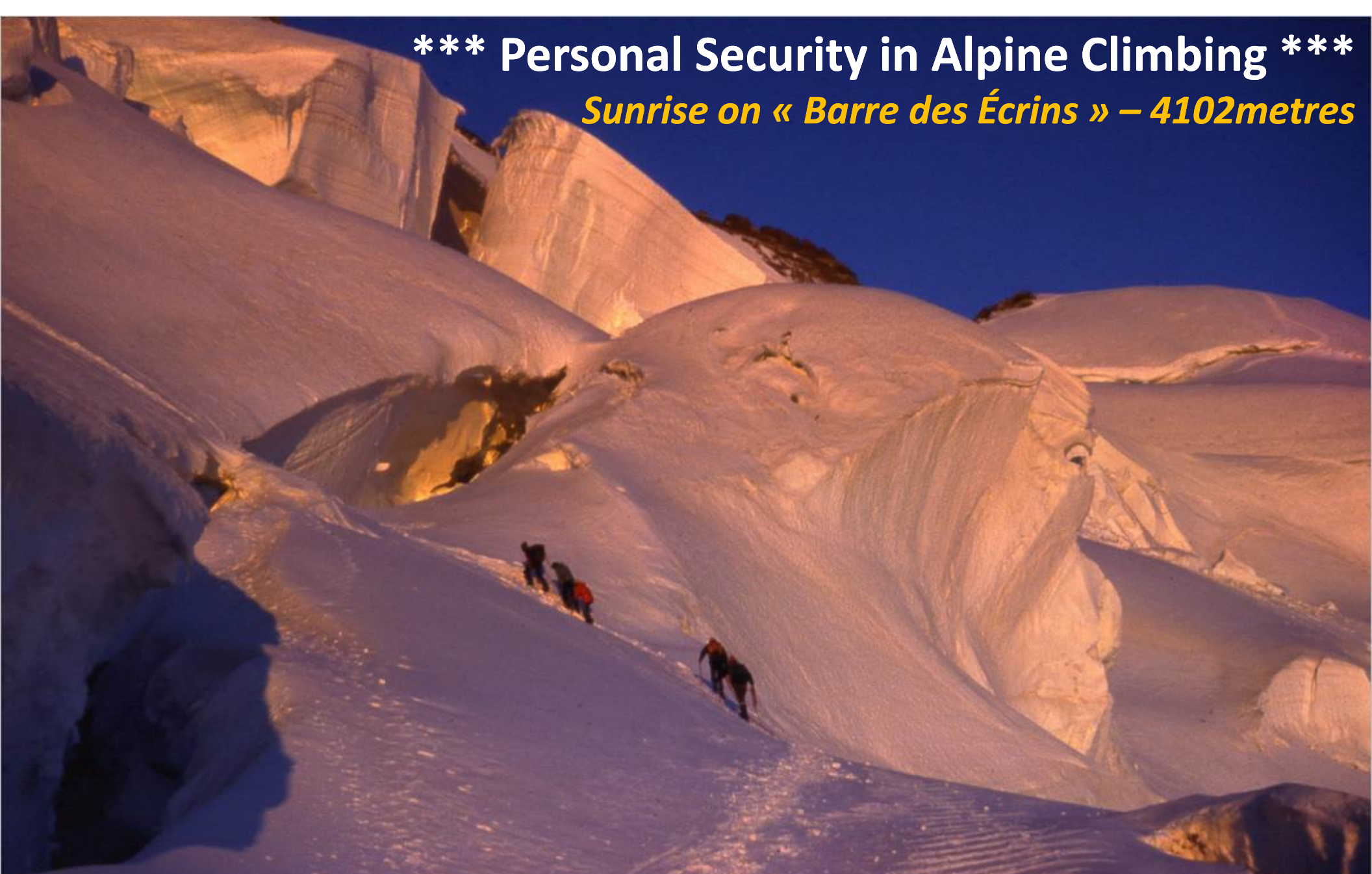
Thank-You!...

