



# CyberSecurity Strategy *for* Critical National Infrastructure!

**Dr David E. Probert**  
**VAZA International**

Dedicated to Ethan, Alice, Hugh, Matthew, Abigail, Micah, Roscoe & Tatiana!


**38<sup>th</sup> International East-West Security Conference**

**"Cybersecurity for Critical National  
Infrastructure" - Strategy & RoadMap**

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# Стратегия Кибербезопасности

\*\*\*\*\* для Критической \*\*\*\*\*

# Национальной Инфраструктуры



[www.Valentina.net/NICE2018/](http://www.Valentina.net/NICE2018/)

Dedicated to Ethan, Alice, Hugh, Matthew, Abigail, Micah, Roscoe & Tatiana!

38<sup>th</sup> International East-West Security Conference

“Cybersecurity for Critical National  
Infrastructure” - *Strategy & RoadMap*

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# “CyberVisions for Business & Governments!”

## Theme (1) - *CyberSecurity for Critical Infrastructure: Business & Governments!...*



- CyberSecurity for Critical National Infrastructure (**CNI**):
- Case Studies of National Government Cyber Programmes
- Operational Cyber Standards, Laws & Regulations

**“Cyber Strategies for Critical Business”**

**6<sup>th</sup> Nov: 9:45 – 10:30**

## Theme (2) – *Intelligent Cyber Surveillance: AI Video Analytics & Biometrics!...*



- **21<sup>st</sup>C** Cyber Landscape for Business & Government Surveillance
- Advanced Surveillance Tools using AI Video Analytics & Biometrics
- Case Studies of Sector Surveillance: Transport, Retail, Culture, Defence...

**“Cyber Surveillance”**

**6<sup>th</sup> Nov: 12:15 – 13:00**

## Theme (3) – *CyberVision 2020 to 2030: YOUR 21<sup>st</sup> C CyberSecurity Toolkit!...*



- Understanding and Mapping the Worldwide Cyber Threats
- Exploring New Cyber Tools using AI & Machine Learning
- Discussion of Cyber Scenarios for **2020 – 2025 – 2030** & Beyond !...

**“Cyber ToolKit”**

**6<sup>th</sup> Nov: 16:15 – 17:00**

**Download: [www.valentina.net/NICE2018/](http://www.valentina.net/NICE2018/)**  
**38<sup>th</sup> International East-West Security Conference**

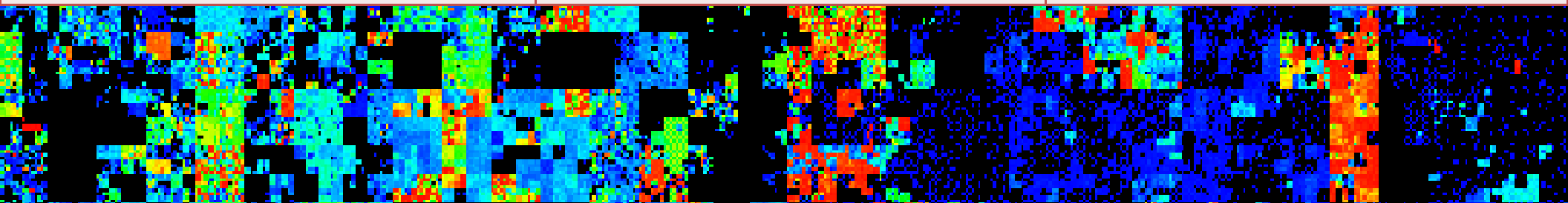
“Cybersecurity for Critical National Infrastructure” - *Strategy & RoadMap*  
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# *Cyber* Security for *Critical* Infrastructure!



1 – Global <i>Cyber</i> Security Landscape “World in Transition”	2 – UN/ITU Cyber Strategy Guide “ <i>Cyber</i> Security Models”	3 -National CyberSecurity Strategies “Secure YOUR Nation”
4 – Case Studies: Georgia & Armenia “Practical Cyber Projects”	5 – TOP 10 <i>Critical</i> National Sectors “Secure YOUR Sector”	6 – Industrial ICS & SCADA Security “Secure YOUR Systems”
7 - Standards, Regulations & Laws “Design to Standards”	8– Professional \$kill\$ Development “\$ Training Investment \$”	9 –YOUR Business Cyber RoadMap! “Multi-Year Cyber Plan”

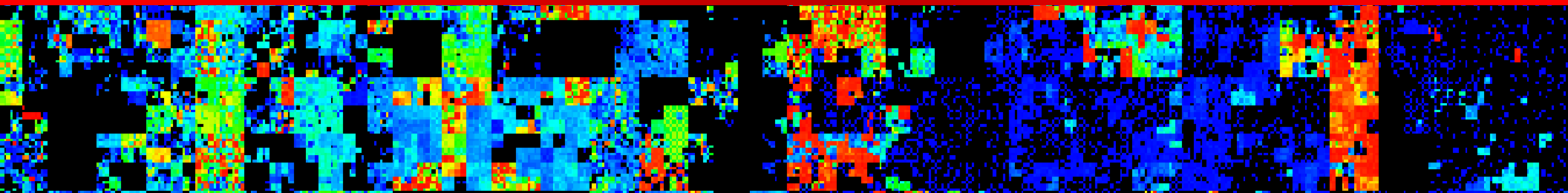




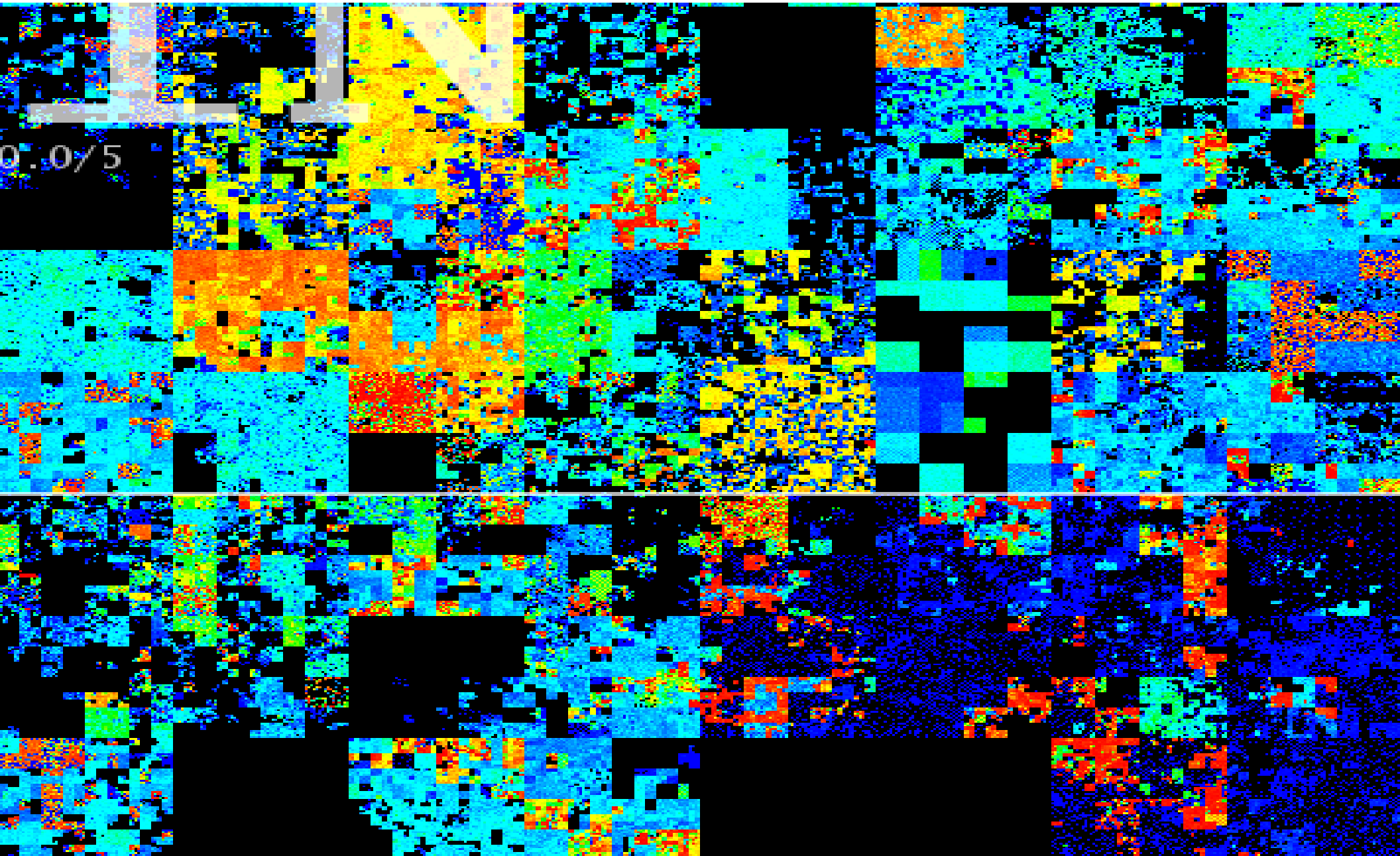
# *Cyber* Security for *Critical* Infrastructure!



## 1 – Global *Cyber* Security Landscape “World in Transition”

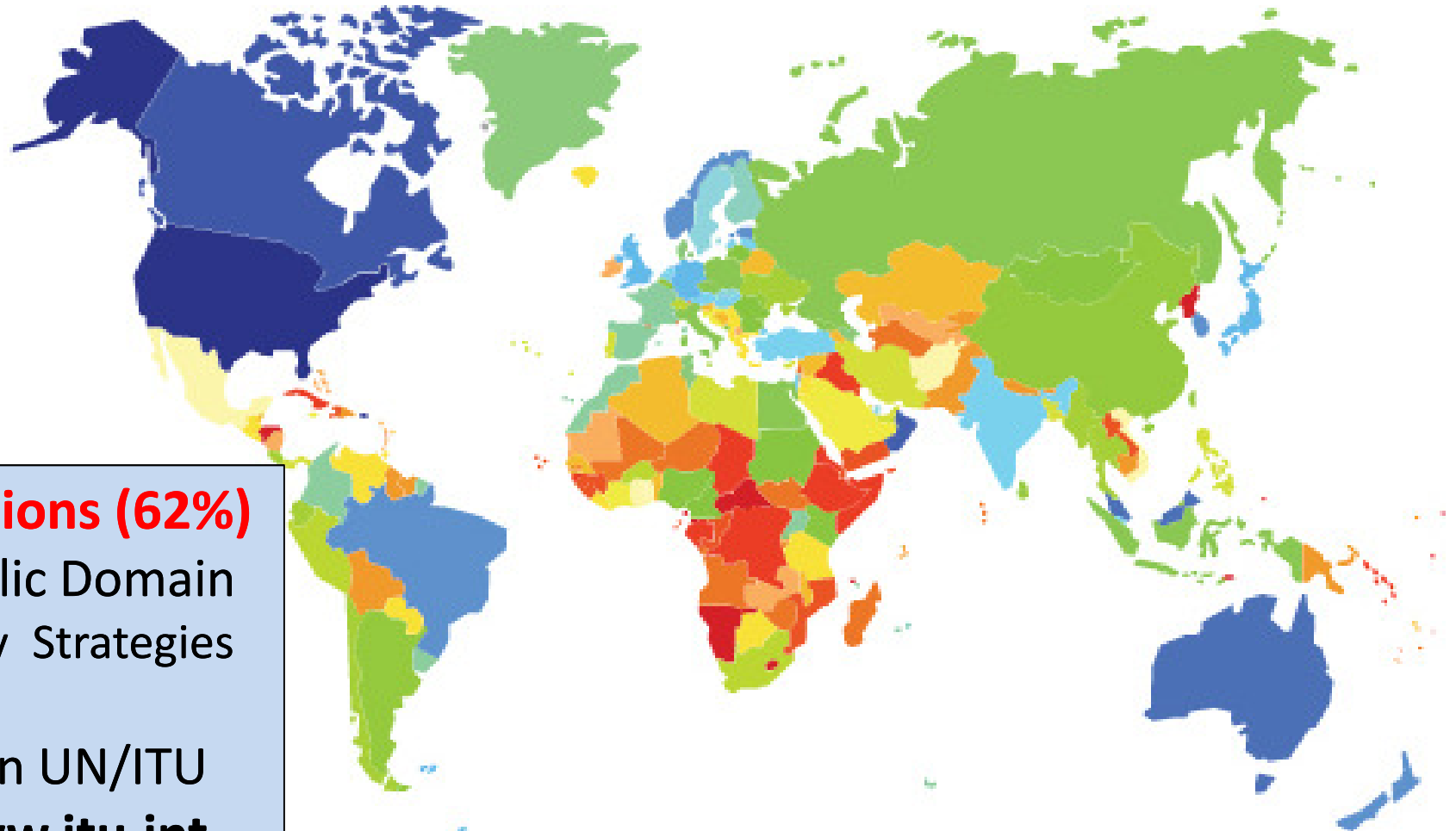


# The Challenging Complexity of *Securing IP Cyberspace*





# UN/ITU – Global Cybersecurity Index



**Just 121 Nations (62%)**

Publish Public Domain  
CyberSecurity Strategies

Available on UN/ITU  
Website: [www.itu.int](http://www.itu.int)

ABIresearch<sup>®</sup>



Global  
Cybersecurity  
Index

National Cybersecurity Commitment



38<sup>th</sup> International East-West Security Conference

“Cybersecurity for Critical National  
Infrastructure” - *Strategy & RoadMap*

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





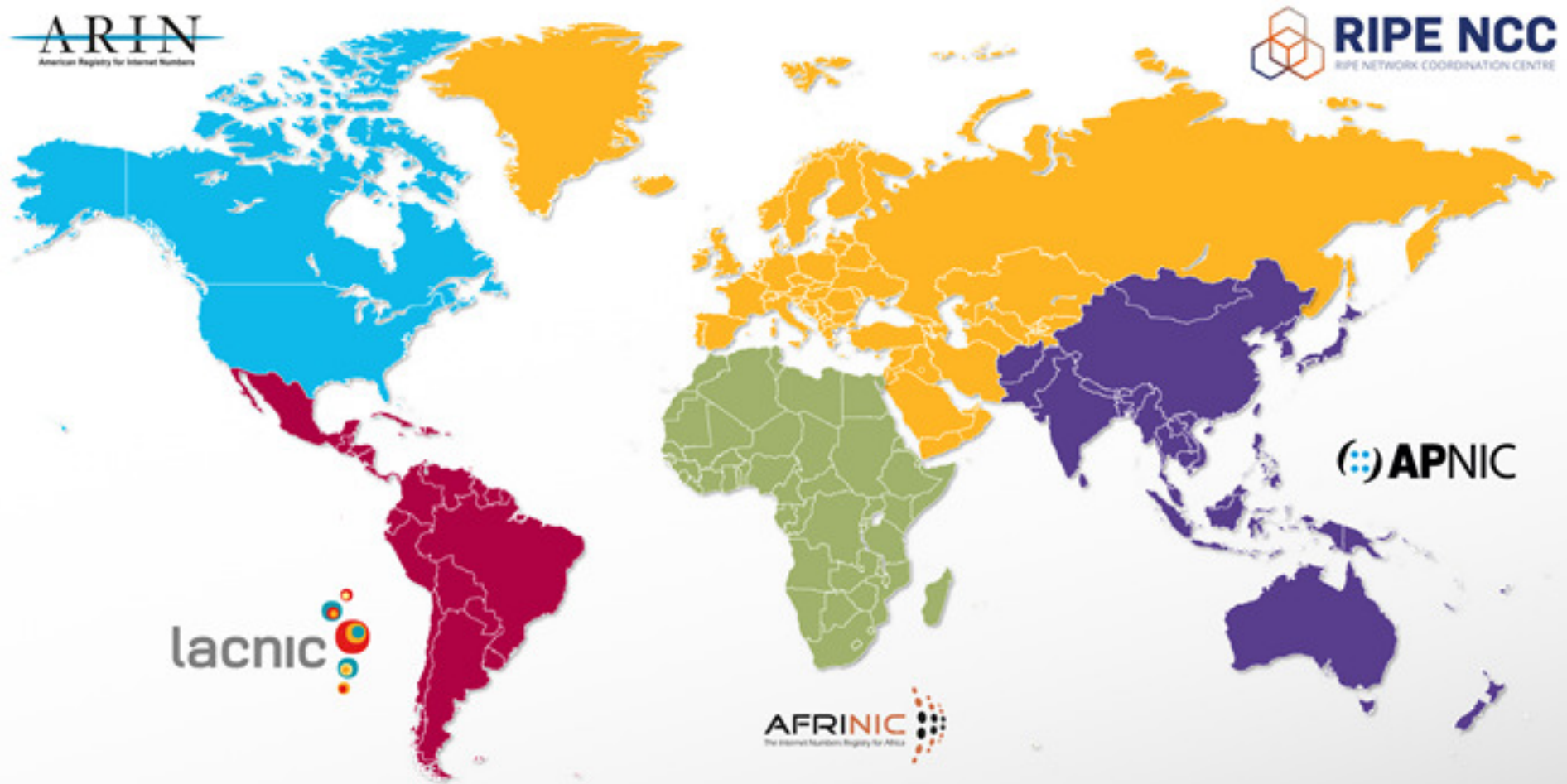
# Densely Populated Regions of IP *Cyberspace*



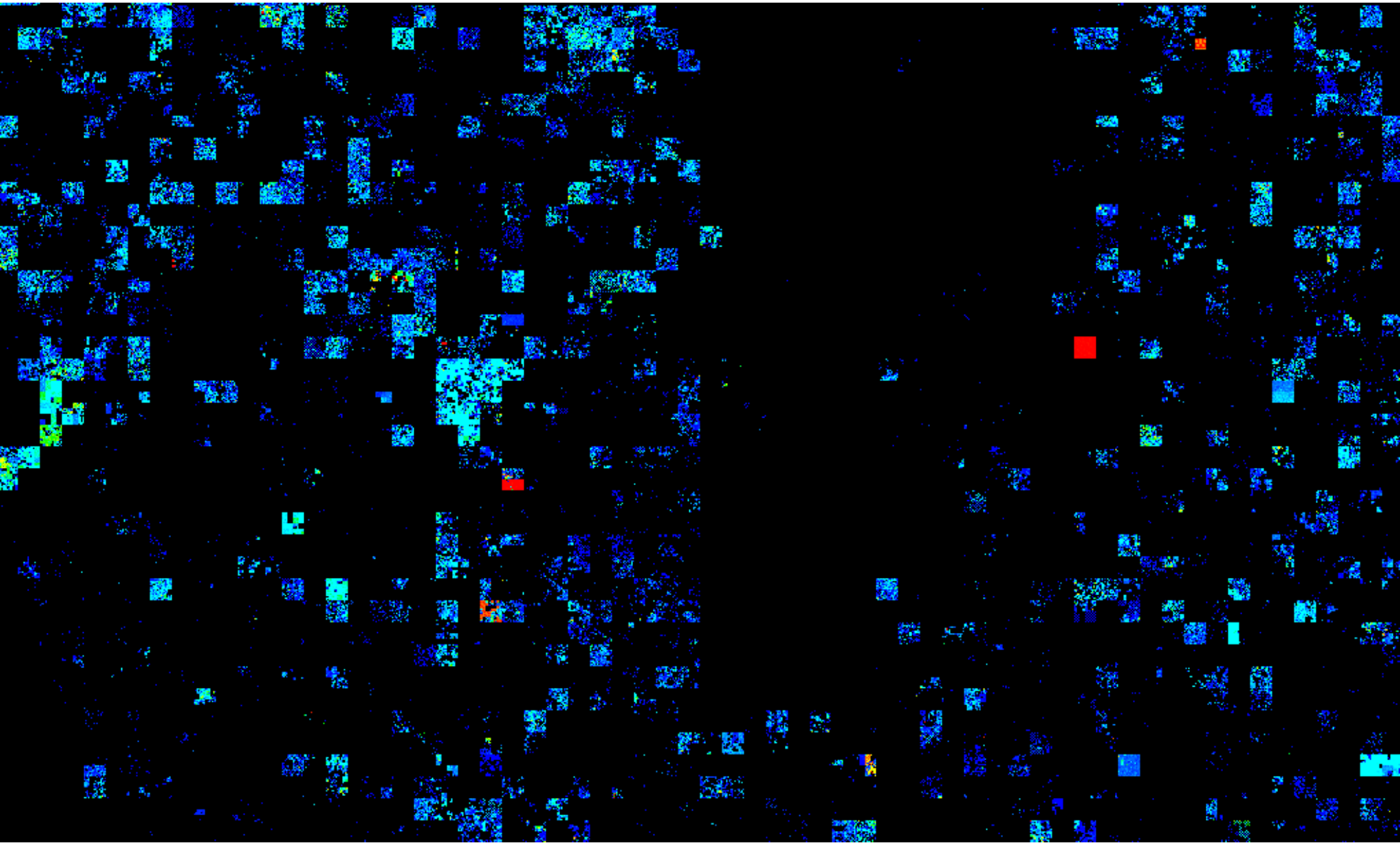


# Global IP Internet Registries:

**RIPE NCC** = *Réseaux IP Européens National Control Centre*

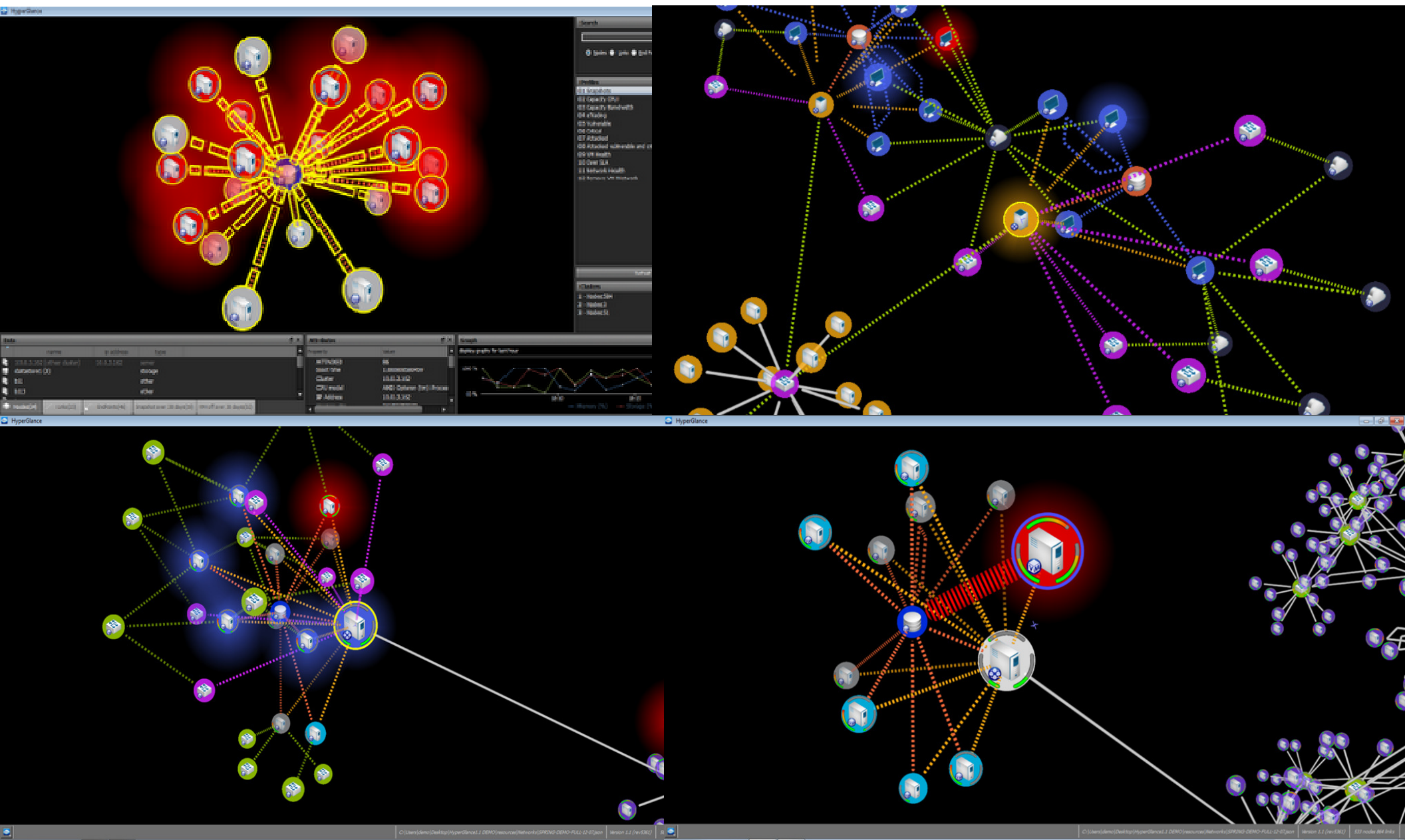


# “Outer Galaxies of Cyberspace” – Other IP Registries

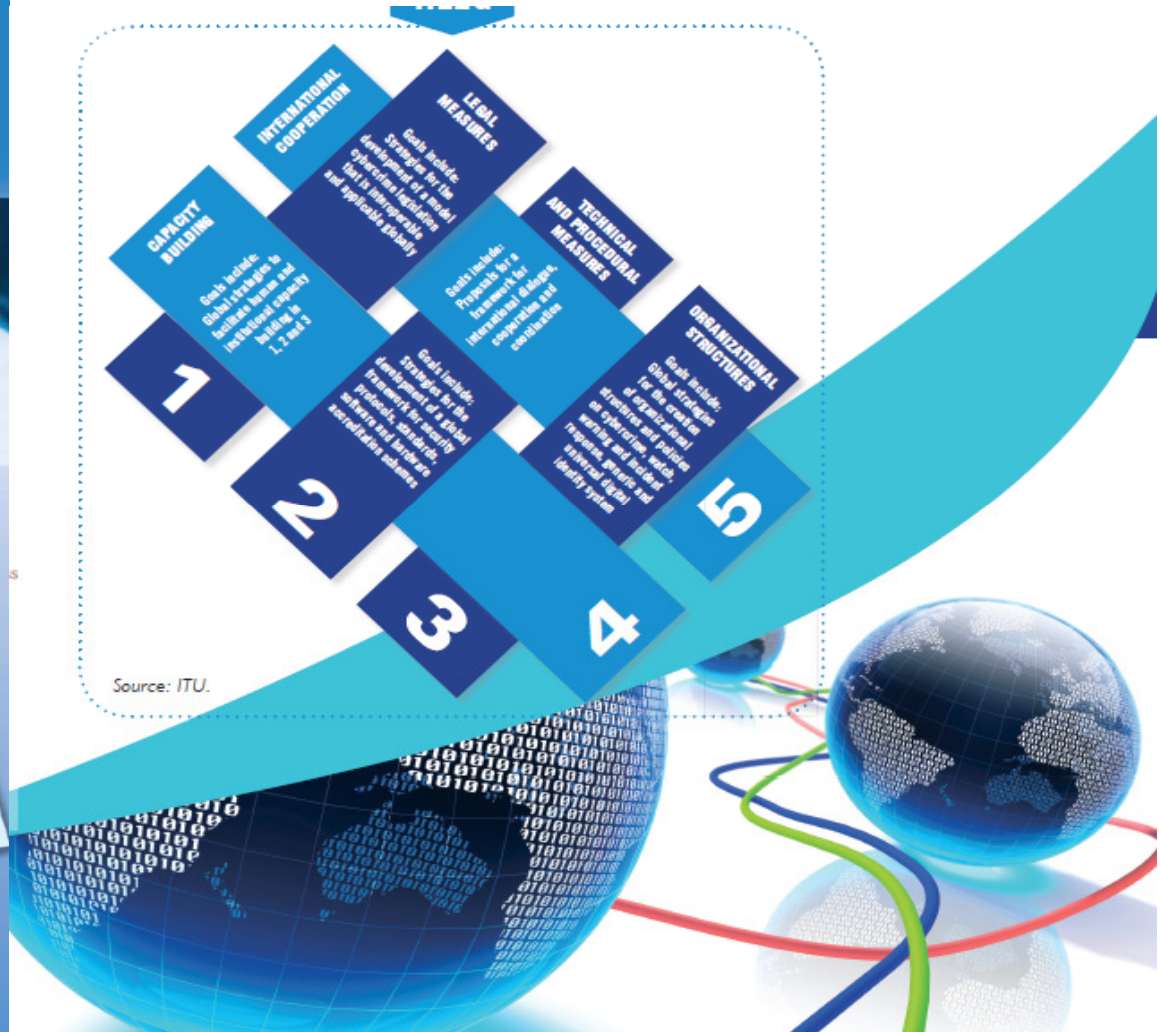




# Smart 3D Network Cyber Simulation: *Hyperglance*



# UN/ITU: High-Level Expert Group – *Global Cybersecurity Agenda* –



Source: ITU.

