



"Smart Security" **Architectures for** ***YOUR* Business!**

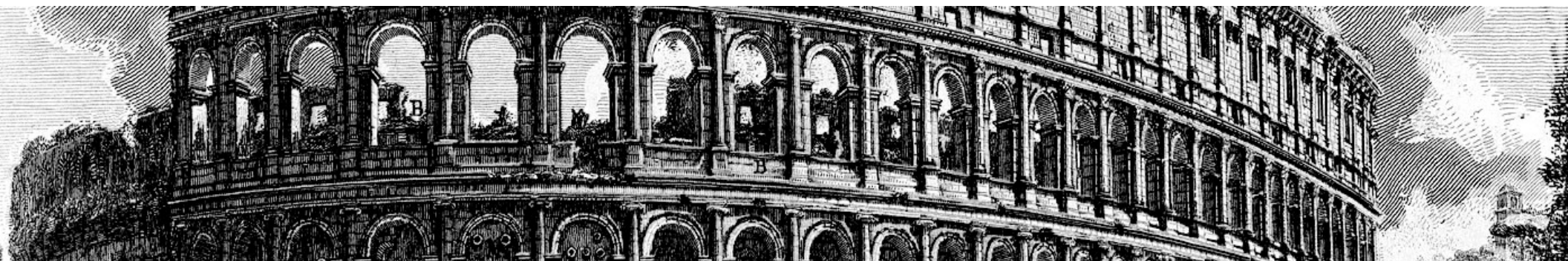
Dr David E. Probert
VAZA International

Dedicated to Grand-Daughters – Abigail, Alice & Tatiana – *Securing YOUR Life!*

34th International East/West Security Conference

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©





“Смарт Архитектура” **- безопасности -** **для *вашего* бизнеса**

Dr David E. Probert
VAZA International

Dedicated to Grand-Daughters – Abigail, Alice & Tatiana – *Securing YOUR Life!*

34th International East/West Security Conference

“21stC Smart Security Architectures”
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



“Smart Cybersecurity”: *Dual Themes*

Theme (1) –**21stC Smart Security Architectures** for **YOUR** Business.....



“Smart Security” Integrates Cyber & Physical Technologies to provide Effective Real-Time Surveillance for both Business & Government. We review Practical Applications for YOUR Critical Business Sectors.

“Integration” : “SMART Real-Time Security & Surveillance” 11:45 21st Nov 2016

Theme (2) –**CyberSecurity Vision: 2017 – 2027 & Beyond**.....



CyberSecurity is becoming transformed with Real-Time Cyber Tools based upon Artificial Intelligence & Machine Learning. These are *Essential* to win the war against CyberCrime and CyberTerrorism

“Intelligence” : “ADAPTIVE Self-Learning CyberSecurity for IoT” 09:00 22nd Nov 2016

Download Slides: www.valentina.net/Rome2016/

Background: **20th to 21stC Cybersecurity**

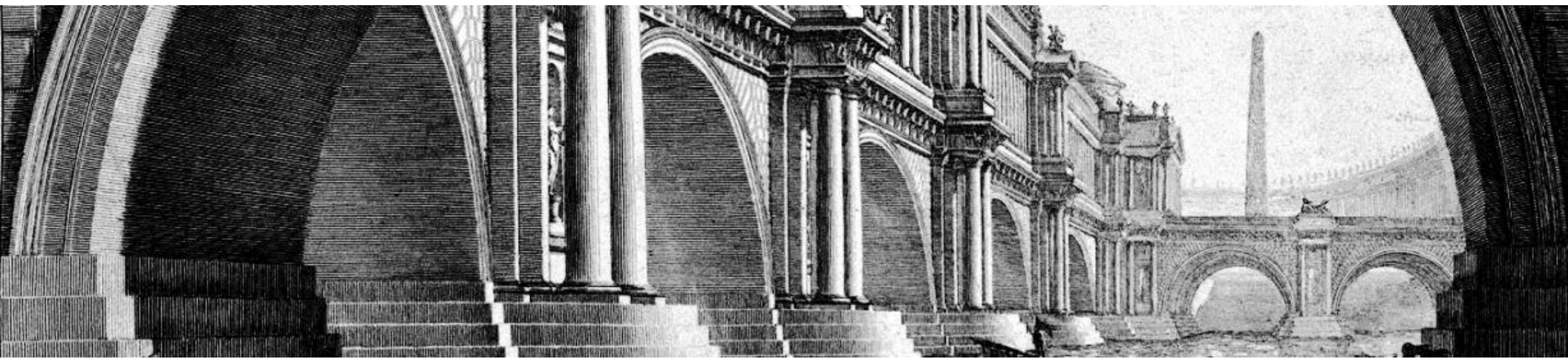
- **20thC : 1995 - 2010** : Focus on Firewalls & Antivirus – based upon Physical “Spatial” Security Models (Castles & Moats)

.....Protection @ ***“Speed of Sound” (Space)***

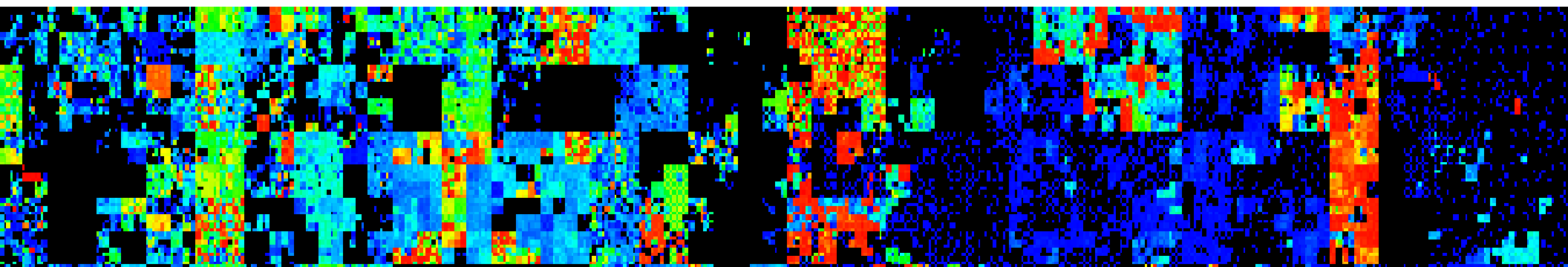
- **21stC : 2010 – 2025** : Focus on Adaptive, and Self-Organising “Cyber” Tools – based upon Temporal Models (AI & Machine Learning)

.....Defending @ ***“Speed of Light” (Time)***

“Smart Security”: 21stC Business Architectures



1 – Background: “21 st C Security Landscape”	2 – Basic “Smart Security” Concepts	3 – Integrated Cyber-Physical Security
4 – Towards “Smart Security” Architectures	5 – “Smart Security” for <i>YOUR</i> Business!	6 – Security Scenarios: Critical Sectors
7 – Smart Security for “Internet of Things”	8 – Practical “Smart Security” Operations	9 – <i>YOUR</i> TOP 3 Actions & RoadMap!



1) 21stC *CyberSecurity* Landscape

- Convergence of Physical & Cybersecurity Operations
- “Cyber” migrates from IT Dept to Main Board: C-Suite
- Global Real-Time Targeted Cyber Attacks – 24/7
- Transition from 20thC Tools (Firewalls & Anti-virus) to “Smart” 21stC Tools (AI & Machine Learning)
- Emergence of Enterprise “Internet of Things” - IoT
- Evolution of Smart Devices, Cities, Economy & Society
- Dramatic increase in Cyber Crime & Cyber Terrorism

There are **Cyber/Terror Attacks** each Week! We urgently need to boost our Business & Government Cyber Defences with “**Real-Time Smart Security**”!

UK CyberSecurity Strategy: 2016 - 2021



NATIONAL CYBER SECURITY STRATEGY 2016-2021

Defend – Deter - Develop



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

34th International East/West Security Conference

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



Cyber-Physical Threat Scenarios

- **Physical “Penetration”**: Operations Perimeter penetrated to allow theft or corruption of Cyber Information / IT Data Bases , Personal ID / Financial Data and Confidential Company Plans
- **Cyber “Hack”**: Malicious changes to Cyber Access Controls & IT Databases to allow Criminals/Terrorists to enter Target Facilities (such as Banking/Finance, Telco/Mobile Operations)
- **Convergent Threats** – Criminals/Terrorists will attack at the weakest links which in the 21stC will be **BOTH** Cyber Network Operations, Physical Security Operations & Internet of Things!

.....**Cyber Attacks** are now fully industrialised with Malicious Code “Kits” & Botnets for sale “*by the hour*” on the **DARKWEB**

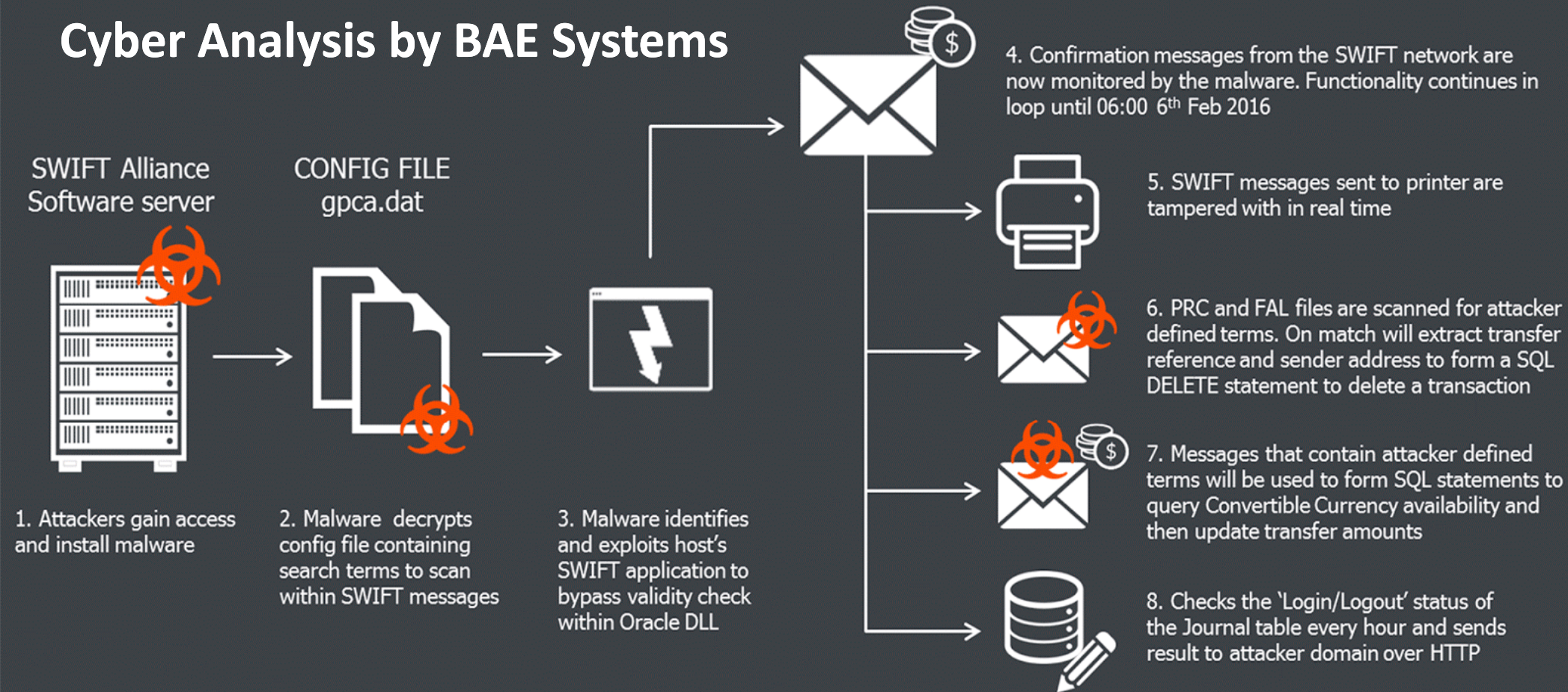
Malware Attack: **SWIFT** Bank Net – 2016



Multiple Cyber Attacks including Cyber Heist of **\$951M** from **Bangladesh Central Bank** of which **\$81M** remains missing!

Malware Attack: **SWIFT** Bank Net – 2016

Cyber Analysis by BAE Systems







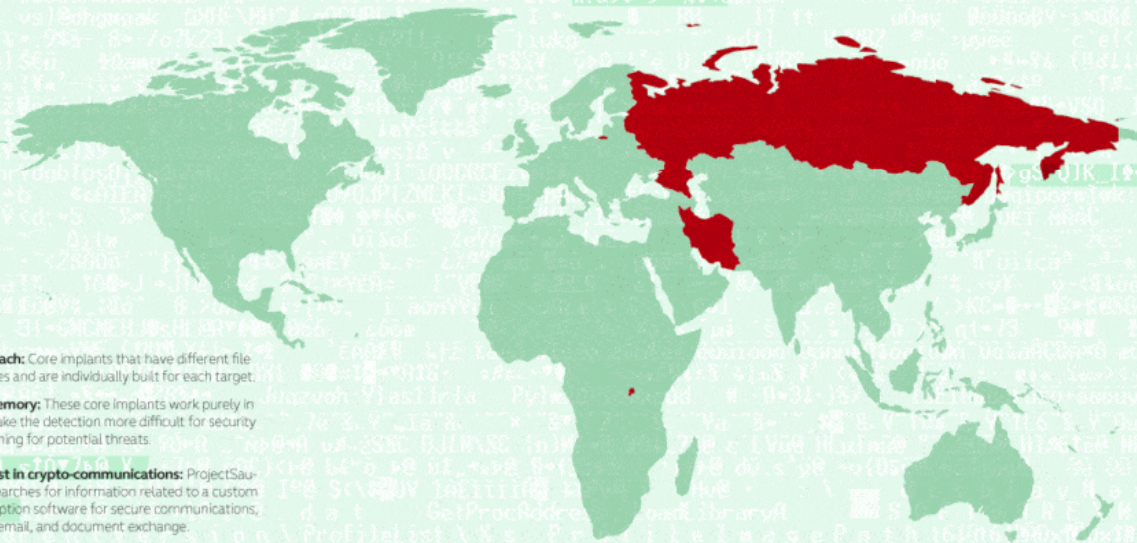
Multiple Cyber Attacks including Cyber Heist of **\$951M from Bangladesh Central Bank of which **\$81M** remains missing!**

Project Sauron: **CyberEspionage** - 2016

ProjectSauron advanced persistent threat

'ProjectSauron' is a unique 'pattern-less' threat actor responsible for highly-targeted, resource-intensive cyber-espionage attacks against government and research organizations as well as communication and financial companies. Victims have been found in the Russian Federation, Iran, and Rwanda but this is likely to represent the tip of the iceberg.

 Government  Military organizations  Scientific research centers  Telecoms providers  Financial organizations



Key features:

-  **Unique approach:** Core implants that have different file names and sizes and are individually built for each target.
-  **Running in memory:** These core implants work purely in memory to make the detection more difficult for security solutions scanning for potential threats.
-  **Special interest in crypto-communications:** ProjectSauron actively searches for information related to a custom network encryption software for secure communications, such as voice, email, and document exchange.
-  **Bypassing air-gaps:** Remsec uses specially-prepared USB drives to jump across air-gaps, carrying hidden compartments in which stolen data is concealed.

Analysed by Symantec and Kaspersky Labs...

- August 2016 -

Known CyberTargets include: Russia, China, Iran, Rwanda, Italy Sweden & Belgium






Other "State-Designed" Cyber Malware include: **Stuxnet, Duqu, Flame, Equation and Regin...**

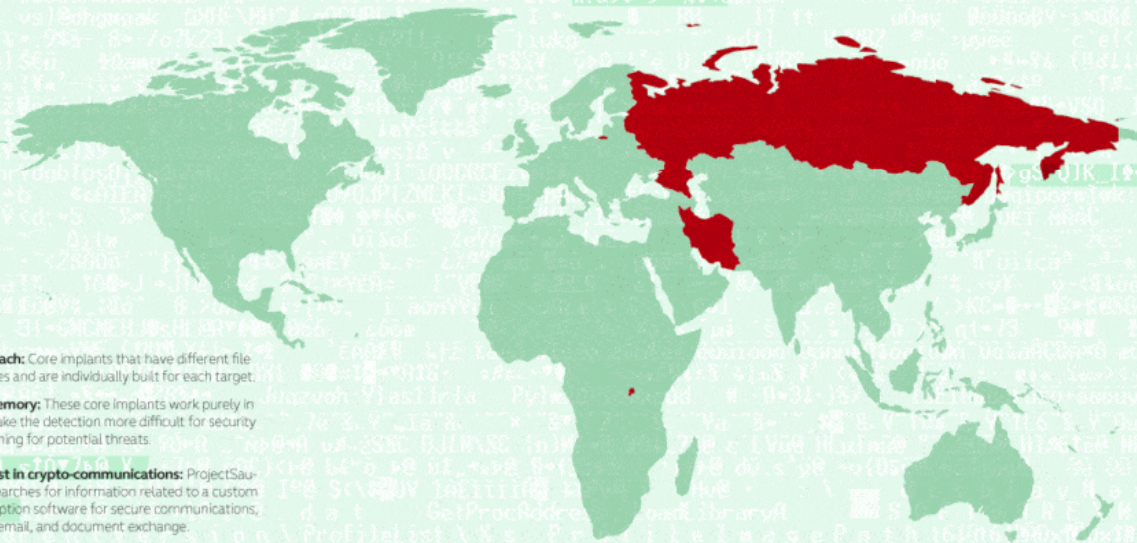
Powerful **APT Malware** that targeted **Critical National Infrastructure: Top Level** Government. Military, Telecoms, Finance and R&D Centres

Project Sauron: **CyberEspionage** - 2016

ProjectSauron advanced persistent threat

'ProjectSauron' is a unique 'pattern-less' threat actor responsible for highly-targeted, resource-intensive cyber-espionage attacks against government and research organizations as well as communication and financial companies. Victims have been found in the Russian Federation, Iran, and Rwanda but this is likely to represent the tip of the iceberg.

 Government  Military organizations  Scientific research centers  Telecoms providers  Financial organizations



Key features:

-  **Unique approach:** Core implants that have different file names and sizes and are individually built for each target.
-  **Running in memory:** These core implants work purely in memory to make the detection more difficult for security solutions scanning for potential threats.
-  **Special interest in crypto-communications:** ProjectSauron actively searches for information related to a custom network encryption software for secure communications, such as voice, email, and document exchange.
-  **Bypassing air-gaps:** Remsec uses specially-prepared USB drives to jump across air-gaps, carrying hidden compartments in which stolen data is concealed.

Analysed by Symantec and Kaspersky Labs...

- August 2016 -

```
KBLOG_ROTATE_SECS = 1
tmp_dir = os.getenv("
drive = "C:\\\\"
SAURON_KBLOG_KEY = "m
create_log = function
local f = ""
```

Other “State-Designed” Cyber Malware include: **Stuxnet, Duqu, Flame, Equation and Regin...**

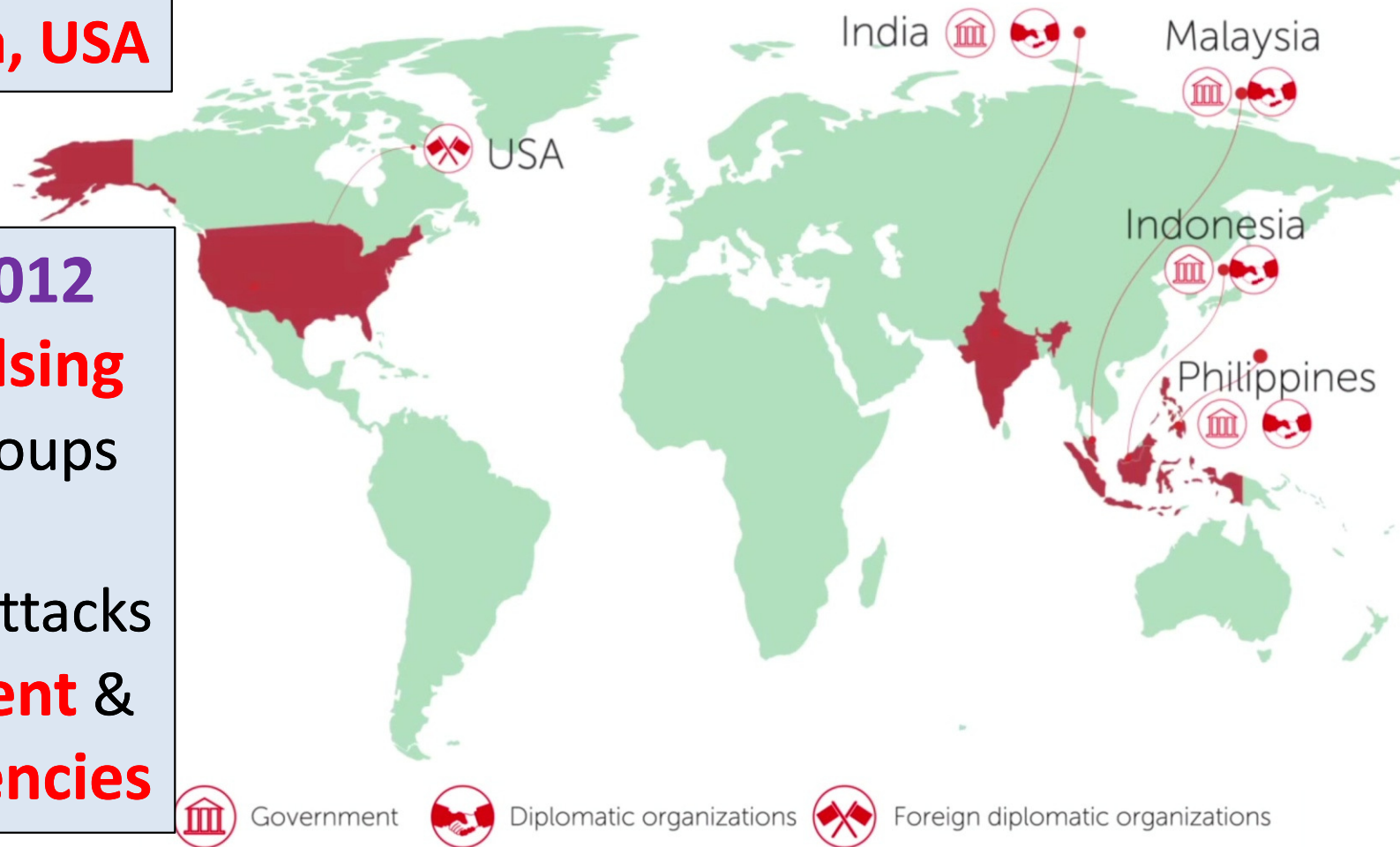
Powerful **APT Malware** that targeted **Critical National Infrastructure:** **Top Level** Government. Military, Telecoms, Finance and R&D Centres