Download Presentation Slides:  
*[www.Valentina.net/East-West2015/](http://www.Valentina.net/East-West2015/)*



# \*\*\* Personal Security in Alpine Climbing \*\*\*

*Sunrise on « Barre des Écrins » – 4102metres*



Security Equipment includes: **50m Rope, Steel Crampons, Ice-Axe & Screws, Karabiners, Helmet...**

31<sup>st</sup> International East/West Security Conference

"Cyber-terrorism(2): Security in Cyberspace"

Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





**Download Presentation Slides:**  
***[www.Valentina.net/East-West2015/](http://www.Valentina.net/East-West2015/)***



**Thank you for your time!**

# Cybersecurity Resources, Reports and More!...

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

Link: [www.valentina.net/vaza/CyberDocs](http://www.valentina.net/vaza/CyberDocs)

31<sup>st</sup> International East/West Security Conference

"Cyber-terrorism(2): Security in Cyberspace"

Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# 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 1<sup>st</sup> Multi-Media and e-Commerce Web-Site for the World's 1<sup>st</sup> Supersonic Car – ThrustSSC – for the World Speed Record.
- **Secure Wireless Networking** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.
- **Networked Enterprise Security** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional engineers & a diverse portfolio of hi-tech security products.
- **Republic of Georgia** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament.
- **UN/ITU** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

*Dr David E. Probert is a Fellow of the Royal Statistical Society. He has a 1<sup>st</sup> 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.*