**The *UN/ITU* Secretary General established “Cybersecurity” as TOP priority!**

## 38<sup>th</sup> International East-West Security Conference

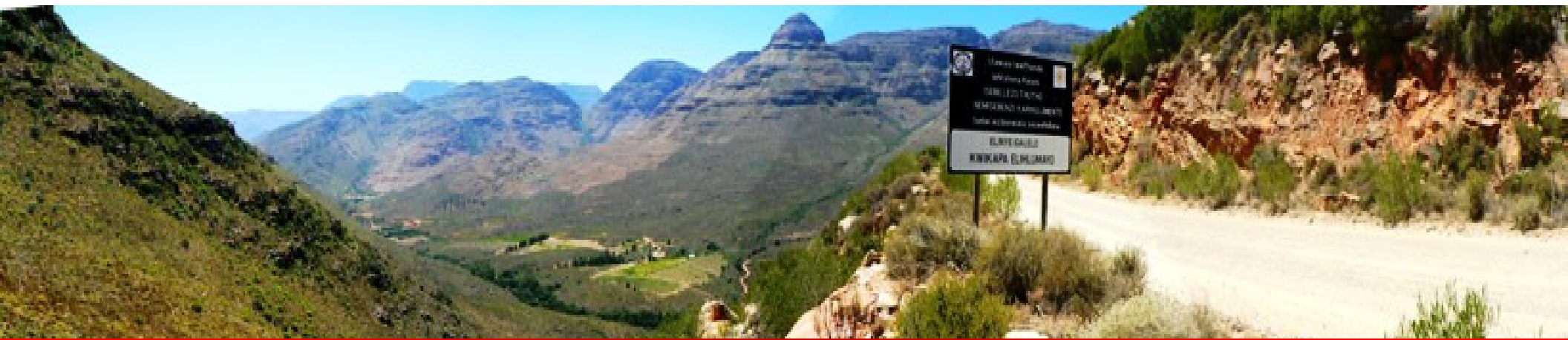
## “Cybersecurity for Critical National Infrastructure”- *Strategy & RoadMap*

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

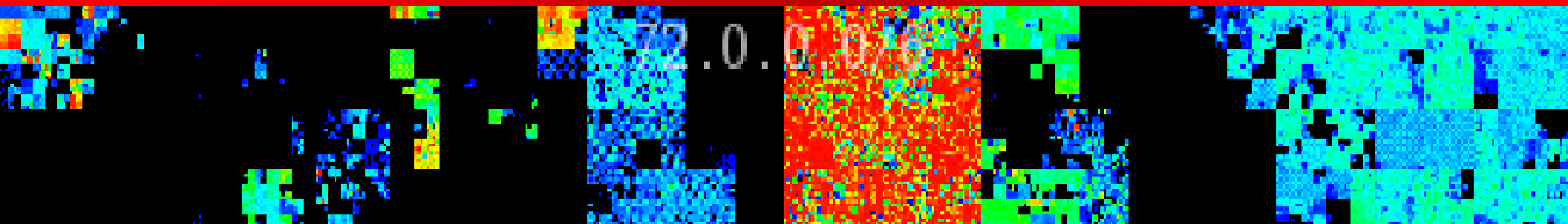
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# *Cyber* Security for *Critical* Infrastructure!



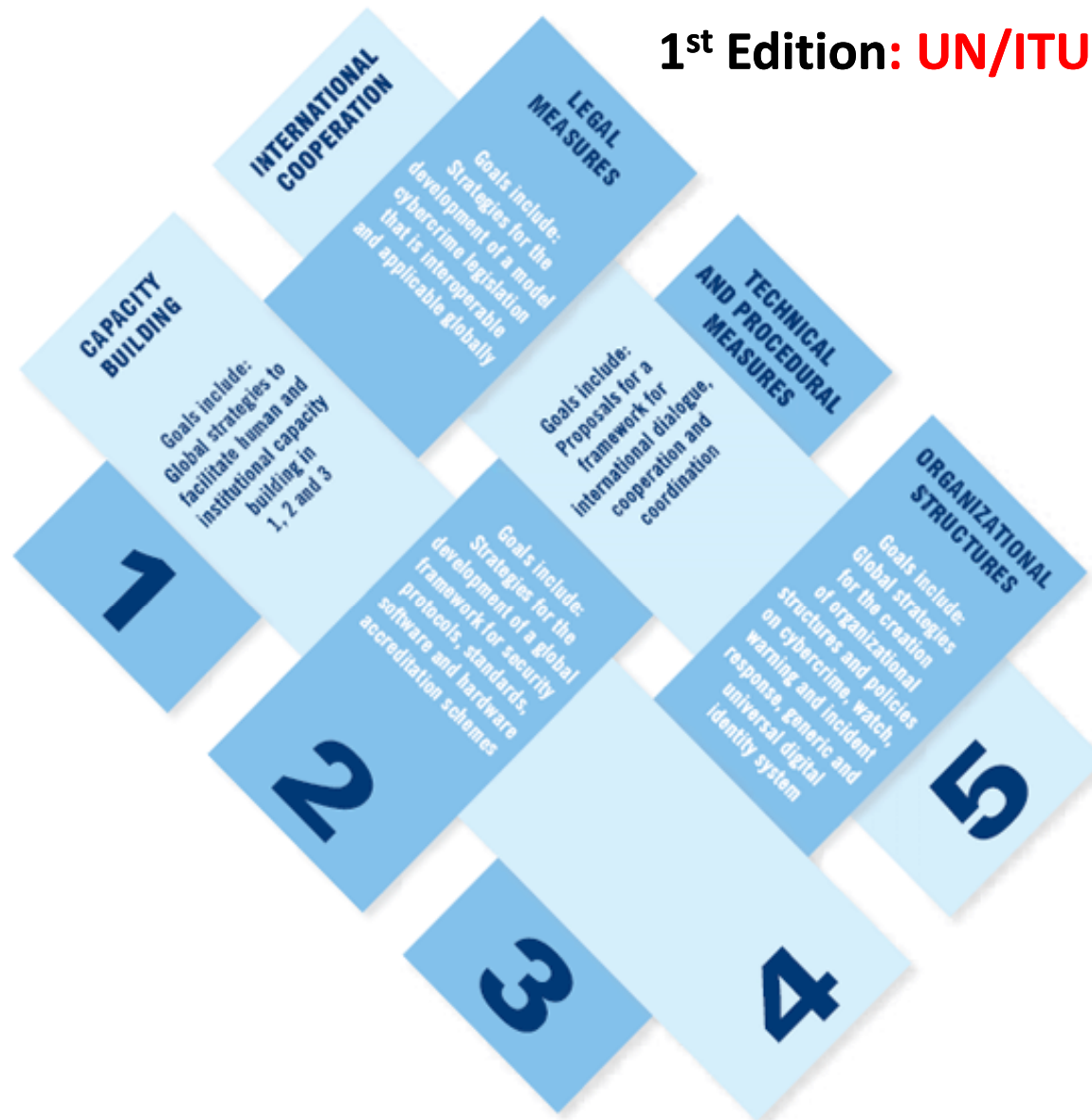
## 2 – UN/ITU *Cyber* Strategy Guide “*Cyber* Security Models”





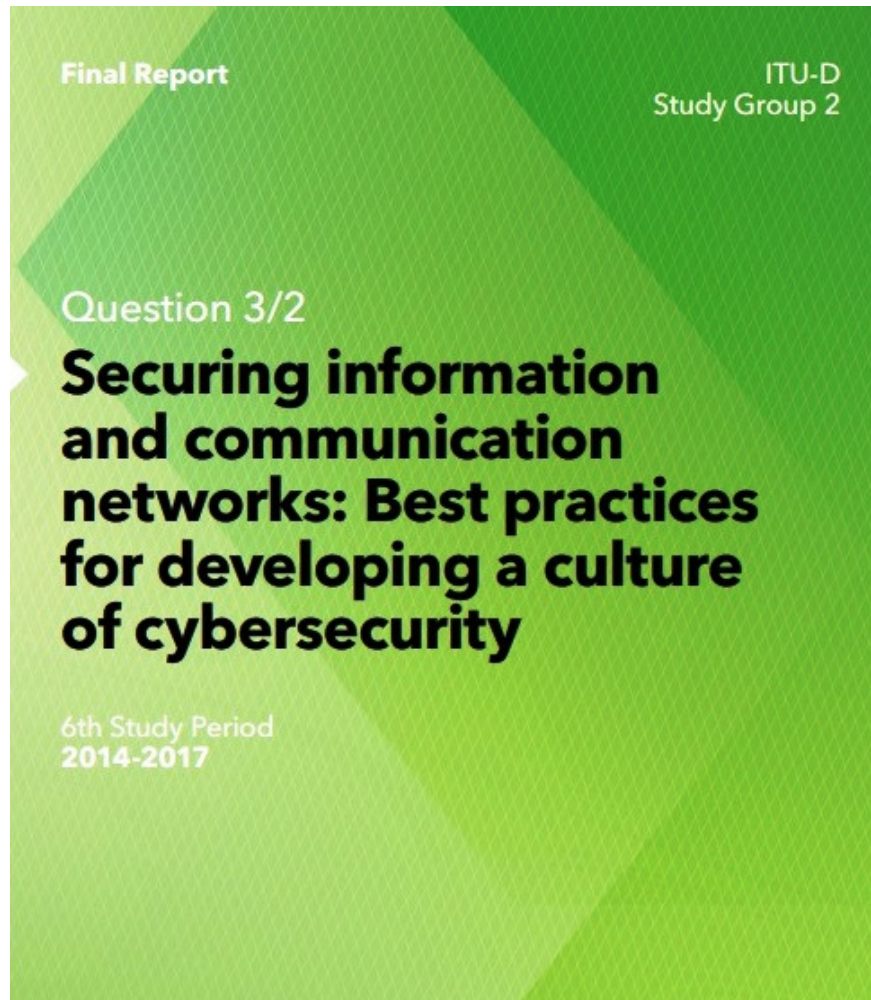
# UN/ITU: Global Cybersecurity Agenda

1<sup>st</sup> Edition: UN/ITU Sept 2011



[www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf)

# UN/ITU Final Report: Securing Info & Comms Networks – Best Cyber Practice!



**Download:** [www.itu.int/pub/D-STG-SG02.03.1-2017](http://www.itu.int/pub/D-STG-SG02.03.1-2017)

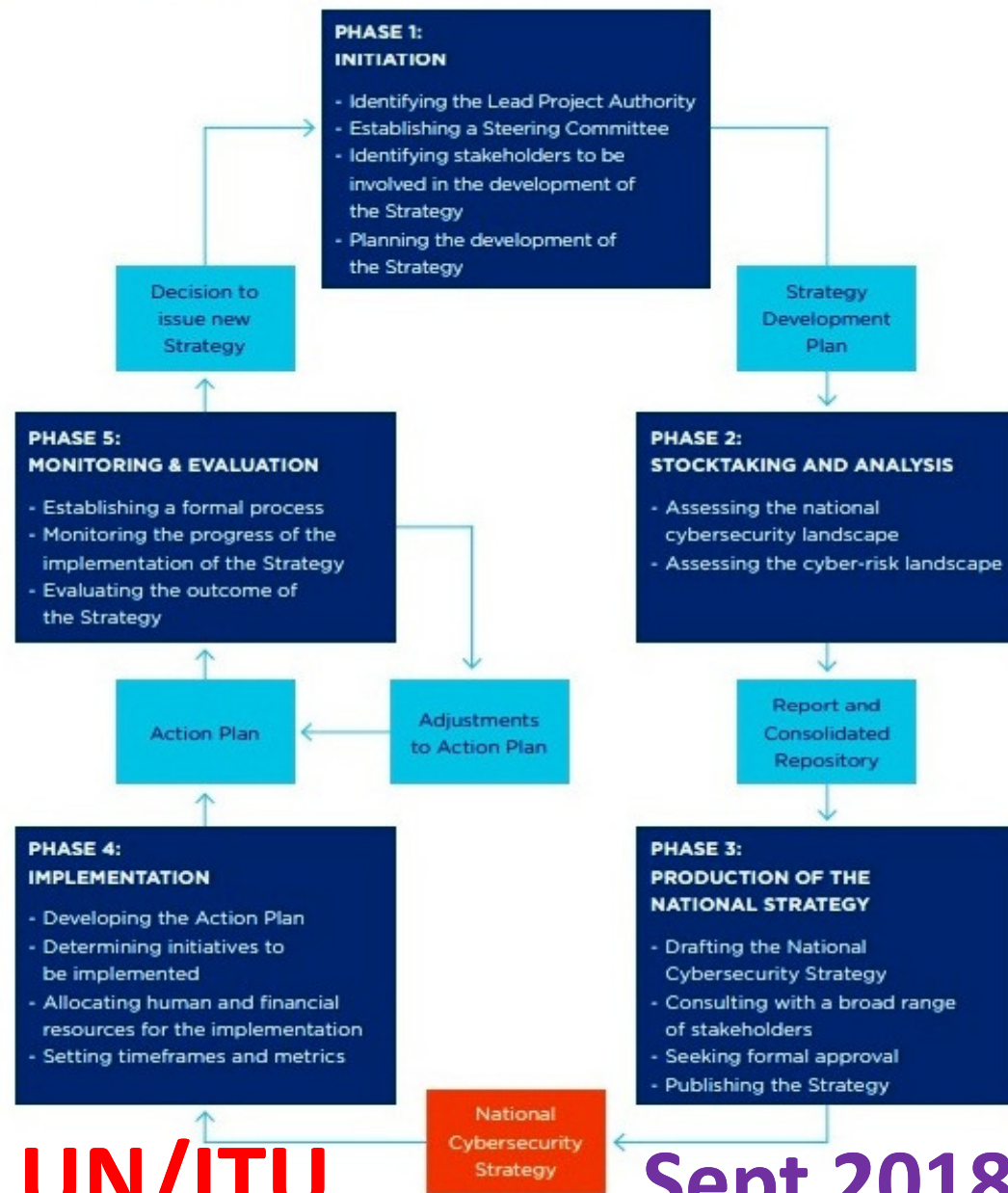


# GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

STRATEGIC ENGAGEMENT IN CYBERSECURITY



Figure 1 - Lifecycle of a National Cybersecurity Strategy



UN/ITU

Sept 2018

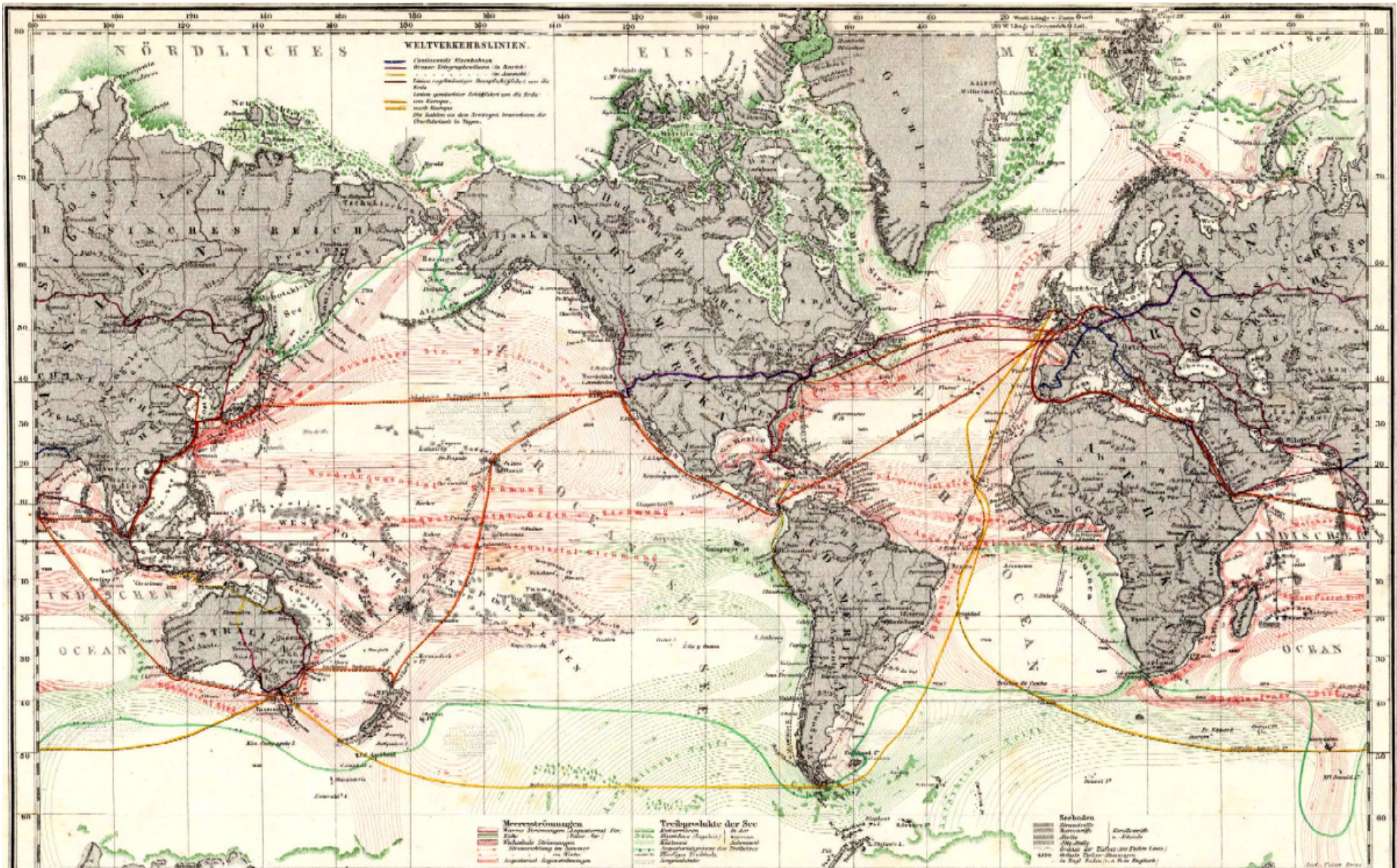
Guide to Developing a National Cybersecurity Strategy

Download: [www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-CYB\\_GUIDE.01-2018-PDF-E.pdf](http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf)





# Worldwide Security in *Cyberspace*!





# Worldwide Security in *Cyberspace*!

- (4) – Capacity Building

- (1) –  
Legal Measures

- (2) –  
Technical  
&  
Procedural  
Measures

- (3) –  
Organisational  
Structures

- (5) – Regional and International Collaboration



# UN/ITU: Global Cybersecurity Agenda – *On-Line*

# G C A

GLOBAL  
CYBERSECURITY  
AGENDA

About GCA

Legal Measures

Technical & Procedural Measures

Organizational Structures

Capacity Building

International Cooperation

DOWNLOAD BROCHURE



**38<sup>th</sup> International East-West Security Conference**

**“Cybersecurity for Critical National Infrastructure” - Strategy & RoadMap**

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# UN/ITU : GCA – The Seven Strategic Goals

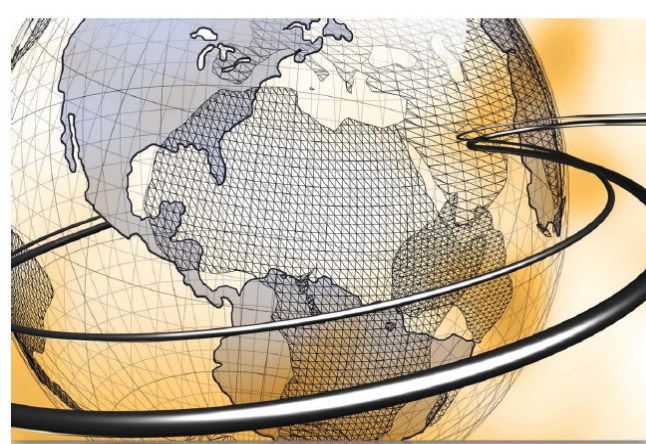
## - *for National & International Cybersecurity* -

### 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 YOUR National Cyber Strategy!***

# United Nations/ITU **Cybersecurity** Guides



## ITU National Cybersecurity/CIIP Self-Assessment Tool

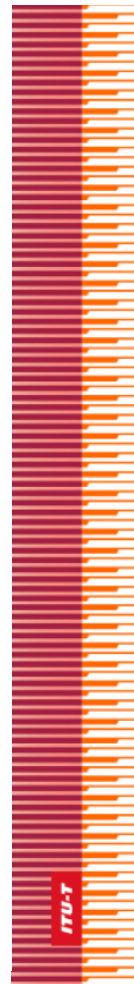
ICT Applications and Cybersecurity Division  
Policies and Strategies Department  
ITU Telecommunication Development Sector

April 2009 Revised Draft

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



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



International Telecommunication Union

## ITU-T

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

## X.1205

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM  
COMMUNICATIONS AND SECURITY

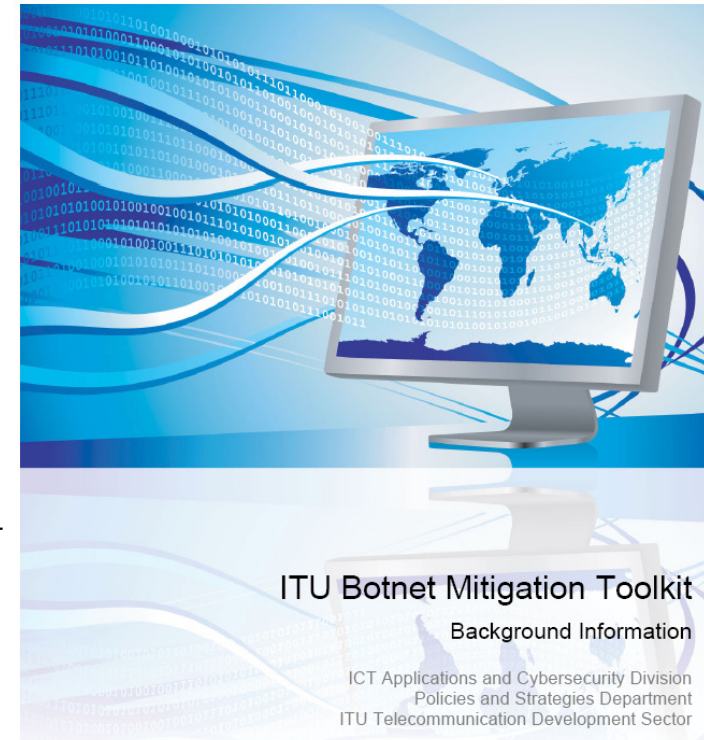
Telecommunication security

### Overview of cybersecurity

### Recommendation ITU-T X.1205



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

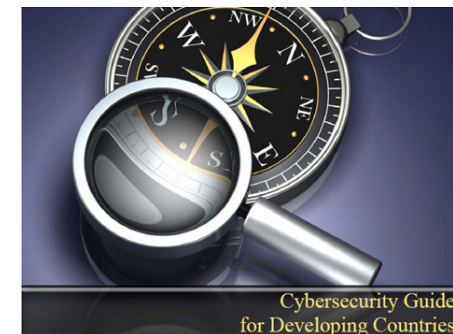


## ITU Botnet Mitigation Toolkit

Background Information

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

January 2008



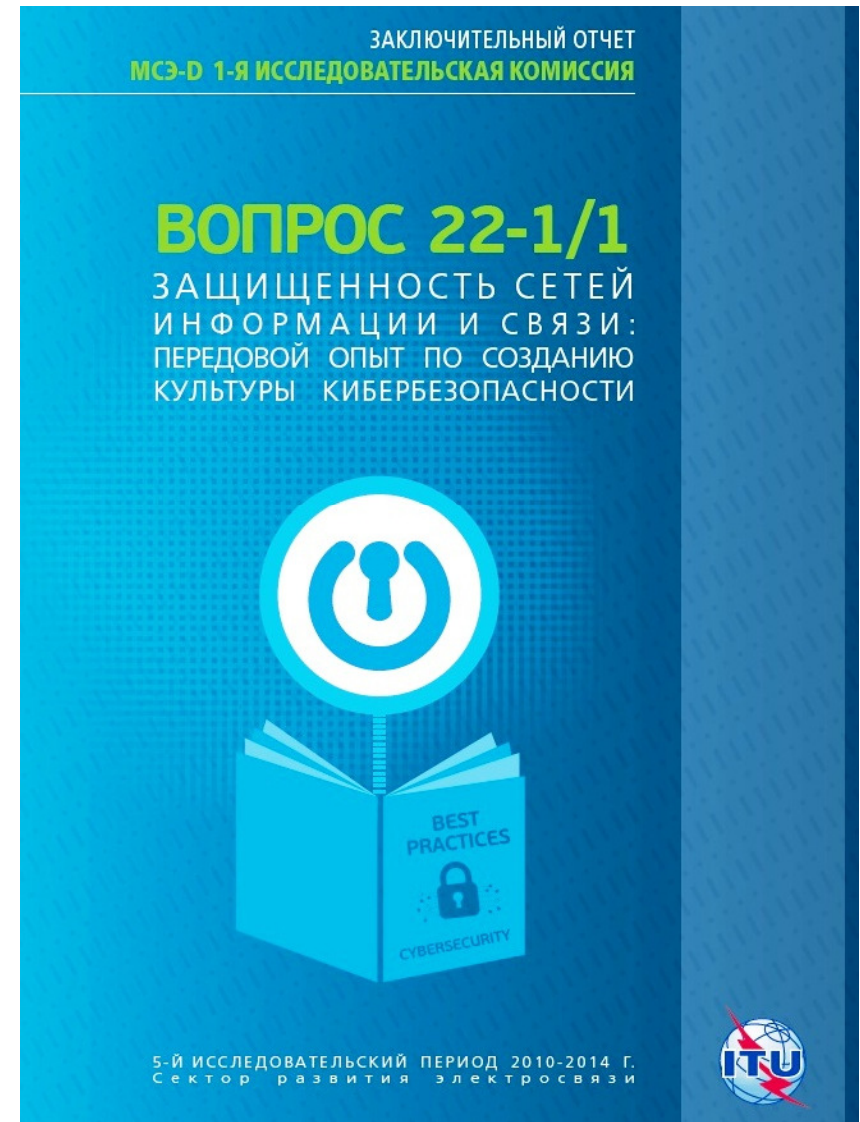
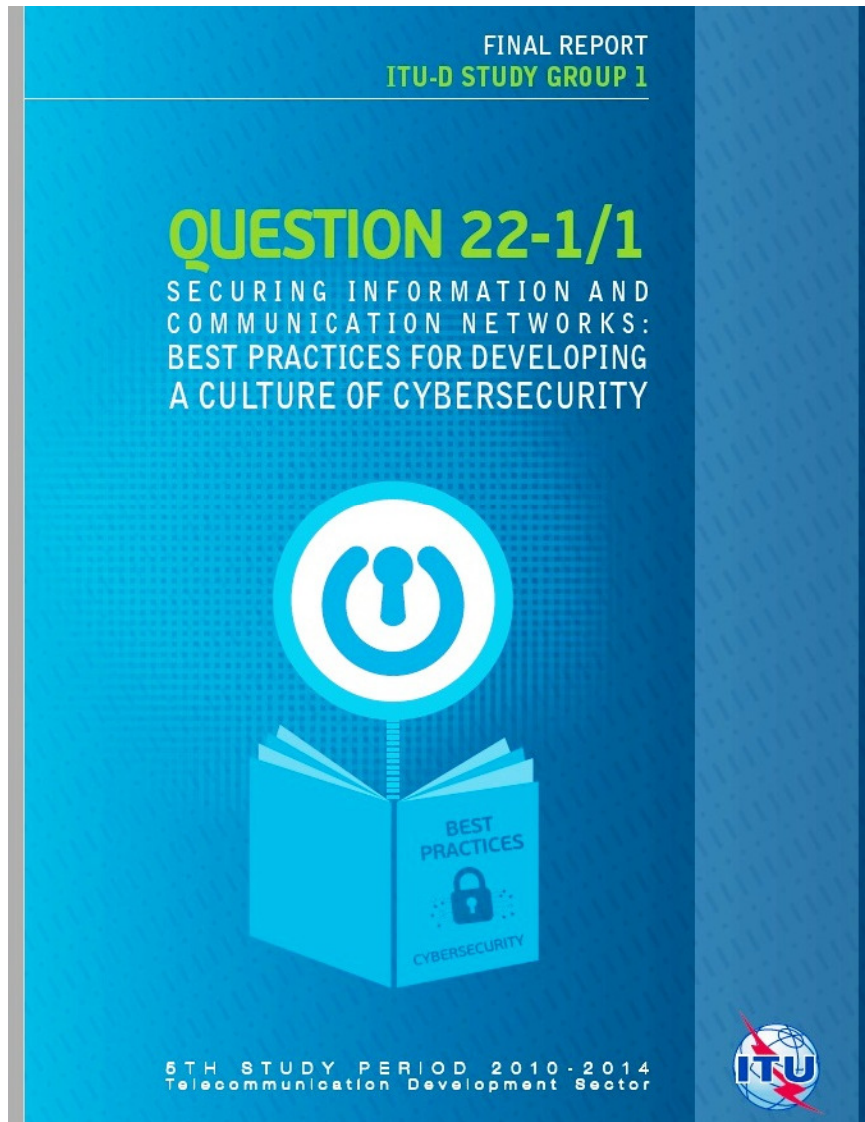
Cybersecurity Guide  
for Developing Countries