CyberEspionage in Asia-Pacific Region

APT Victims were in
Malaysia, Philippines
Indonesia, India, USA

Attacks from **2012**
onwards by **Helling**
and **Naikon** Groups

VICTIMS OF THE HELLSING CYBERESPIONAGE GROUP



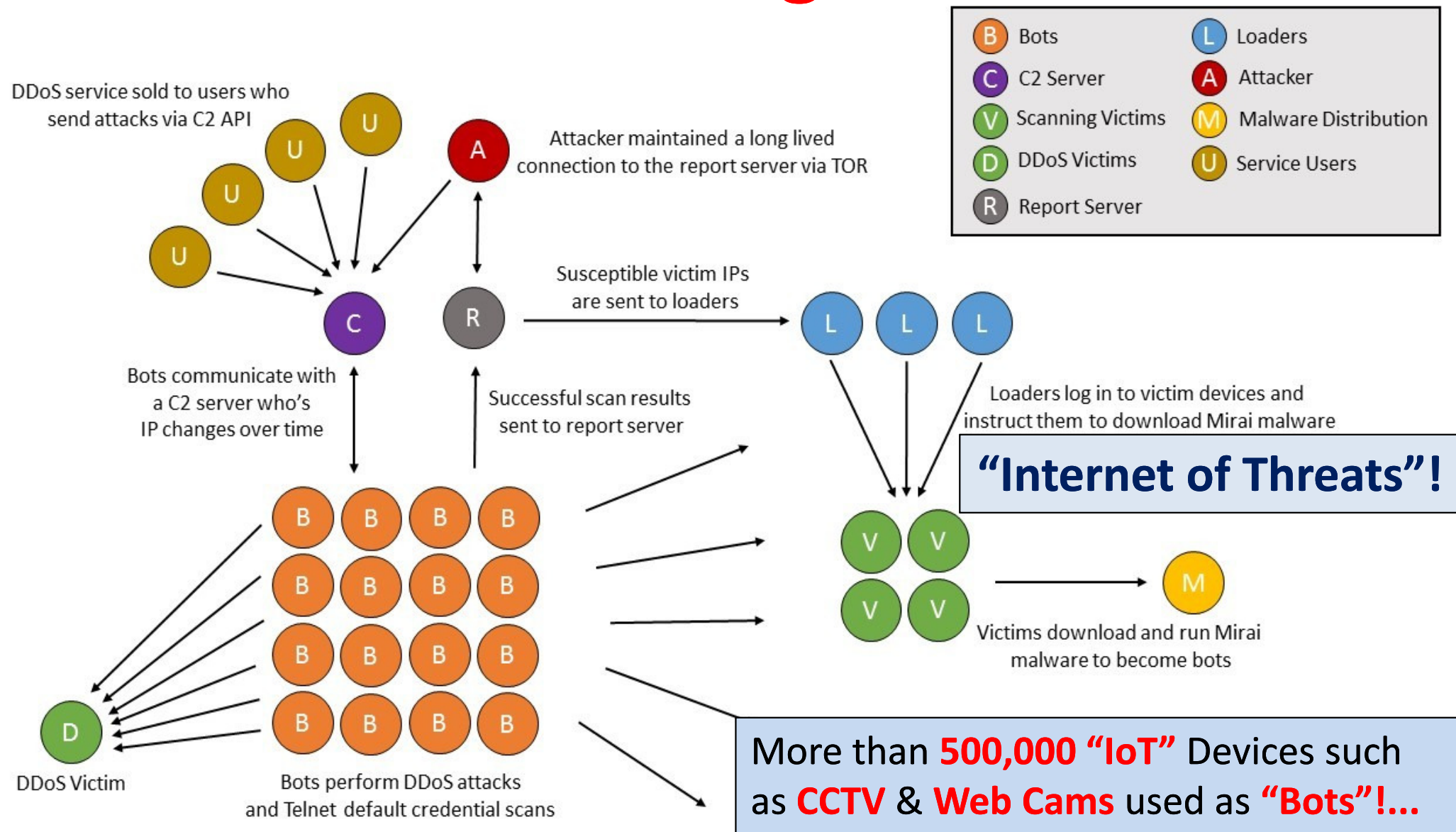
Targets of **APT** Attacks
were **Government &**
Diplomatic Agencies

Analysed by **Kaspersky Labs**: **April 2015**
34th International East/West Security Conference

"21stC Smart Security Architectures"
- **Real-Time Cyber-Physical Integration** -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



Massive DDoS Attack using Mirai BotNet from “Internet of Things” - 21st Oct 2016



CyberAttack: **Tesco Bank** – 6th Nov 2016



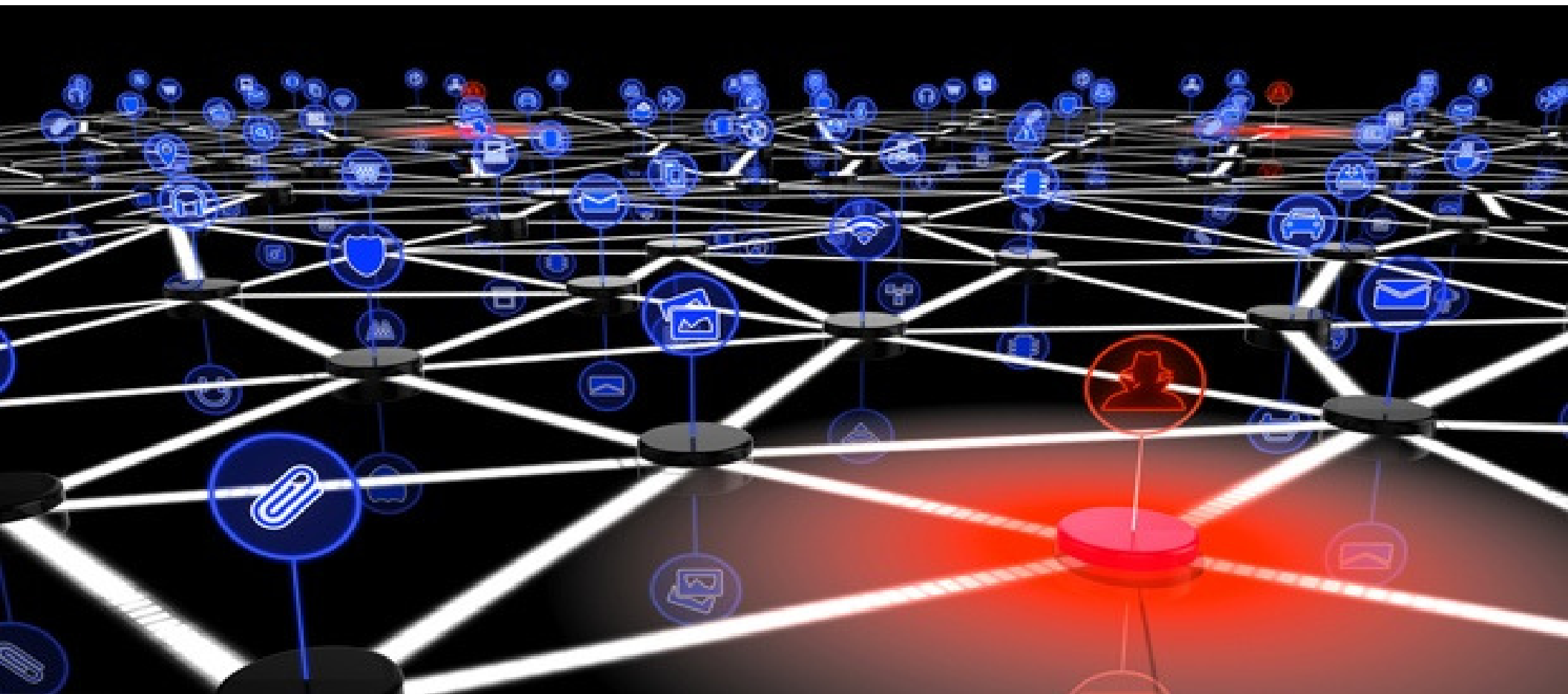
6th Nov 2016: Cyber Criminals from Brazil & Spain hack 40,000 TESCO Bank Accounts with reported Theft of £2.5m from 9,000

CyberAttack: SberBank - Сбербанк: 8th Nov 2016



Massive DDoS Attack from **24,000 “Bot” Devices (Internet of Things)**
Hits SberBank, Alfa Bank, Moscow Bank, RosBank, Moscow Exchange
- **Peak Web IP Requests of 660,000/Sec** quoted by **Kaspersky Labs** -

CyberAttack: **SberBank - Сбербанк**: 8th Nov 2016



Massive DDoS Attack from **24,000 “Bot” Devices (Internet of Things)**
Hits SberBank, Alfa Bank, Moscow Bank, RosBank, Moscow Exchange
- **Peak Web IP Requests of 660,000/Sec** quoted by **Kaspersky Labs** -

Categories of *Cybersecurity* Threats

- The complexity of Cyber threats means that several frameworks have been developed to classify cyber risks such as the **UN/ITU Guidelines**:

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

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

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

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

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

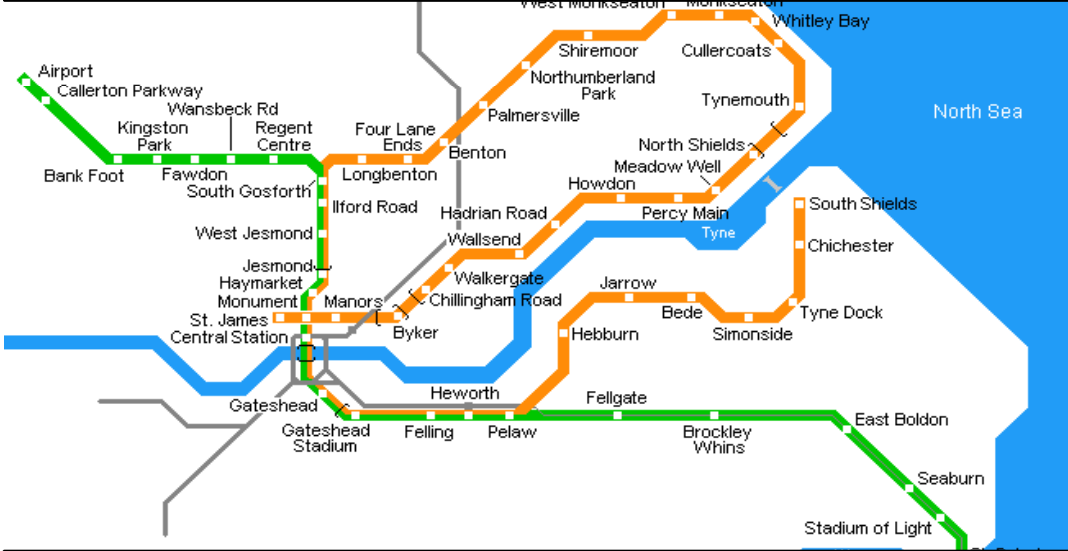
Category 6 : Other Unconfirmed Incidents – *These are alerts that require further investigation to understand whether they are actually malicious or “false positives”...*

We next put these **Hybrid Cyber and Physical Security Risks** into a **Personal Context...**

International Security: *“Family Perspective”*



Jeju Island – South Korea: **“Simon”**



Newcastle – UK: **“Philip”**

Global 24/7 Security Risks & Threats !



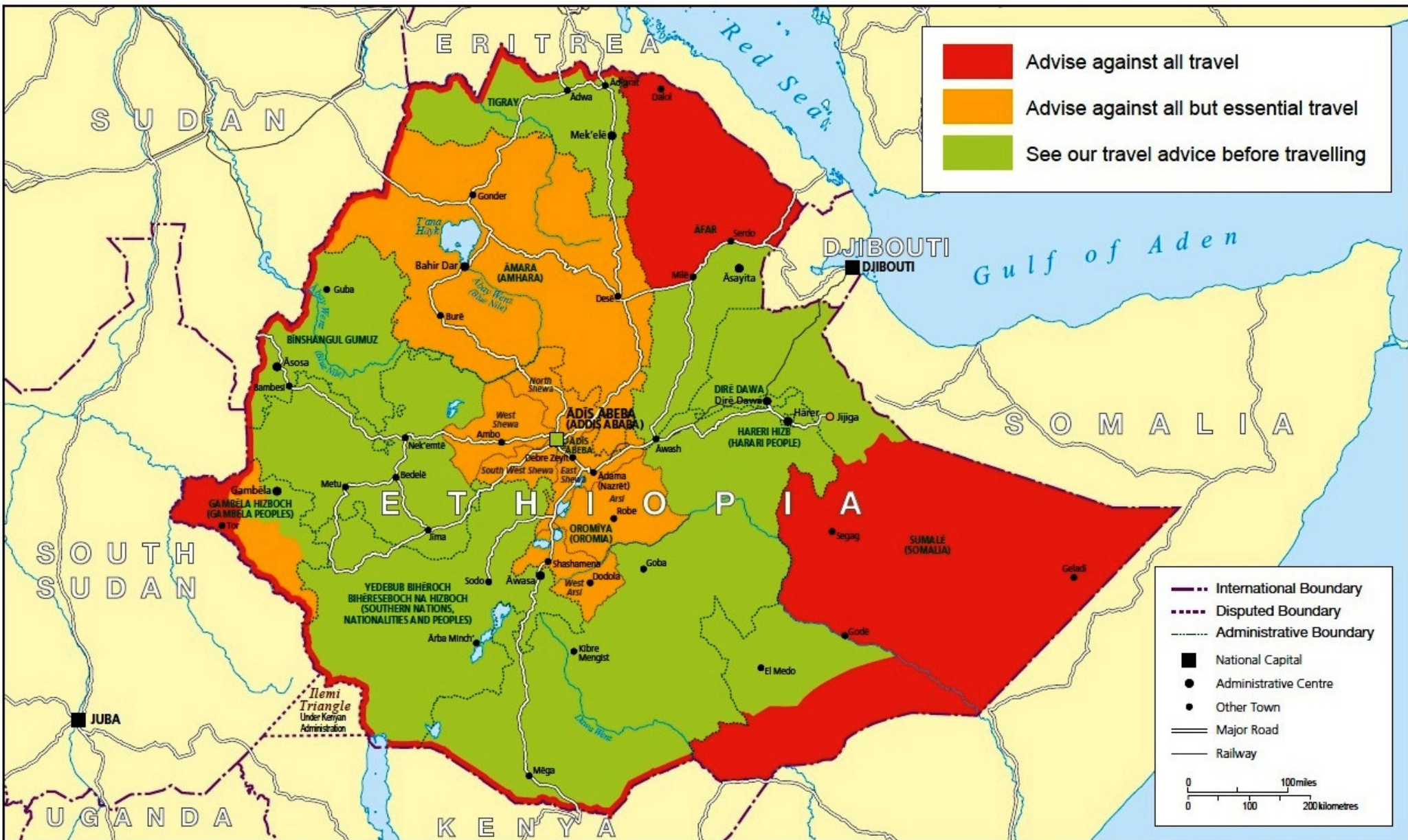
Cambridge – UK: **“Joanna”**



Gambella – Ethiopia: **“Susan”**



Security in Ethiopia: “State of Emergency”



Cybersecurity in Ethiopia



CYBERWELLNESS PROFILE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA



BACKGROUND

Total Population: 86 539 000

(data source: [United Nations Statistics Division](#), December 2012)

Internet users, percentage of population: 1.90%

(data source: [ITU Statistics](#), December 2013)

More than 60% of the UN/ITU Member Nations still have no Public Domain Government Info & Cybersecurity Strategy

So 120 Nations have minimal Cyber Protection for their Business & Critical Sectors !

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- None.

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- None.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Ethiopia does not have an officially recognized national CIRT. A CIRT Assessment is currently being carried out by the ITU.

1.2.2 STANDARDS

Ethiopia does not have an officially approved national or sector specific cybersecurity framework for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Ethiopia.

www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Ethiopia.pdf (2015)



Cybersecurity Market Sectors

- Anti-Virus/Firewall
- ID Authentication
- Encryption/Privacy
- Risk & Compliance
- Mobile Device Security
- Anti-Fraud Monitoring
- Website Protection
- S/W Code Verification
- AI & Machine Learning
- Enterprise IoT Security
- Cloud Security Services
- Big Data Protection
- RT Log/Event Analytics
- Real-Time Threat Maps
- Smart Biometrics
- Training & Certification

Global Trend is towards ***Adaptive & Intelligent Cybersecurity Solutions/Services...***
....Traditional ***Anti-Virus/Firewall Tools*** no longer fully effective against ***“Bad Guys”!***

Cybersecurity Market Size & Growth

- **2015: Worldwide Estimated - \$97 Billion**
- **2020: Worldwide Projected - \$170 Billion**
 - North America: - \$64Bn – 10.0% CAGR (38%)
 - Europe: - \$39Bn – 7.2% CAGR (23%)
 - Asia-Pacific: - \$38Bn – 14.1% CAGR (22%)
 - Middle East & Africa: - \$15Bn – 13.7% CAGR (9%)
 - Latin America: - \$14Bn – 17.6% CAGR (8%)

(**Source:** “Micro Market Monitor” & “Markets and Markets” –
Estimated and Extrapolated from projections for 2014 – 2019)

- **2025: Worldwide @ 10% CAGR - \$275 Billion**

Cyber Solutions from Corporations

- Consultancy, Networking and Services -

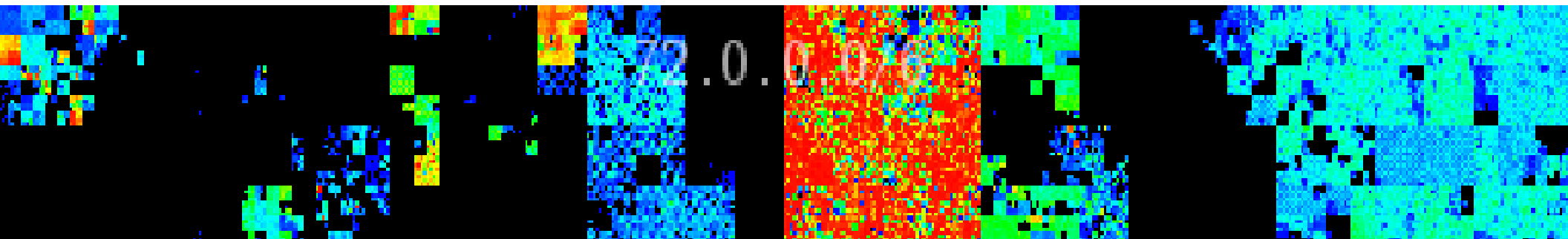
- **Sophos Group (UK)**—Security Solutions
- **CISCO** – Threat Protection Security
- **Northrop Grumman** – Cyber & Homeland Security Services
- **PwC** – Cyber Consultancy
- **Intel Security Group (McAfee)** – Malware & Threat Protection
- **British Telecom** – Security Mgt
- **Juniper Networks** –Threat Intel, Protection and Network Security
- **Ernst Young** – Cyber Consultancy
- **Booz Allen and Hamilton** – Cyber Solutions & Services
- **Kaspersky Lab(RU)** – Security Solutions
- **Symantec (US)** – Security Solutions
- **BAE Systems** – Cyber Risk Mgt
- **IBM** – Solutions & Services
- **Deloitte** – Cyber Consultancy
- **Raytheon** – Cyber & Homeland Security Services (USA + Global)
- **Thales** – Secure IT Solutions
- **Lockheed Martin** –Cyber Solutions
- **Dell Secure Networks** – Managed Network & Computing Security Services
- **AT&T**-Network Security & Services
- **HP** – Enterprise Cybersecurity Solutions

ALL Major IT Vendors now invest in Cyber Solutions as Hi-Growth Sector

“Smart Security”: *Business Architectures*



1 – Background: “21 st C Security Landscape”	2 – Basic “Smart Security” Concepts	3 – Integrated Cyber-Physical Security
4 – Towards “Smart Security” Architectures	5 – “Smart Security” for <i>YOUR</i> Business!	6 – Security Scenarios: Critical Sectors
7 – Smart Security for “Internet of Things”	8 – Practical “Smart Security” Operations	9 – <i>YOUR</i> TOP 3 Actions & RoadMap!



2) - “Smart Security” - = *Integrated “Cyber-Physical” Operations* =

- Defence against 21stC CyberCrime & Terror Attacks requires Operations in *Real-Time @ Light Speed!*
 - Smart Target *Surveillance*, Profiling & Tracking
 - User & Device *Authentication* – “Internet of Things”
 - Cyber *Biometrics* & *Forensics* – Pre/Post Attack
 - Real-Time Analysis of *Social Media*, eMail & Blogs
 - *Self-Adaptive* User, IT Asset & Net Traffic *Modelling*
 - *Human-Machine Teaming* for Effective Cyber-Defence

.....*Mitigation of Attacks* requires *“Smart Security”*
Computing Solutions running @ Light Speed!