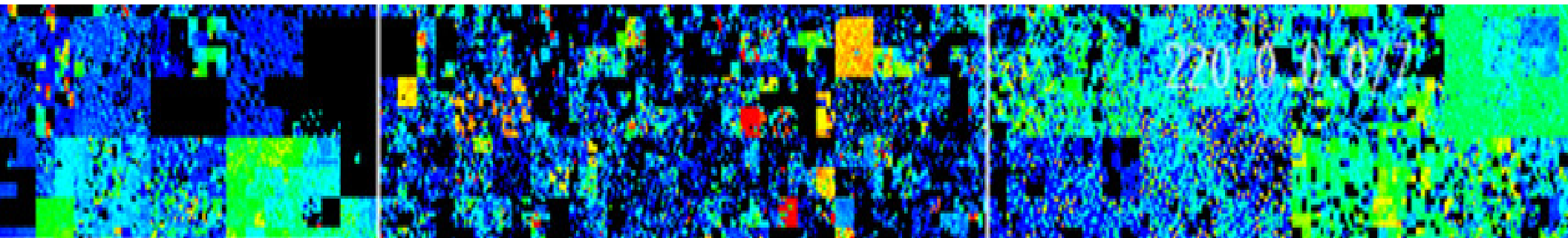


# CyberTerrorism (2): “Security in Cyberspace”

International East-West Security Conference: Terracina, Italy

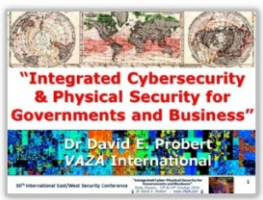


## BACK-UP SLIDES



# Smart Sustainable Security – “Theme Trilogy”

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



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

**“Operational Convergence”**

**13<sup>th</sup> Oct: 09:10 – 09:50**

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



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

**“Architecture & Standards”**

**13<sup>th</sup> Oct: 14:30 – 15:10**

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



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

**“Intelligent Applications”**

**14<sup>th</sup> Oct: 11:15 – 11:55**

**Download Slides:** [www.valentina.net/East-West2014/](http://www.valentina.net/East-West2014/)

**31<sup>st</sup> International East/West Security Conference**

**‘Cyber-terrorism(2): Security in Cyberspace’**

Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015

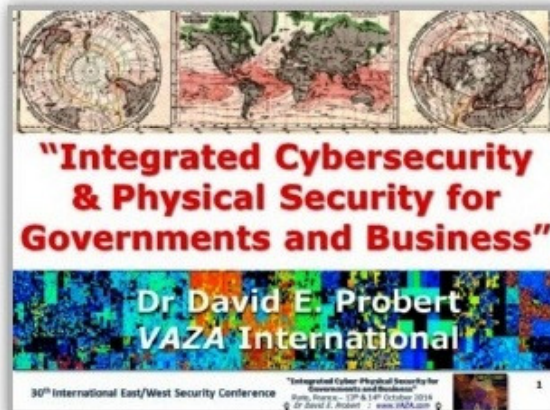
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



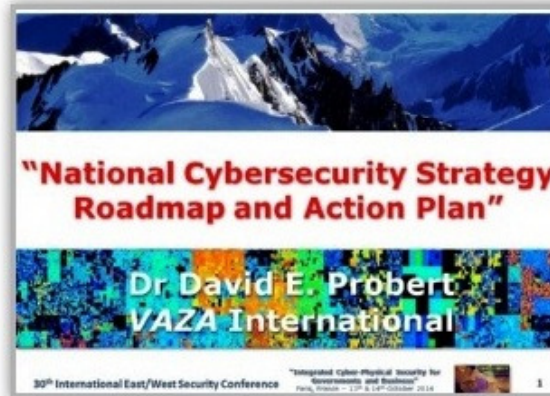
# East-West Security Conference – Paris 2014

## - *Cybersecurity Presentation Slides (PDF)* -

### Smart Sustainable Security - "Theme Trilogy"



**(1) Smart Security**



**(2) National Security**



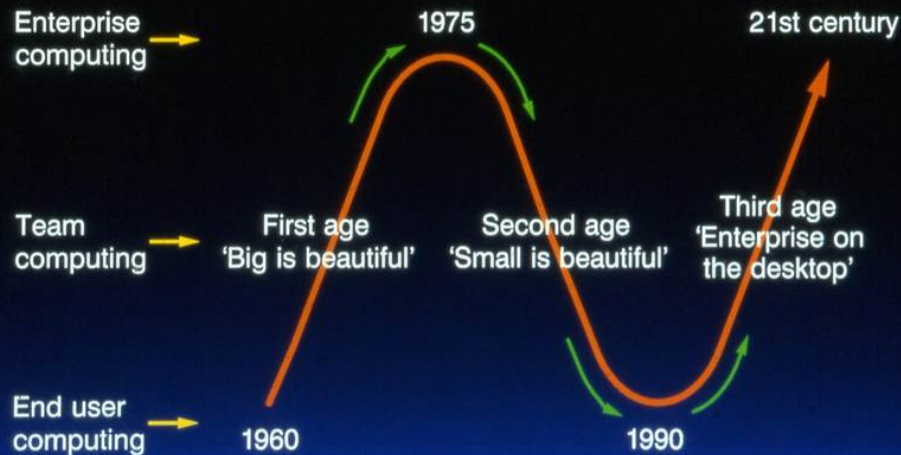
**(3) Critical Security**

**Download Link:** [www.valentina.net/East-West2014/](http://www.valentina.net/East-West2014/)



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

## Overview: Ages of Computing



## 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



## Second Age of Computing

1975 → 1990 - *Bridge*

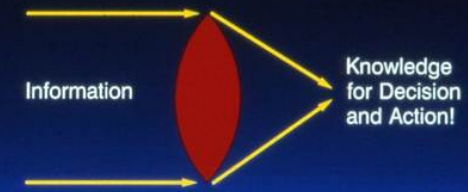
- Emergence of Networking Architecture - 'Distributed Architecture'
- 'Small is BEAUTIFUL'
- Created Open Systems: OSI
- Focus on INFORMATION - a DYNAMIC Universe