# - UN/ITU *CyberSecurity* Agenda -

## Best Practice for CyberSecurity Culture



Link: [www.itu.int/en/publications/](http://www.itu.int/en/publications/)

38<sup>th</sup> International East-West Security Conference

"Cybersecurity for Critical National  
Infrastructure" - *Strategy & RoadMap*

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

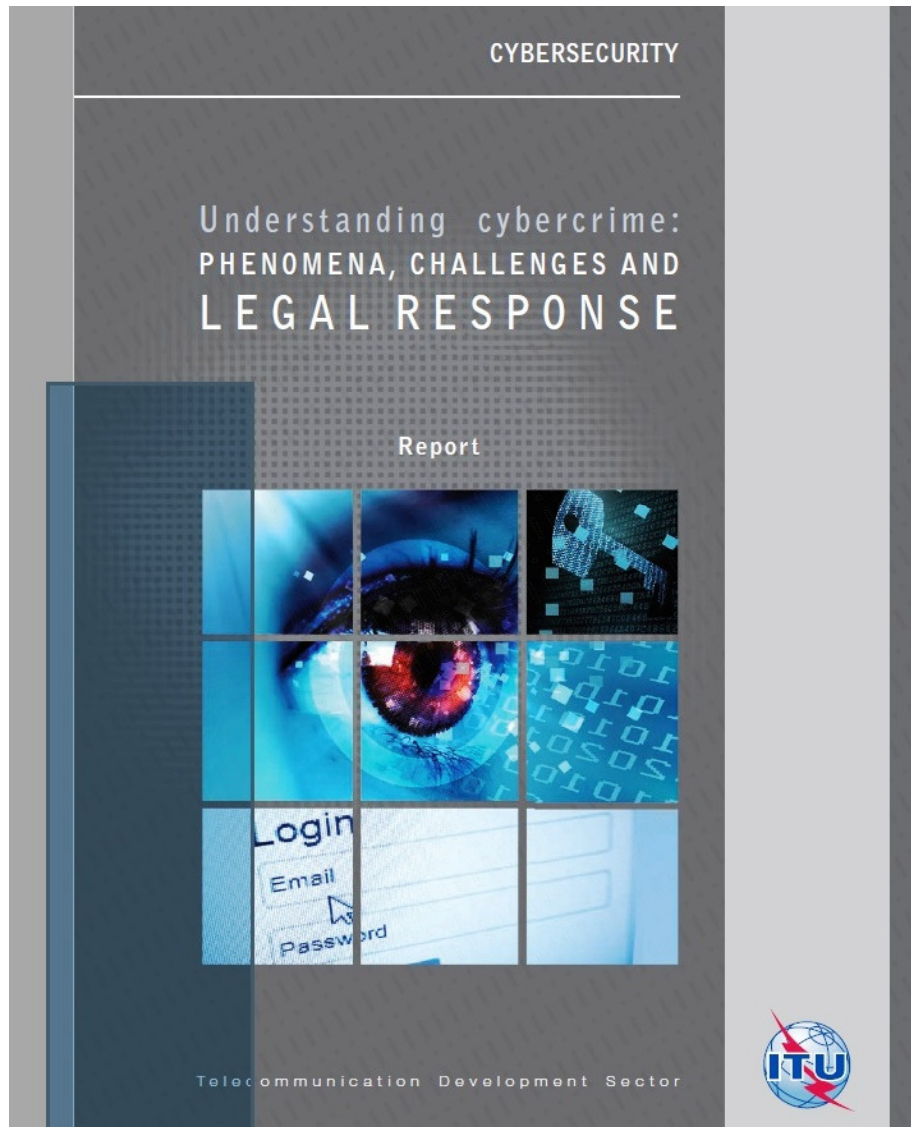
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# - UN/ITU CyberSecurity Agenda -

## Understanding CyberCrime (Eng/Rus)



Link: [www.itu.int/en/publications/](http://www.itu.int/en/publications/)

38<sup>th</sup> International East-West Security Conference

"Cybersecurity for Critical National Infrastructure" - Strategy & RoadMap

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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



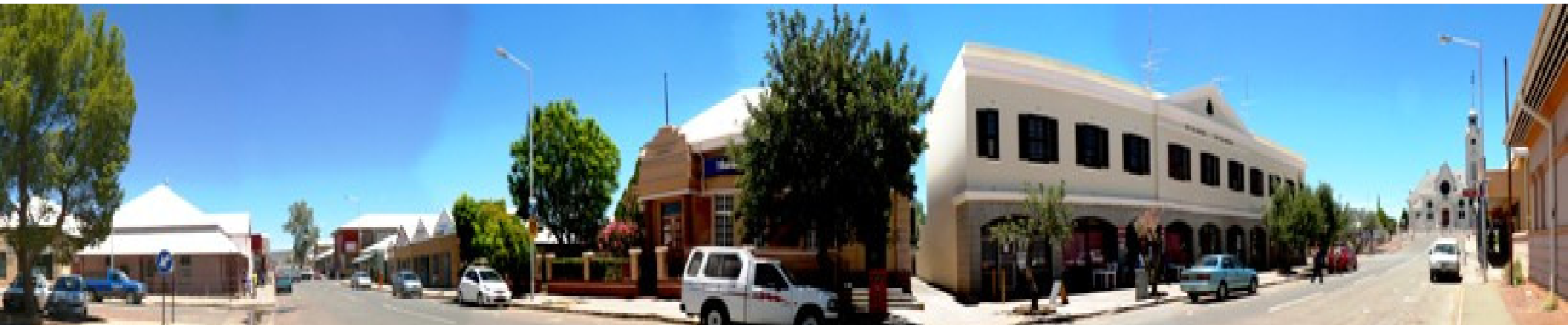
# UN/ITU *National CyberSecurity Strategy* Toolkit (*NCS*) – Global Cyber Partnership



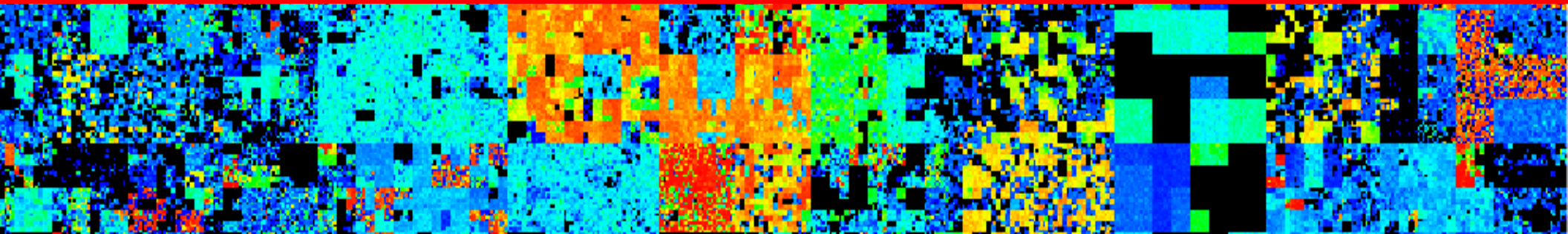
**12 International Partners :** *CyberSecurity Toolkit to help Nations to Design & Implement Effective CyberSecurity Programmes based upon “Best Practice”...*

**Download Link:** [www.itu.int/pub/D-STR-CYB\\_GUIDE.01-2018](http://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018) - Sept 2018

# *Cyber*Security 2018-2025 & *Beyond*!...



## 3- National *Cyber* Security Strategies “Secure **YOUR** Nation”





# UN/ITU: National Cybersecurity Strategies



[www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx](http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx)





# UK CyberSecurity Strategy: 2016 - 2021



## NATIONAL CYBER SECURITY STRATEGY 2016-2021

Defend – Deter - Develop



**5 Year Programme** Launched by UK Chancellor Philip Hammond: **Tuesday 1<sup>st</sup> November 2016**

“Cybersecurity for Critical National Infrastructure” - *Strategy & RoadMap*  
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# US Government : *Office of Cybersecurity*



- Following 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*

# Canadian Government : **CCIRC**

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



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



# Australian Government : **CSPC**

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



Cyber Security Operations Centre (CSOC)



# Malaysian Government: *MOSTi*

The screenshot shows the official website of CyberSecurity Malaysia, an agency under MOSTi. The header includes the agency's logo, the date '15 August 2010 13:56:32', a search bar, and a navigation menu with links to Home, About Us, Our Services, Events, Knowledge Bank, Community, Media Centre, and Contact Us. The main content area is titled 'Securing Our Cyberspace' and features a large graphic of orange building blocks forming a path. Below this, there is a grid of service tiles: 'Upcoming Event' (CSM-ACE 2010), 'Financial Assistance' (MyCC), 'Training' (Training Programs), 'Cyber999' (a service for handling incidents), 'Registration' (Malaysia Information Security Professional), 'Online Survey' (National Strategy for Cyber Security Acculturation and Capacity Building Program), 'Media' (CyberSecurity Malaysia Corporate Video), 'Media' (Cyber Security Song), and 'CyberSAFE Ambassador' (Join Us CyberSAFE Ambassador Program). A 'News Coverage' section at the bottom lists three articles from 06/08/2010: 'Critical Agencies Told To Get ISMS Certification To Face Cyber Threat', 'X-MAYA 3: BENCHMARKING THE NATIONAL CYBER CRISIS MANAGEMENT PLAN', and 'Protecting Agencies From Cyber Attacks'. Social media icons for Facebook and Twitter are visible on the left, and a 'MORE ...' link is at the bottom right.



# Singapore Government : *SITSA*



The screenshot shows the Singapore Government website with the SITSA press release. The header includes the Singapore Government logo and navigation links. The left sidebar lists various categories like News, Events, and Publications. The main content area features a search bar and a list of press releases, with the most recent one dated 30 September 2009. The press release text describes the establishment of SITSA to safeguard Singapore against IT security threats.

**30 September 2009**

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

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

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

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

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

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

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

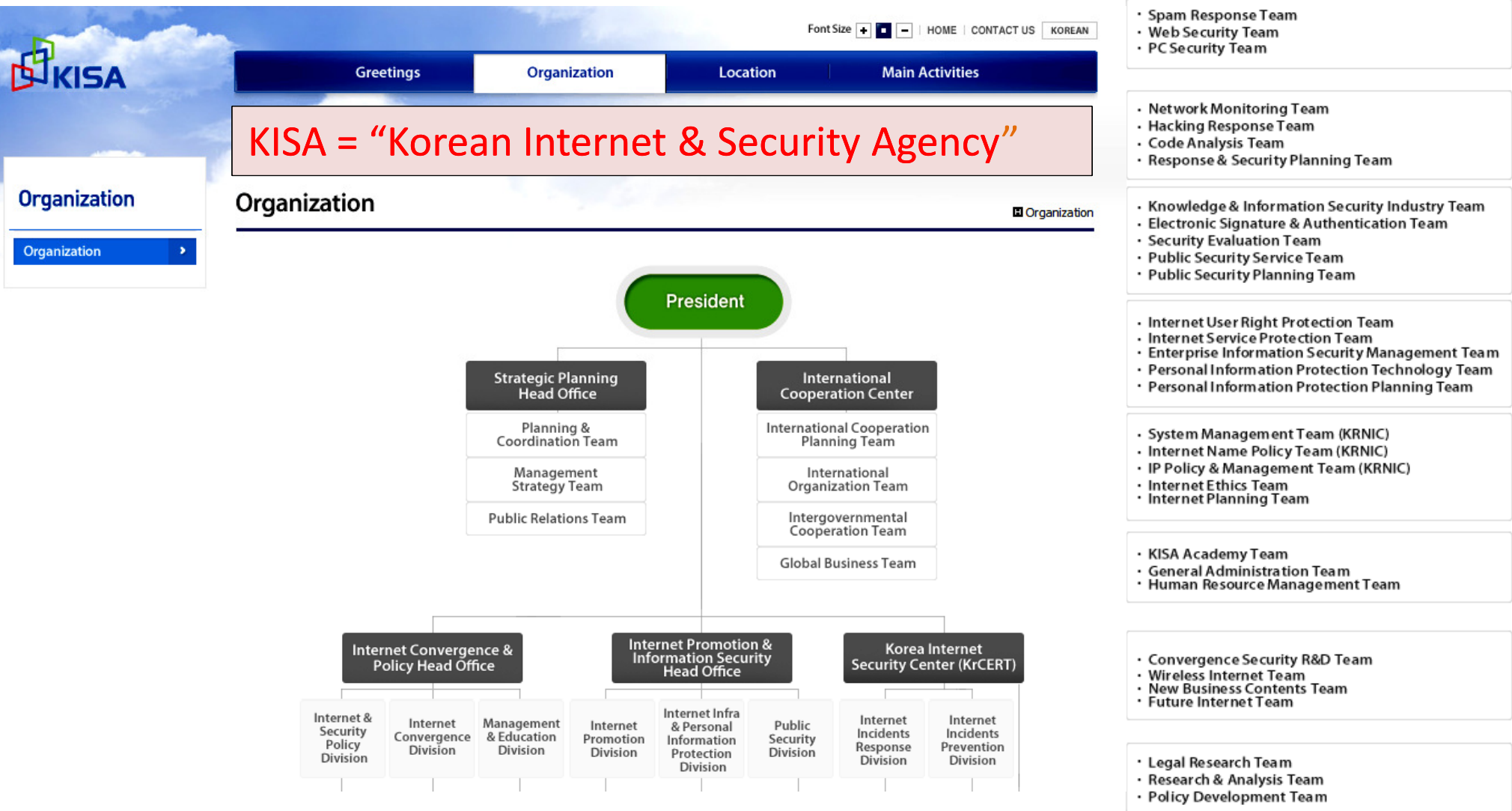


**"Cybersecurity for Critical National Infrastructure" - Strategy & RoadMap**  
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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



# South Korea Government: **KISA**





# Euro Network & Info Security Agency: **enisa**



[Site Map](#) | [Accessibility](#) | [Contact](#) | [Legal Notice](#)

Search Site

[Home](#) | [About ENISA](#) | **[Our Activities](#)** | [Publications](#) | [Press & Media](#) | [Events](#) | [Public Procurement](#) | [Recruitment](#)

you are here: [home](#) → [our activities](#) → [cert](#)

## CERT

[What's new](#)

[Overview](#)

[Support](#)

[Other work](#)

[Events](#)

[About us](#)

## 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



**"Cybersecurity for Critical National Infrastructure" - Strategy & RoadMap**

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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

# National Cybersecurity for Latin America & Caribbean:

## - CITE/CICTE/OAS -

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

- **CITE** = Inter-American Telecomms 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 \(Bolivarian Republic of\)](#)



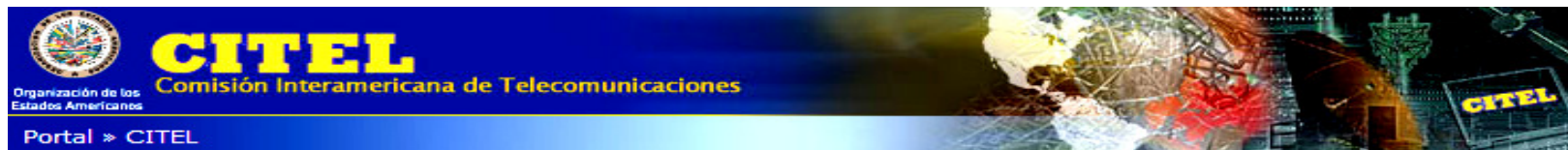
[Colombia](#)



[Guyana](#)



[Saint Kitts and Nevis](#)



"Cybersecurity for Critical National Infrastructure" - *Strategy & RoadMap*  
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# National **Cybersecurity** Agencies: Common Roles

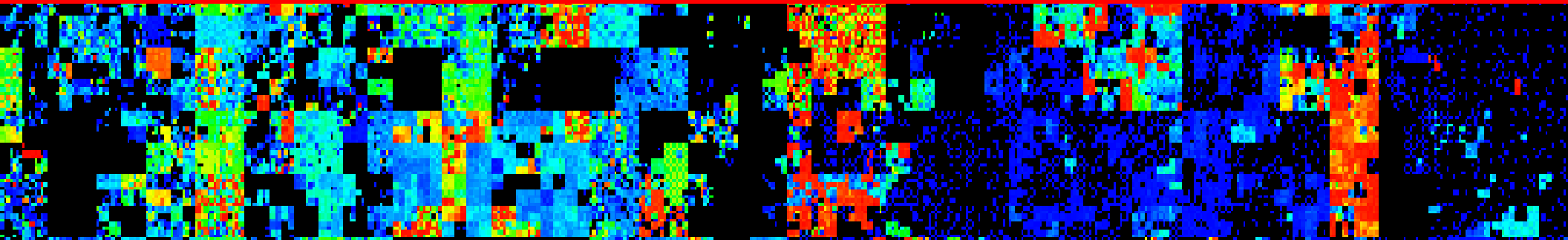
- Common roles and responsibilities for all these National Cyber Agencies:
  - **Cyber Alerts:** Management of the National Response to Cyber Alerts, and Attacks
  - **Education:** Co-ordination of the National Awareness and Skills Training Programmes
  - **Laws:** Leadership role in the development and approval of new cyber legislation
  - **Cybercrime:** Facilitation for building a National Cybercrime or e-Crime Unit
  - **Standards:** Setting the national cybersecurity standards and auditing compliance
  - **International:** Leadership in the promotion of international partnerships
  - **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 consider a couple of Practical National CyberSecurity Case Studies from the Countries of **Armenia** and **Georgia**!....*

# *Cyber* Security for *Critical* Infrastructure!



## 4 –Case Studies: Georgia & Armenia “Practical *Cyber* Projects”





# Personal *“Eastern Experiences”*: 1991 - 2014



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

**Projects including *Cybersecurity, eGovernance & Internet Solutions***

# Cybersecurity for Armenia and Georgia

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



## "Roadmap for Real-Time Armenia"

\*E-Government, E-Commerce and E-Security\*



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

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

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

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

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



## "Real-Time Georgia"

\*Securing Government & Enterprise Operations\*



Dr David E Probert

VAZA International

1<sup>st</sup> Georgian IT Innovation Conference

Tbilisi : 29<sup>th</sup> & 30<sup>th</sup> October 2008

1

Author : Dr David E Probert

Copyright : [www.vaza.com](http://www.vaza.com) – Oct 2008

"Cybersecurity for Critical National Infrastructure"- *Strategy & RoadMap*  
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# Cybersecurity *for the* Georgian Parliament



**Critical Infrastructure Audit during UN Cybersecurity Mission: Georgian Parliament**

**38<sup>th</sup> International East-West Security Conference**

**"Cybersecurity for Critical National  
Infrastructure" - Strategy & RoadMap**  
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©

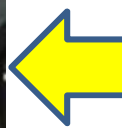


# Timeline of “Cyber” Activities in Georgia

- **1994/1995** – Specification of 1<sup>st</sup> WebSite for the Georgian Parliament with CIO – Nodar Mosashvili - ([www.parliament.ge](http://www.parliament.ge))
- **2007** – Full Security Audit for Georgian Parliament with new CIO – Merab Gotsiridze (*Classified EU Report for EU/TACIS*)
- **2008** – Invited Presentation on “Real-Time Georgia” at the 1<sup>st</sup> GITI Conference (Georgian IT Innovations)
  - Link: [www.valentina.net/vaza/GITI.pdf](http://www.valentina.net/vaza/GITI.pdf)
- **2009** – Cybersecurity Audit of Georgian Government Ministries & Critical Sectors (*Classified Report for UN/ITU Programme*)
- **2010** – Invited Presentation on Integrated National Security (Cyber-Vardzia) at the 3<sup>rd</sup> Regional GITI Conference in Tbilisi
  - Link: [www.valentina.net/GITI2010/CyberVardzia-PaperV7.pdf](http://www.valentina.net/GITI2010/CyberVardzia-PaperV7.pdf)



# From 1<sup>st</sup> Parliament.Ge WebSite in 1994 to National Georgian **CyberSecurity** in 2008...



Opening Discussions in Moscow – 1994 – to Build 1<sup>st</sup> Government Website for Georgian Parliament



Dinner Reunion in Tbilisi – 2008



38<sup>th</sup> International East-West Security Conference

“Cybersecurity for Critical National Infrastructure”- *Strategy & RoadMap*

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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



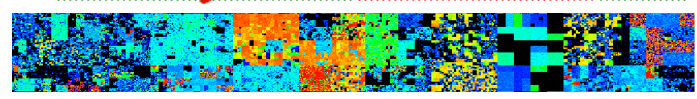
# Case Study: White Paper: 21<sup>st</sup> C Georgia – “Cyber-Vardzia”

\* 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)





# Georgian IT Conference – Tbilisi - 2008





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





# Mt Kazbek (5033metres) - Caucasus



© Dr David E Probert

# Sunset across the Kakhetian Steppes





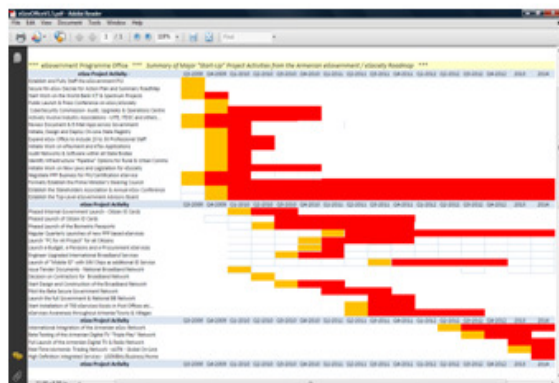
# Timeline of “Cyber” Activities in Armenia

- **2008** – Discussions with Armenian Delegation at the First Regional IT Innovation Conference (GITI - Tbilisi, Georgia)
- **2009** – *Spring* – Invited Keynote Presentation at National IT Seminar, and meetings with Minister of Economy, Central Bank of Armenia and CAPS/USAID Programme
- **2009** – *Summer* – National Programme & RoadMap on eGovernance, eCommerce and Cybersecurity (USAID)
- **2012** – *Summer* – Invited CyberSecurity & eGovernance MasterClasses @ UITE DigiTec Conference - Yerevan



## “Roadmap for Real-Time Armenia”

*\*E-Government, E-Commerce and E-Security\**



### *“Increasing Business Opportunities for the Armenian ICT Cluster through the development of E-Government, E-Commerce and E-Security”*

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

## Executive Summary

**a) MISSION:** This final report summarises and documents the outcomes from my 21 day Mission to Armenia. The primary tasks, funded by USAID/CAPS Armenia were to support the Ministry of Economy in the further development of the National eGovernment RoadMap, as well as providing expert advice in the area of the proposed “Triple Play” Broadband Network, Cybersecurity, eGovernance, Public-Private Partnerships (PPP), ICT Vertical Clusters and e-Gov Interoperability Standards. During the course of this work, I conducted an extensive review of all previous materials including an analysis of the experience “Best Practices” of more than 20 other countries.

**b) ANALYSIS:** This work was challenging since it required the practical integration and prioritization of a diverse range of both partially funded and proposed projects. A key section within the report is the overall integrated 5 year eGovernment RoadMap and supporting Project Spreadsheet. The successful implementation of such a long term multi-dimensional programme will require the establishment of an eGovernment Programme Office with a full range of business & technical skills

**Final Report:** [www.slideshare.net/DrDavidProbert/realtimearmenia](http://www.slideshare.net/DrDavidProbert/realtimearmenia)

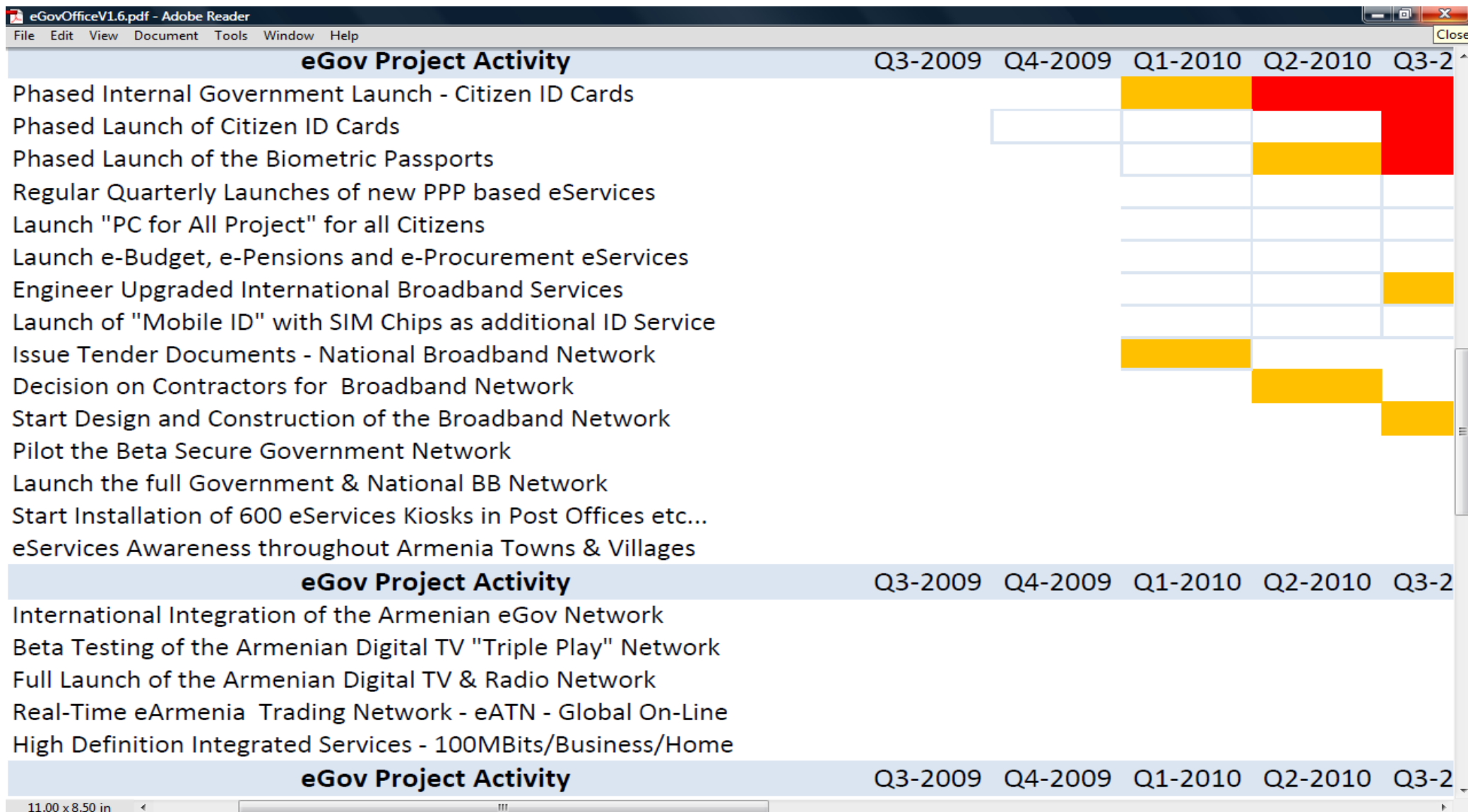
“Cybersecurity for Critical National Infrastructure”- *Strategy & RoadMap*  
Nice, France – 5th/6th Nov 2018