“Smart Security” = Cyber + PSIM + SIEM

- **Cyber:** Spans **ALL ICT** Networks, Servers & Devices
- **PSIM:** **P**hysical **S**ecurity **I**ntegration **M**anagement
- **SIEM:** **S**ecurity **I**nformation & **E**vent **M**anagement

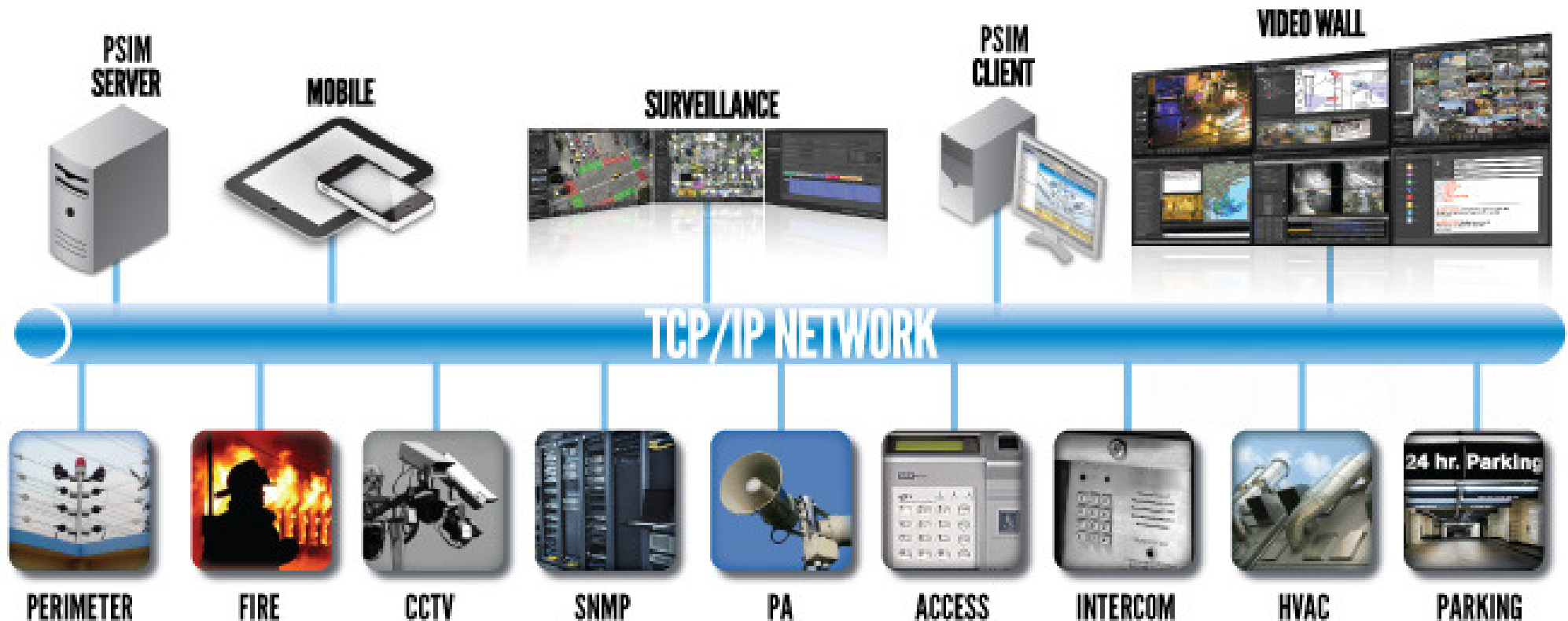


Image: AventuraCCTV.com/PSIM : New York, USA
34th International East/West Security Conference

“21stC Smart Security Architectures”
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



Transition from 20thC to 21stC “*Smart Security*”

- **Integrated Cyber-Physical Security 2016-2021:**
 - Every Business & Nation will need to transition from the traditional 20thC culture & policy of massive physical defence to the connected “neural” 21stC world of in-depth intelligent & integrated real-time cyber defence
- **National Borders:**
 - Traditional physical defence and geographical boundaries remain strategic national assets but they need to be integrated with cyber defence assets.
- **Critical National Information Infrastructure:**
 - 21stC national economies function electronically, & yet they are poorly defended in cyberspace, and open to criminal, terror & political attacks
- **Multi-Dimensional Cyber Defence:**
 - Nations need to audit their critical infrastructure – government, banks, telecommunications, energy, & transport – and to upgrade to international cybersecurity standards based upon accepted “best practice” (ISO/IEC)

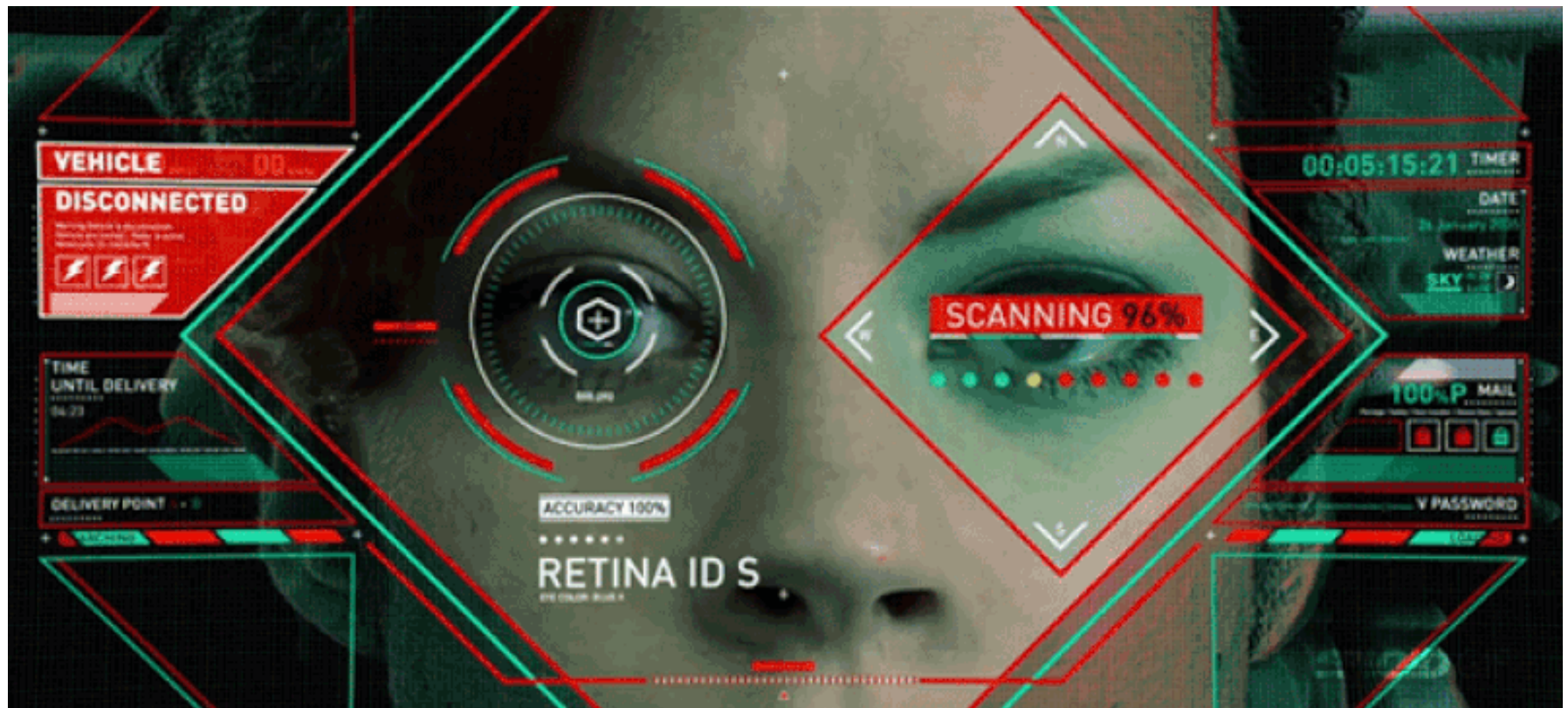
Smart Security: *Tracking “Bad Guys”*

- Mitigating Global Cyber Crime & CyberTerrorism requires us to **Profile & Track** the “**Bad Guys**” in “Real-Time” with “Smart Security” - Intelligent Networked Computing Systems:
 - **3D Video Analytics** from CCTV Facial Profiles
 - Track On-Line **Social Media**, eMail & “Cell” Comms
 - Scan “**DarkWeb**” for “Business Deals”, Plans & Messages
 - Check, Track & Locate **Mobile** Communications
 - Track “**Bad Guys**” in National **Transport Hubs**
 - Deploy **RFID Devices** to Track High-Value & Strategic “Assets”
 - Use **Real-Time ANPR** for Target Vehicle Tracking

...**Cyber Computing Smart Applications** can now Track Massive Databases of Target “**Bad Guy**” Profiles **@ Light Speed!...**

Smart Security: *Tracking “Bad Guys”*

- Mitigating Global Cyber Crime & CyberTerrorism requires us to **Profile & Track** the “**Bad Guys**” in “Real-Time” with “Smart Security” - Intelligent Networked Computing Systems:

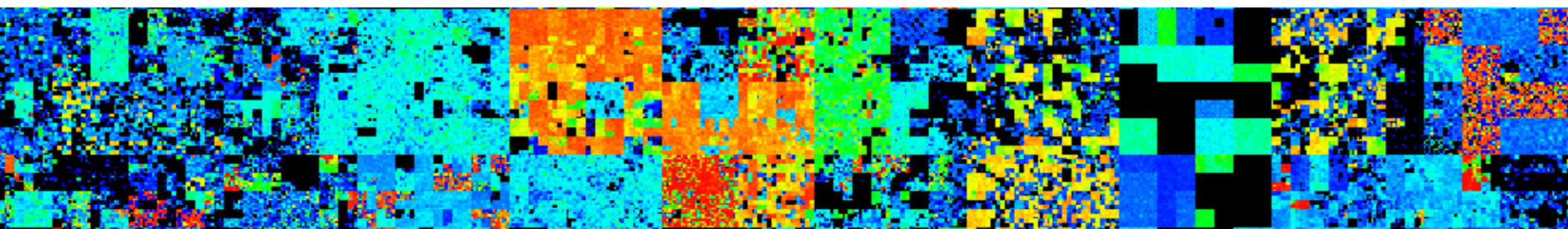


...*Cyber Computing Smart Applications* can now Track Massive Databases of Target “**Bad Guy**” Profiles @ *Light Speed!...*

“Smart Security”: 21stC Business Architectures



1 – Background: “21 st C Security Landscape”	2 – Basic “Smart Security” Concepts	3 – Integrated Cyber-Physical Security
4 – Towards “Smart Security” Architectures	5 – “Smart Security” for <i>YOUR</i> Business!	6 – Security Scenarios: Critical Sectors
7 – Smart Security for “Internet of Things”	8 – Practical “Smart Security” Operations	9 – <i>YOUR</i> TOP 3 Actions & RoadMap!



3) Integrated *Cyber-Physical* Solutions

- **ALL Security Tools** will evolve from Physical to Integrated “Smart” Cyber-Physical during 3 to 5 years.
- **Advanced 21st “Smart” Cyber-Physical Security Solutions:**
 - Intelligent “Bad Guy” Profiling & Tracking
 - Real-Time Social Media & On-Line Monitoring
 - CCTV, Facial Recognition & Video Analytics
 - Integrated Cyber-Biometrics & Digital Forensics
 - ANPR Vehicle Location and GPS/Aerial Tracking
 - Adaptive AI/ML Behavioural Modelling of Net Traffic & Users

*....We explore these Integrated **Cyber Solutions** in-depth & their Business Implementation in Critical Sector Scenarios*

Integration of *Physical and Cybersecurity*

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

Physical Security Operations

Cyber Security Operations



Smart Security = Virtual Integration

Corporate CSO-led Security Team
ONE – Shopping List!



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

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

Contrast between our Physical & Cyber Worlds

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

Physical World = “Space”

- Top-Down
- Dynamic
- Secrecy
- Territorial – “Geographical Space”
- Government Power
- Control
- “Speed of Sound”
- Padlocks & Keys
- Assets & Objects
- Hierarchical
- Carbon Life
- Tanks & Missiles
- Mass Media

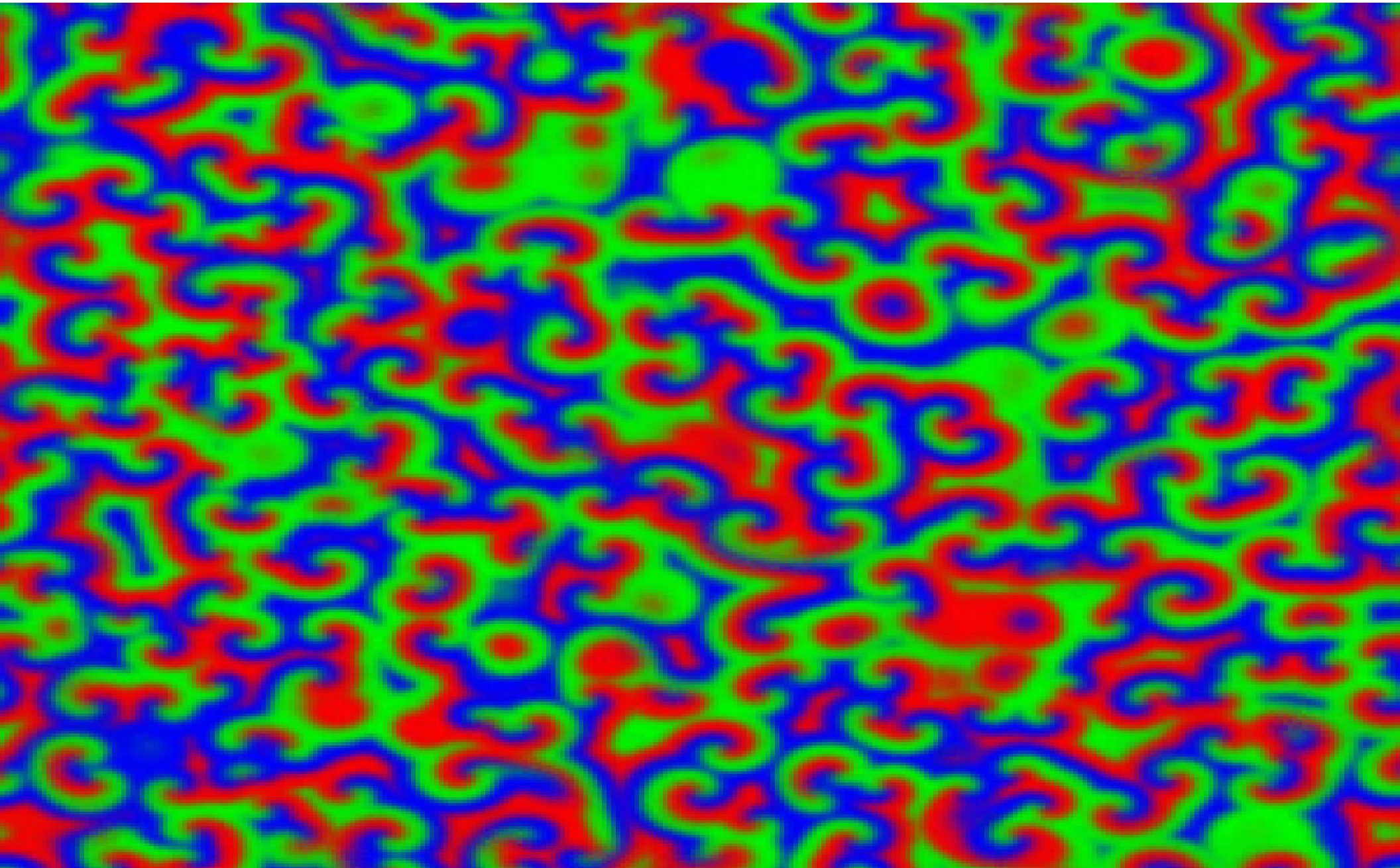
Cyber World = “Time”

- Bottom-Up
- Self-Organising
- Transparency
- Global – “Real-Time”
- Citizen Power
- Freedom
- “Speed of Light”
- Passwords & Pins
- Events & Experience
- Organic
- Silicon Life
- Cyber Weapons & “Smart Bots”
- Social Media

“Smart Security” requires Embedded Networked Intelligence in ALL “IoT” Devices

“Smart” Autonomous Chemical Oscillator:

- Belousov–Zhabotinsky Reaction (BZ) -*

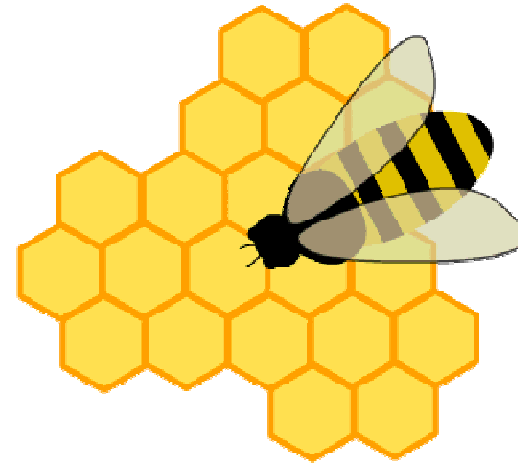
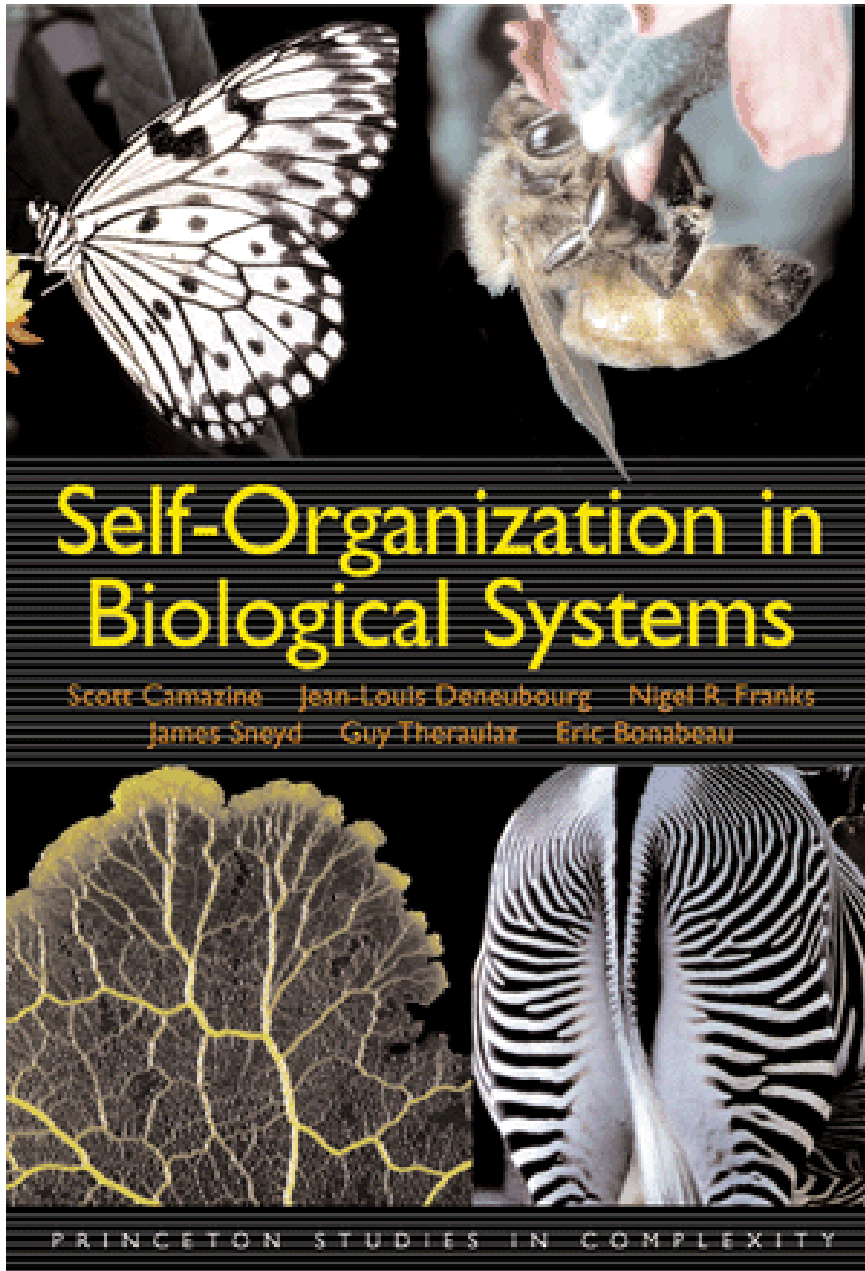


Self-Organisation in “*Bio-Sciences*”

- Organic DNA-based Life has Adaptation, Learning & Intelligence based upon Self-organisation:
 - **Bee Hives** with regular Honeycombs
 - **Ant Colonies** & Termite Hills
 - **Migrating Birds** fly in “V” Echelon Formations
 - **Plant Life** adapts to Light, Gravity, Chemicals & Fluids
 - **Sociable Weaver Birds** build huge nests for security
 - **Mammalian Brains** evolved from Neural Networks

*...“Smart Security for the **IoT** will be based upon Principles of **Bio-Adaptation, Self-Organisation & Self-learning!**”...*

Self-Organisation in “*Bio-Systems*”



“Smart Sustainable Security” in Nature!



The Sociable Weaver Bird

“World’s largest Bird Nests”

***** Southern Africa *****



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

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

“Smart Security”: 21stC Business Architectures



1 – Background: “21stC Security Landscape”

2 – Basic “Smart Security” Concepts

3 – Integrated Cyber-Physical Security

4 – Towards “Smart Security” Architectures

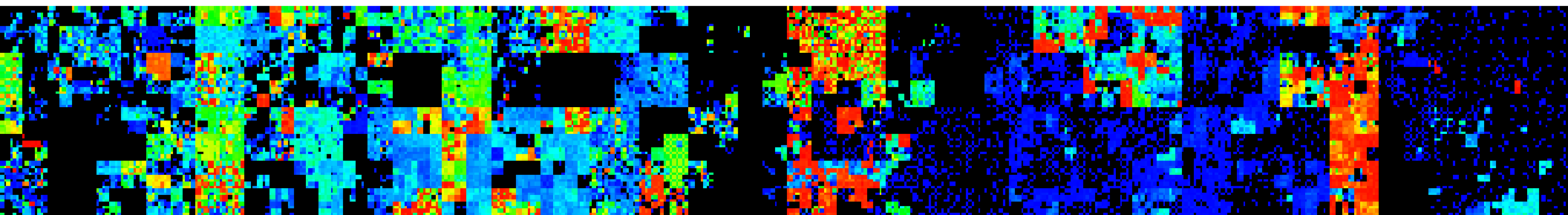
5 – “Smart Security” for *YOUR* Business!

6 – Security Scenarios: Critical Sectors

7 –Smart Security for “Internet of Things”

8 - Practical “Smart Security” Operations

9 – ***YOUR*** TOP 3 Actions & RoadMap!

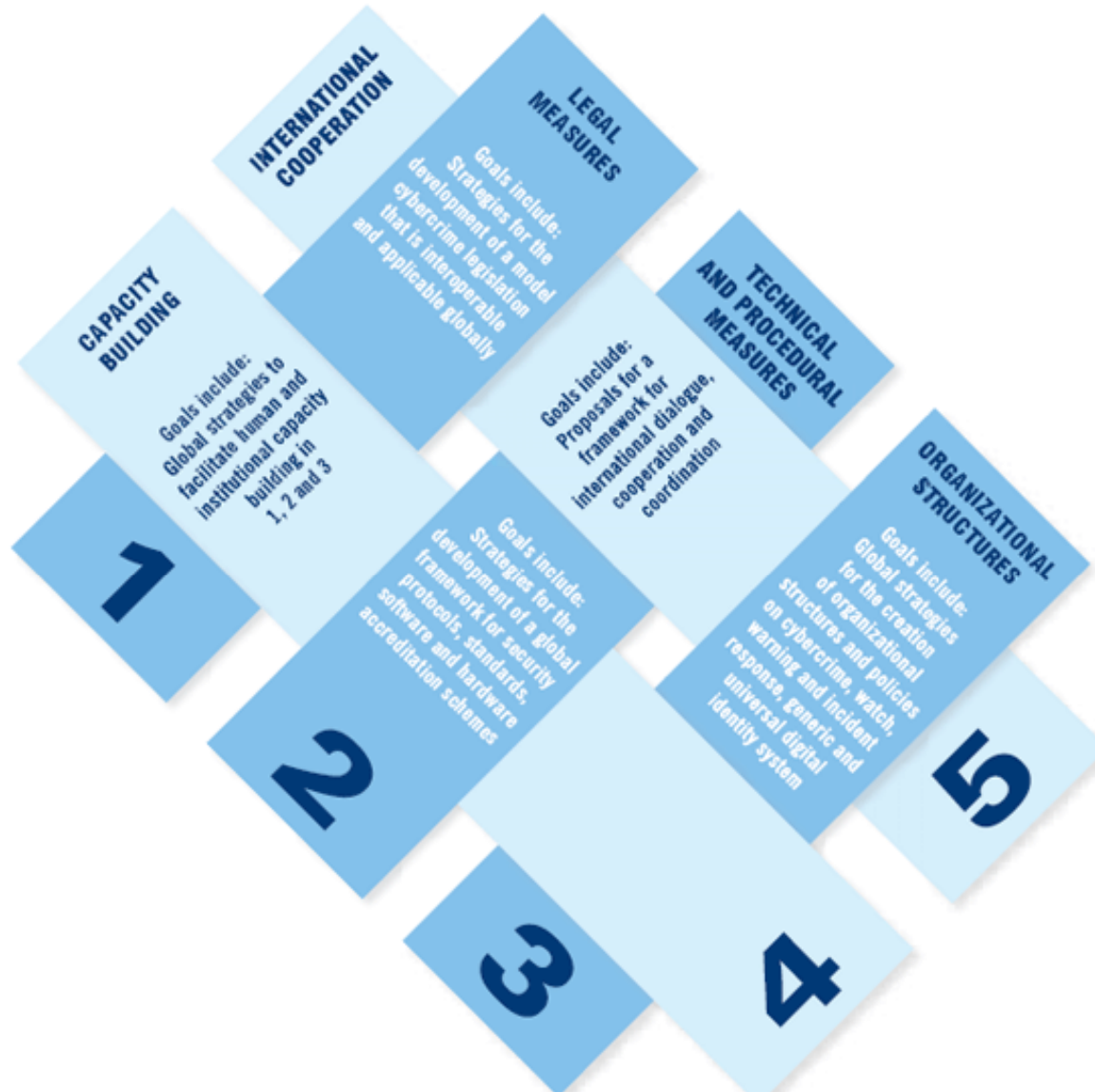


4) Towards “*Smart Security*” Architectures

- Leading International Organisations have already designed 21stC “State of the Art” Frameworks, Standards and *Cybersecurity Architectures*:
 - **UN/ITU** – Global Cybersecurity Agenda (GCA)
 - **NATO** – National Cybersecurity Framework
 - **EU/ENISA** – National Cybersecurity Strategies
 - **NIST** – National Institute of Standards & Technology
 - **SANS** – Critical Security Controls
 - **ISO/IEC** – International Standards – ISO 27000 Series