## 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



# 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.

# Cybersecurity: NATO Research Analysis

NATIONAL SECURITY THREATS	CYBER ATTACK ADVANTAGES	ATTACK CATEGORIES	TARGETS	CYBER ATTACK MITIGATION STRATEGIES	EFFECTIVENESS
ESPIONAGE	IT VULNERABILITIES	CONFIDENTIALITY	MILITARY FORCES	NEXT GEN NET IPV6	SOLVES SOME Q'S, CREATES OTHERS
PROPAGANDA	HIGH ASYMMETRY	INTEGRITY	GOV/CIV INFRASTRUCTURE	BEST MIL DOCTRINE SUN TZU	INSUFFICIENT FOR CYBER WAR
DENIAL-OF-SERVICE (DOS)	ANONYMITY	AVAILABILITY		DETERRENCE	LACKS CREDIBILITY
DATA MODIFICATION	INADEQUACY OF CYBER DEFENSE			ARMS CONTROL	CANNOT PROHIBIT, INSPECT CYBER
INFRASTRUCTURE MANIPULATION	THE RISE OF NON-STATE ACTORS				

Author: Kenneth Geers - [www.ccdcoe.org/publications/books/Strategic\\_Cyber\\_Security\\_K\\_Geers.PDF](http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF)



# UN/ITU : GCA – The Seven Strategic Goals

## - *for National & International Cybersecurity* -

### The Seven Goals:

- 1 Elaboration of strategies for the development of a **model cybercrime legislation** that is globally applicable and interoperable with existing national and regional legislative measures.
- 2 Elaboration of global strategies for the creation of appropriate national and regional **organizational structures** and policies on **cybercrime**.
- 3 Development of a strategy for the establishment of globally accepted minimum **security criteria and accreditation schemes for hardware and software applications and systems**.
- 4 Development of strategies for the creation of a global framework for **watch, warning and incident response** to ensure cross-border coordination between new and existing initiatives.
- 5 Development of global strategies for the creation and endorsement of a **generic and universal digital identity system** and the necessary **organizational structures** to ensure the recognition of digital credentials across geographical boundaries.
- 6 Development of a *global strategy to facilitate* **human and institutional capacity building** to enhance knowledge and know-how across sectors and in all the above-mentioned areas.
- 7 Proposals on a framework for a *global multi-stakeholder strategy* for **international cooperation, dialogue and coordination** in all the above-mentioned areas.

*....These 7 goals can be achieved through the implementation of **National CERTs!***



# Common Cyber Attacks: Reducing The Impact

Most cyber attacks are composed of four stages: **Survey**, **Delivery**, **Breach** and **Affect**. The following security controls, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

**81%**  
OF LARGE COMPANIES  
REPORTING BREACH

**£600K -  
£1.15m**  
AVERAGE COST OF  
SECURITY BREACH

Source: 2014 Information Security Breaches Survey sponsored by the Department for Business, Innovation and Skills.



## User Education

Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.



## Controls For The Affect Stage

Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help. 10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.



## Patch Management

Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.



## Secure Configuration

Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.



## User Access

Well maintained user access controls can restrict the applications, privileges and data that users can access.



## Monitoring

Monitor and analyse all network activity to identify any malicious or unusual activity.



## User Training

User training is extremely valuable in reducing the likelihood of successful social engineering attacks.



## Network Perimeter Defences

Can block insecure or unnecessary services, or only allow permitted websites to be accessed.



## Malware Protection

Malware protection within the internet gateway can detect malicious code in an imported item.



## Malware Protection

Can block malicious emails and prevent malware being downloaded from websites



## Password Policy

Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.



## Device Controls

Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.



## Secure Configuration

Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

## Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

**CERT-UK**

Link: [www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility](http://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility)

31<sup>st</sup> International East/West Security Conference

"Cyber-terrorism(2): Security in Cyberspace"

Terracina, Italy : 25<sup>th</sup>-26<sup>th</sup> May 2015

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©