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





# eGovernance RoadMap for Armenia: 2009 - 2014



"Cybersecurity for Critical National Infrastructure" - Strategy & RoadMap

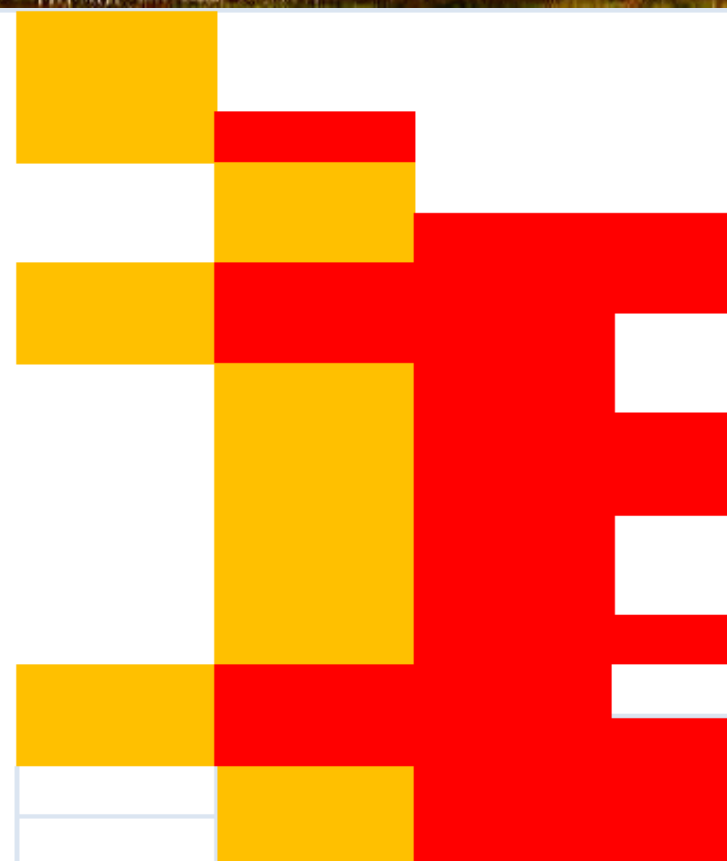
Nice, France - 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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



# **“Security” - Dual Summits of Mt Ararat - “Growth”**

Establish and Fully Staff the eGovernment PIU  
Secure RA eGov Decree for Action Plan and Summary RoadMap  
Start Work on the World Bank ICT & Spectrum Projects  
Public Launch & Press Conference on eGov/eSociety  
CyberSecurity Commission- Audit, Upgrades & Operations Centre  
Actively Involve Industry Associations - UITE, ITDSC and others...  
Review Document & E-Mail Apps across Government  
Initiate, Design and Deploy On-Line State Registry  
Expand eGov Office to include 20 to 30 Professional Staff  
Initiate Work on ePayment and eTax Applications  
Audit Networks & Software within all State Bodies  
Identify Infrastructure "Pipeline" Options for Rural & Urban Comms  
Initiate Work on New Laws and Legislation for eSociety  
Negotiate PPP Business for PKI/Certification eService  
Formally Establish the Prime Minister's Steering Council  
Establish the Stakeholders Association & Annual eGov Conference  
Establish the Top-Level eGovernment Advisory Board



eGov Project Activity

Q3 2009 Q4 2009 Q1 2010 Q2 2010



# USAID eGovernance and Cybersecurity Mission: *Mt Aragats – South Summit (3879m) – Armenia*



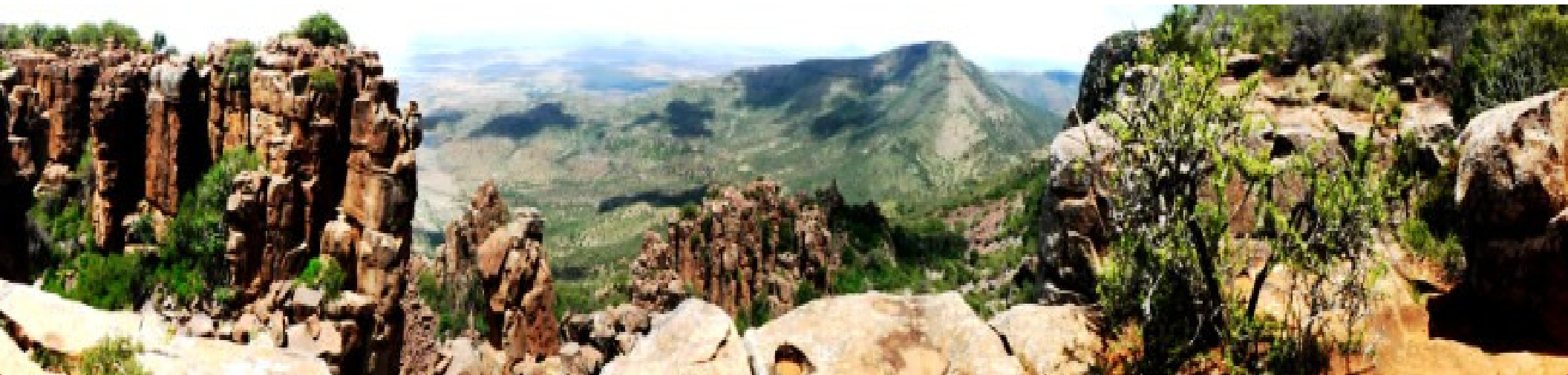
# Mt Ararat from the Air (5137Metres)



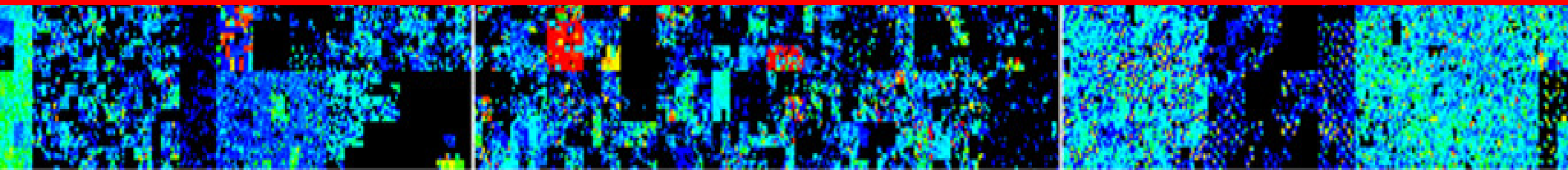
Yerevan (Armenia) to Tbilisi (Georgia): 108 miles – 20 mins



# *Cyber* Security for *Critical* Infrastructure!



## 5 – TOP 10 Critical National Sectors “Secure YOUR Sector”



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

- ***Birth of CNI:*** Early proposals appeared around 20 to 25 years ago, during the mid-1990s, after birth of commercial internet
- ***International discussions*** from G8, OECD and EU around 15 to 20 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 10 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.



# TOP 10 Critical National Sectors

1: Financial Services	2: Emergency Services	3: Telecomms & IT Services
4: Transport, Ports & Hubs	5: Government & Defence	6: Healthcare & Food Sector
7: Chemical & Oil Industry	8: Civil Nuclear & Space Sector	9: Energy & Water Utilities

**UK, USA & European Governments all provide Models for Critical Sectors!**

***Our Table lists the TOP 10 Sectors that require Enhanced CyberSecurity!***

# ***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
- ***Telecommunications, Mobile & IT Services:***
  - Interception of wired & wireless communications, and penetration of secure government & military communications networks
- ***Transportation, Ports, Hubs & Tourism:***
  - Cyber Terrorism against airports, air-traffic control, coach/train transport hubs, & malicious penetration of on-line travel networks
- ***Energy & Water Utilities***
  - Manipulation and disruption of the national energy grid & utilities through interference of the process control network (SCADA)

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



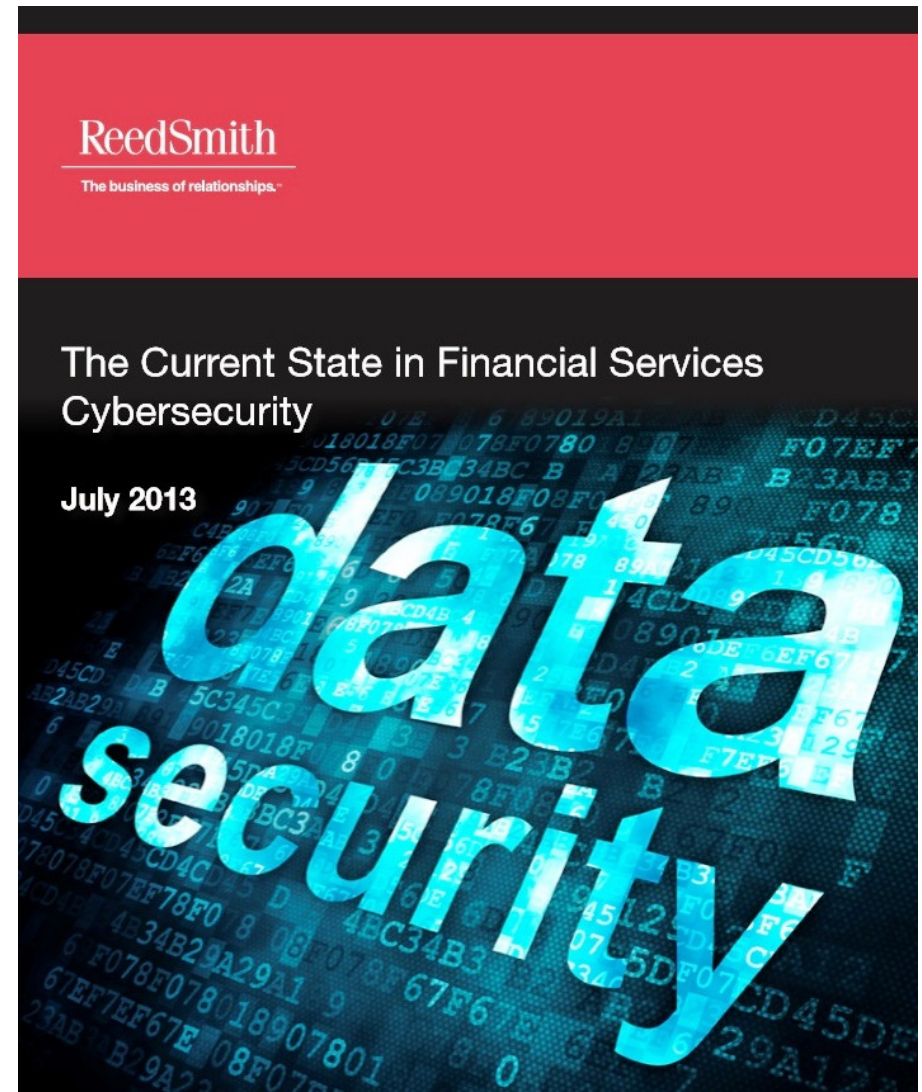
# Cybersecurity for *Banking & Finance*



**New York State**

**Department of Financial Services**

*Report on Cyber Security in the Banking Sector*



**"Cybersecurity for Critical National Infrastructure"- Strategy & RoadMap**  
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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



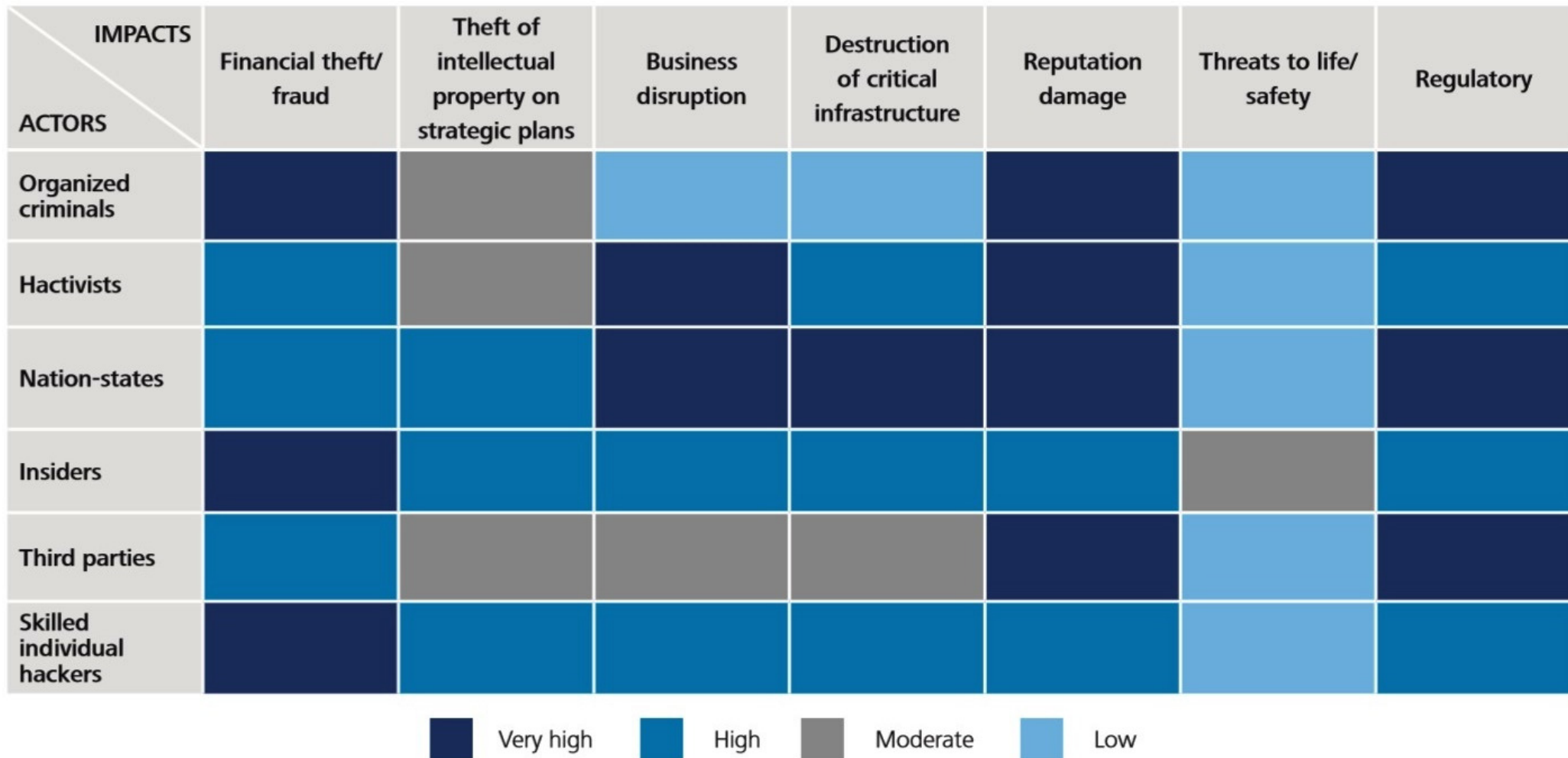
# Banking & Finance Sector: *Cybersecurity Threats*

- *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



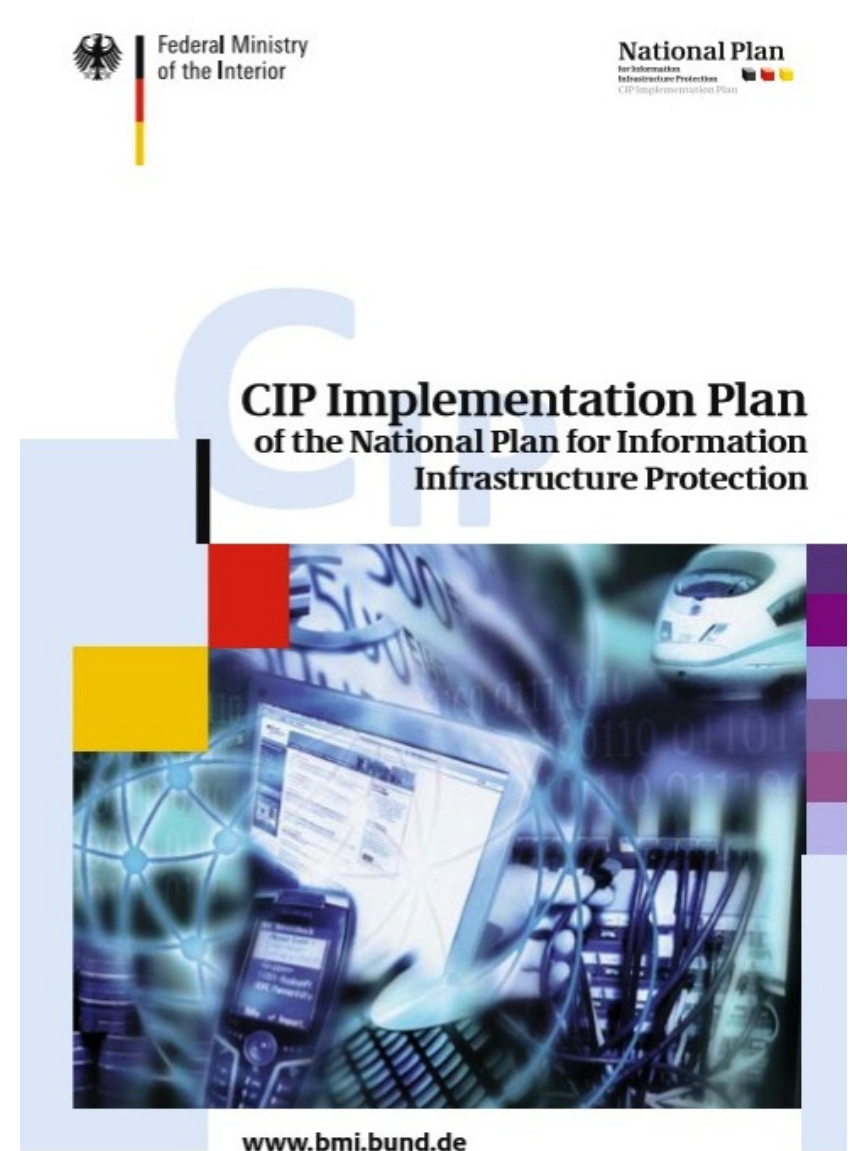
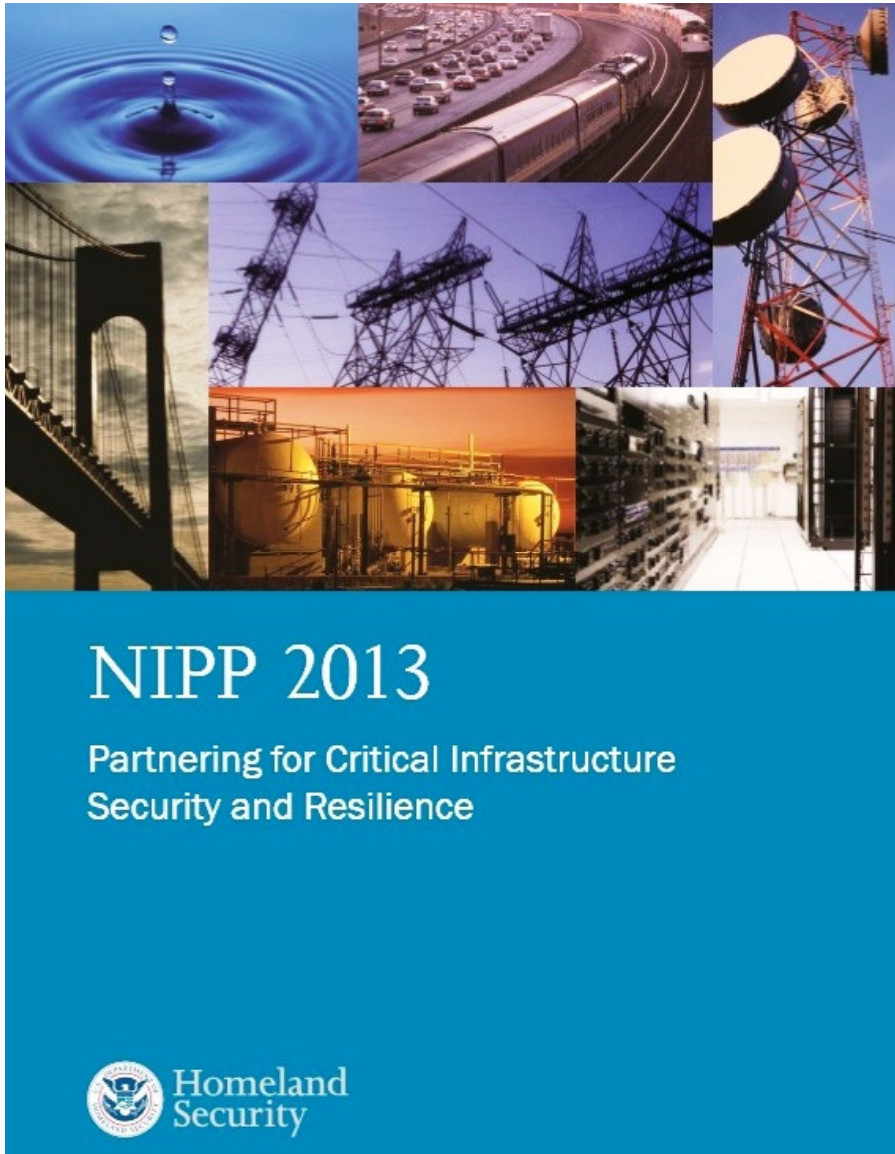
# Cybersecurity Threats & Risks for the Banking & Finance Sector

A typical cyber risk heat map for the banking sector



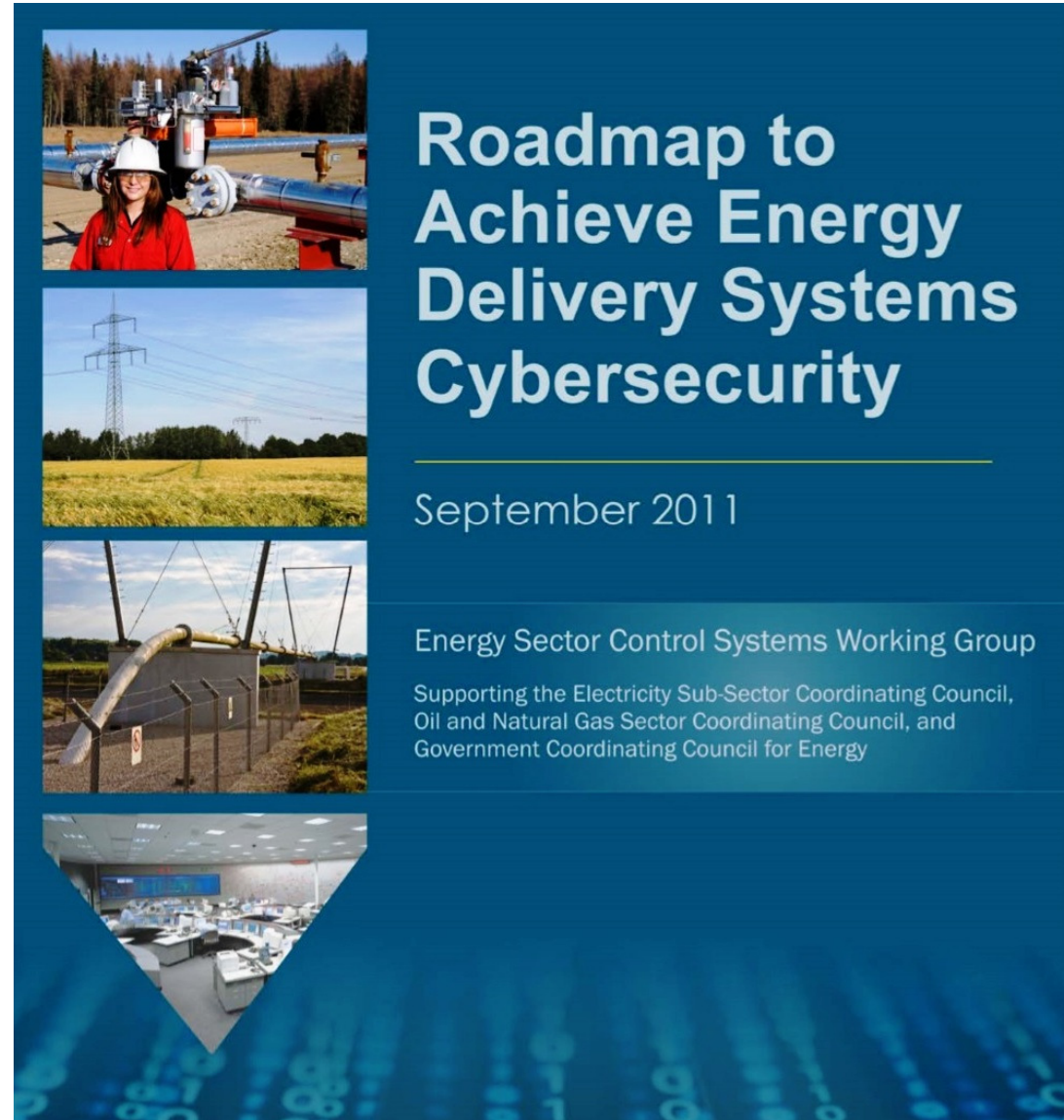
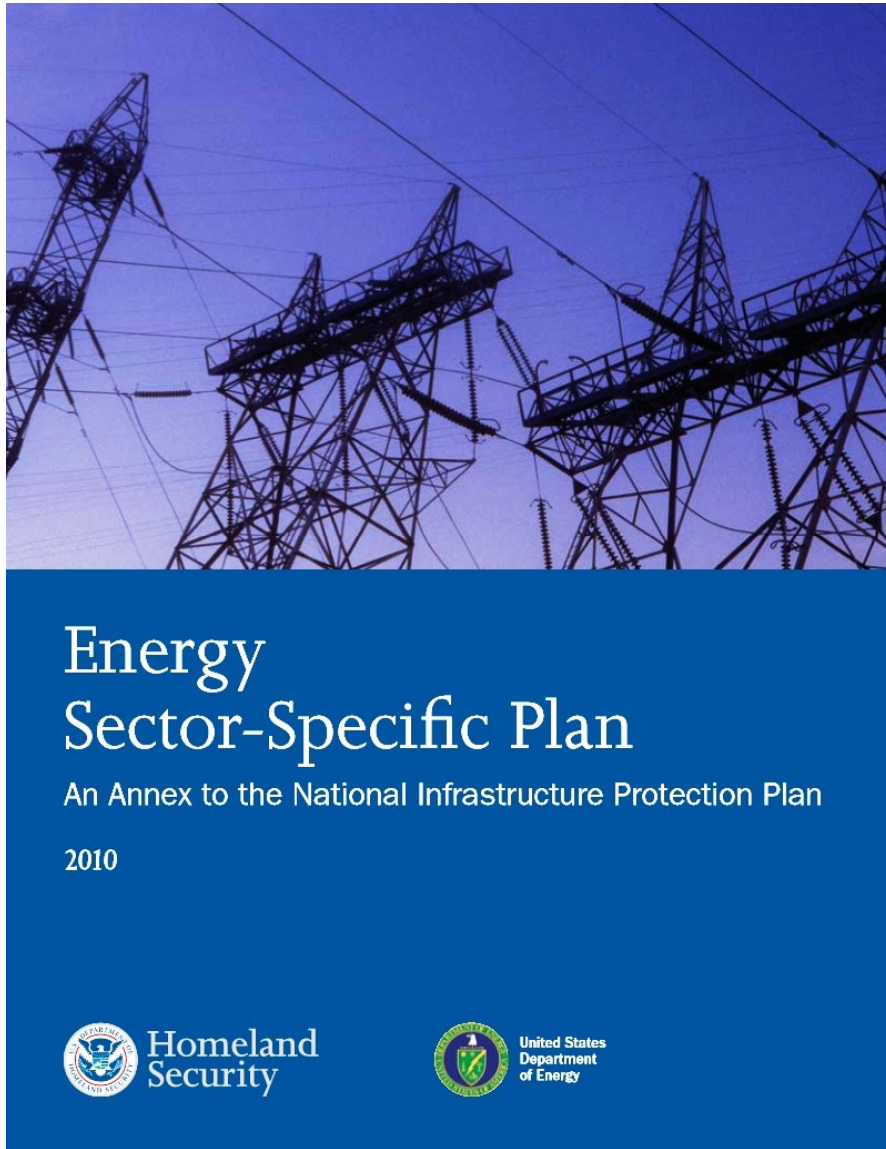
Source: Deloitte Center for Financial Services analysis