**...UN, NATO, EU are for *Government* whilst
NIST/SANS are more focused upon *Business***

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



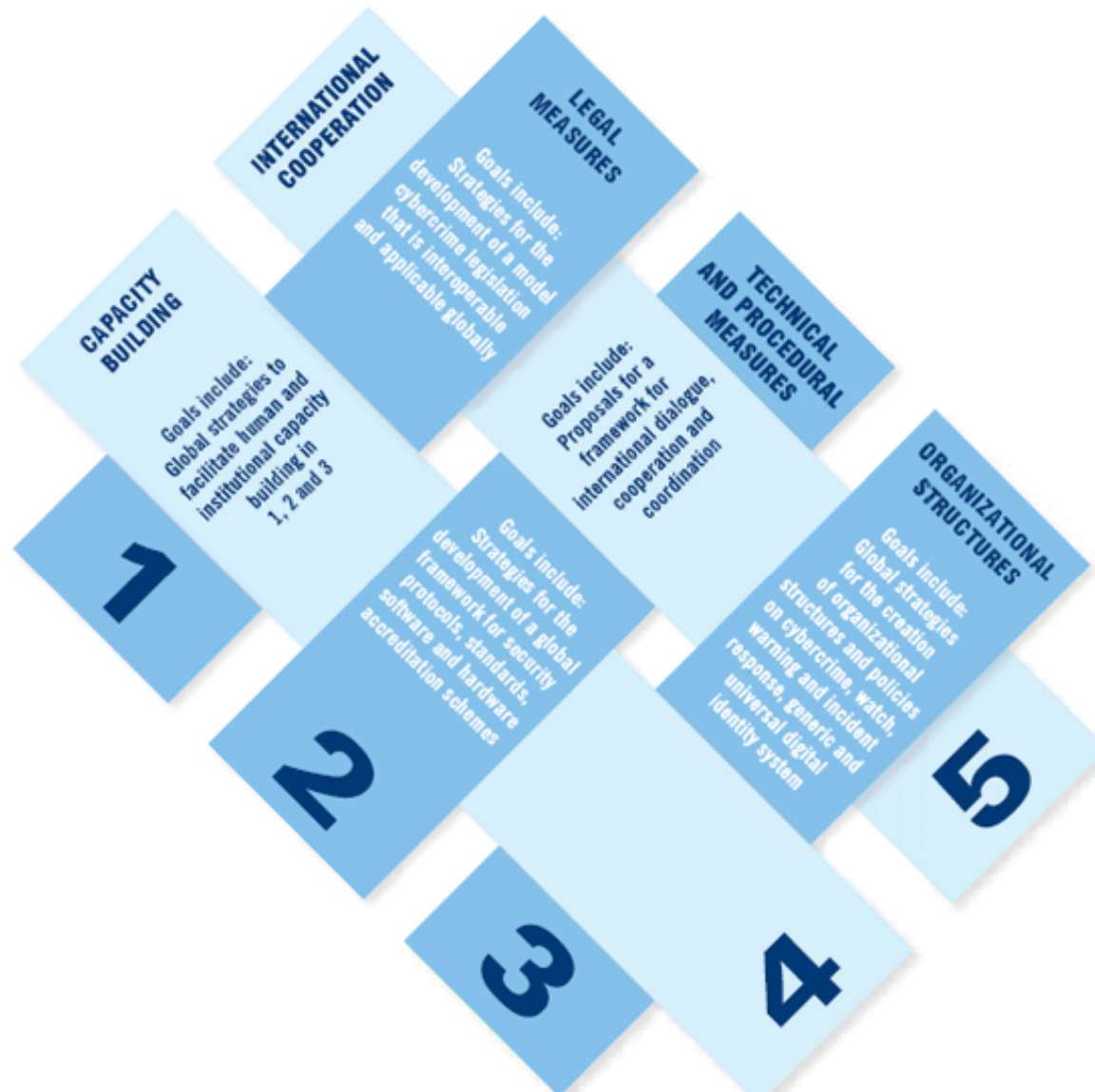
The UN/ITU GCA - Global Cybersecurity Agenda:

- 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**.

www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

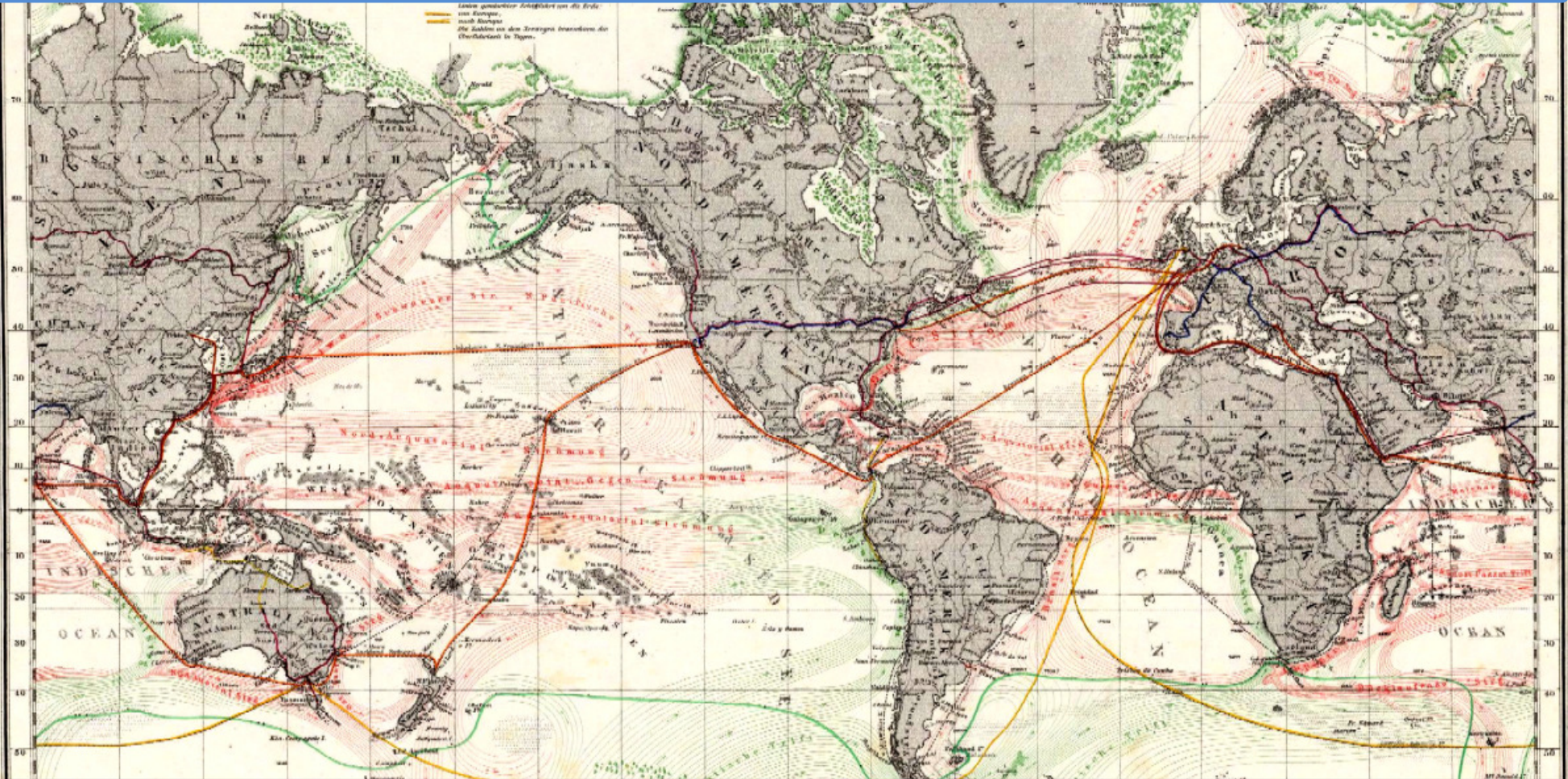
UN/ITU:– *Global Cybersecurity Agenda (GCA)*



www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

UN/ITU Worldwide Security in *Cyberspace*!

Capacity Building



Regional and International Collaboration

UN/ITU Worldwide Security in *Cyberspace*!

- (4) – Capacity Building

- (1) –
Legal Measures

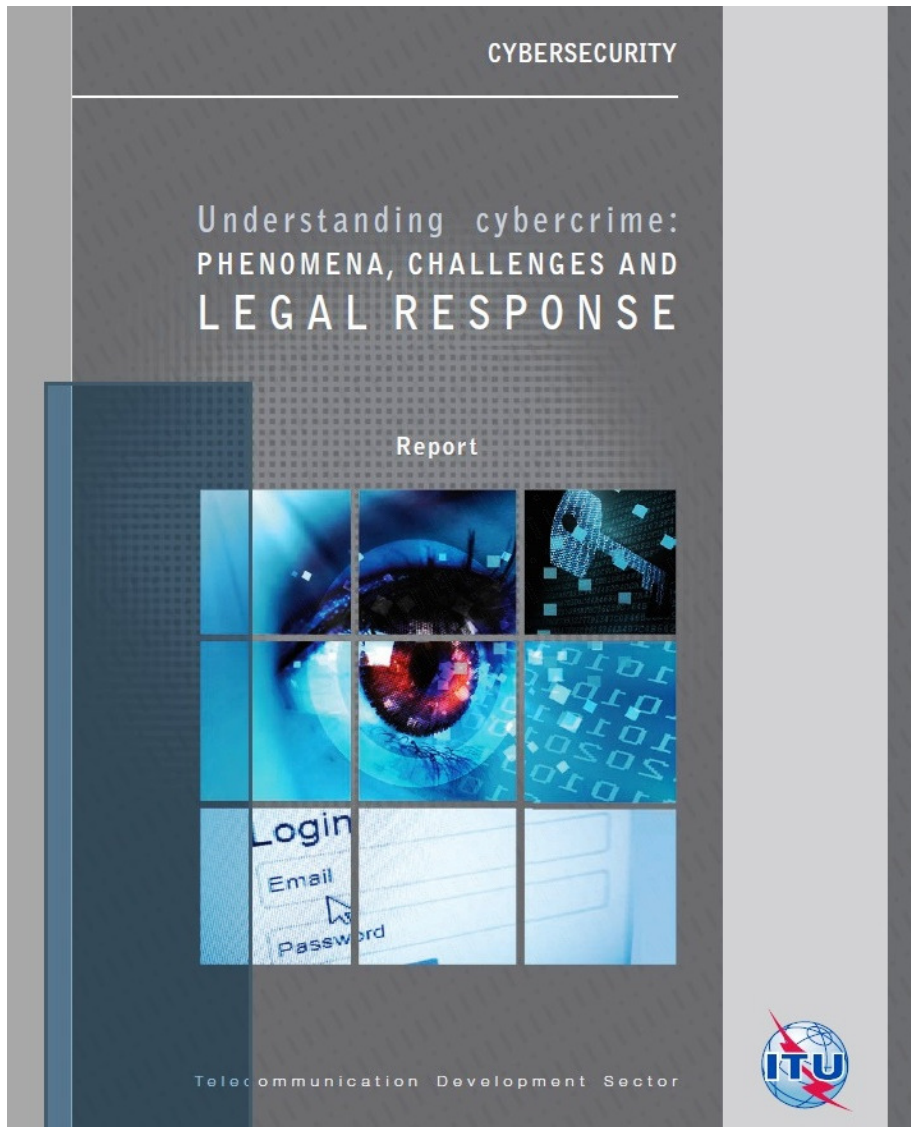
- (2) –
Technical
&
Procedural
Measures

- (3) –
Organisational
Structures

- (5) – Regional and International Collaboration

- UN/ITU CyberSecurity Agenda -

Understanding CyberCrime (Eng/Rus)



Link: www.itu.int/en/publications/

34th International East/West Security Conference

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



- UN/ITU *CyberSecurity* Agenda - Quest for CyberConfidence (Eng/Rus)



Link: www.itu.int/en/publications/

34th International East/West Security Conference



"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©

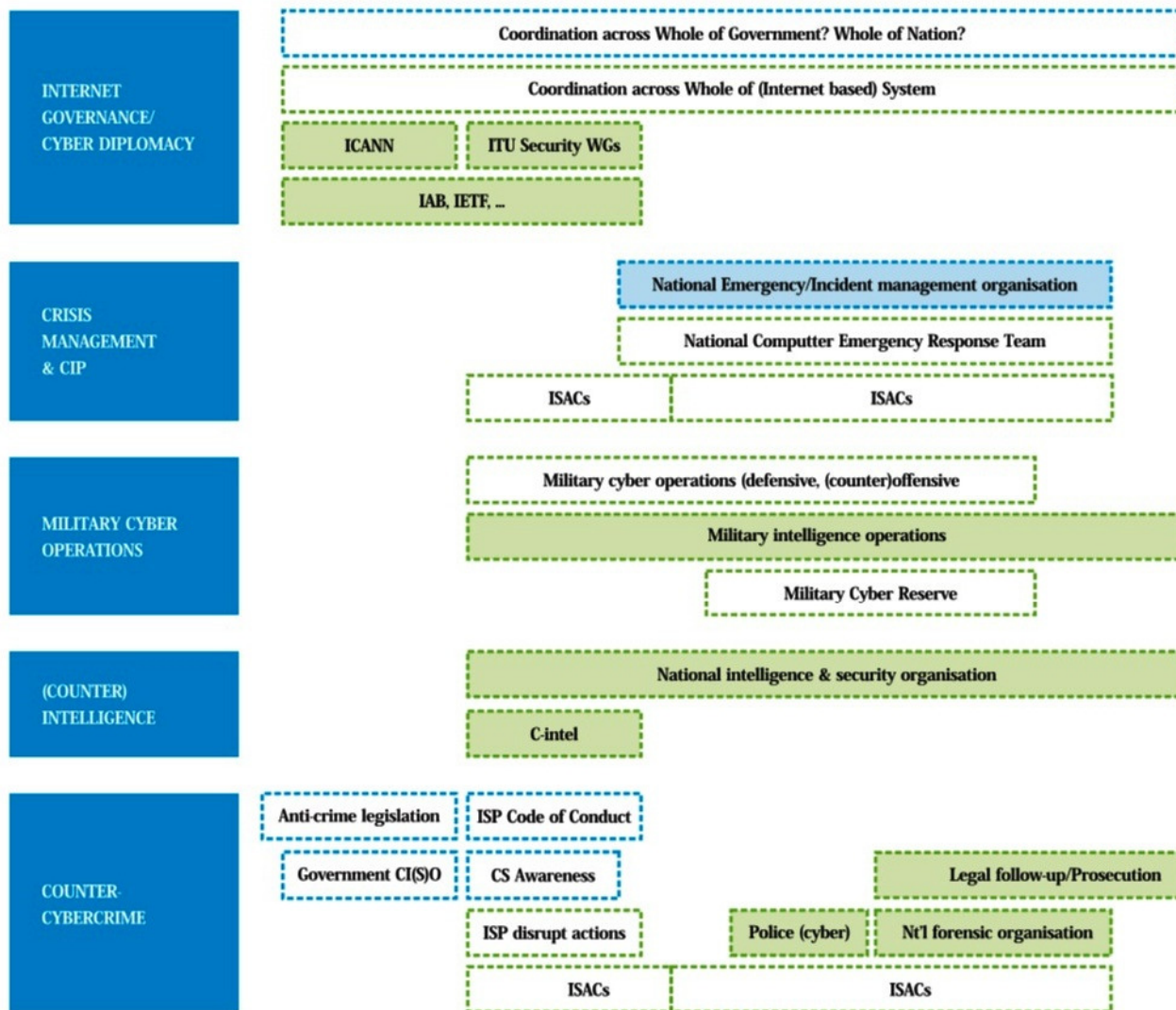


UN/ITU *National CyberSecurity Strategy* Toolkit (*NCS*) – Global Partnership - 2016



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

Link: www.itu.int/en/ITU-D/Cybersecurity/



NATO *Cybersecurity* Framework Manual

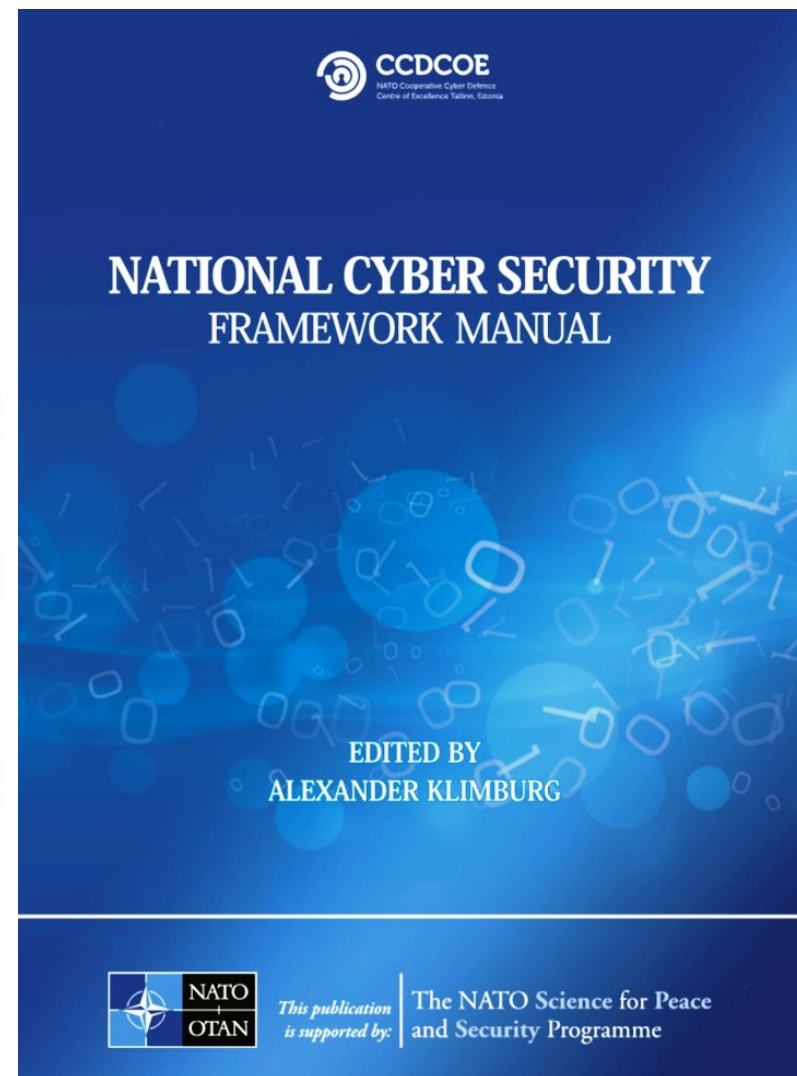


Figure 6: The Organisational Picture Across Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in

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



NATO Cybersecurity Framework:

- Organisational Architecture -

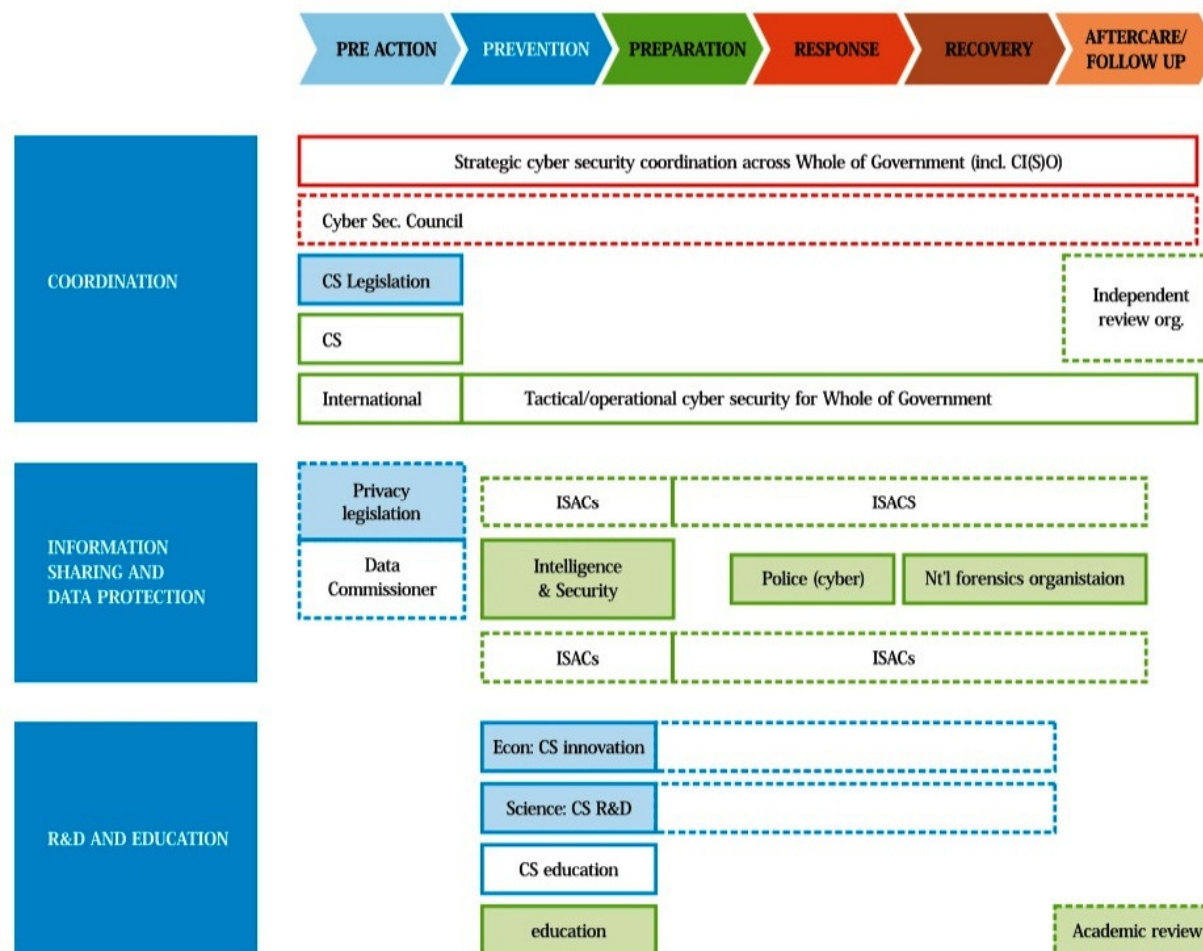


Figure 7: The Organisational Picture of the Cross-Mandates (red = strategic, blue = operational, green = tactical at the national level; shaded = embedded in existing organisation; dashed = option selected by some nations)

EU Agency for Info Security: **ENISA**



ENISA Strategic Security Framework
Provides effective “**Cyber**” model for
National **Governments** & Ministries



National Cyber Security Strategies

Practical Guide on Development and Execution



An evaluation Framework for National
Cyber Security Strategies

- **ALL EU Countries** now have approved **National Cybersecurity Strategies** -
www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

“21stC Smart Security Architectures”
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



NIST *Cybersecurity* Framework

National Institute of Standards & Technology

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Web: www.nist.gov/cyberframework/

34th International East/West Security Conference

"21stC Smart Security Architectures"

- Real-Time Cyber-Physical Integration -

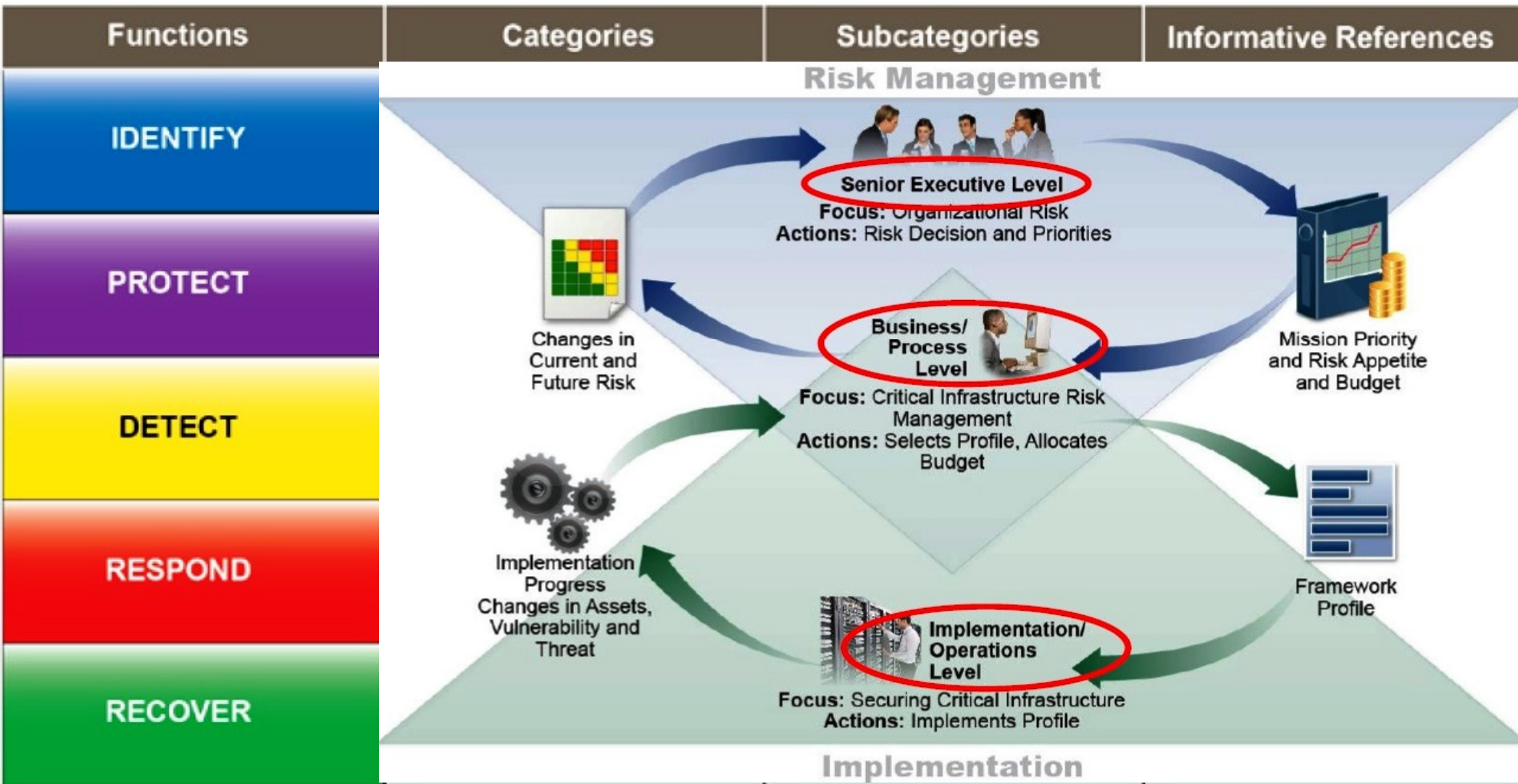
- Rome, Italy, 21st-22nd November 2016 -

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



NIST *Cybersecurity* Framework

National Institute of Standards & Technology



Web: www.nist.gov/cyberframework/

34th International East/West Security Conference

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



Critical Security Controls (CSC)

- Top 20 Cyber Defense Actions – The SANS Institute –

- 1) Inventory of Authorised and Unauthorised Devices
- 2) Inventory of Authorised and Unauthorised Software
- 3) Secure Configurations for Hardware and Software
- 4) Continuous Vulnerability Protection & Remediation
- 5) Malware Defenses
- 6) Applications Software Security
- 7) Wireless Access Control
- 8) Data Recovery Capability
- 9) Security Skills Assessment and Training
- 10) Secure Configurations for Network Devices
- 11) Limitation of Network Ports, Protocols & Services
- 12) Controlled Use of Administrative Privileges
- 13) Boundary Defence
- 14) Maintenance, Monitoring and Analysis of Audit Logs
- 15) Controlled Access Based on the Need to Know
- 16) Account Monitoring and Control
- 17) Data Protection
- 18) Incident Response and Management
- 19) Secure Network Engineering
- 20) Penetration Testing and Red Team Exercises

The Critical Security Controls
for
Effective Cyber Defense

Version 5.0



1

SANS = **S**ysAdmin, **A**udit, **N**etworking and **S**ecurity

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

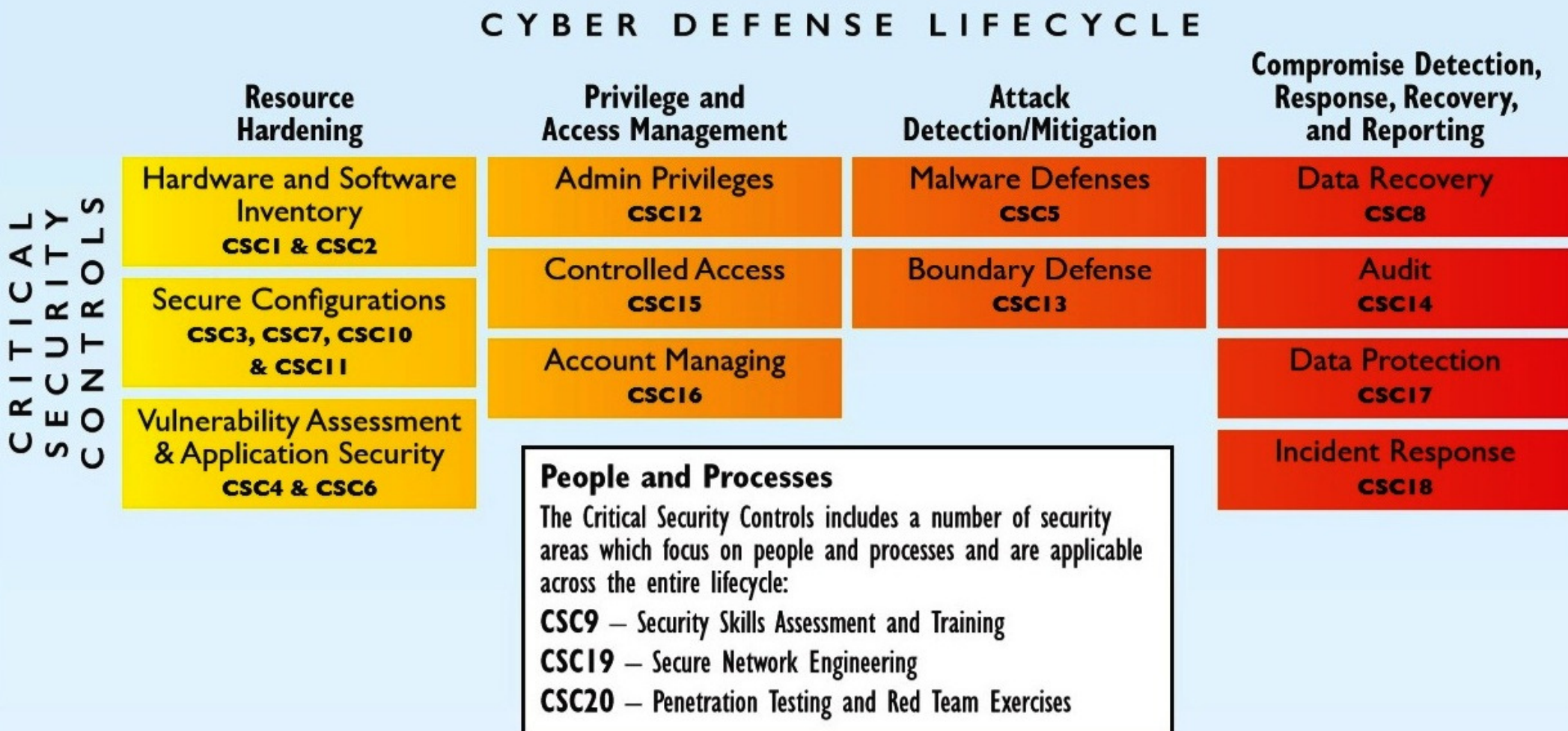
"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



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” cyber-security lifecycle. SANS has created a mapping allocating the Controls across four phases:



SANS = SysAdmin, Audit, Networking and Security

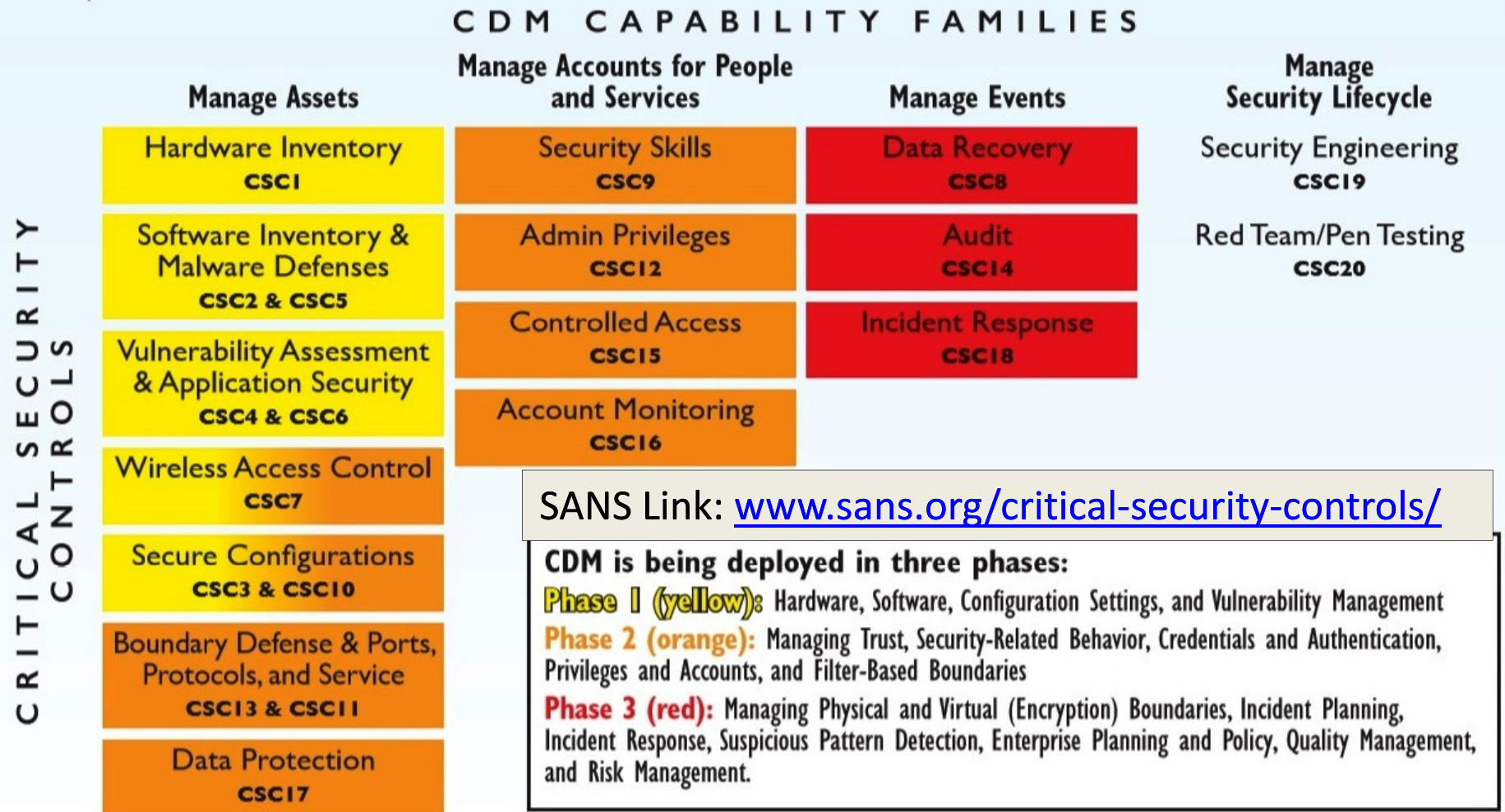
Link: www.sans.org/critical-security-controls/

“21stC Smart Security Architectures”
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



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

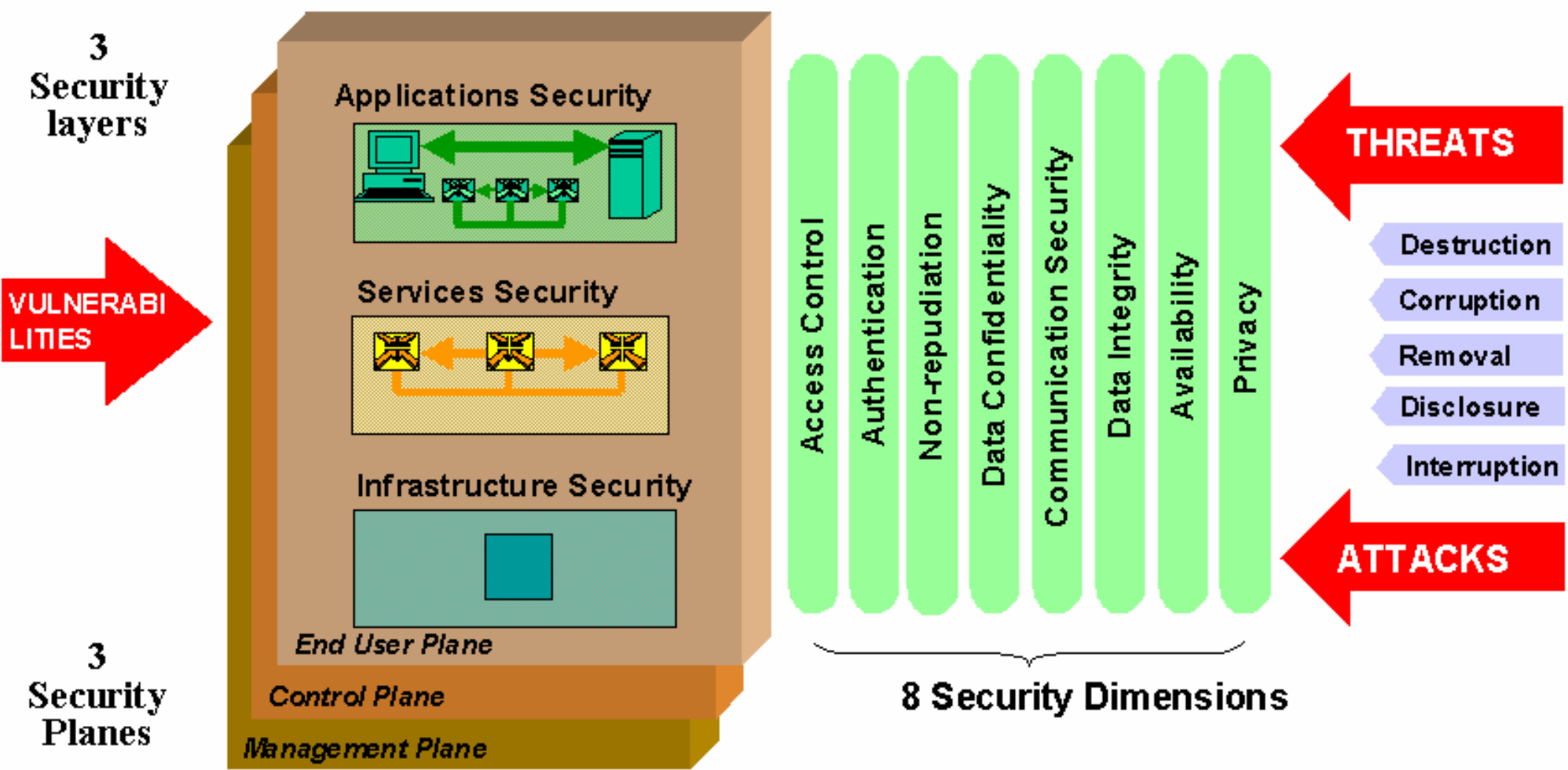
The Department of Homeland Security Continuous Diagnostics and Mitigation program has multiple phases of security product and services offerings across cybersecurity. The Critical Controls map directly against those CDM phases:



Cybersecurity Standards: *Key Players*

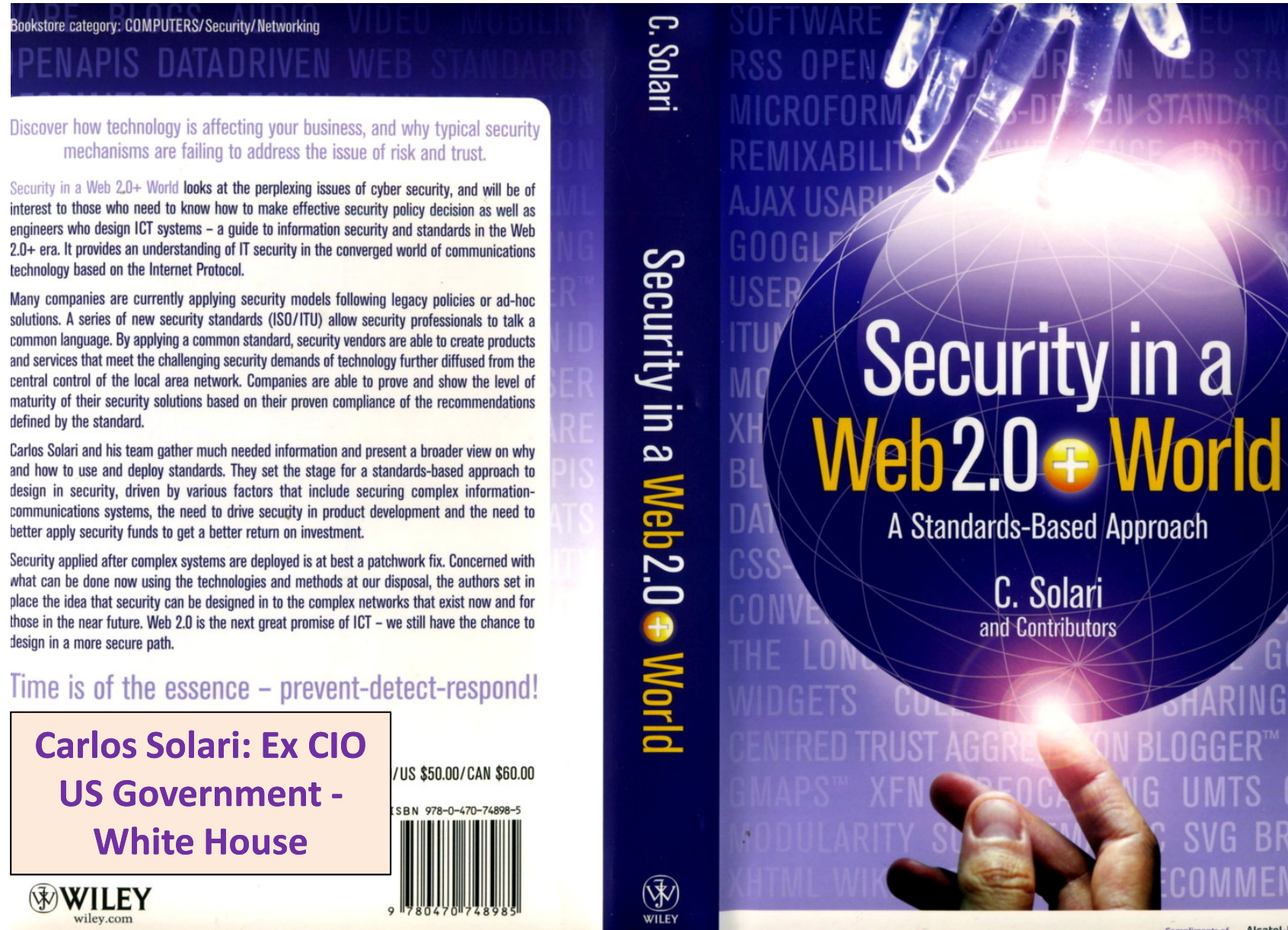
- ***Multiple Players:*** There are multiple international that publish standards relating to physical and cyber security. In general these standards, recommendations and guidelines are complementary:
 - ***ENISA*** – European Network and Information Security Agency
 - ***ISO*** – International Standards Organisation (ISO27xxx Series)
 - ***IETF*** – Internet Engineering Task Force
 - ***ETSI*** – European Telecommunications Standards Institute
 - ***IEEE*** – Institute of Electrical and Electronic Engineers
 - ***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 -**



"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



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).