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





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





# Cybersecurity for the *Healthcare Sector*



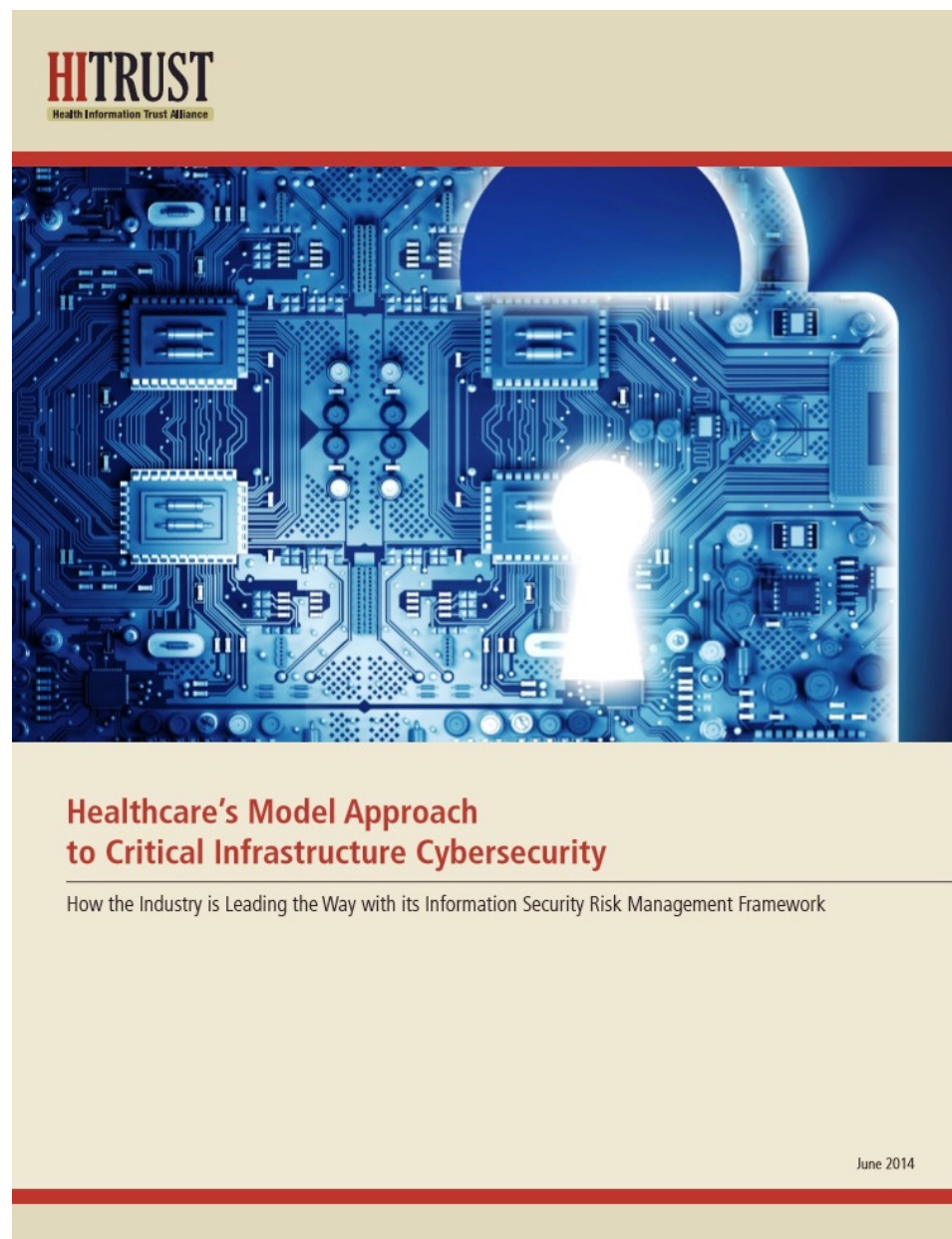
**A SANS Analyst Whitepaper**

*Written by Barbara Filkins*

February 2014

*Sponsored by  
Norse*

©2014 SANS<sup>™</sup> Institute



## Healthcare's Model Approach to Critical Infrastructure Cybersecurity

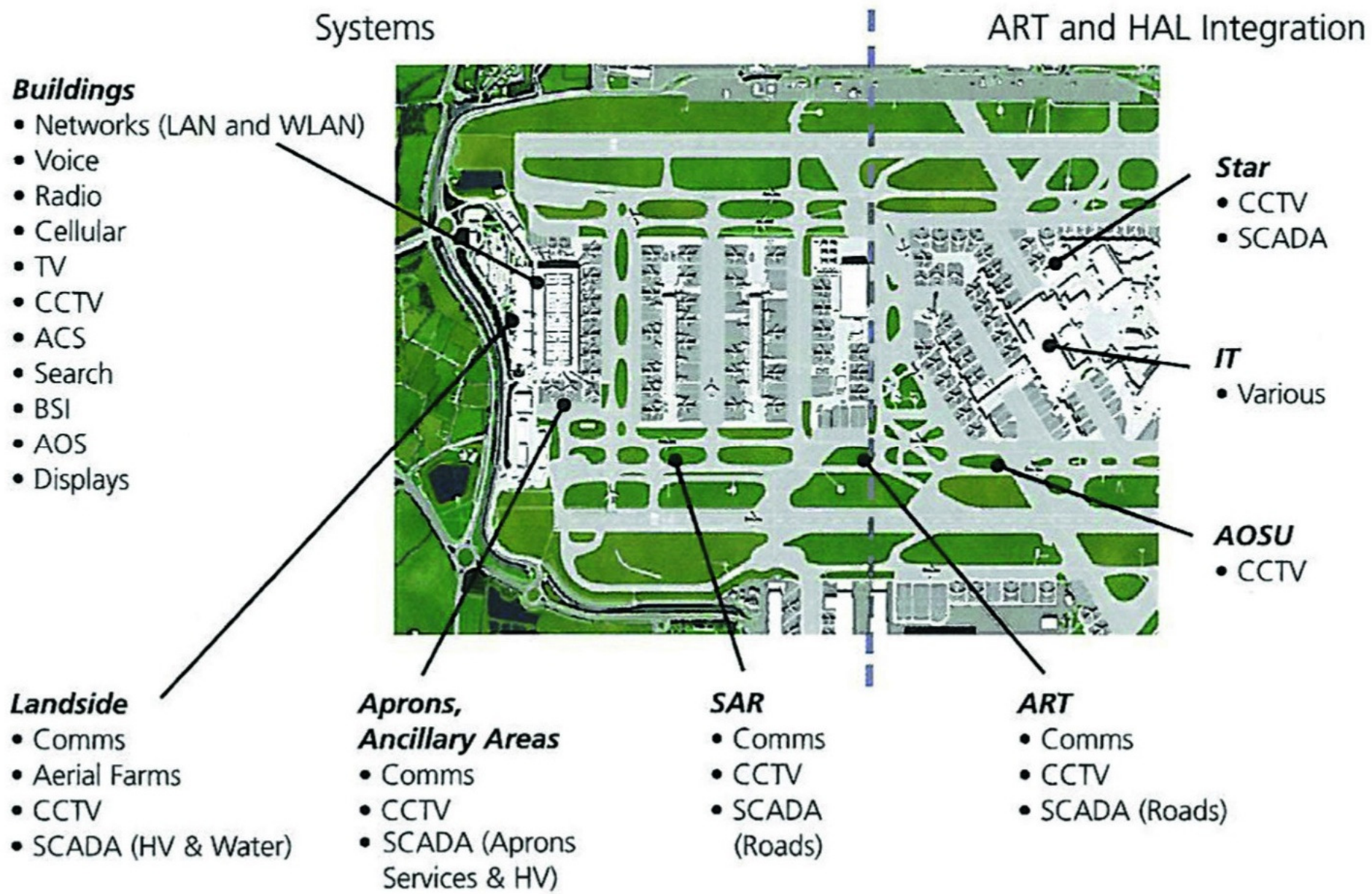
How the Industry is Leading the Way with its Information Security Risk Management Framework

June 2014





# 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



# Cybersecurity: NATO Research Analysis

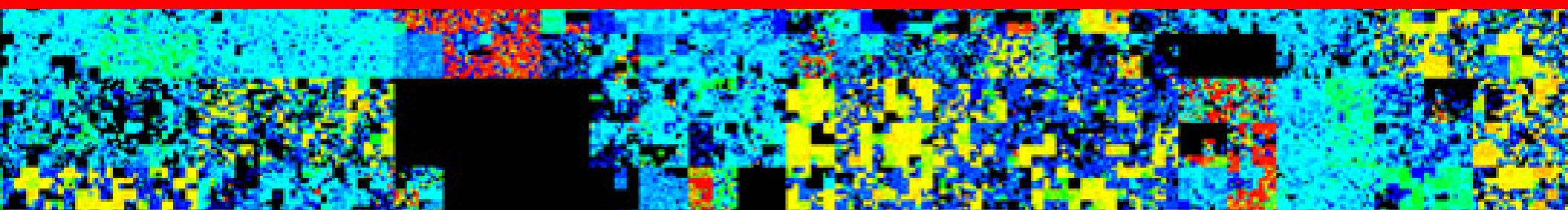
NATIONAL SECURITY THREATS	CYBER ATTACK ADVANTAGES	ATTACK CATEGORIES	TARGETS	CYBER ATTACK MITIGATION STRATEGIES	EFFECTIVENESS
ESPIONAGE	IT VULNERABILITIES	CONFIDENTIALITY	MILITARY FORCES	NEXT GEN NET IPV6	SOLVES SOME Q'S, CREATES OTHERS
PROPAGANDA	HIGH ASYMMETRY	INTEGRITY	GOV/CIV INFRASTRUCTURE	BEST MIL 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)

# *Cyber* Security for *Critical* Infrastructure!



## 6 – Industrial ICS & SCADA Security “Secure YOUR Systems”





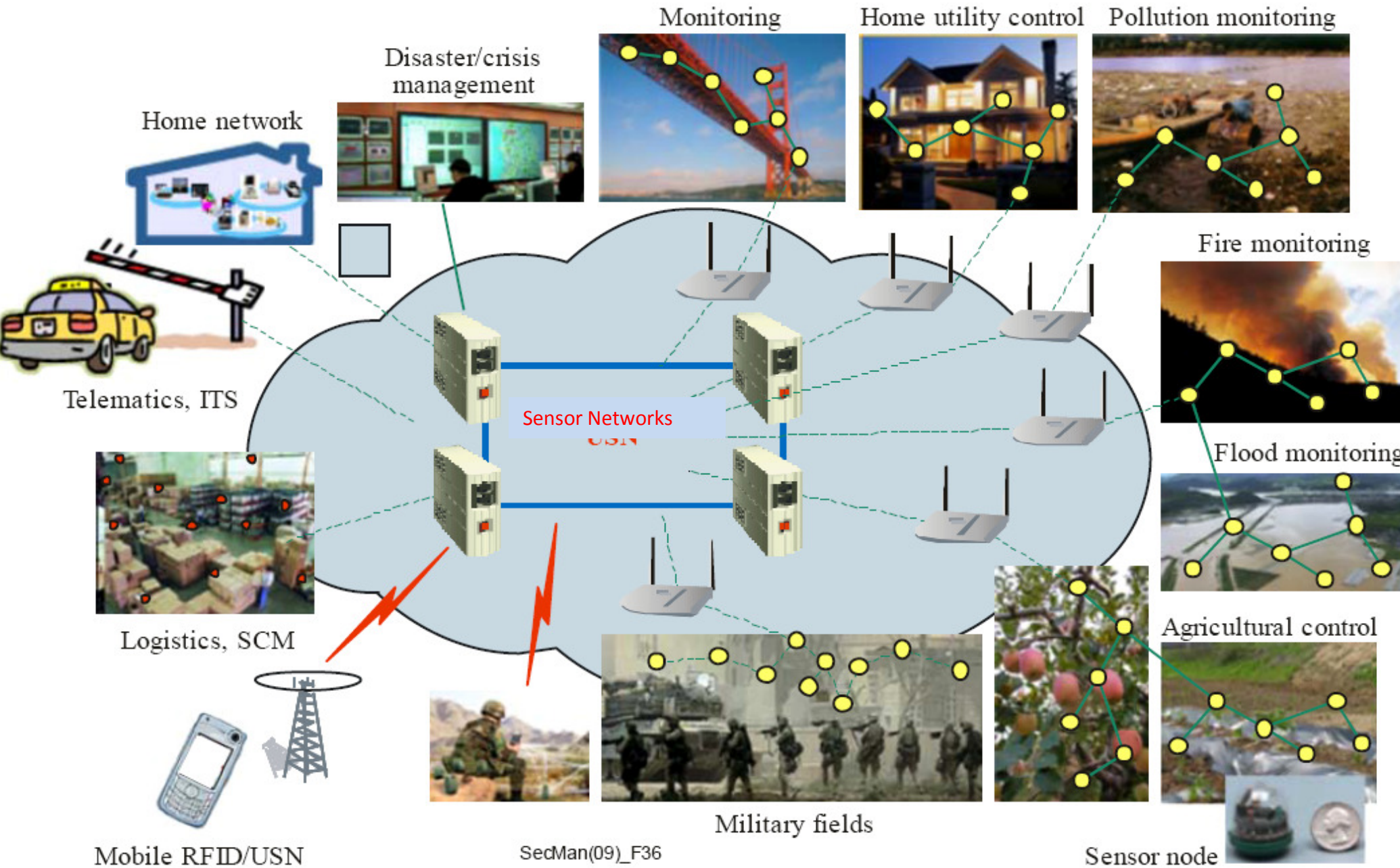
# Critical Energy Industry Sector : *“Cybersecurity for Automated Industrial Control & Safety Systems”*



Protect against *“Stuxnet”* type designer malware that attacks **ICS/SCADA** systems

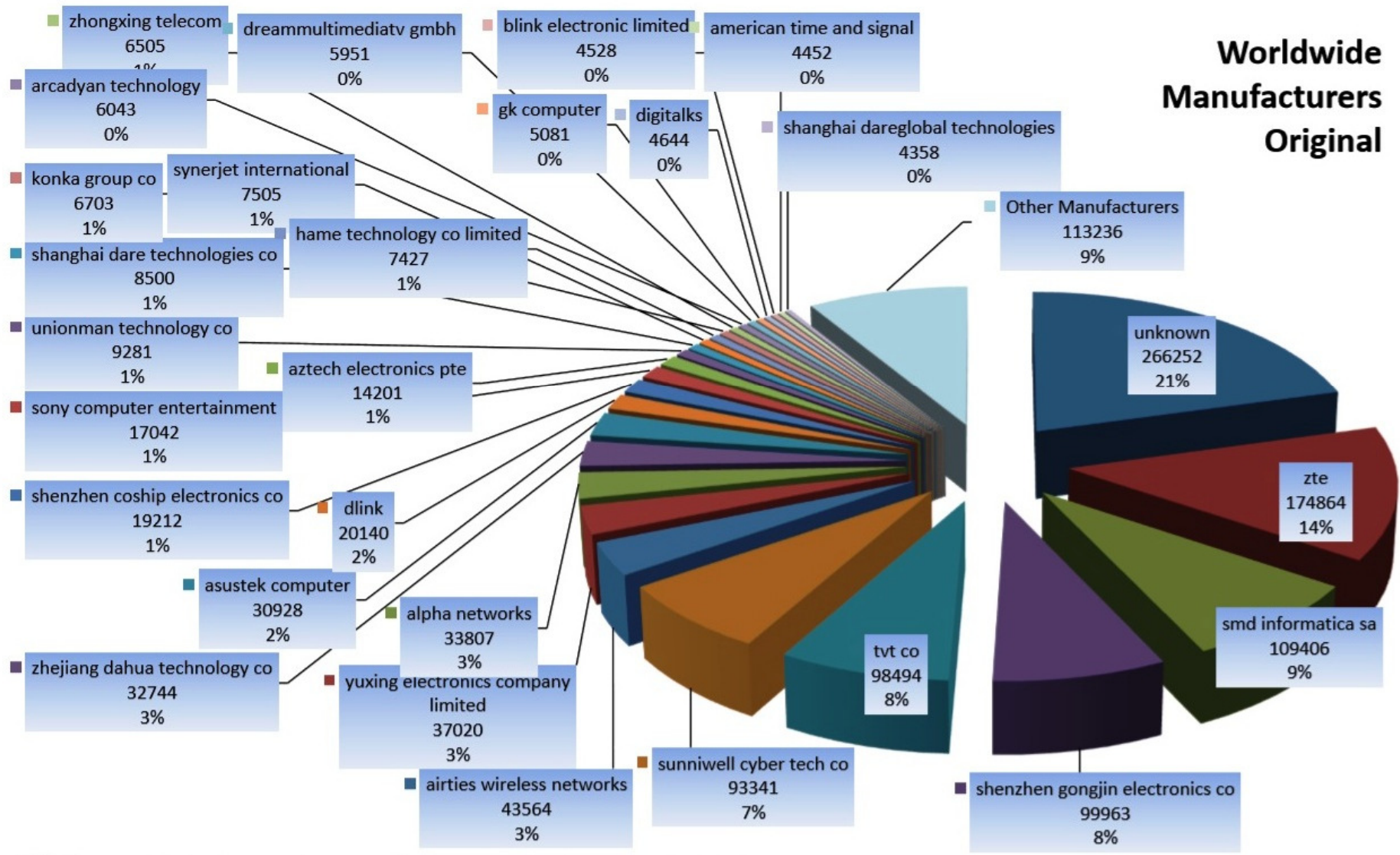


# Cybersecurity for Critical Sector Networks: “Internet of Things”



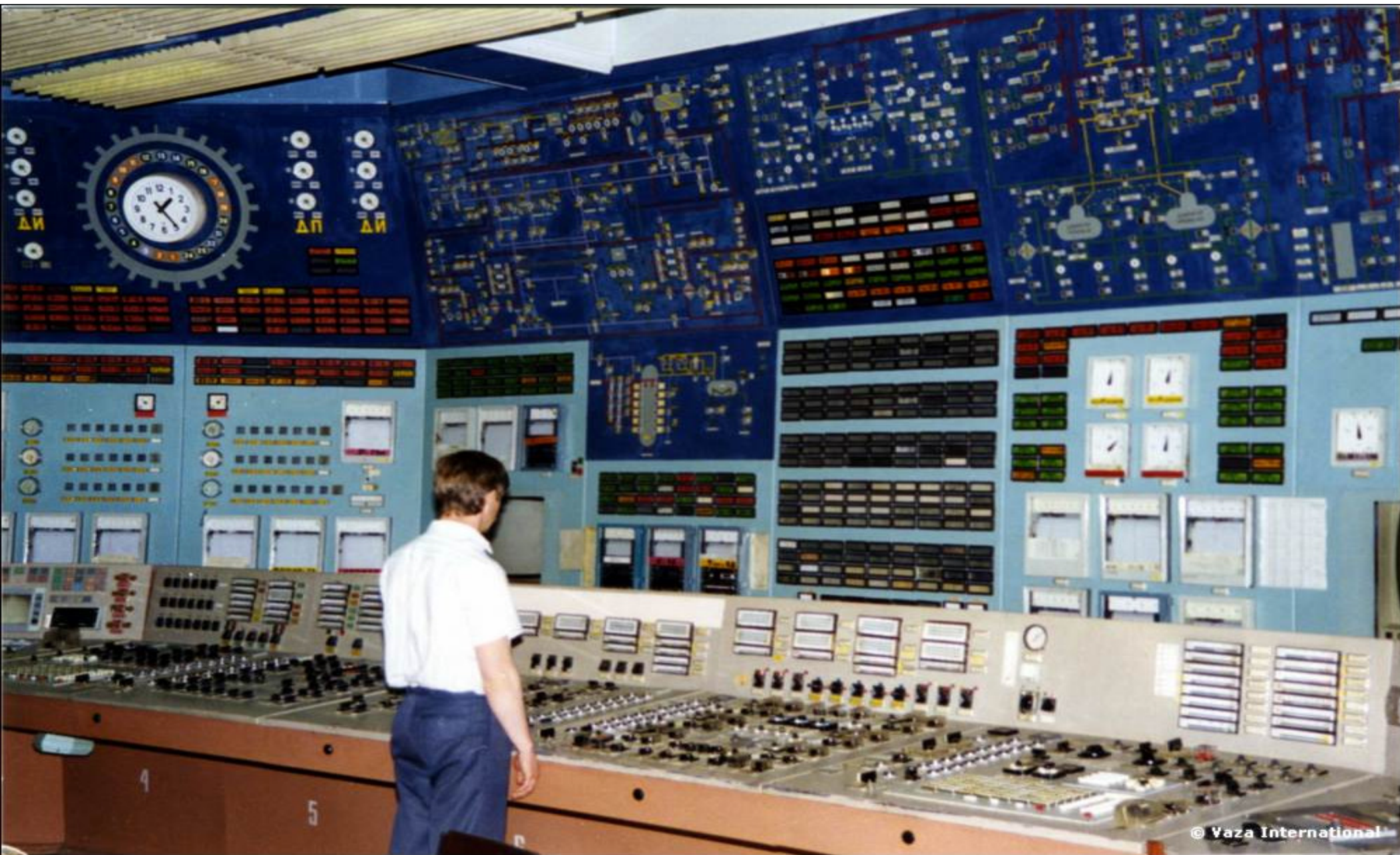


# Vulnerable Legacy Devices: “IoT”





# Control Room - *Kola Nuclear Power Station* - Russia



© Vaza International



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



© Vaza International





## Karnasurt Mine: Revda, Arctic Russia!

38<sup>th</sup> International East-West Security Conference

"Cybersecurity for Critical National  
Infrastructure" - Strategy & RoadMap

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# Karnasurt Mine: Revda – Kola Peninsula, Russia - 2000



**"Cybersecurity for Critical National Infrastructure" - Strategy & RoadMap**

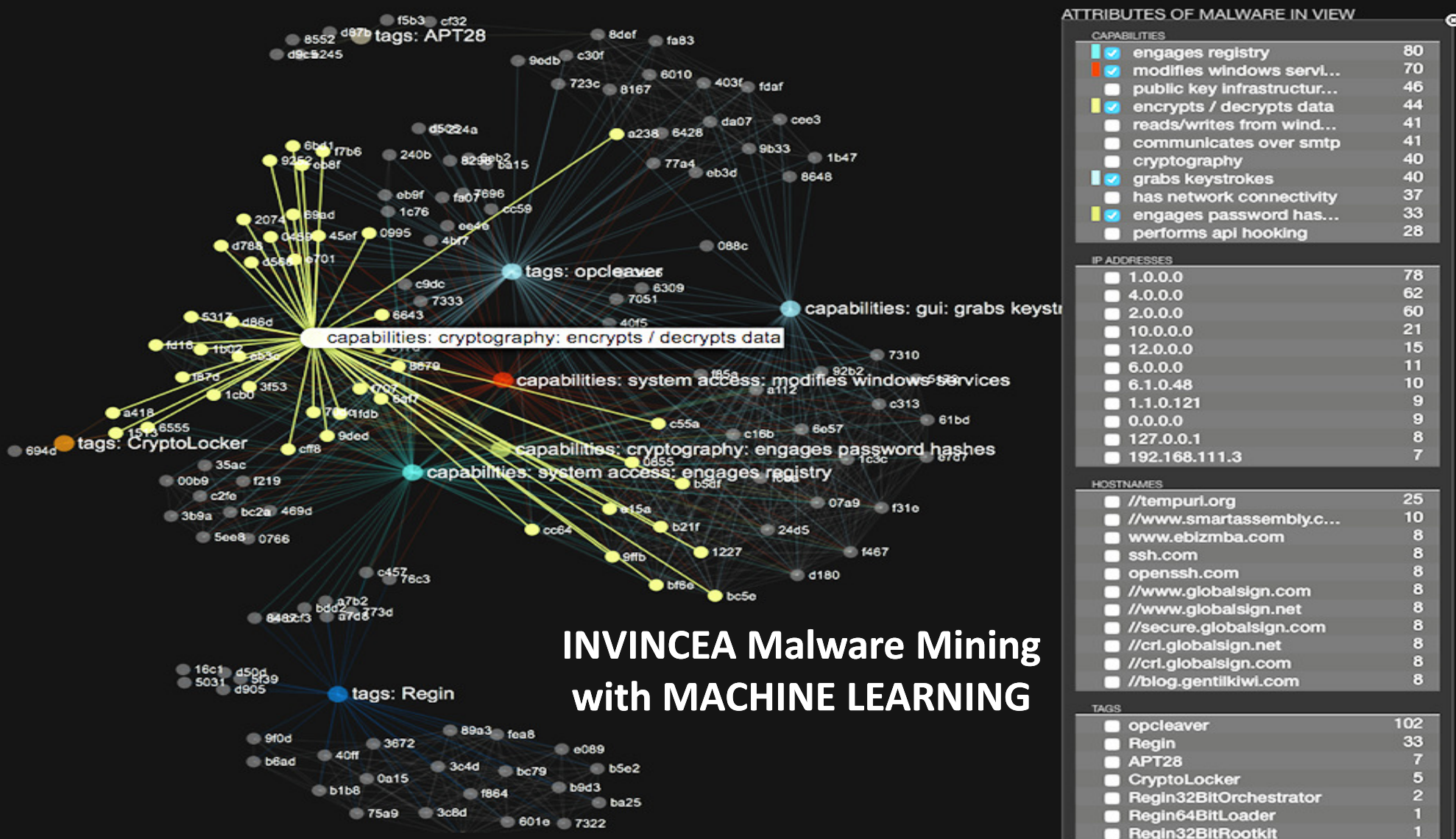
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# Cybersecurity using Malware Data Mining based on “AI/Machine Learning”: *Sophos*





# Cybersecurity using Malware Data Mining based on “AI/Machine Learning”: *Sophos*

## Invincea to Become Part of Sophos Synchronized Security



## Sophos Cybersecurity Tools using Machine/Deep Learning from Invincea: 2017

# Cybersecurity using Malware Data Mining based on “AI/Machine Learning”: *Sophos*

## Synchronized Security



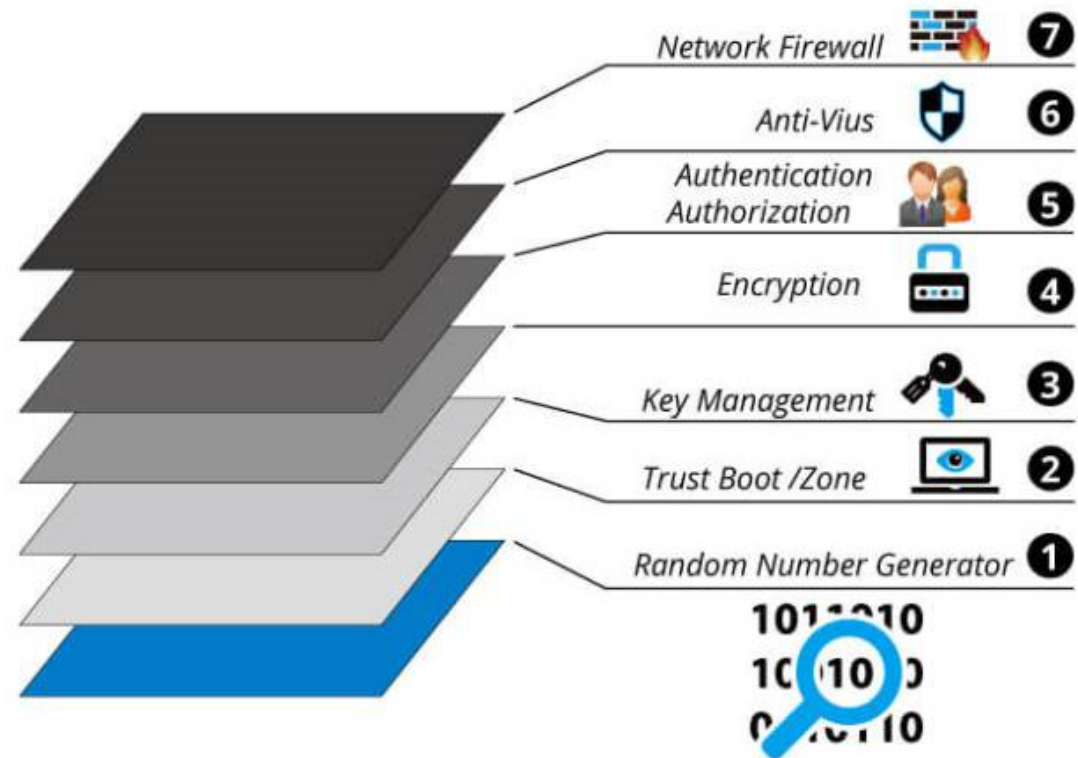
Invincea Cyber Tools fully embedded in Sophos Intercept X Deep Learning: 2018



# IoT Cybersecurity: *7-Level Architecture*

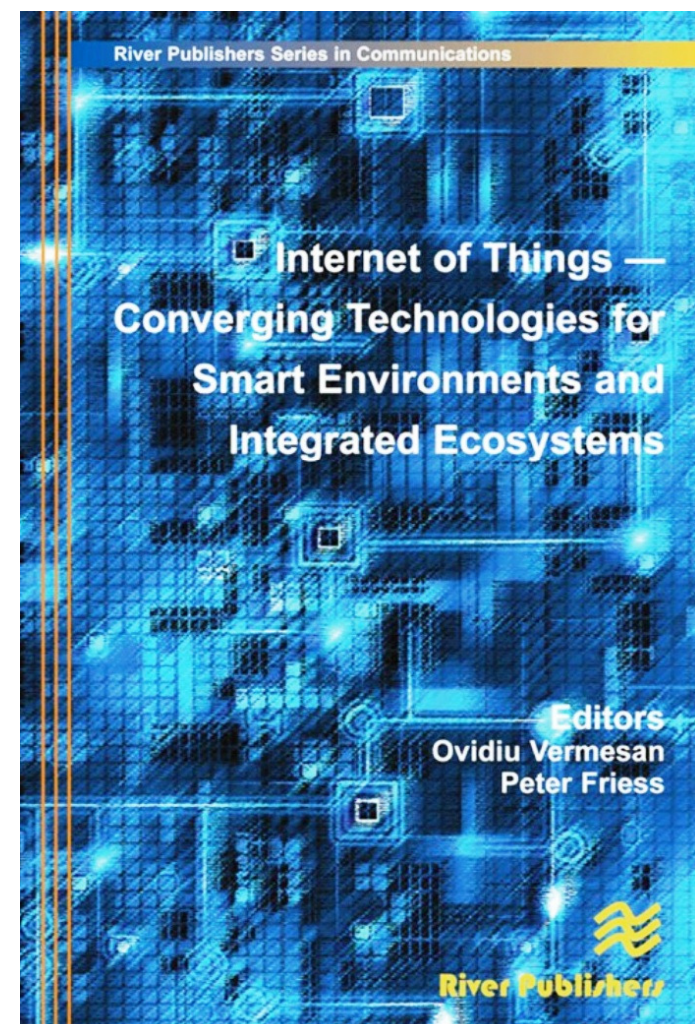
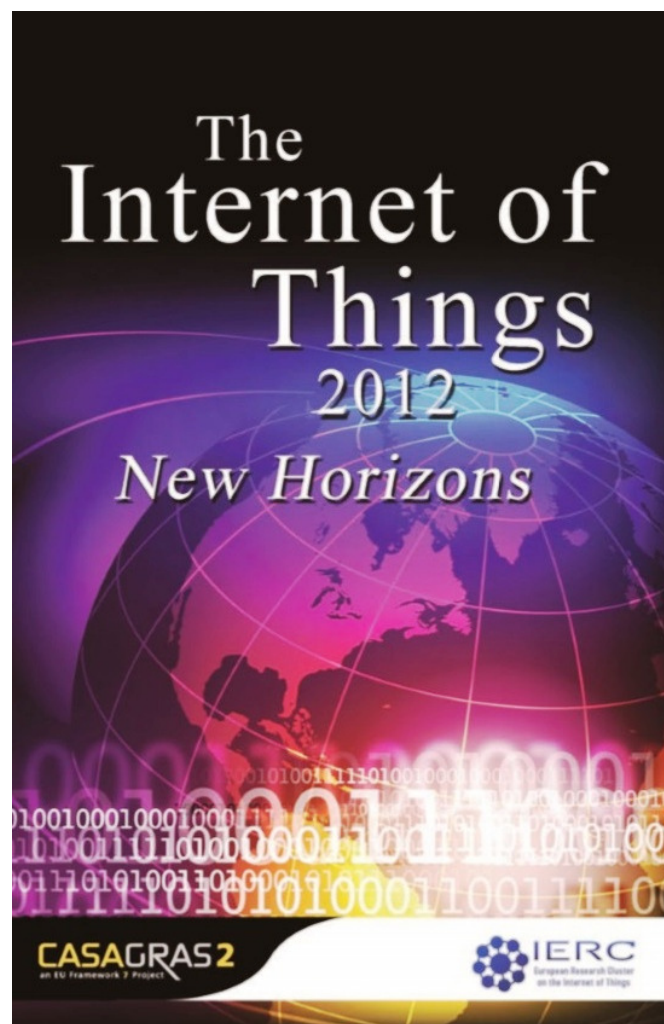


## Cyber Security - 7 Security Layers Structure





# EU/IERC – *Research Cluster Reports on* *“Smart Systems” & “Internet of Things”*





# IoT - UK Government: Code of Practice for "Consumer IoT Security" – Oct 2018



Department for  
Digital, Culture,  
Media & Sport

## Code of Practice for Consumer IoT Security



October 2018

### 12) Make installation and maintenance of devices easy

Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.

Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. Clear guidance to users on how to configure devices securely can also reduce their exposure to threats.

Primarily applies to:

**Device Manufacturers**

**IoT Service Providers**

**Mobile Application Developers**



16

Code of Practice for Consumer IoT Security

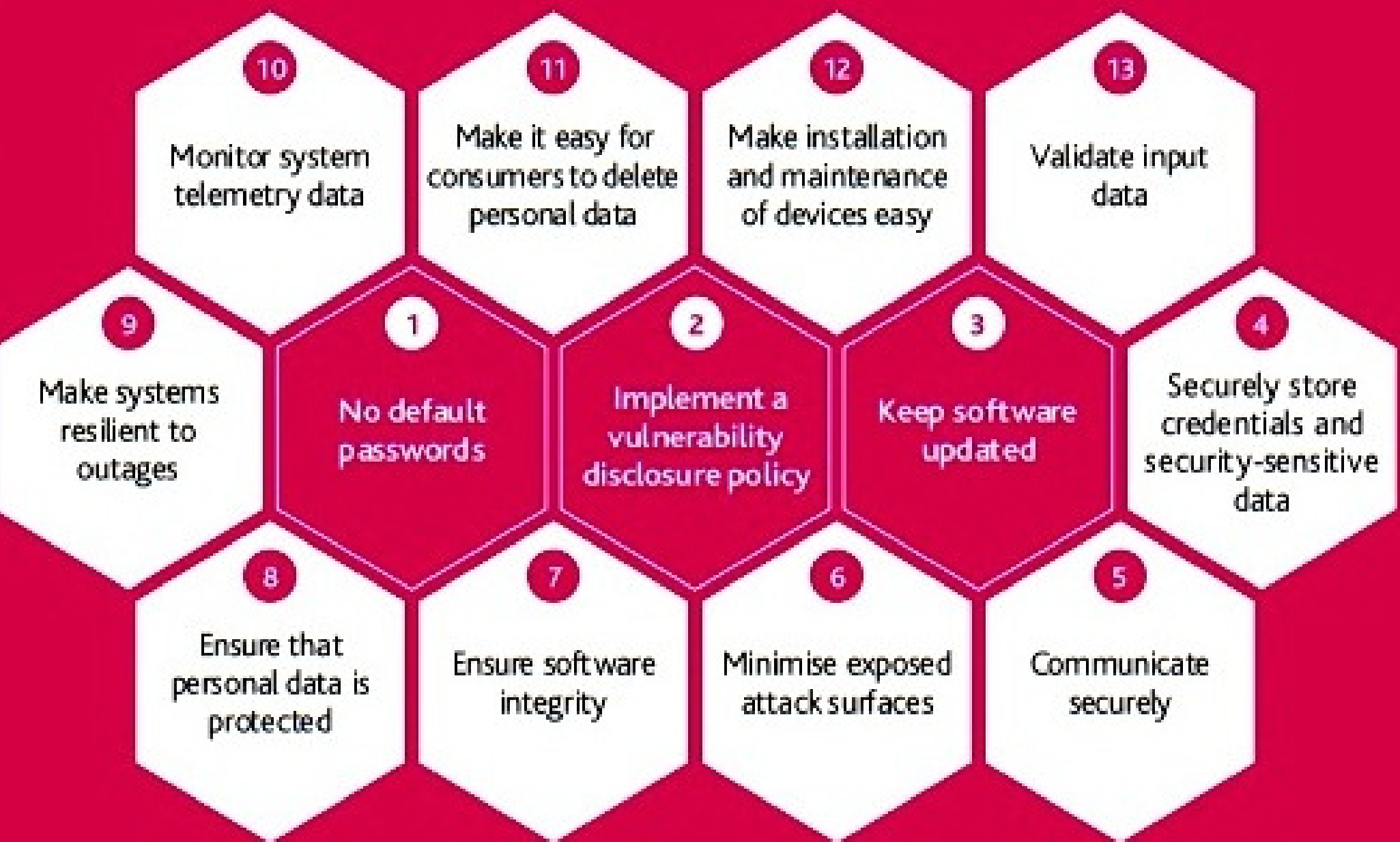
"Cybersecurity for Critical National  
Infrastructure" - *Strategy & RoadMap*

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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



# IoT - UK Government: Code of Practice



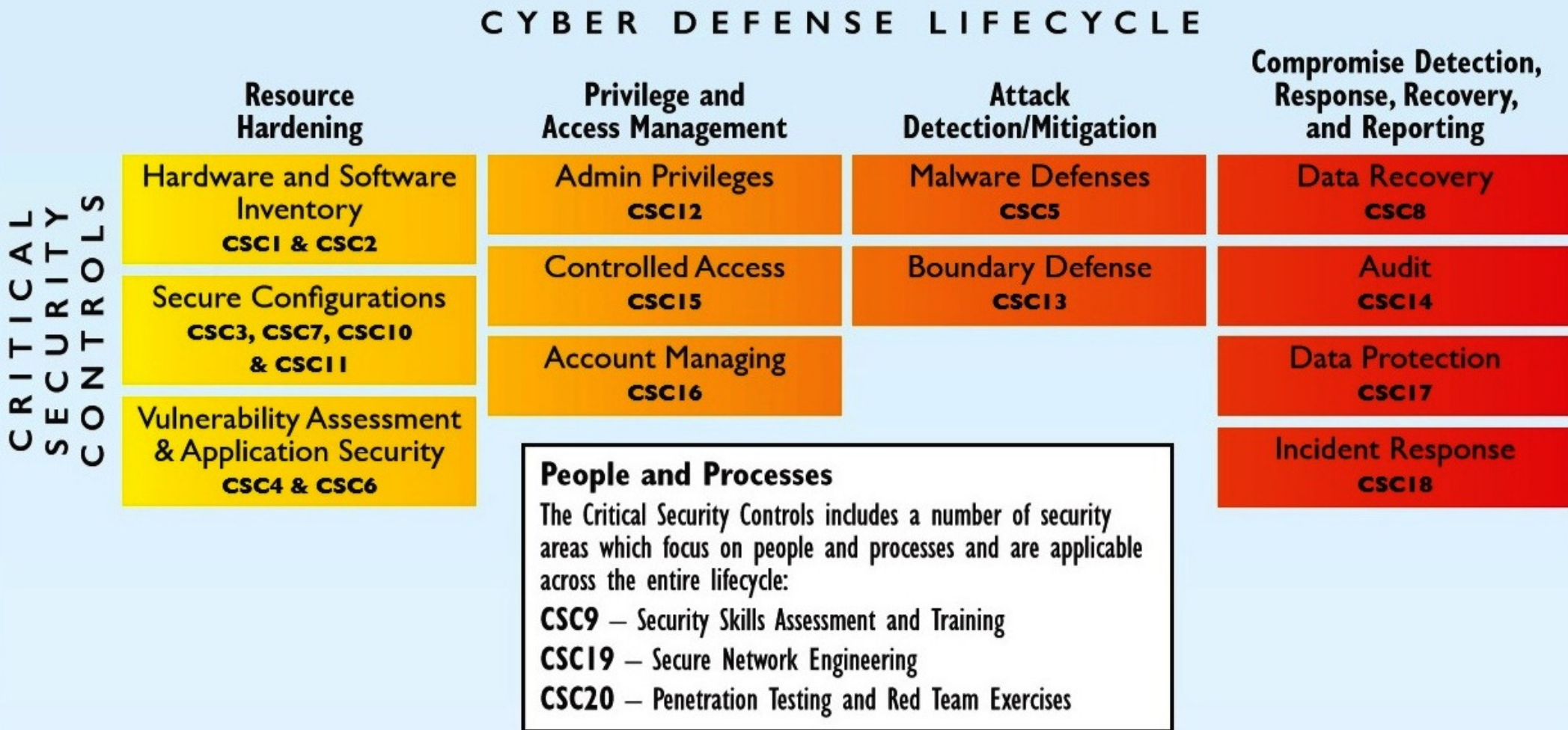
October 2018



# SANS: Critical Security Controls (CSC)

## Mapping the Controls Across the Cyber Defense Lifecycle

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

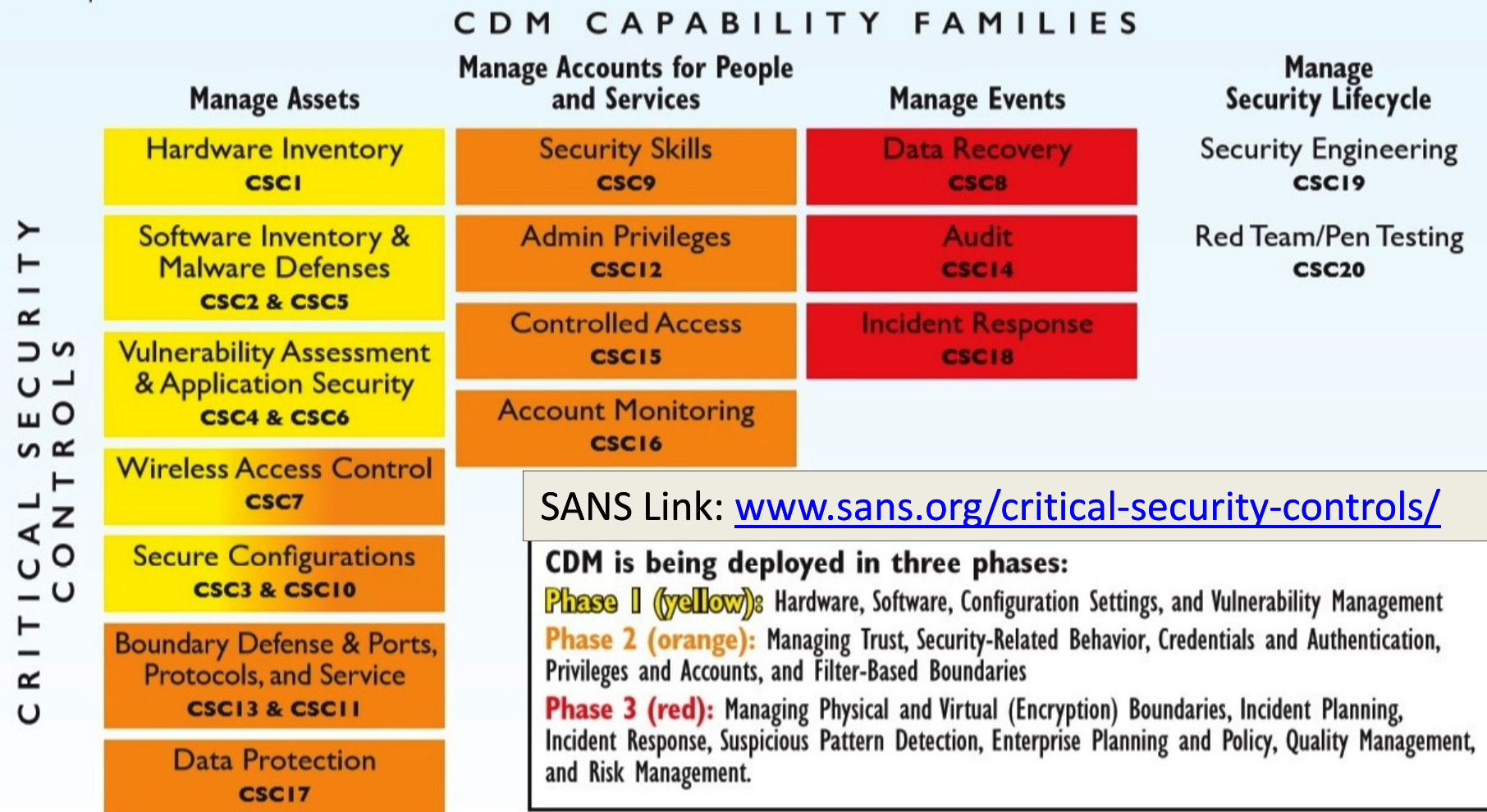


**SANS** = SysAdmin, Audit, Networking and Security

Link: [www.sans.org/critical-security-controls/](http://www.sans.org/critical-security-controls/)

# Mapping the **SANS** Critical Security Controls: **US Govt – Dept of Homeland Security CDM Program**

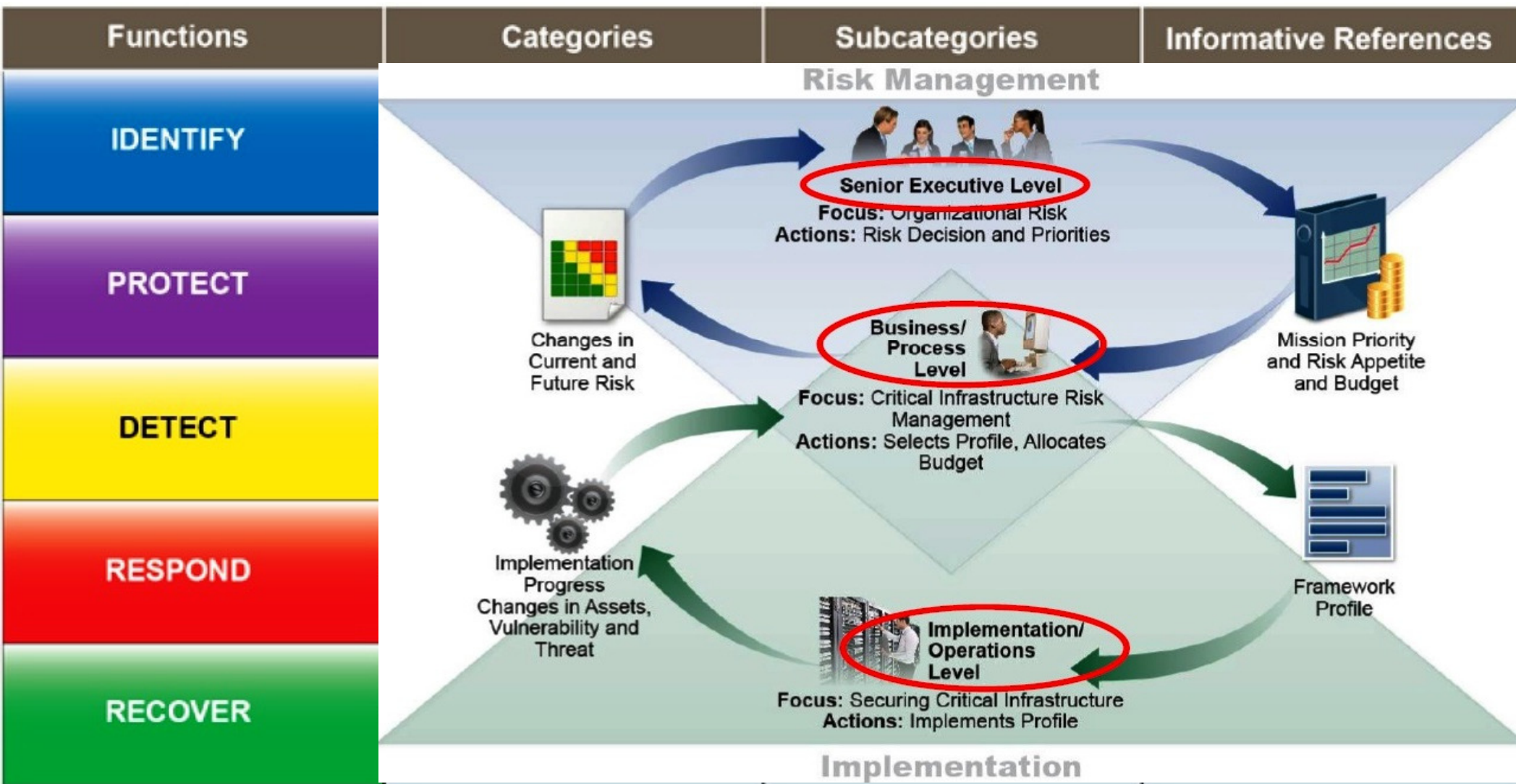
The Department of Homeland Security Continuous Diagnostics and Mitigation program has multiple phases of security product and services offerings across cybersecurity. The Critical Controls map directly against those CDM phases:





# NIST *Cybersecurity* Framework

*National Institute of Standards & Technology*



**Web:** [www.nist.gov/cyberframework/](http://www.nist.gov/cyberframework/)

38<sup>th</sup> International East-West Security Conference

"Cybersecurity for Critical National Infrastructure" - *Strategy & RoadMap*

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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



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

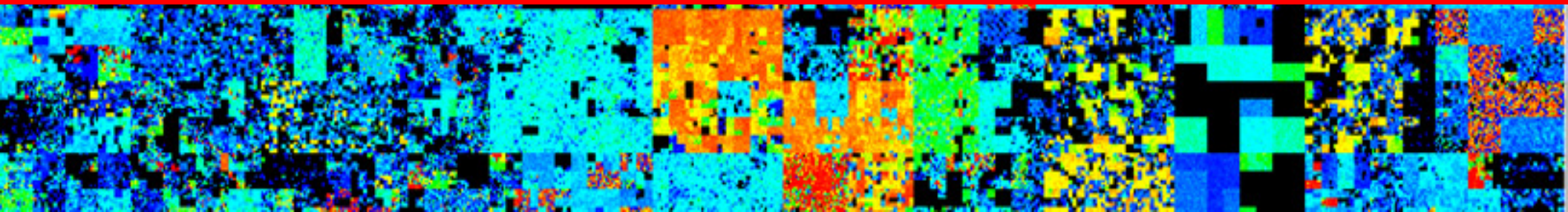




# *Cyber* Security for *Critical* Infrastructure!



## 7 – Standards, Regulations & Laws “Design to Standards”

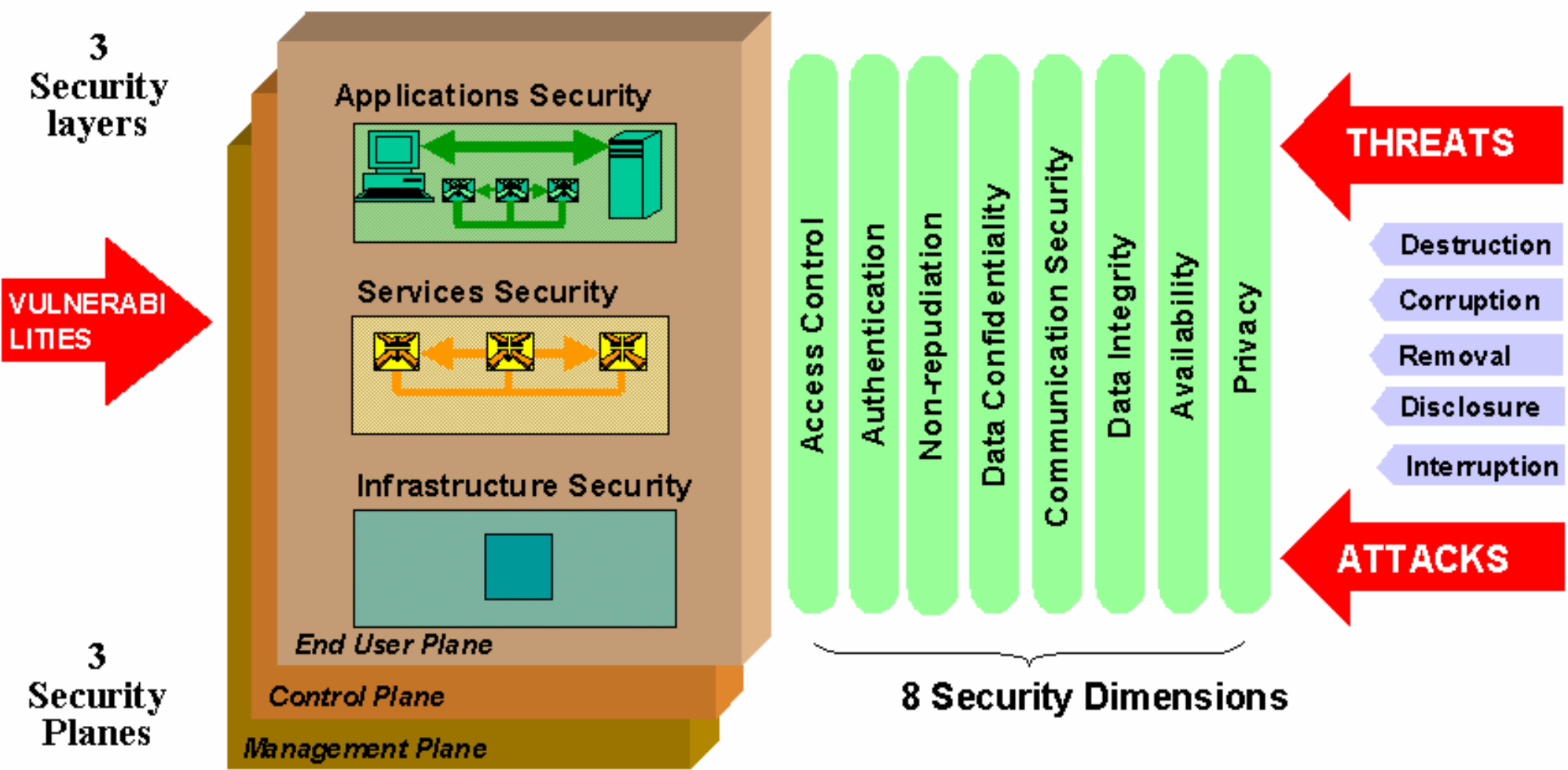


# Global Cybersecurity Standards: *Players*

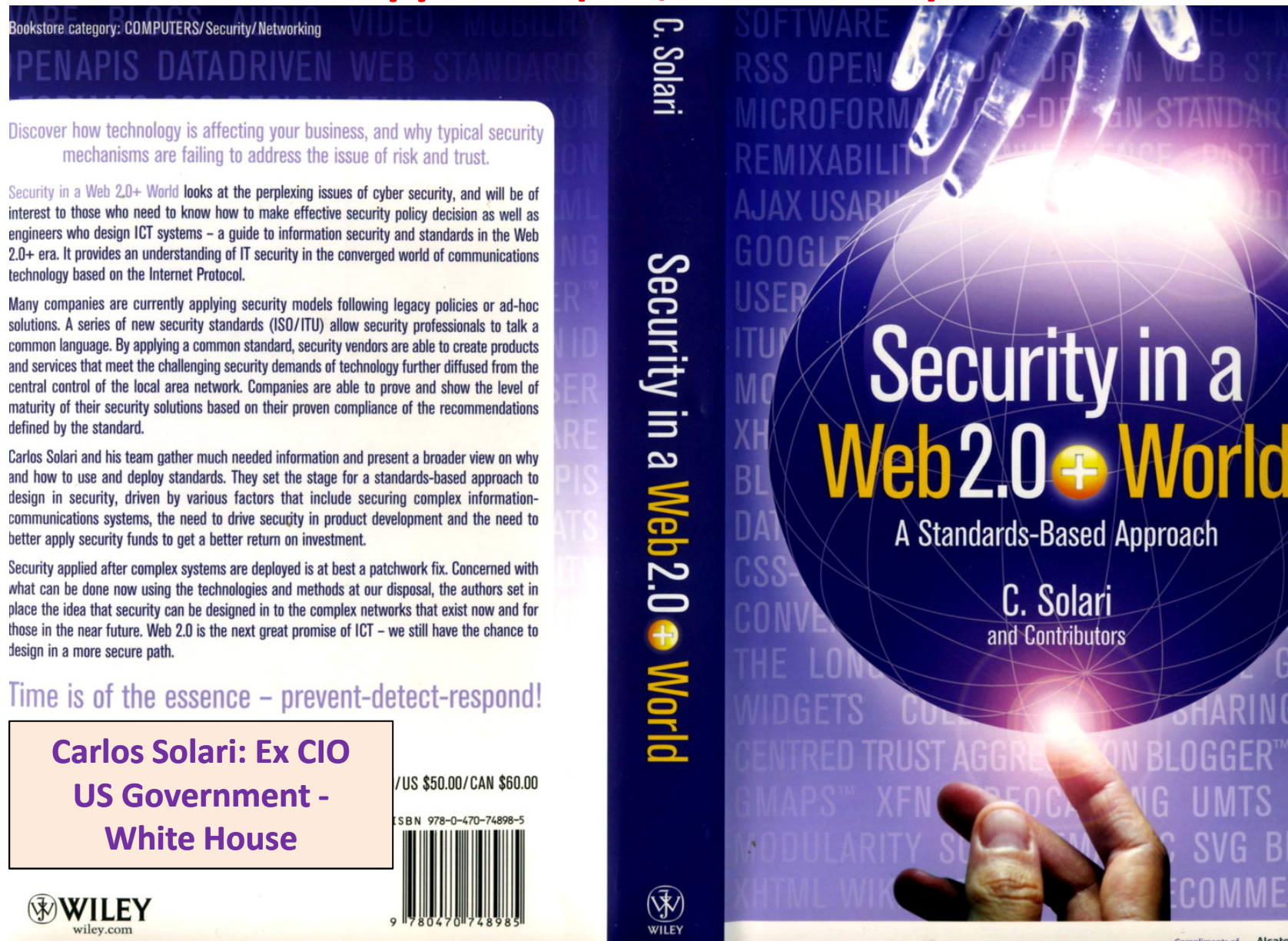
- **UN/ITU:** We shall be focusing in this short talk on the technical security standards & recommendations published by the ITU as their X-Series
- **Partnerships:** The ITU works closely in partnership with many agencies for emerging Cybersecurity, ICT, Networking & Mobile Comms Standards
  - **ENISA** – 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