NIST Security Publications: *“800 Series”*

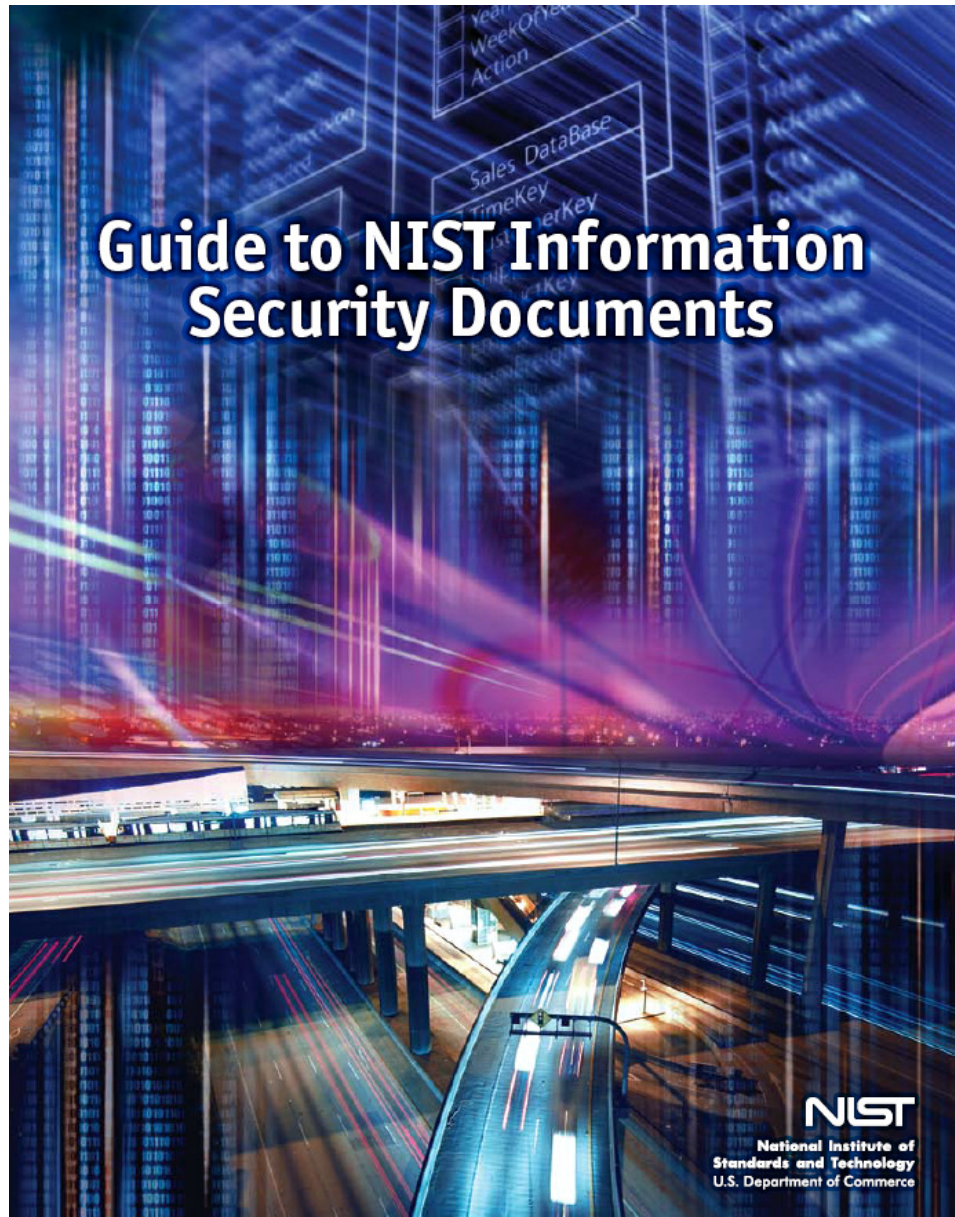
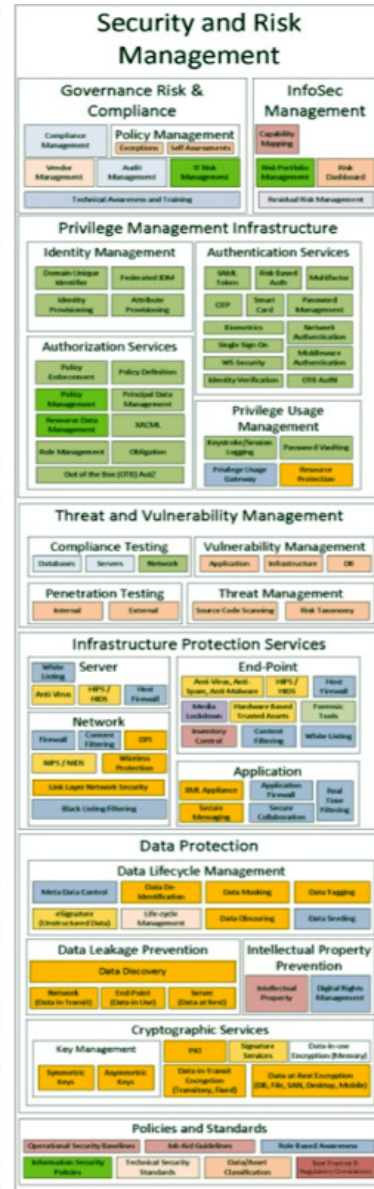


TABLE OF CONTENTS	
Introduction	1
Topic Clusters	2
Annual Reports	2
Audit & Accountability	2
Authentication	3
Awareness & Training	4
Biometrics	4
Certification & Accreditation (C&A)	5
Communications & Wireless	6
Contingency Planning	7
Cryptography	7
Digital Signatures	8
Forensics	9
General IT Security	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
Families	22
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
Legal Requirements	35
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	38

NIST: Cloud Security Architecture



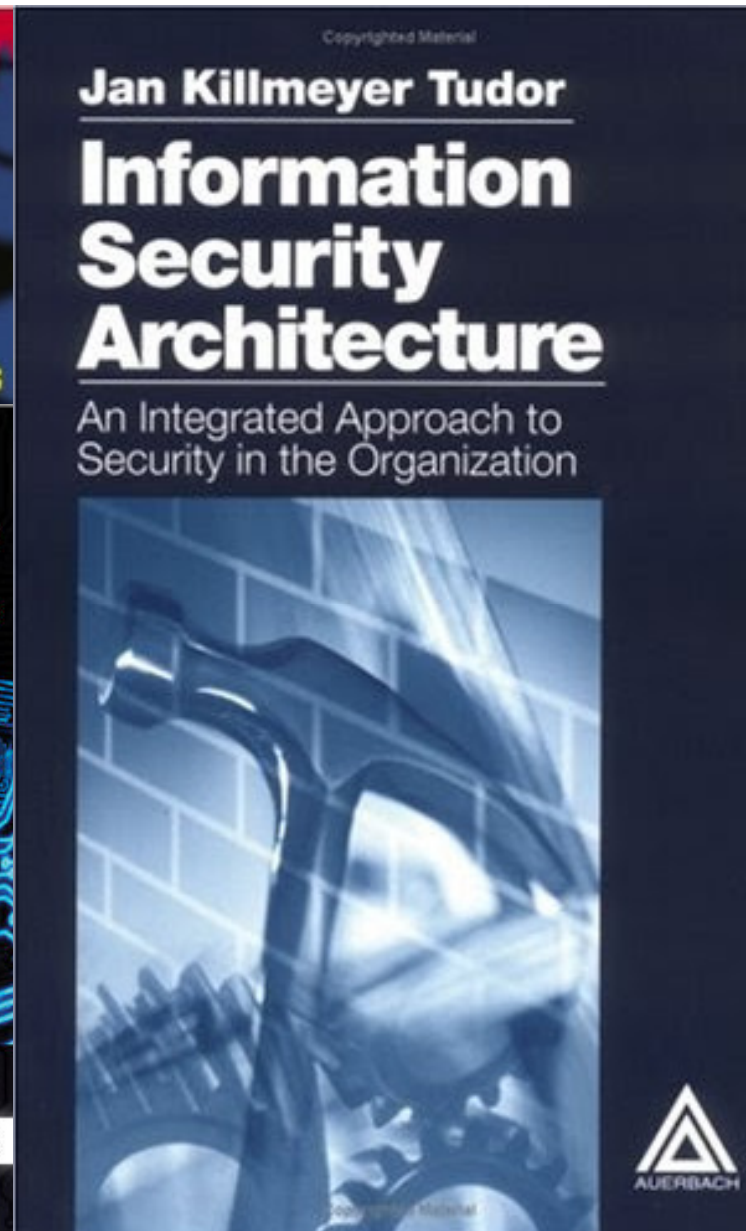
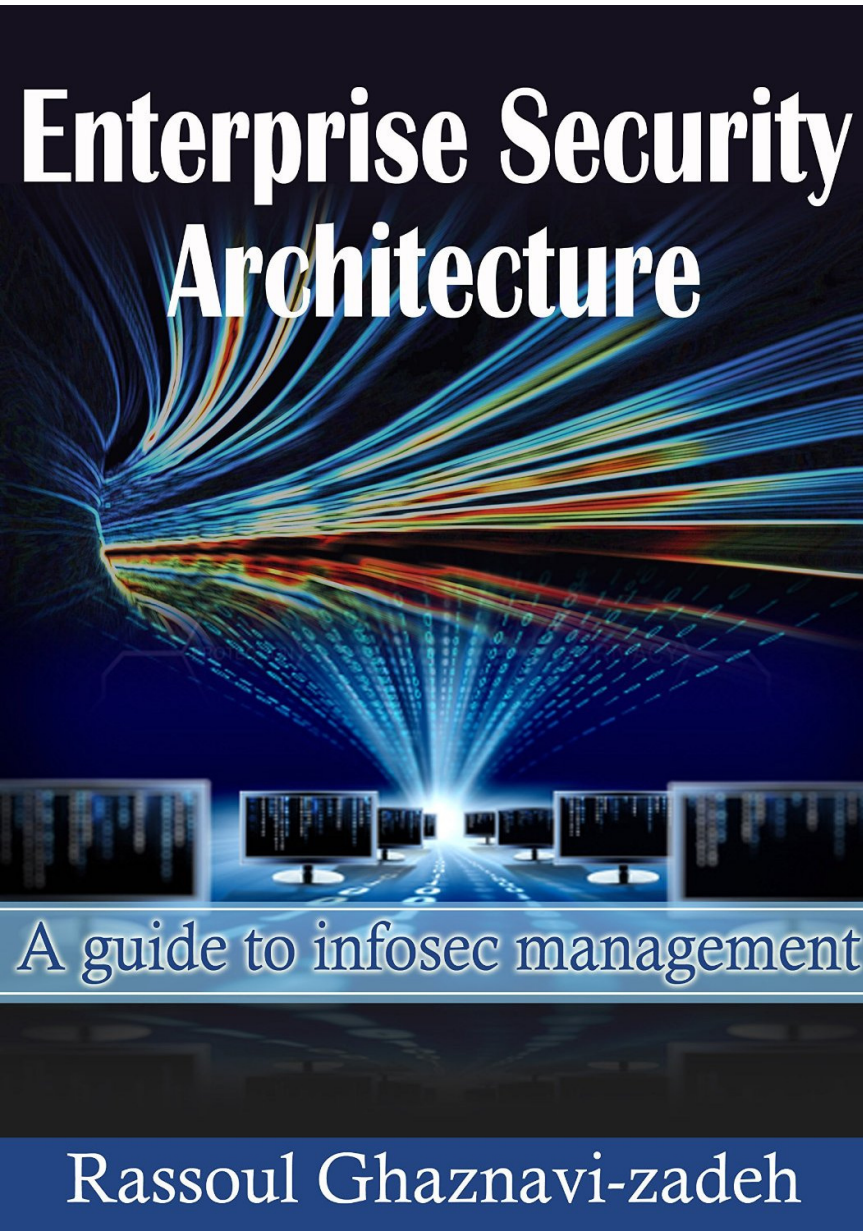
SP 800-53 Security Control Families					
ID	Code	Family Name	ID	Code	Family Name
AC		Access Control	IP		Media Protection
AT		Awareness and Training	PE		Physical and Environmental Protection
AU		Audit and Accountability	PL		Planning
CA		Security Assessment and Authorization	PS		Personnel Security
CM		Configuration Management	RA		Risk Assessment
CP		Contingency Planning	SA		System and Services Acquisition
IA		Identification and Authentication	SC		System and Communications Protection
IR		Incident Response	SI		System and Information Integrity
MA		Maintenance	PM		Program Management

NIST: Cloud Security Standards & Reference Model
34th International East/West Security Conference

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
 - Rome, Italy, 21st-22nd November 2016 -
 © Dr David E. Probert : www.VAZA.com ©



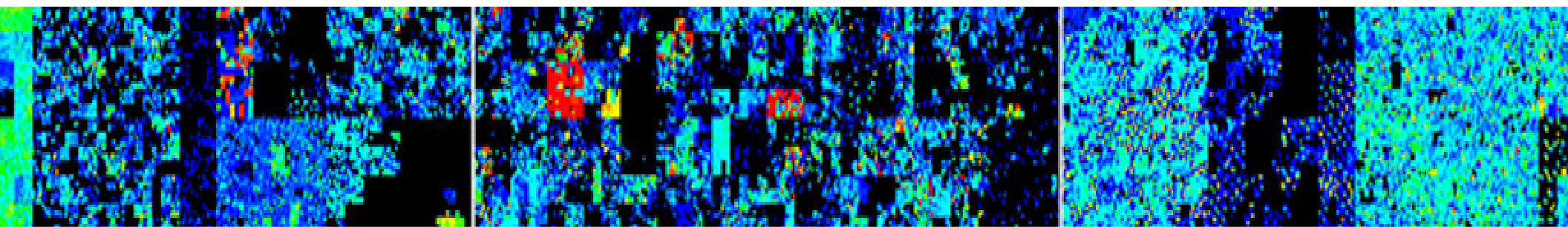
Info Security Architecture: **Publications**



"Smart Security": 21stC Business Architectures



1 – Background: "21 st C Security Landscape"	2 – Basic "Smart Security" Concepts	3 – Integrated Cyber-Physical Security
4 – Towards "Smart Security" Architectures	5 – "Smart Security" for <i>YOUR</i> Business!	6 – Security Scenarios: Critical Sectors
7 – Smart Security for "Internet of Things"	8 – Practical "Smart Security" Operations	9 – <i>YOUR</i> TOP 3 Actions & RoadMap!



5) “*Smart Security*” for *YOUR* Business

- Recruit Professionally Qualified *CSO/Director*
- Organise Top-Level *Security Workshop* to explore possible and actual Cyber/Physical Threats
- Develop *Inventory* of current Security Assets and identify “gaps” that require new investment
- Discuss and Agree Multi-Year “Smart Security” Investment & Business *Action Plan & RoadMap*
- Implement *YOUR* Security Plan as Board Level *Strategic Programme* across ALL Units/Functions

...Staff Training with “Simulated” Threat Scenarios!..

CISSP– International “Cyber” Certification

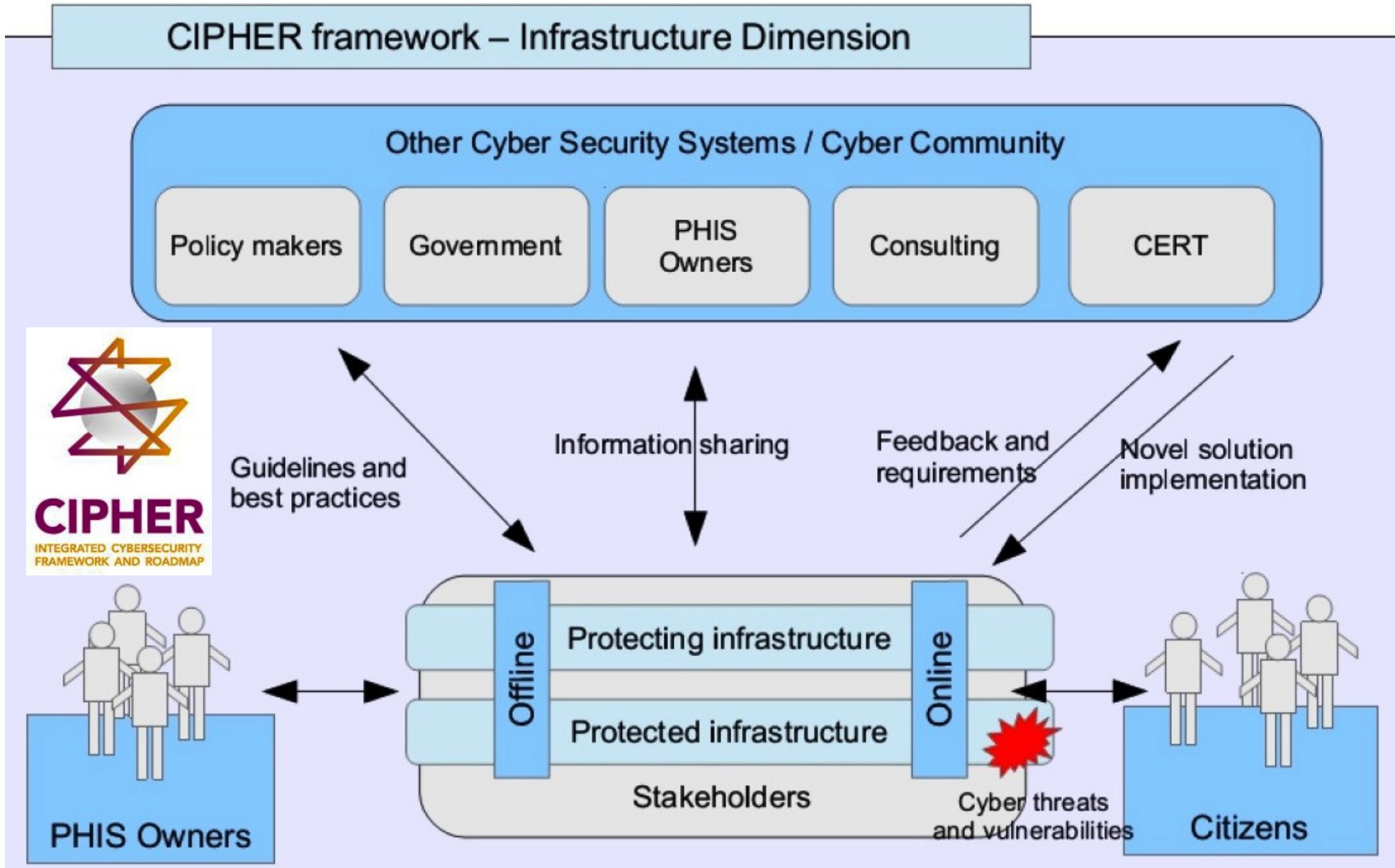
- The **CISSP** – Certified Information Systems Security Professional is one of the highest international qualifications from the **(ISC)²**, and is based upon the core tenets of **Confidentiality, Integrity & Availability**:

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



- ***An in-depth study of all these security topics would fill an intensive 3 month schedule!***

Cipher Integrated CyberSecurity RoadMap



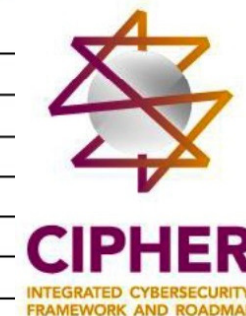
Link: Cipherproject.eu/cipher_webapp/
34th International East/West Security Conference

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



Cipher Integrated CyberSecurity RoadMap

A		B	C
1			
2		ORGD - ORGANISATIONAL DIMENSION	
3		ORGD – CYBER SECURITY PLAN	
4	ORGD.1	Develop a cyber security plan (e.g. roles, engaged staff members and departments, procedures, policies) (suggested outcome: organisational registry)	
5	ORGD.2	Keep your cyber security plan up to date and aligned with the European and your national cyber security plan, as well as with the international standards. Communicate the changes to your employees.	
6	ORGD.3	Incorporate in the cyber security plan the information obtained from other processes/segments/departments in your institution (that may influence the plan development) in your institution. Communicate the changes to all departments.	
7	ORGD.4	Develop protocols and apply resources to organise subgroups to identify and resolve specific security issues related to private data.	
8		ORGD – ONLINE ASPECTS	
9	ORGD.5	Develop and implement the information sharing protocol for vulnerability disclosure and mitigation (in order to clearly describe when, how, by which means information about vulnerabilities have to be shared). (suggested outcome: organisational registry)	
10	ORGD.6	Define procedures for incident analysis and reporting .	
11	ORGD.7	Adopt and implement effective security assurance program to mitigate potential insider threats.	
12		Check if your security assurance program identifies:	
13	ORGD.8	<ul style="list-style-type: none"> Allowed / disallowed software/services installed on employees computers Procedures for securing removable media or other external devices managing or storing information. 	
14			
15	ORGD.9	Provide requirements for firewalls, monitoring, and other cyber security solutions .	
16	ORGD.10	Define procedures for patches and updates installation . Identify responsible person and record the changes introduced to your system.	
17		ORGD – OFFLINE ASPECTS	
18	ORGD.11	Identify the contact points in your National CERT (Computer Emergency Response Team) and set up smooth communication and cooperation protocols (e.g. mechanisms for notification of incidents involving personal data breaches).	
19	ORGD.12	Ensure that changes of regulations and of directives that are in force in your country are tracked and that privacy policy in your organisation follows these changes. Set up the plan for (periodic) validation of the privacy policy, as well as of the information system, in order to ensure they are to be up to date with the current law and standards.	
20	ORGD.13	Include in your business continuity process the security requirements for the information stored . Test and regularly update the business continuity plans to ensure they are up to date and effective.	



Ready | INF DIMENSION | **ORG DIMENSION** | OPR DIMENSION | INF REGISTRY | PRV REGISTRY | ORG REGISTRY | OPR REGISTRY |

Link: Cipherproject.eu/cipher_webapp/
34th International East/West Security Conference

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



Smart Security: *Technology & Operations*

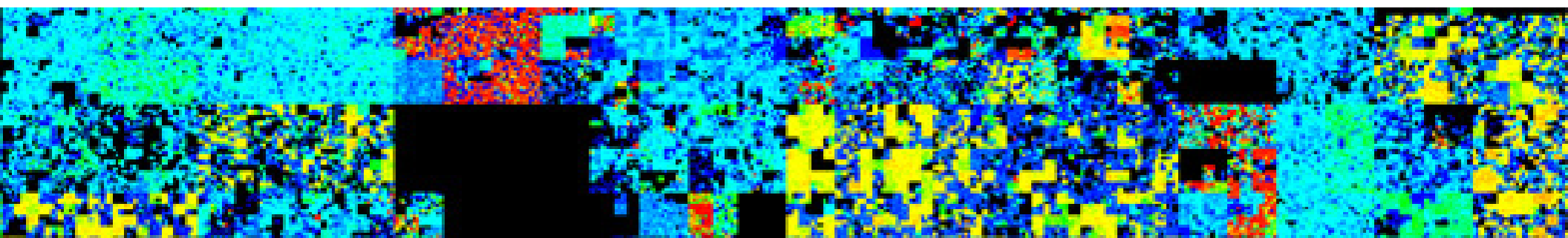
- ***“Smart Security”*** spans the “Real-Time” Protection of physical buildings, staff and cyber facilities, networks & information assets.
 - ***Technologies:*** Advanced ICT Security technologies include Biometrics, RFID Encryption, PKI Authentication, ID Management, DDoS & Malware Detection
 - ***Operations:***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

*...In the next sections we'll explore both **“Critical Sectors”** and the Integration of **Cyber & Physical Operations** which is the real essence of **“Smart Security”***

"Smart Security": 21stC Business Architectures



1 – Background: “21 st C Security Landscape”	2 – Basic “Smart Security” Concepts	3 – Integrated Cyber-Physical Security
4 – Towards “Smart Security” Architectures	5 – “Smart Security” for <i>YOUR</i> Business!	6 – Security Scenarios: Critical Sectors
7 – Smart Security for “Internet of Things”	8 – Practical “Smart Security” Operations	9 – <i>YOUR</i> TOP 3 Actions & RoadMap!



(6) Security Sectors: *Threat Scenarios*

- **Hybrid Security Threats** may potentially target **ANY** and **ALL YOUR** Business and Government Sectors!....
 - a) Finance & Banking** – ATMs, Fraud, Money Laundering
 - b) Transport & Tourism** – Airports, Metro, Tourist Sights
 - c) Energy & Utilities** – Nuclear, Chemical & Water Resource
 - d) Government & Defence** – Intel Theft, Hacking, Military
 - e) Education & Research** – Campus-Wide Armed Attacks
 - f) Industry & Manufacturing** – Competitive Espionage
 - g) Retail, Sports & Culture** – Shopping Malls, Olympics

....**CSOs** are advised to **URGENTLY** define practical & effective action plans to mitigate such attacks!...

Critical Sector Case Study: **Banks & Finance**

- **Banks & Financial** Institutions are prime targets for cybercriminals.
 - **Access** to Accounts is usually indirect through phishing scams, infected websites with malicious scripts, and personal ID Theft.
 - **On-Line bank transfers** are also commonly used for international money laundering of funds secured from illegal criminal and political activities
 - **Instant Money Transfer Services** are preferred for crimes such as the classic “Advanced Fee Scam” as well as Lottery and Auction Scams
 - **Cyber-Extortion & Ransomware** are now epidemic via web & email phishing
 - **National & Commercial Banks** have also been regular targets of DDOS Cyberattacks from politically motivated and terrorist organisations
 - **Penetration Scans:** Banks are pivotal to national economies and will receive penetration scans and Cyberhacks both “direct” & with “Bots” & Trojans
 - **On-Line Banking** networks including ATMs, Business and Personal Banking are at the “sharp end” of financial security and require significant efforts towards end-user authentication & transaction network security
- ...”Smart Security”** will become mandatory for **ALL** Financial Institutions!

Critical Sector Case Study: *Governments*

- **Cyber Agencies:** Over 70 National Governments (from 193 UN/ITU Member States) have now Cybersecurity Agencies & Programmes
- **eGovernment Services** are critically dependant upon strong cybersecurity with authentication for the protection of applications, and citizen data
- **Compliance Audit:** All Government Ministries & Public Agencies should receive in-depth ICT security audits and full annual compliance reviews
 - 1) National Defence Forces
 - 2) Parliamentary Resources
 - 3) Land Registry & Planning System
 - 4) Citizen IDs and Passports
 - 5) Laws, Legislations, and Policies
 - 6) Civilian Police, Prisons & National e-Crimes Unit (NCU)
 - 7) National CERT – Computer Emergency Response Team
 - 8) Inter-Government Communications Network
 - 9) eServices for Regional & International Partnerships
 - 10) Establishment of cybersecurity standards & compliance
 - 11) Government Security Training and Certification

“Smart Security” for Critical Sectors:

YOUR Shopping and To Do List!

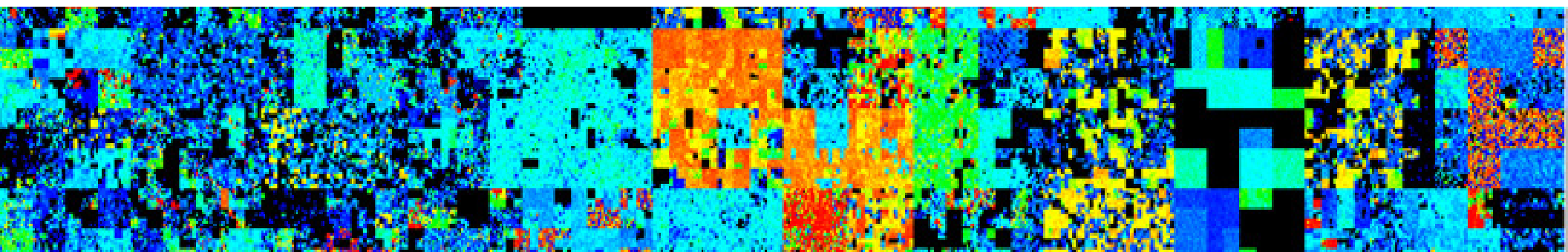
- **Security Audit:** In-Depth Security Audit and Action Report - Spanning BOTH Physical and Cybersecurity Operations, Assets and Technologies
- **International Standards:** Understand and Implement Security Policies and Programmes to International Standards – ISO/IEC, UN/ITU, IEEE, NIST, ASIS, ISF
-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

*....YOUR Top Priority is Professional **Cybersecurity Training & Certification** with regular course “Top-Ups” since the field is moving at Supersonic Speed!*

“Smart Security”: 21stC Business Architectures



1 – Background: “21 st C Security Landscape”	2 – Basic “Smart Security” Concepts	3 – Integrated Cyber-Physical Security
4 – Towards “Smart Security” Architectures	5 – “Smart Security” for <i>YOUR</i> Business!	6 – Security Scenarios: Critical Sectors
7 – Smart Security for “Internet of Things”	8 – Practical “Smart Security” Operations	9 – <i>YOUR</i> TOP 3 Actions & RoadMap!



7) Smart Security for “Internet of Things”

- Securing the “Internet of Things” (IoT) is moving to the Top of the Business Security Agenda!...
- Major IoT Attacks have been recorded such as the Mirai BotNet/DYN DDoS Attacks (Sept/Oct 2016)
- Legacy “IoT” Devices are vulnerable to BotNet penetration due to weak or zero(!) cyber defence
- **YOUR** Business needs to engineer a security programme to mitigate “IoT” Hacks & Attacks!

...Effective solutions use a “Smart” integration of Cyber Interfaces, Biometrics & Encryption...

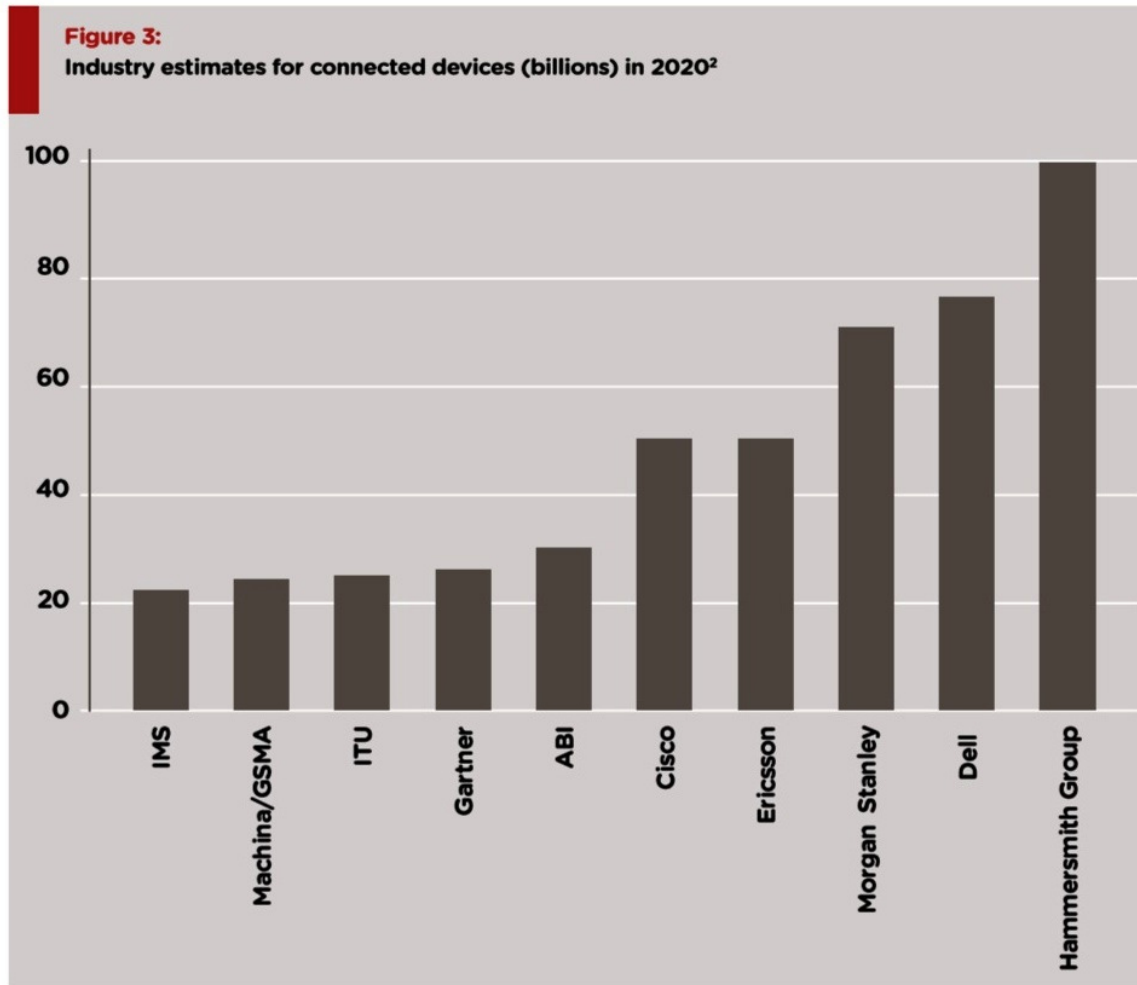
Cyber-Physical Threats from the “IoT”

- **ALL Networked Devices** are at risk from Cyber-Hacking, Penetration and Remote Control
- **IoT Devices:** Smart Phones, Home Controls, Vehicles, Industrial Controls, Smart Cities, Power Stations, Utilities, Medical Devices.....
- **Legacy Assets:** Many legacy assets including cars, medical implants, industrial SCADA controls are INSECURE against Cyber Attacks!

The Internet of Things



2020 Estimates for “IoT” Connectivity



¹ 'Internet of Things Connections Counter', Cisco Systems, 2014

² <http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10>; <https://www.abiresearch.com/market-research/product/1016390-over-30-billion-wireless-connected-devices/>; 'Forecast: The Internet of Things, Worldwide 2013', Gartner, 2013; 'The State of Broadband 2012: Achieving digital inclusion for all', Broadband commission, 2012; 'The Internet of Things: How the next evolution of the Internet is changing everything', Cisco Systems, 2011; 'Towards 50 Billion Connected Devices', Ericsson Research, 2010; 'The Internet of Things: Networked objects and smart devices', The Hammersmith Group, 2010; <http://www.marketplace.org/topics/tech/indie-economics/2020-there-will-be-10-web-connected-devices-human>; 'The Connected Life: A USD 4.5 trillion global impact in 2020', GSMA and Machina Research, 2012; <http://www.itpro.co.uk/626209/web-connected-devices-to-reach-22-billion-by-2020>

³ 'The Internet of Things is Now', Morgan Stanley, 2014

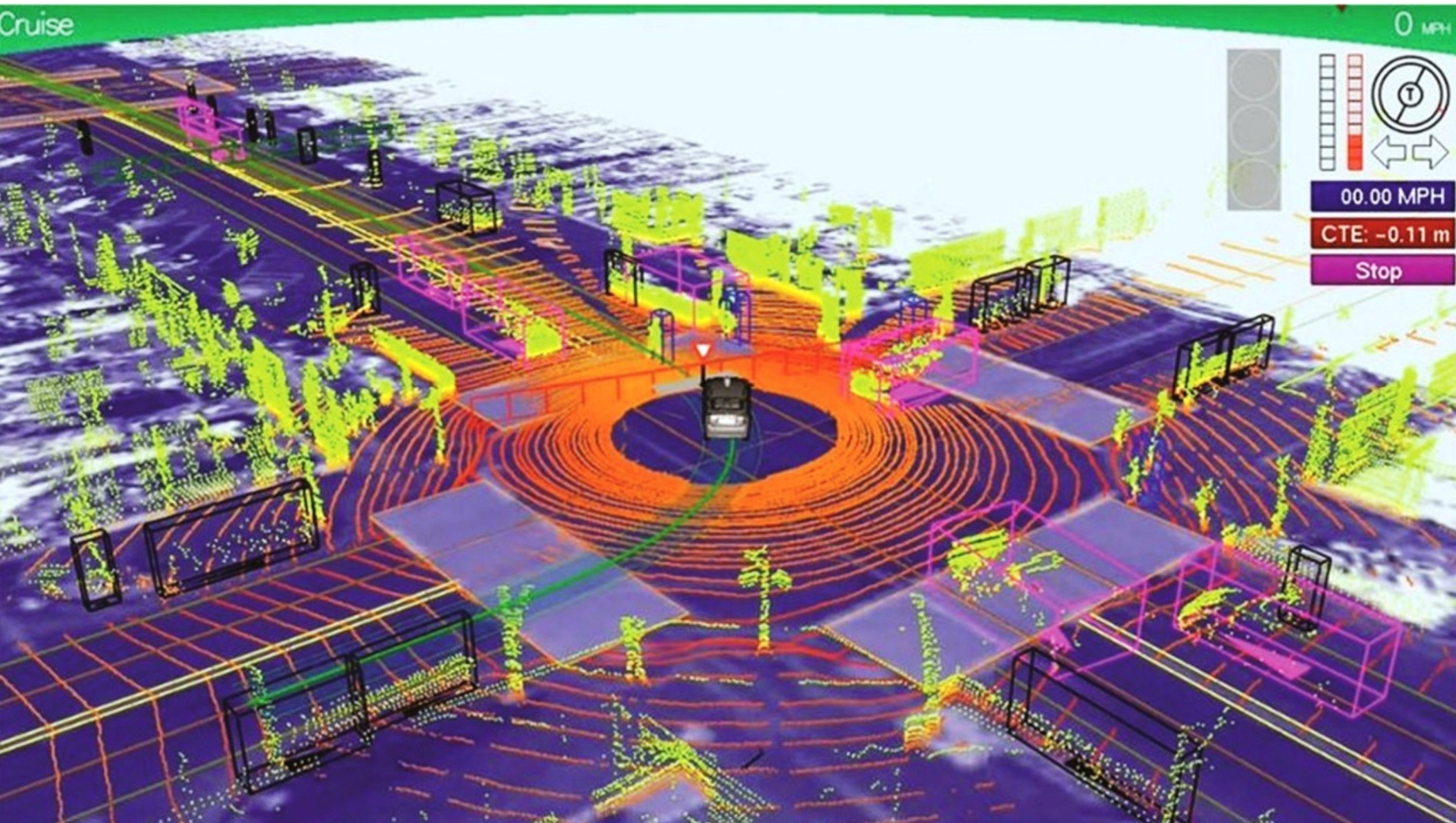
"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



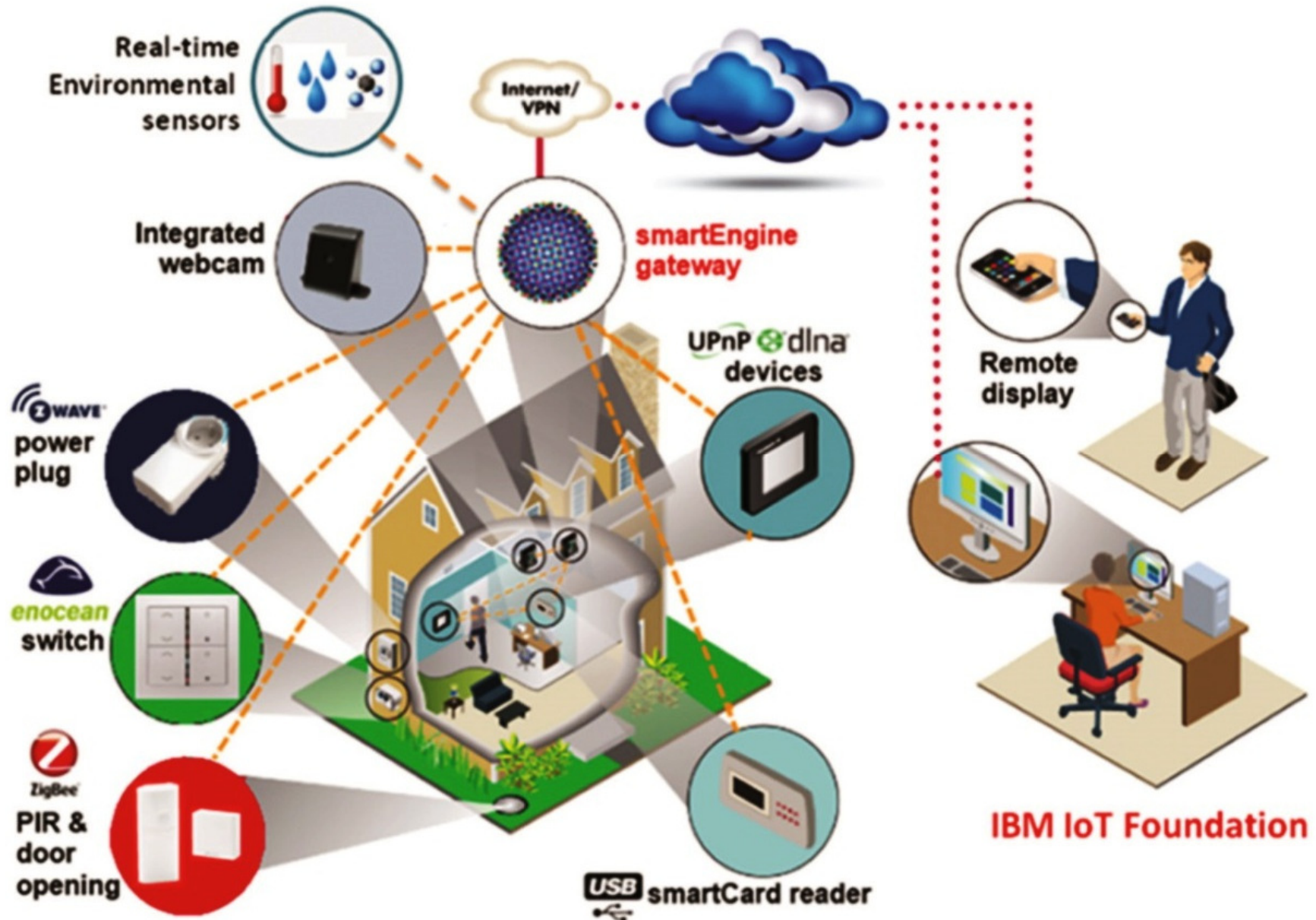
“IoT Devices”: *Wristbands and Watches*



“Google Car”: *Computer Vision View*



“IoT” Connectivity in the Home: IBM





RESEARCH PAPER

on

The Compromised Devices of the Carna Botnet

(used for "Internet Census 2012")

by Parth Shukla,

Information Security Analyst,

Australian Computer Emergency Response Team (AusCERT),

University of Queensland.

Email: pparth@auscert.org.au

Twitter: <http://twitter.com/pparth>

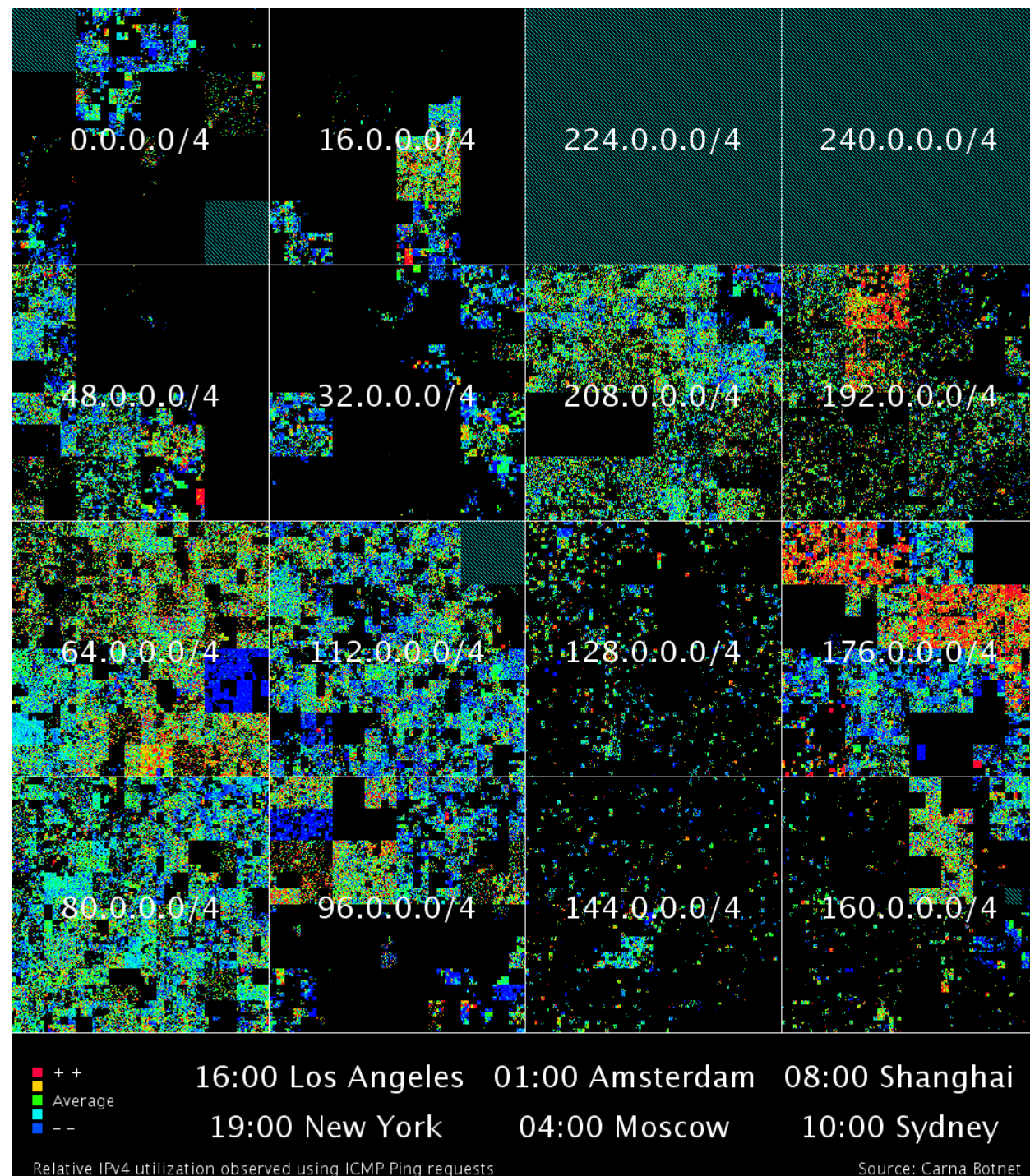
Version 1

20 August 2013 – Released to AusCERT members

25 August 2013 – Released to the Public

Carna Botnet exposed Legacy
Vulnerabilities in *"IoT" Devices*

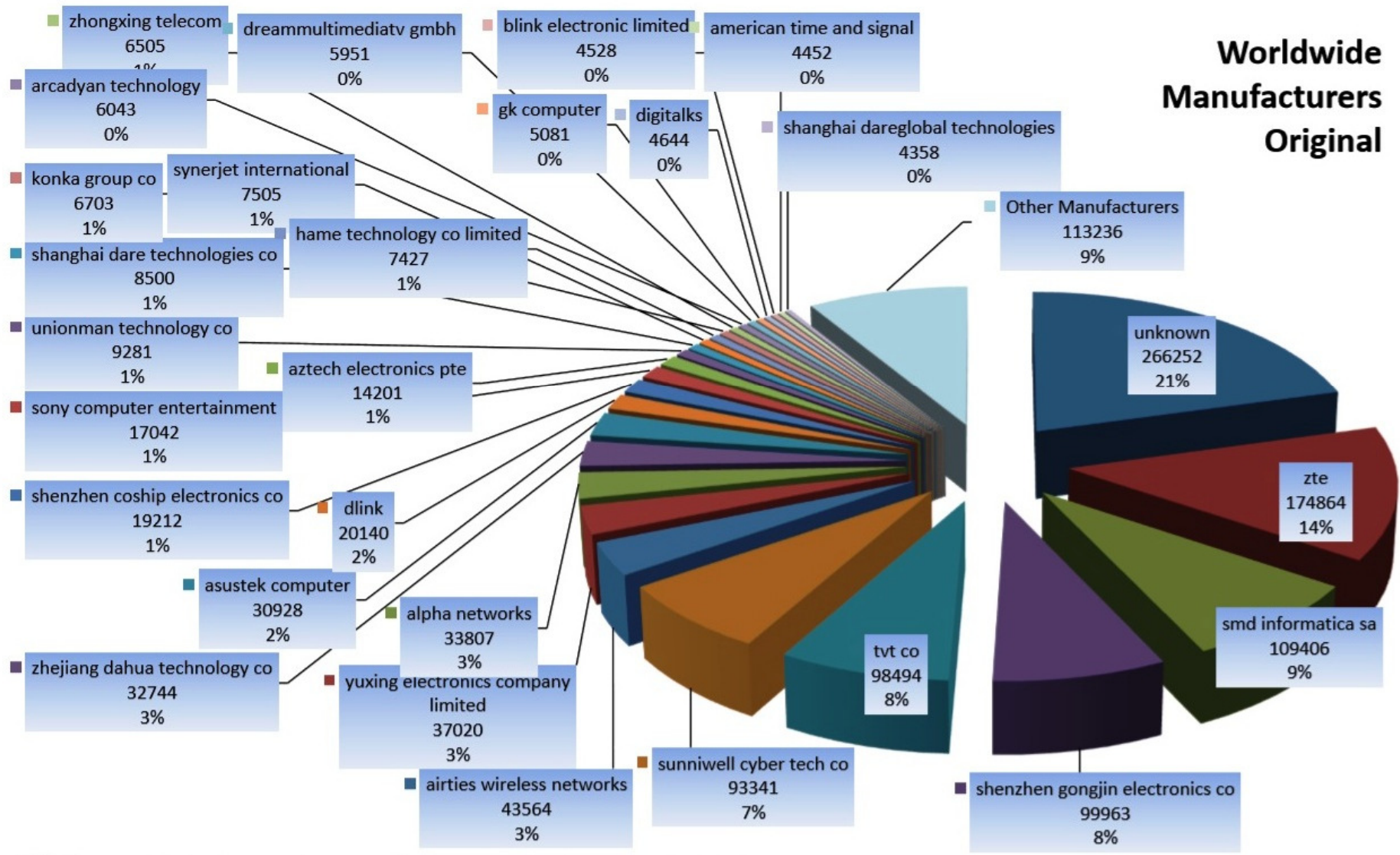
34th International East/West Security Conference



"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



Vulnerable Legacy Devices: “IoT”



Practical **Security Solutions** for the “IoT”

- **European Union - IERC:** Extensive “IoT” research during the last 5 years including security.
- **IEEE IoT Community, Journal & Conference :** Recent international focus upon IoT Security Standards and Engineering Practical Solutions.
- **Advanced Cyber Tools:** Sustainable IoT Network Security requires innovative 21stC Adaptive & Self-learning tools based upon research into Artificial Intelligence and Machine Learning.