# UN/ITU – X.805 *Cybersecurity Architecture*



# Recommended Book: Security in a Web2.0 World – - A Standards Based Approach(UN/ITU - X.805) – Author: C. Solari -



"Cybersecurity for Critical National  
Infrastructure"- *Strategy & RoadMap*

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





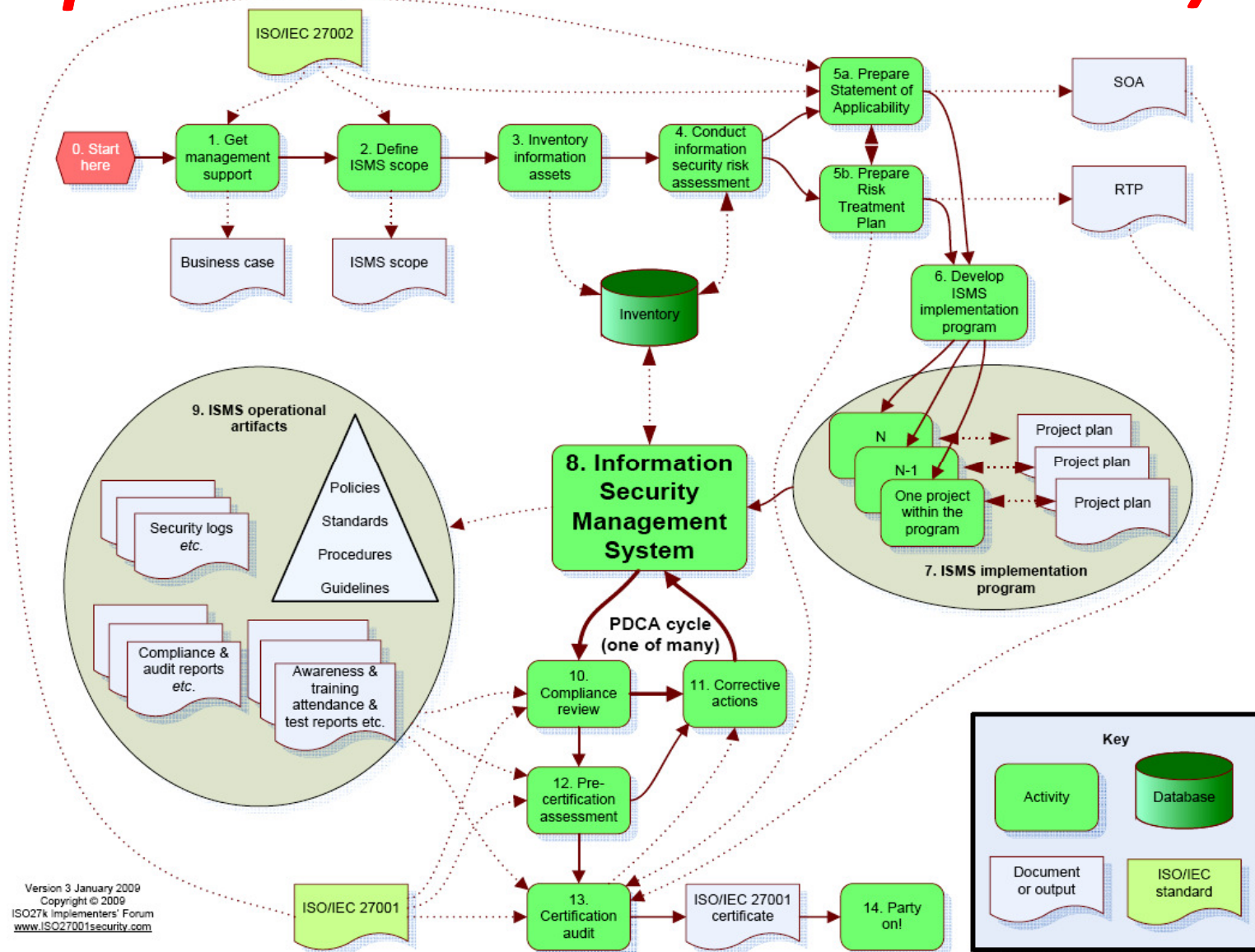
# Other Cyber & Physical Security Standards:

## - **ISO/IEC** – **NIST** – **ENISA**- **ISF** - **IEEE** -

- **ISO/IEC:** These are often adopted as “best practice” for operational aspects of security including the ISO27001 – Information Security Management System, and the ISO27002 – ISMS Code of Practice
- **NIST:** The comprehensive publications of the “800 Series” from the Computer Security Division are complementary to the ITU standards
- **ENISA:** The European Networks Security Agency publishes many detailed security studies and recommendations, with some useful work and guidelines for the establishment of national CERTs
- **ISF** – Information Security Forum – Founded 1989 to provide research, analysis and methodologies for Information Security and Risk Management
- **IEEE:** An important global player in ICT standards, and a key ITU partner in the development of new standards for open network cybersecurity

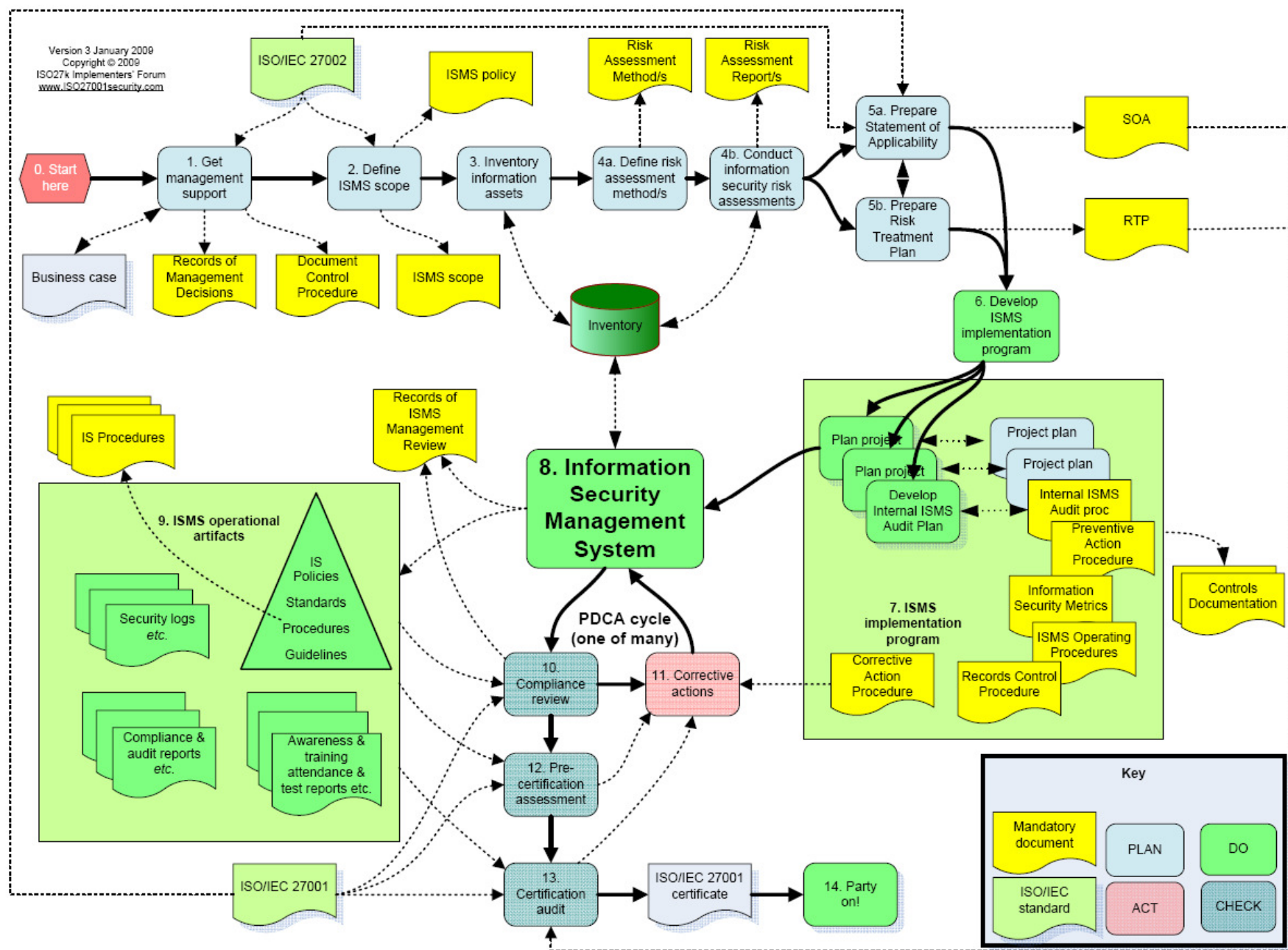
# “Information Security Management System”

## - *Implementation Process: ISO27001/2* -





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

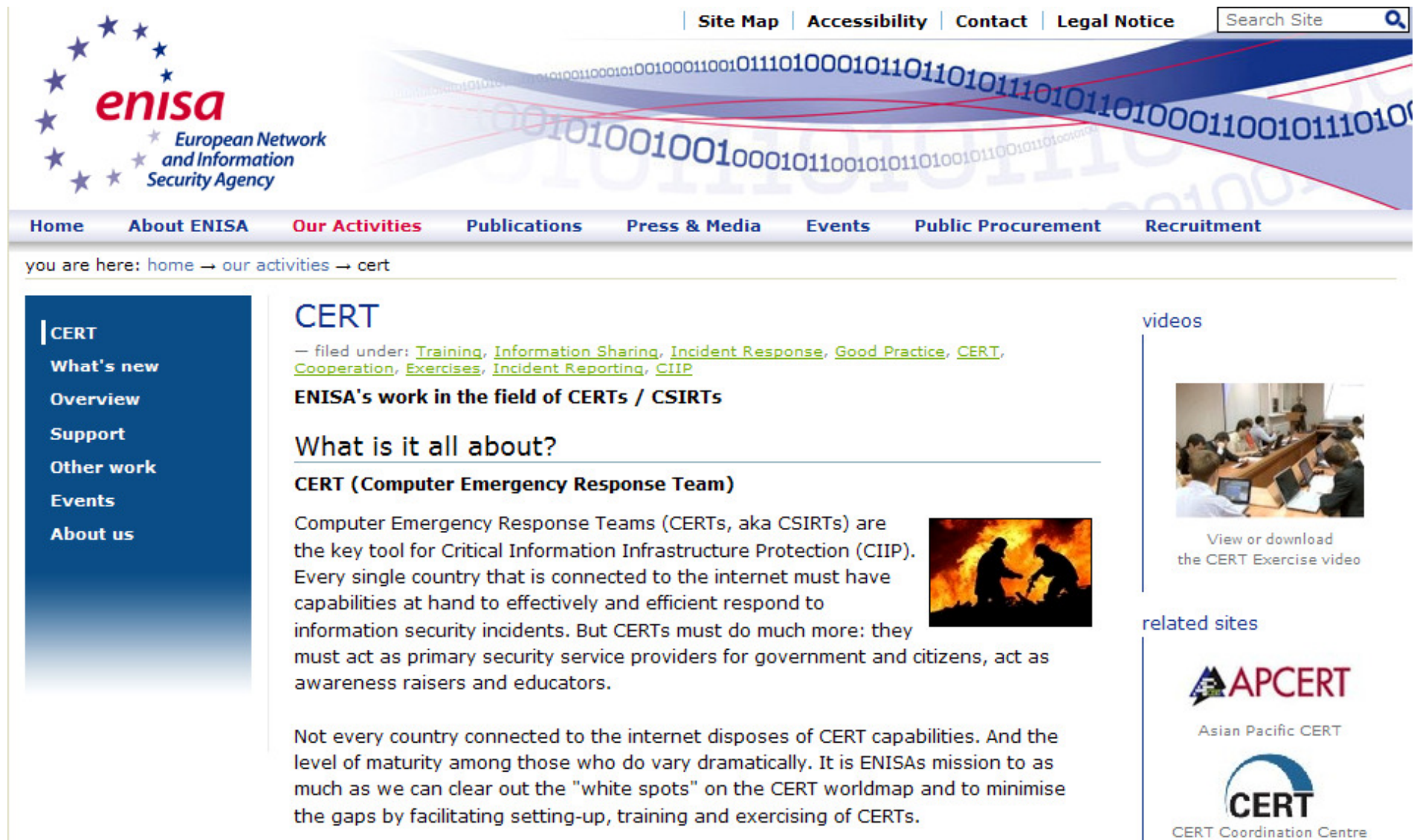


"Cybersecurity for Critical National Infrastructure" - Strategy & RoadMap  
Nice, France – 5th/6th Nov 2018

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



# enisa: European Network & Information Security Agency



The screenshot shows the ENISA website with a header containing the ENISA logo, navigation links (Site Map, Accessibility, Contact, Legal Notice), and a search bar. A secondary navigation bar includes links for Home, About ENISA, Our Activities, Publications, Press & Media, Events, Public Procurement, and Recruitment. A breadcrumb trail reads "you are here: home → our activities → cert".

**CERT**


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

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

**What is it all about?**


**CERT (Computer Emergency Response Team)**

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




Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is 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



# UK *Cybercrime* Legislation

UK CYBERCRIME LEGISLATION	
1.	The Official Secrets Acts - 1911 to 1989
2.	The Public Records Acts - 1958 to 1967
3.	The Data Protection Act - 1998
4.	The Freedom of Information Act - 2000
5.	The Human Rights Act - 1998
6.	The Computer Misuse Act 1990
7.	The Copyright Designs and Patents Act 1988
8.	The Civil Evidence Act 1968
9.	The Police and Criminal Evidence Act 1984
10.	The Wireless Telegraphy Act 1949 - 2006
11.	The Communications Act 2003
12.	The Regulation of Investigatory Powers Act 2000 (RIPA)
13.	The Telecommunications Regulations 2000 (Interception)
14.	The Civil Contingencies Act 2004
15.	The Anti-Terrorism, Crime and Security Act 2001
16.	The Forgery and Counterfeiting Act 1981
17.	The Fraud Act 2006
18.	Police Justice Act 2006
19.	The Theft Act - 1978 to 1996
20.	The Cybersecurity Strategy - Cabinet Office - June 2009

"Cybersecurity for Critical National Infrastructure" - Strategy & RoadMap  
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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



# 1. UK Official Secrets Acts 1911 to 1989

- Official Secrets Acts 1911 to 1989
  - *Unauthorised Disclosure of Official Information*
- Under the **Official Secrets Act 1989**, it is an offence for a Crown servant or government contractor to disclose official information in any of the protected categories if the disclosure is made without lawful authority and is damaging to the national interest. It is also an offence if a member of the public, or any other person who is not a Crown servant or government contractor under the Act, has in his or her possession, official information in one of the protected categories, and the information has been disclosed without lawful authority, or entrusted by a Crown servant or government contractor on terms requiring it to be held in confidence.
- **Cybersecurity Relevance:** *Covers all electronic communications, documents and media whatever format.*





# NATO *Cybersecurity* Framework Manual

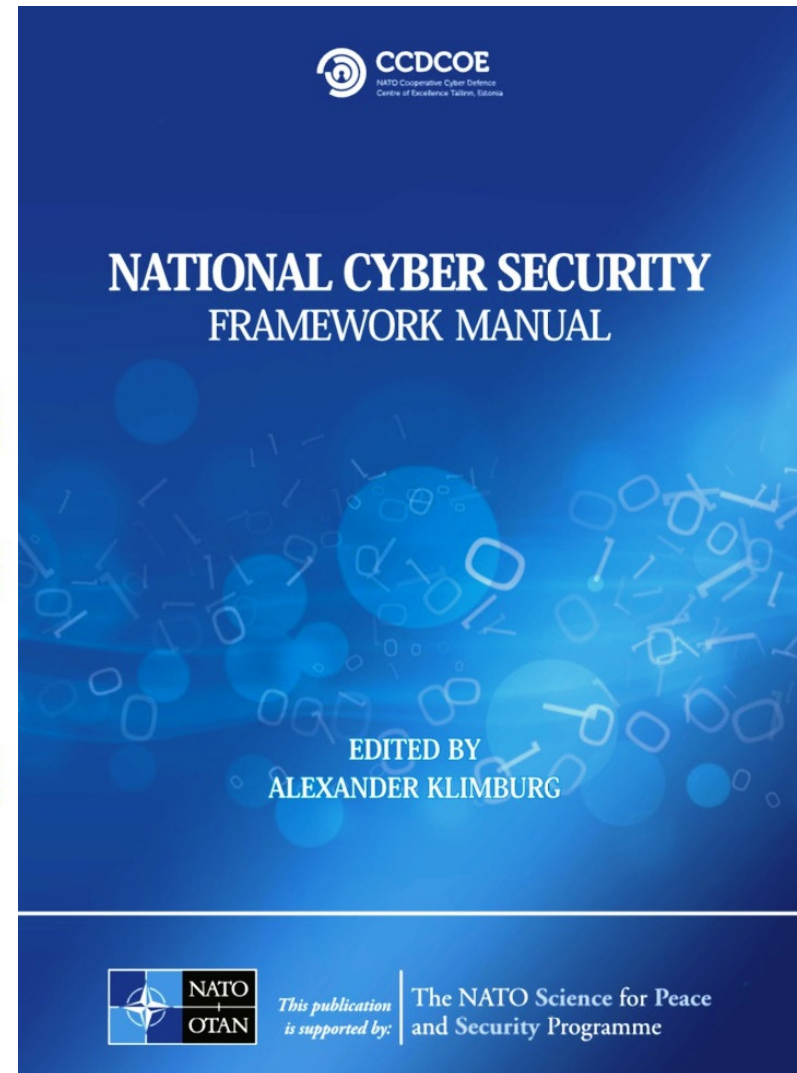
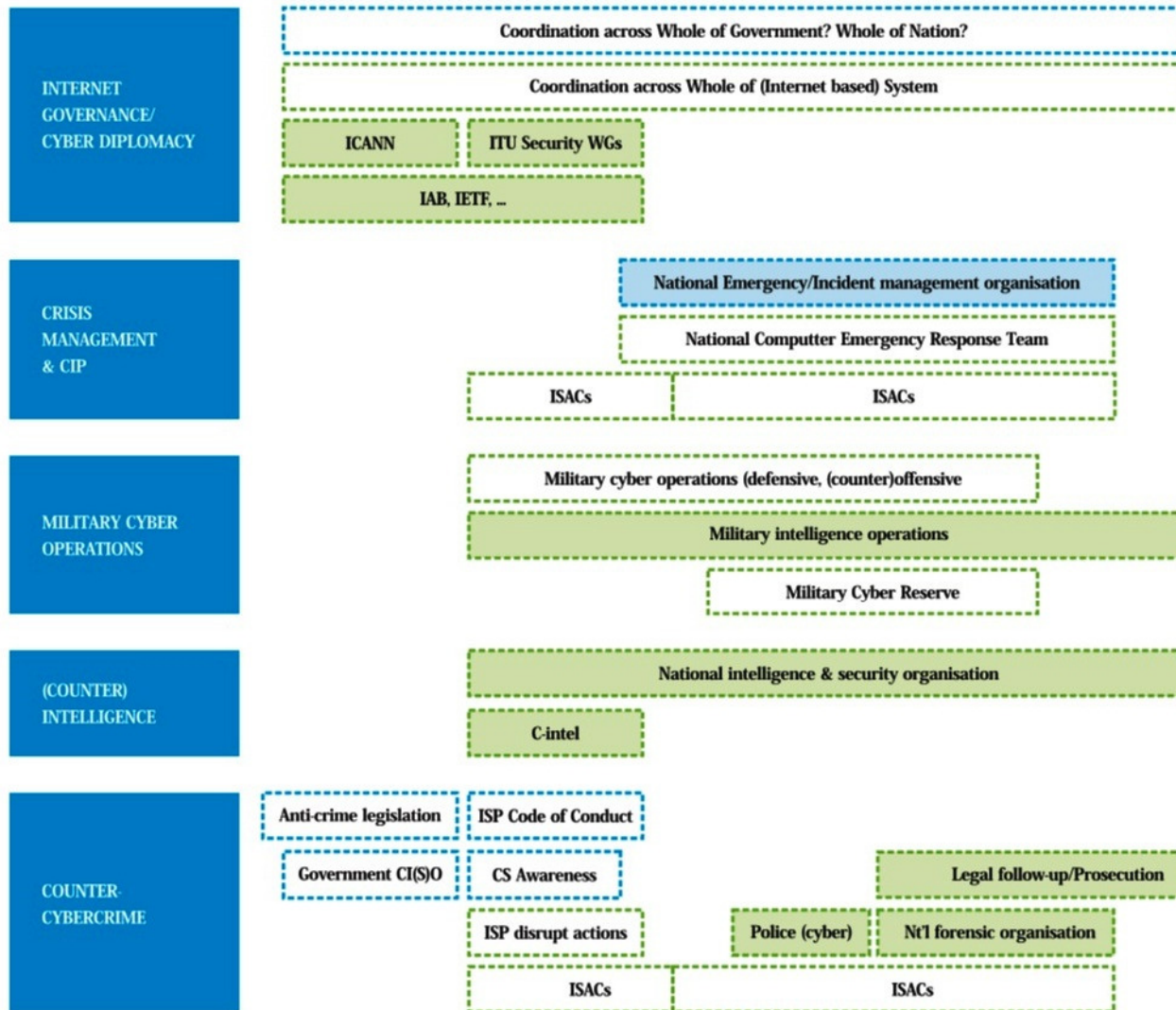
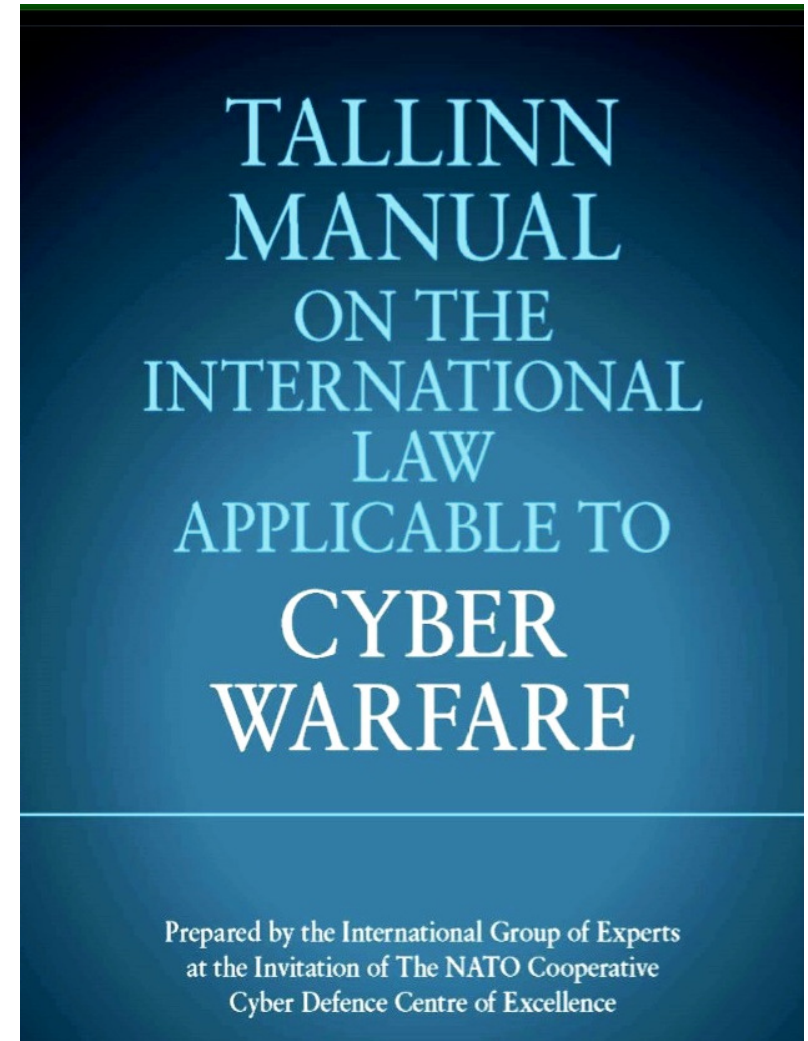
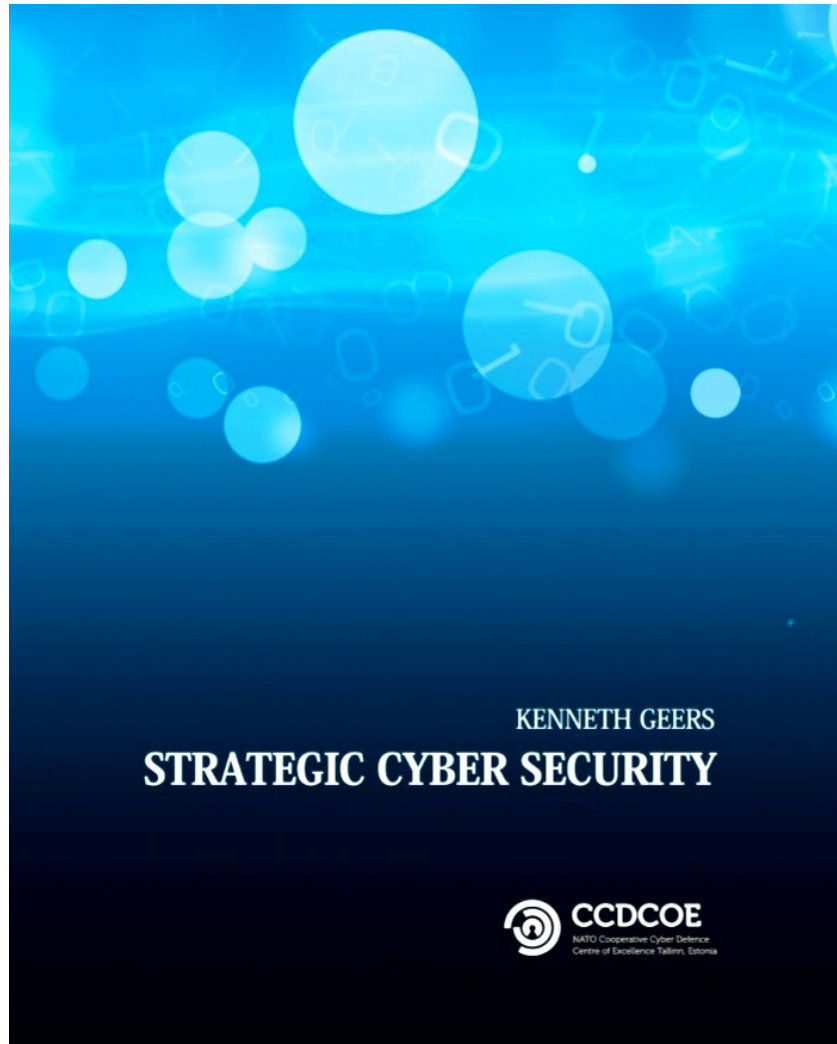


Figure 6: The Organisational Picture Across Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in

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



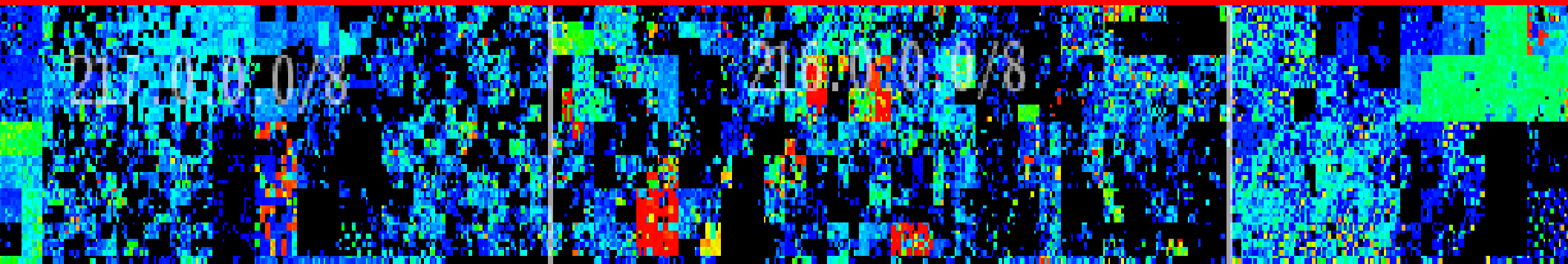
Recommended Cyber Reference Books: from **NATO** - [ccdcoe.org/tallinn-manual.html](http://ccdcoe.org/tallinn-manual.html)



# *Cyber* Security for *Critical* Infrastructure!



## 8 – Professional \$kill\$ Development “\$ Training Investment \$”



# 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:***

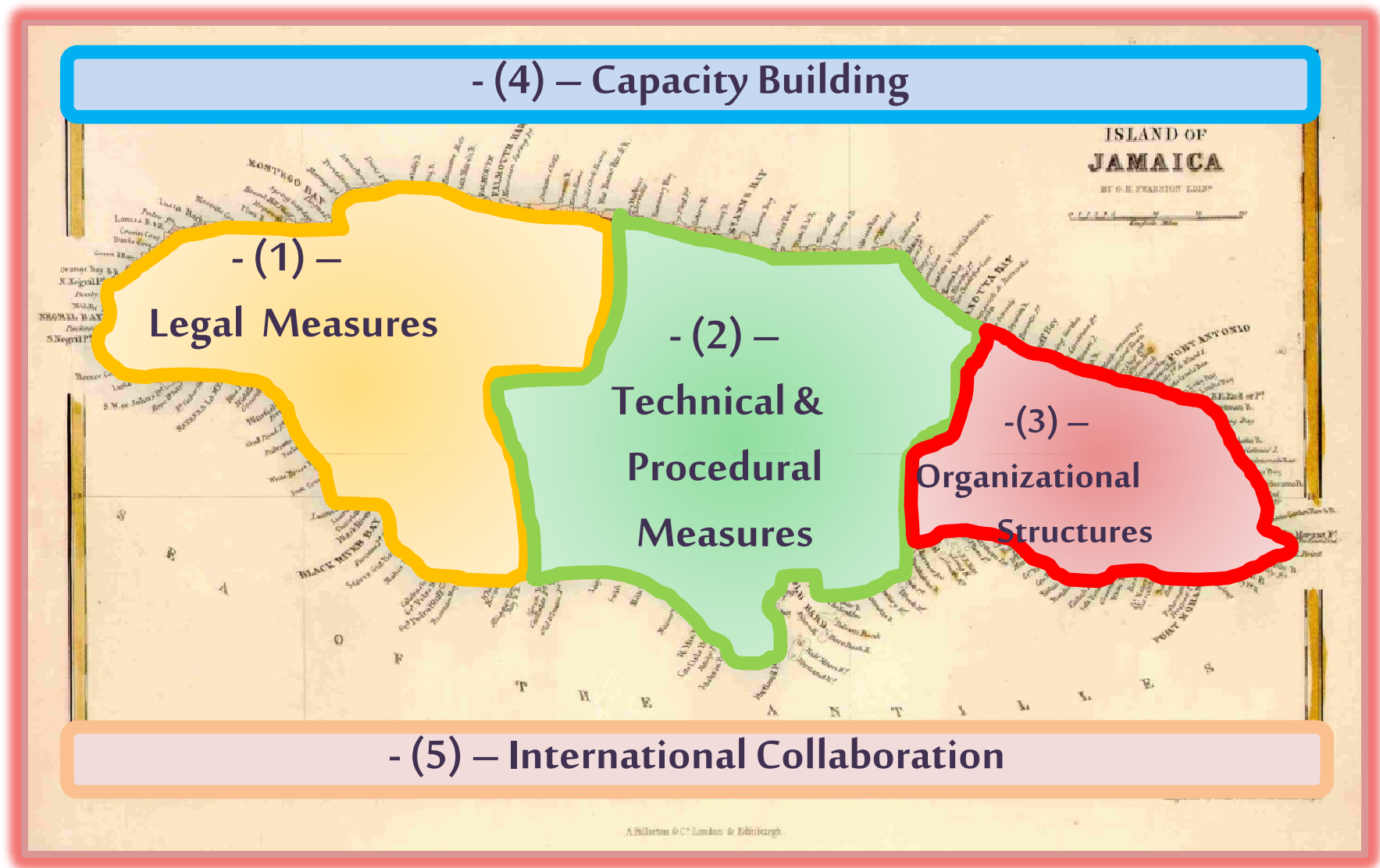
- 1) Access Control
- 2) Application Security
- 3) Business Continuity and Disaster Recovery
- 4) Cryptography
- 5) Information Security and Risk Management
- 6) Legal, Regulations, Compliance and Investigations
- 7) Operations Security
- 8) Physical (Environmental) Security
- 9) Security Architecture 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 3 Short Talks @ NICE have provided the foundations!***



# Securing **Jamaica** in **Cyberspace**! : 2010 - 2018



# ITU: **Cybersecurity** Training – UTECH, Kingston, **JAMAICA**

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





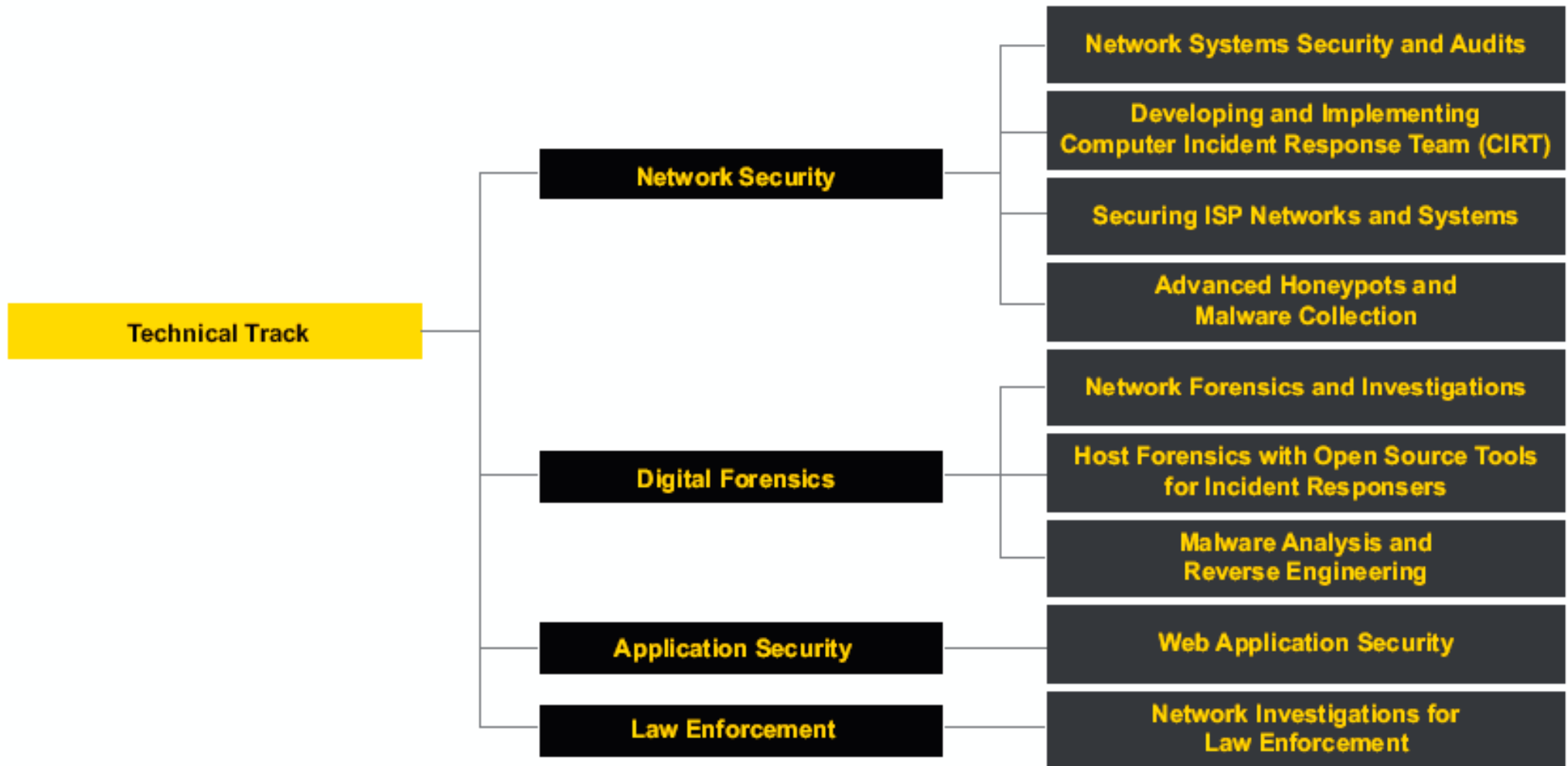
# IMPACT : Worldwide *Cybersecurity* Alliance

IMPACT International Partners: ITU, UN, INTERPOL and CTO



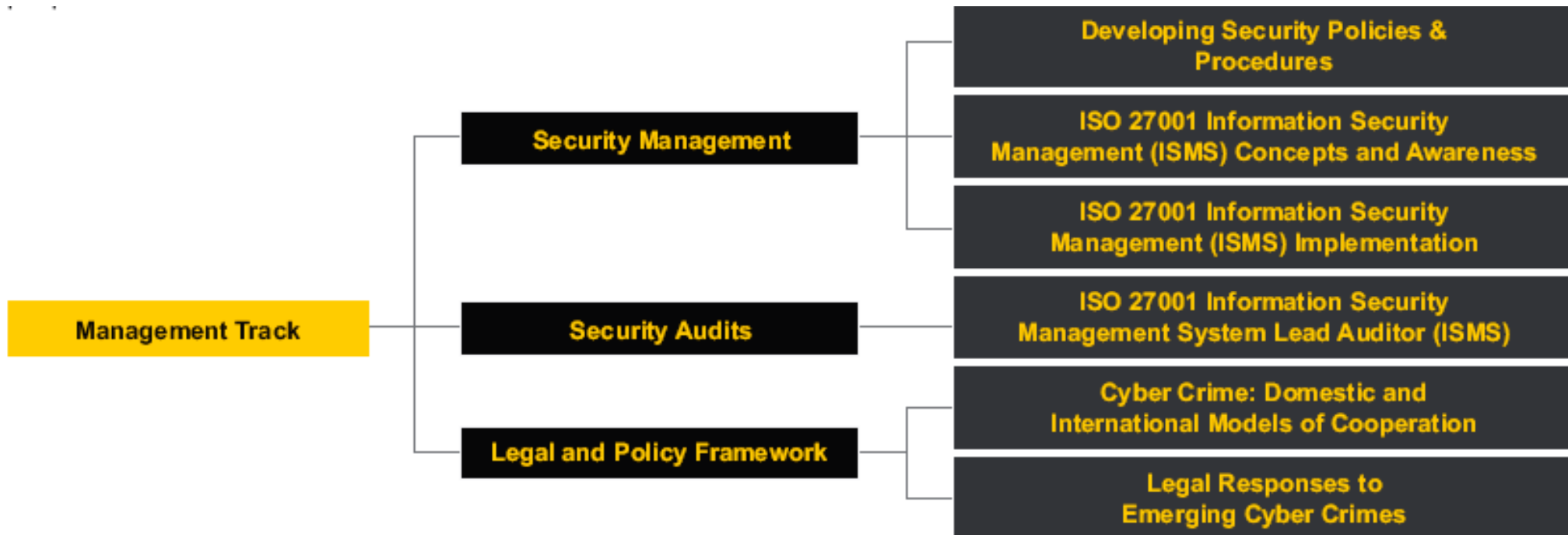
Industry Partners include: Symantec, Kaspersky Labs, Cisco, Microsoft, (ISC)<sup>2</sup>, F-Secure, EC-Council, Iris, GuardTime, Trend Micro and the SANS Institute

# IMPACT: *Cybersecurity Technical Training*





# IMPACT: *Cyber Management Training*



# *MSc CyberSecurity Courses:* Certified by the UK Government – **GCHQ/CESG**



"Cybersecurity for Critical National  
Infrastructure" - *Strategy & RoadMap*  
Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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

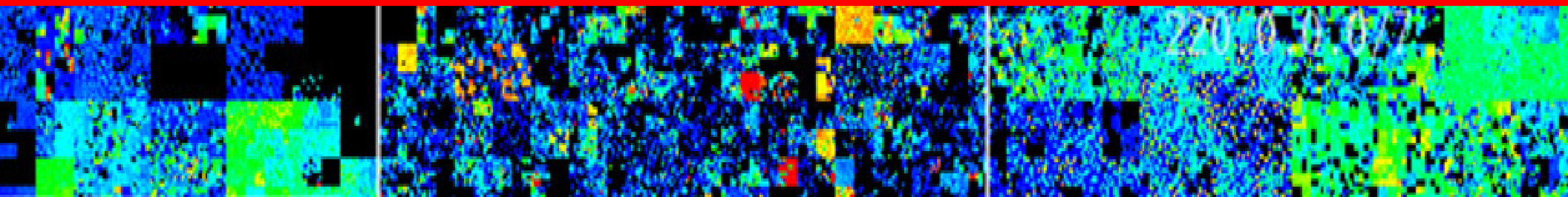




# *Cyber* Security for *Critical* Infrastructure!



## 9 – *YOUR Business Cyber RoadMap* “Multi-Year *Cyber* Plan”



# National Cybersecurity Project RoadMap:

## *Spanning the UN/ITU Cybersecurity Framework*

Jamaican Cybersecurity Roadmap														
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)-														

"Cybersecurity for Critical National  
Infrastructure"- Strategy & RoadMap

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# 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 Cyber Security*

# Critical Economic Sectors: *Cyber RoadMaps*

Each Critical Service Sector such as Banking & Finance, Civil & National Defence, Telecommunications and Energy will require its own Cyber Strategy, Risk Assessment, Roadmap & Action Plan:

➤ In this talk we've discussed some practical ways in which you may develop Strategies, Actions and Activities for CyberSecurity in each Critical Sector...

➤ We've also reviewed the Operational Priorities & Security Policies that are required to significantly reduce Cybercrime & Cyber Terrorism Attacks!.....





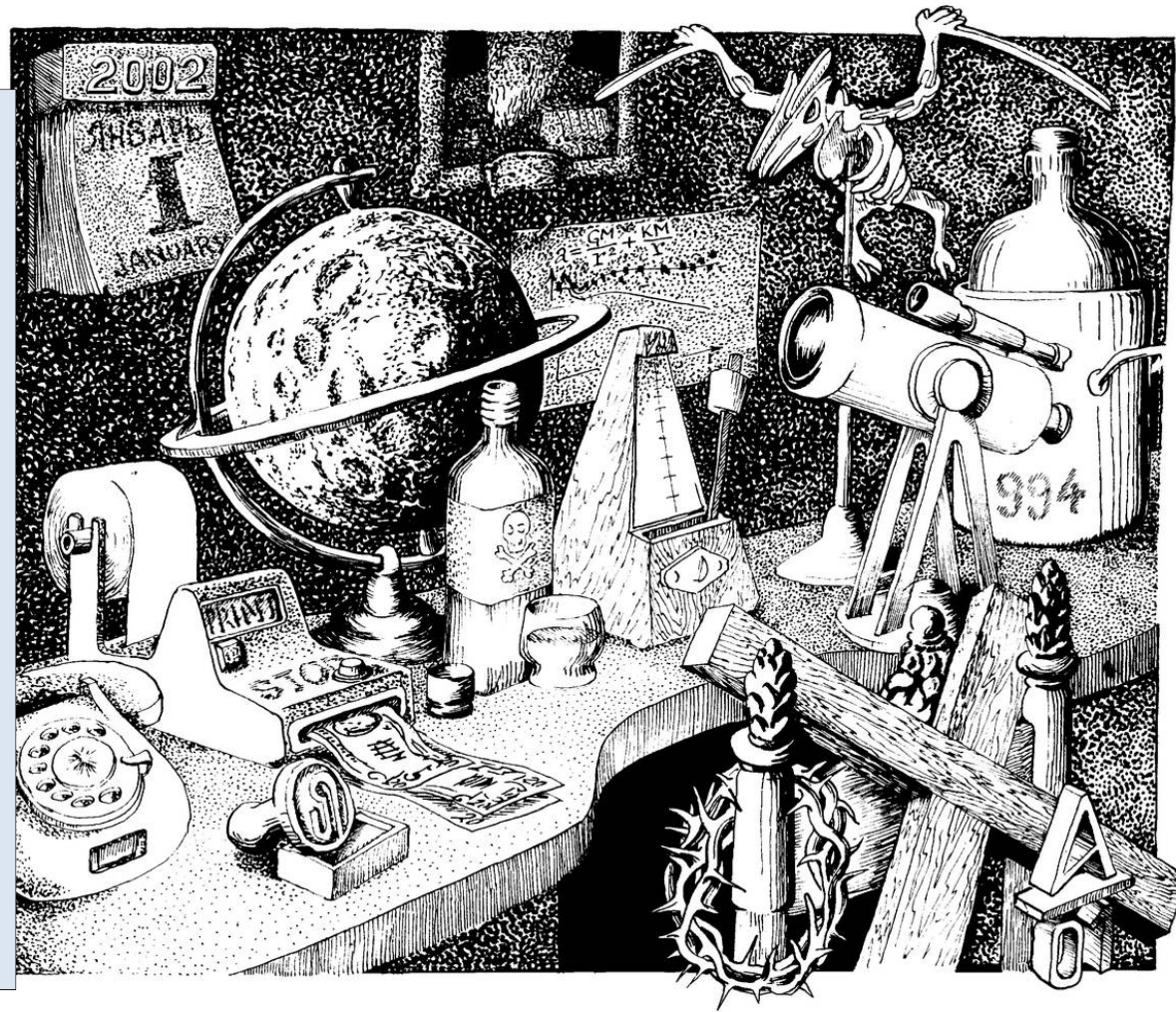
# YOUR Cybersecurity *Action Plan*!...

- **Phase 1:** Define your Cybersecurity STRATEGY and OBJECTIVES
- **Phase 2:** Establish, Resource & Rrain your Cybersecurity ORGANISATION
- **Phase 3:** Agree and Communicate Technical & Operational Standards
- **Phase 4:** Review, Audit and Upgrade all ICT Systems during next year
- **Phase 5:** On-Going Operational Management by CSO/CISO, including regular compliance audits and technical upgrades to new Cyber Threats

.....In summary, the adoption of **International Standards** for YOUR National & Enterprise ICT systems and **ISO Operational Procedures** will have a Major Impact on **Cybercrime**, & reduce **Cyber Attacks** on YOUR **Critical National Infrastructure**

# ***“Real-Time Defence”*** from ***Cyber Attacks”***

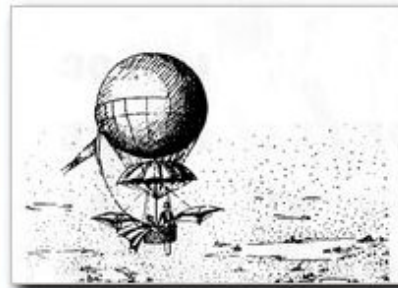
***.....Energising*** YOUR  
Business & Government  
with an Intelligent  
***Cyber\$ecurity \$trategy,***  
***Roadmap & Cyber Tools***  
will increase your  
Defence from “Cyber”  
***Threats and Attacks!***



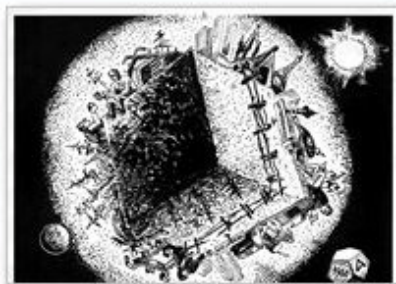
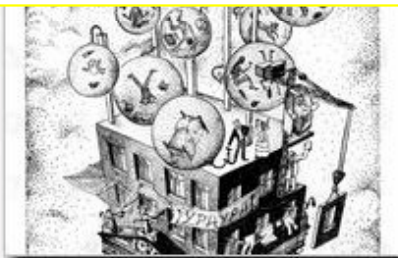
**“The Director’s Desk – Scientific Institute” - 2002**

Pen & Ink Drawing by **Dr Alexander Rimski-Korsakov**





## The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov



**Web Link:** [www.valentina.net/ARK3/ark2.html](http://www.valentina.net/ARK3/ark2.html)

**38<sup>th</sup> International East-West Security Conference**

**"Cybersecurity for Critical National Infrastructure" - Strategy & RoadMap**

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# CyberVision 2020-2030 & Beyond!

- "**CyberVisions**" for Business & Government -



**CyberVision: 2020 to 2030**  
**YOUR 21<sup>st</sup>C CyberSecurity ToolKit!**

Dr David E. Probert  
VAZA International

**(1) CyberVision: 2030**



Intelligent **Cyber** Surveillance  
**AI Video Analytics & Biometrics!**

Dr David E. Probert  
VAZA International

**(2) Cyber Surveillance**



**CyberSecurity Strategy for**  
**Critical National Infrastructure!**

Dr David E. Probert  
VAZA International

**(3) Critical CyberSecurity**

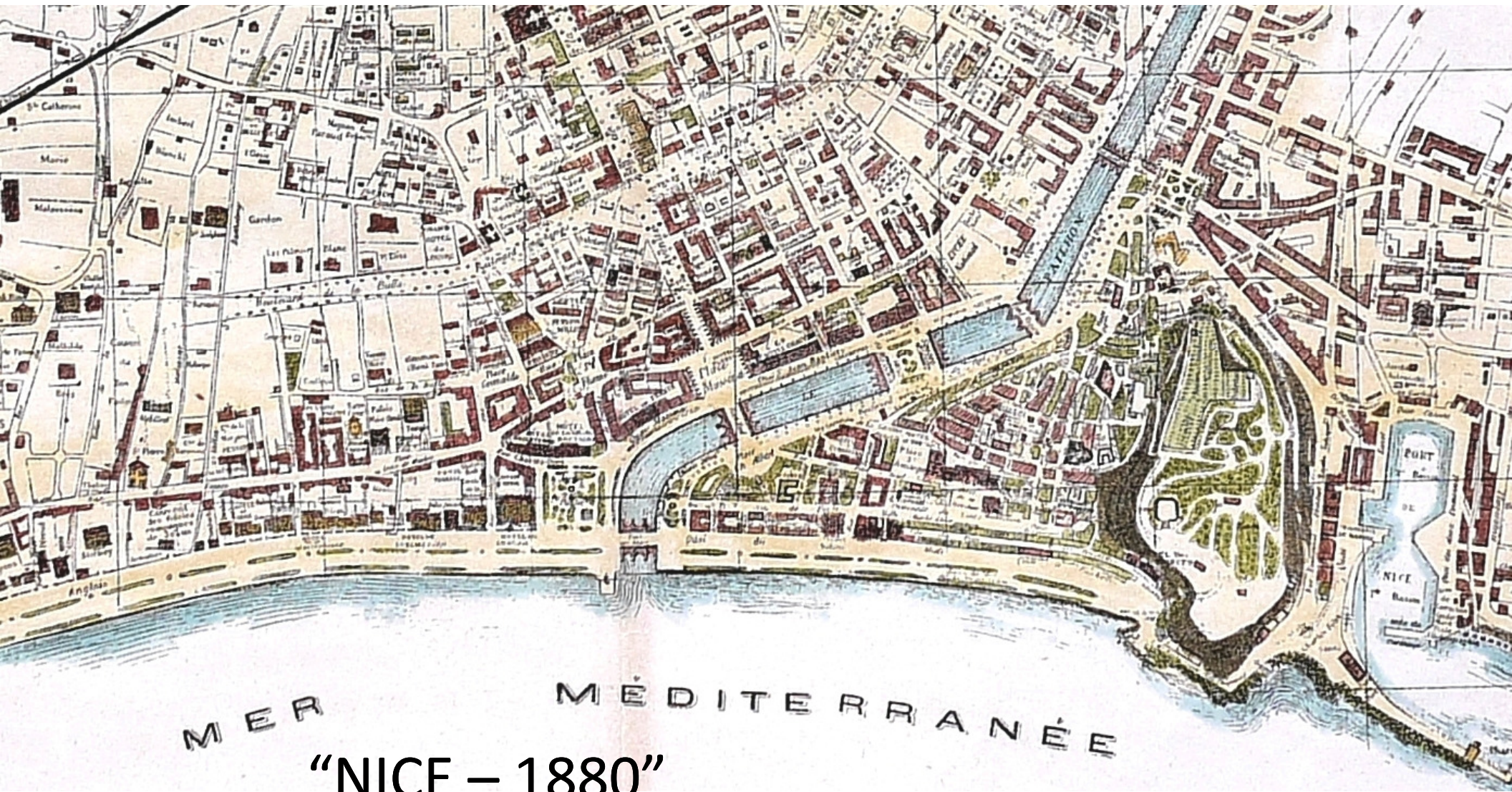
\*\*\* 38th International East-West **Security** Conference: NICE, France-2018 \*\*\*

Download **Cyber** Slides: [www.valentina.net/NICE2018/](http://www.valentina.net/NICE2018/)



# *Cyber*Vision 2020-2030 & *Beyond*!...

*38<sup>th</sup> East-West Security Conference: Nice, UK*



“NICE – 1880”

38<sup>th</sup> International East-West Security Conference

“Cybersecurity for Critical National Infrastructure” - Strategy & RoadMap

Nice, France – 5<sup>th</sup>/6<sup>th</sup> Nov 2018

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





# *Cyber*Vision 2020-2030 & *Beyond*!...

*38<sup>th</sup> East-West Security Conference: Nice, UK*

**Thank-You!**

**Download Presentation Slides:**

***[www.Valentina.net/NICE2018/](http://www.Valentina.net/NICE2018/)***



**Download Presentation Slides:**  
***[www.Valentina.net/NICE2018/](http://www.Valentina.net/NICE2018/)***



**Thank you for your time!**

# Additional *Cybersecurity* Resources

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

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

"Cybersecurity for Critical National Infrastructure"- Strategy & RoadMap  
Nice, France – 5th/6th Nov 2018

© 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, and then by UN/ITU to review Cybersecurity for the Government Ministries.
- **UN/ITU** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

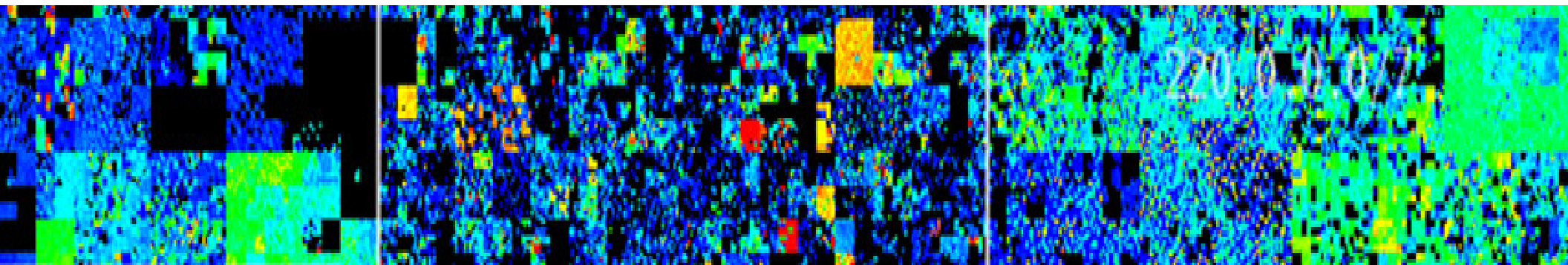
*Dr David E. Probert is a Fellow of the Royal Statistical Society, IEEE Life Member and 1<sup>st</sup> Class Honours Maths Degree (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata), and his full professional biography is featured in the Marquis Directory of Who's Who in the World: 2007-2020 Editions.*

# **Cyber** Security for **Critical** Infrastructure!

## 38<sup>th</sup> East-West Security Conference: **NICE**



# BACK-UP SLIDES





# “Surfing the Evolutionary **Cyber Waves**”

- *Nearly 50 Years of **AI & CyberSecurity**!* -

- 1970 – BT Research Labs – IBM 360 – Digital PCM
- 1976 – AI Thesis – Stochastic Learning Automata
- 1982 – AI & Expert Systems: UK Govt Programme
- 1991 – EARN/TERENA: European Networks Board
- 1992 – International Net Conference: RAS, Moscow
- 1994 – EMEA – Internet, Security & eCommerce
- 2007 – Georgian Parliament Security Projects
- 2009 – Armenia eGovernance & CyberSecurity
- 2010 – Georgian Cybersecurity Audit & Roadmap

....Global Marketplace for **“Cyber” AI/ML Apps** will  
mainstream during the **Next 7 Years: 2018 – 2015** !