Useful Publications on “Internet of Things”


Government
Office for Science



The Internet of Things: making the most of the Second Digital Revolution

A report by the UK Government Chief Scientific Adviser



“21stC Smart Security Architectures”
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



European Research Cluster: *Internet of Things*



ABOUT IERC

IoT European Research Cluster

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

European Dimension

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

Global Dimension

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

Internet of Things

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

[Home](#) [News](#) [Events](#) [Documents](#) [Newsletters](#) [About IERC](#) [Partners](#) [Links](#) [Contact](#)

IERC OBJECTIVES

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

EVENTS

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

NEWS

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

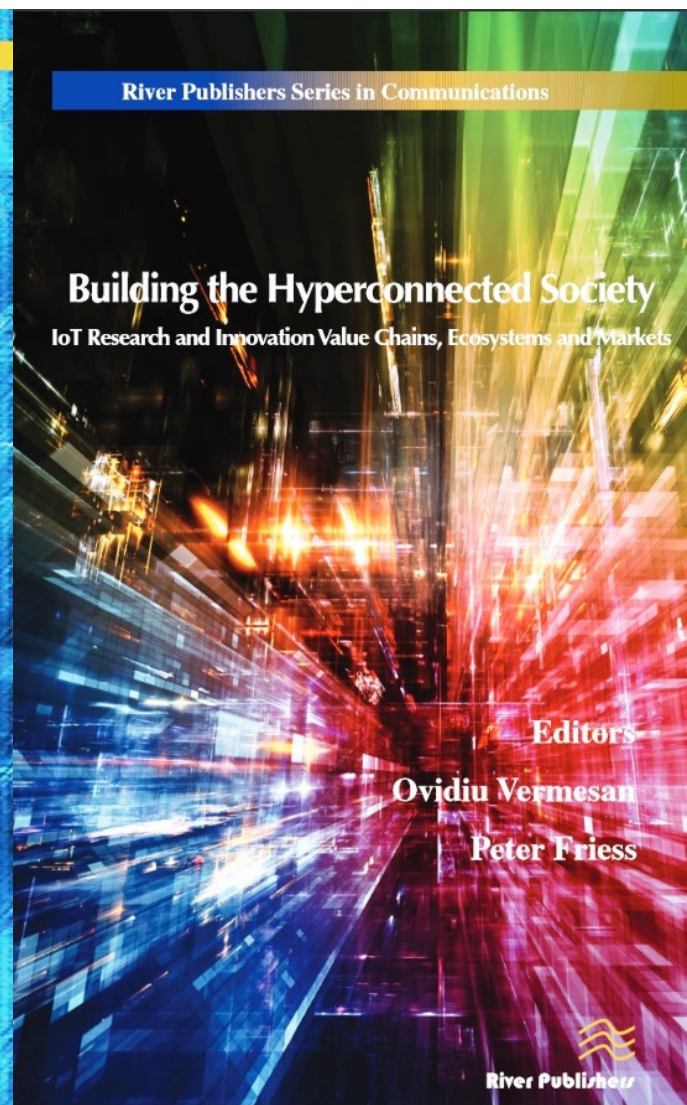
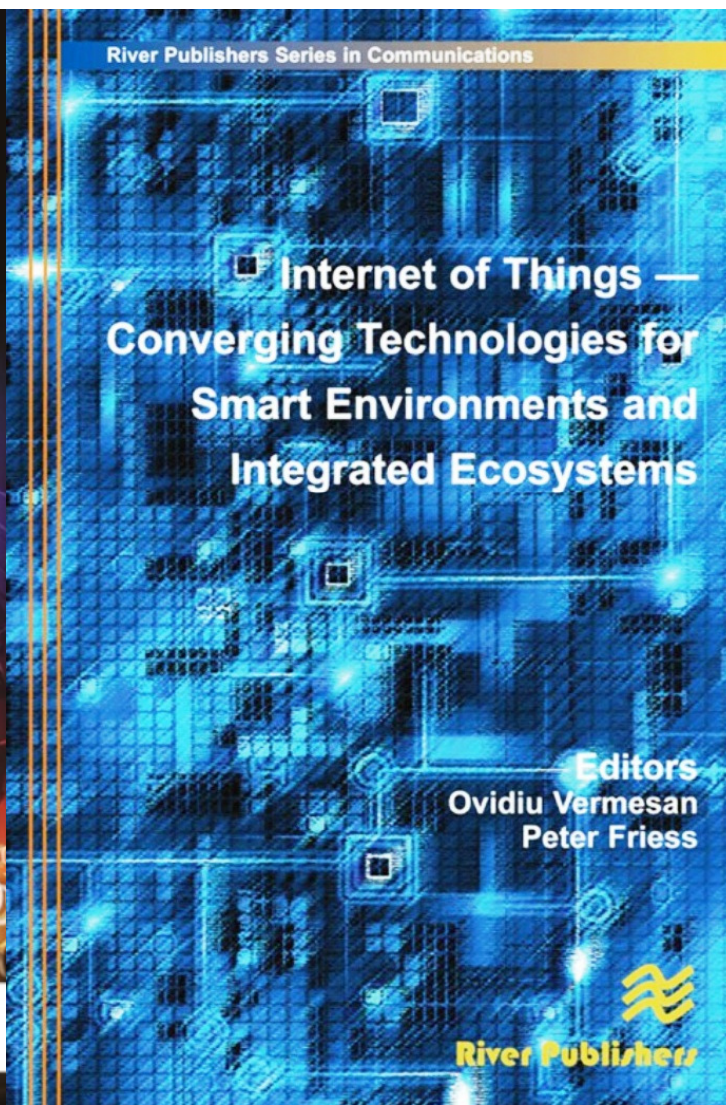
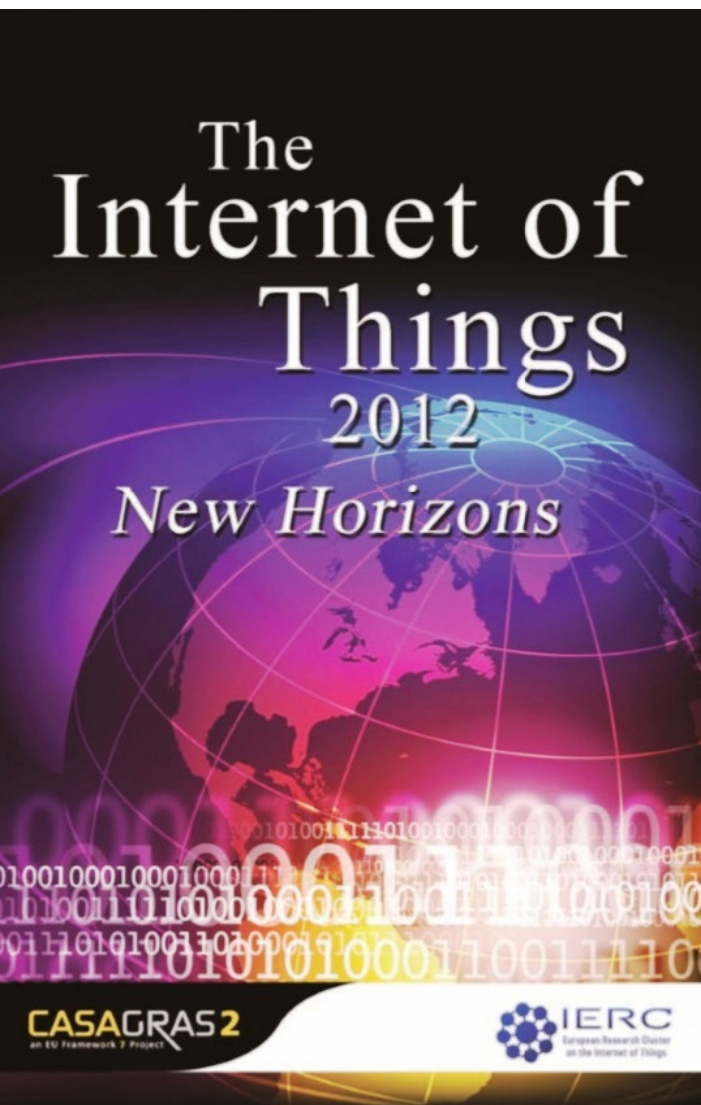
DOCUMENTS

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

"21stC Smart Security Architectures"
- **Real-Time Cyber-Physical Integration** -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©

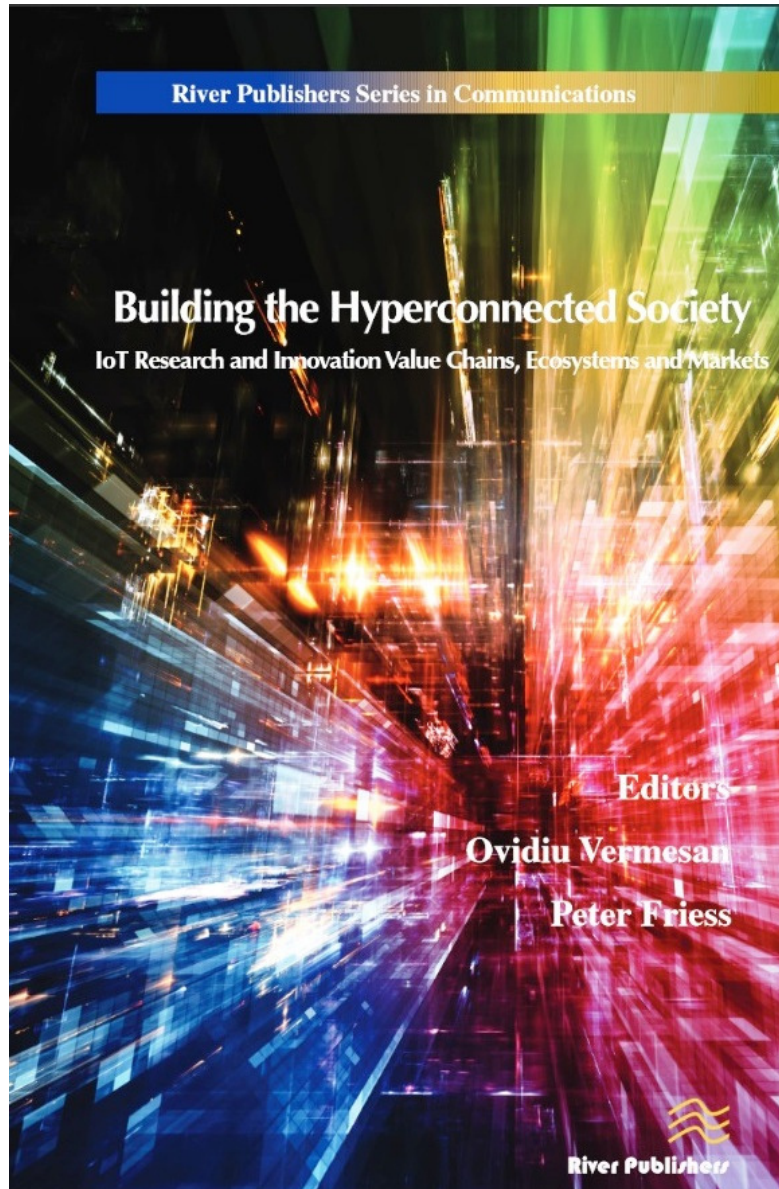


IERC – Research Cluster Reports on *“Smart Systems” & the Internet of Things*



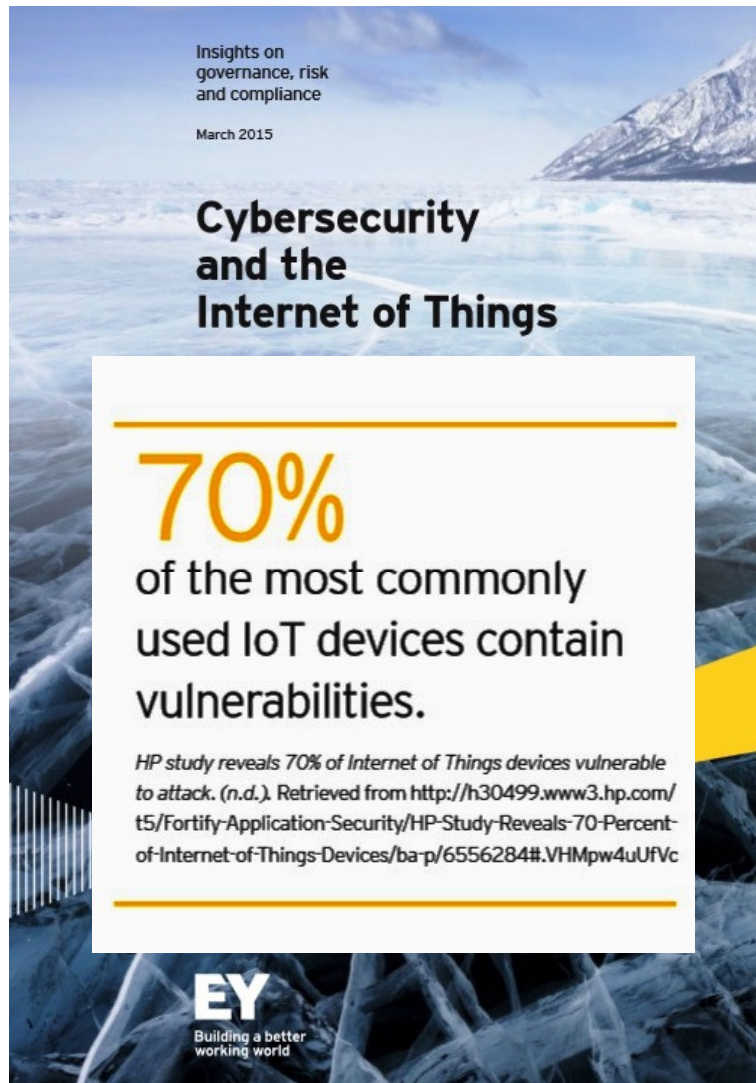
- Security for the Internet of Things -

Security & Privacy in Hyperconnected Society

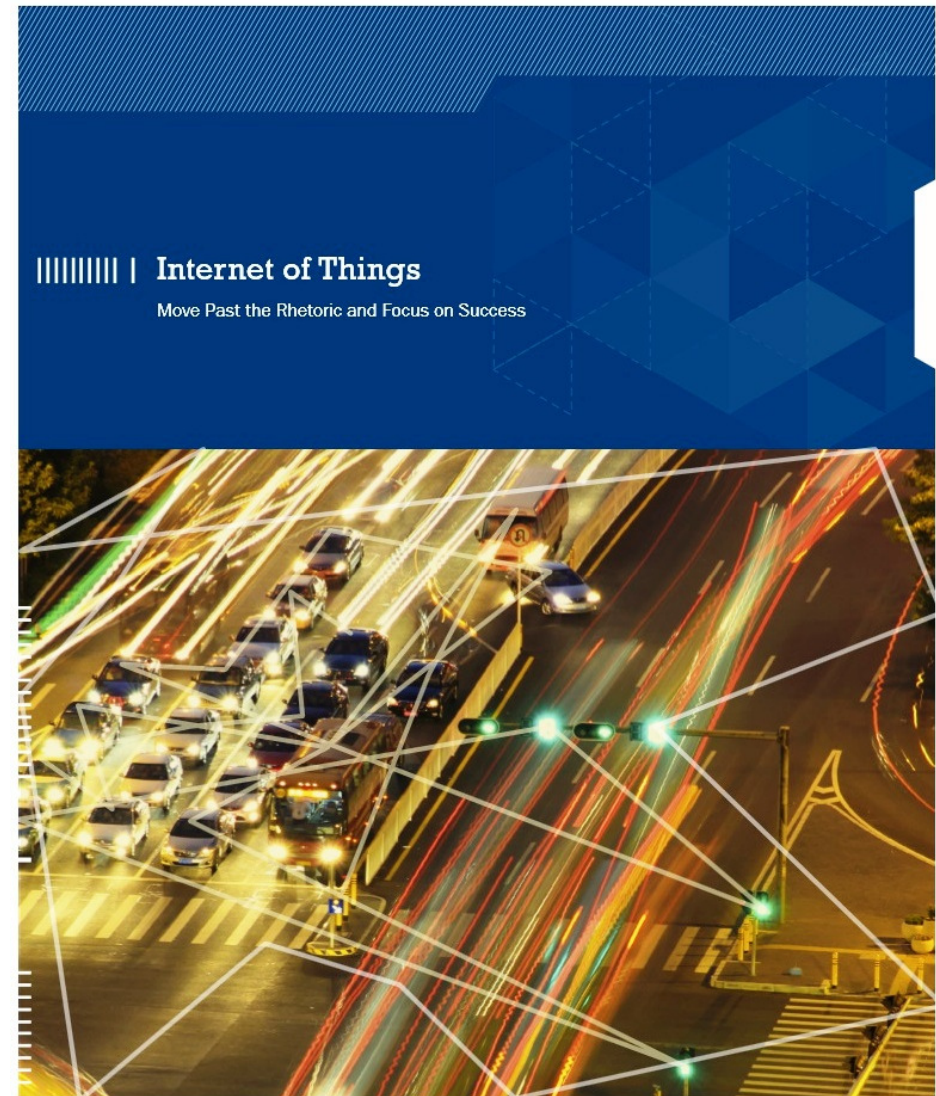


Securing the Internet of Things – Security and Privacy in a Hyperconnected World	189
6.1 Introduction	189
6.2 End-to-End Security and Privacy by Design	191
6.3 Physical IoT Security	192
6.3.1 Selected Low-Cost Attacks	192
6.3.2 Key Extraction Attacks and Countermeasures	195
6.4 On Device Security and Privacy	197
6.4.1 Mediated Device Access for Security and Privacy	198
6.4.2 Encryption	198
6.4.3 Integrity	200
6.4.4 Data Minimisation	200
6.5 Unobservable Communication	201
6.5.1 Resisting Network Traffic Analysis	202
6.6 Access Control Based on Policy Management	203
6.7 Security and Privacy in the IoT Cloud	206
6.7.1 Verifiable and Authenticity Preserving Data Processing	207
6.7.2 Structural Integrity and Certification of Virtualized Infrastructure	207
6.7.3 Privacy Preserving Service Usage and Data Handling	208
6.7.4 Confidentiality of (Un-)structured Data	209
6.7.5 Long Term Security and Everlasting Privacy	209
6.7.6 Conclusion	210
6.8 Outlook	210

Consultant Reports: *Internet of Things*



Ernst and Young Global Limited



Booz, Allen and Hamilton

Hamilton

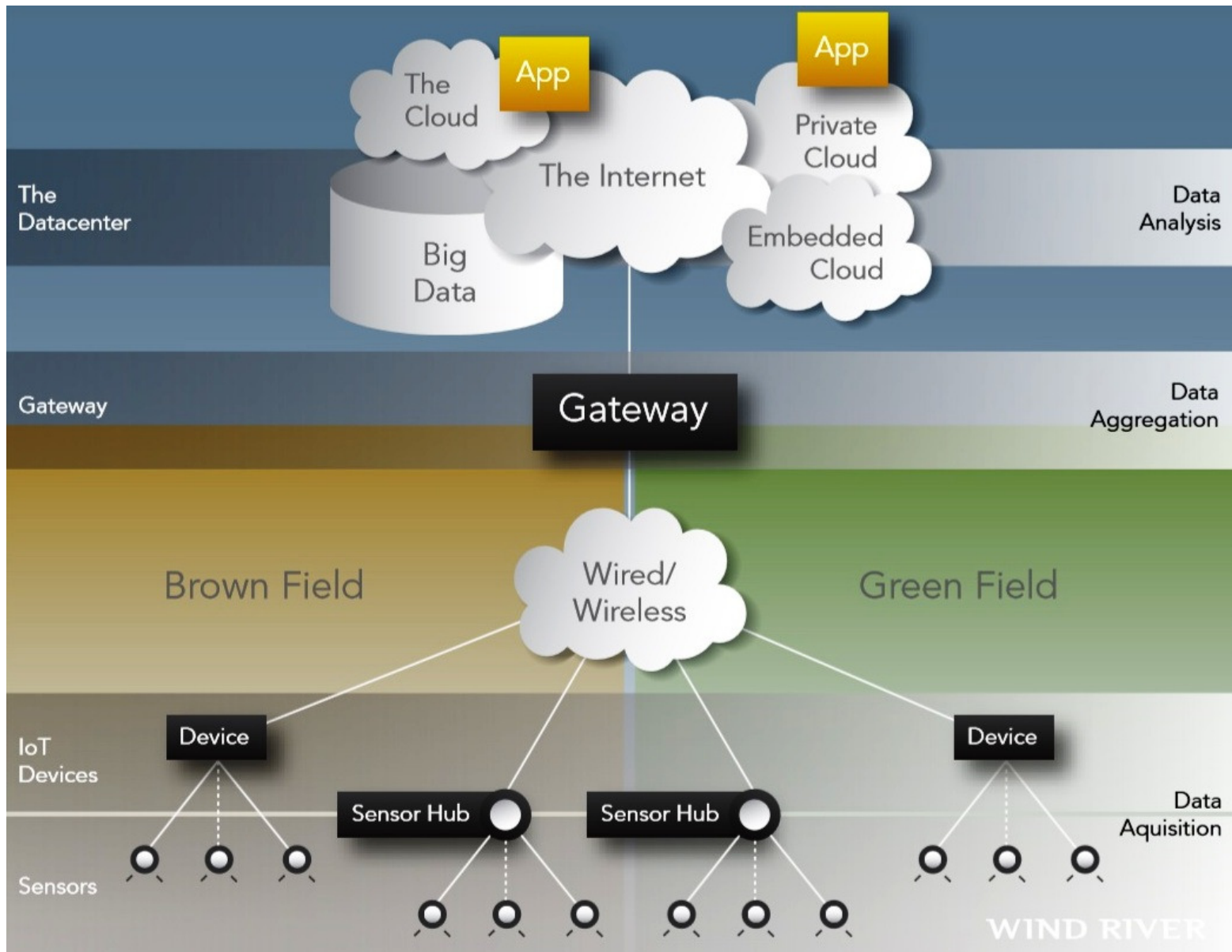
Innovate Forw

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



90

Internet of Things: *Cybersecurity Model*



Copyright: *Wind River – Intel Corporation*

34th International East/West Security Conference

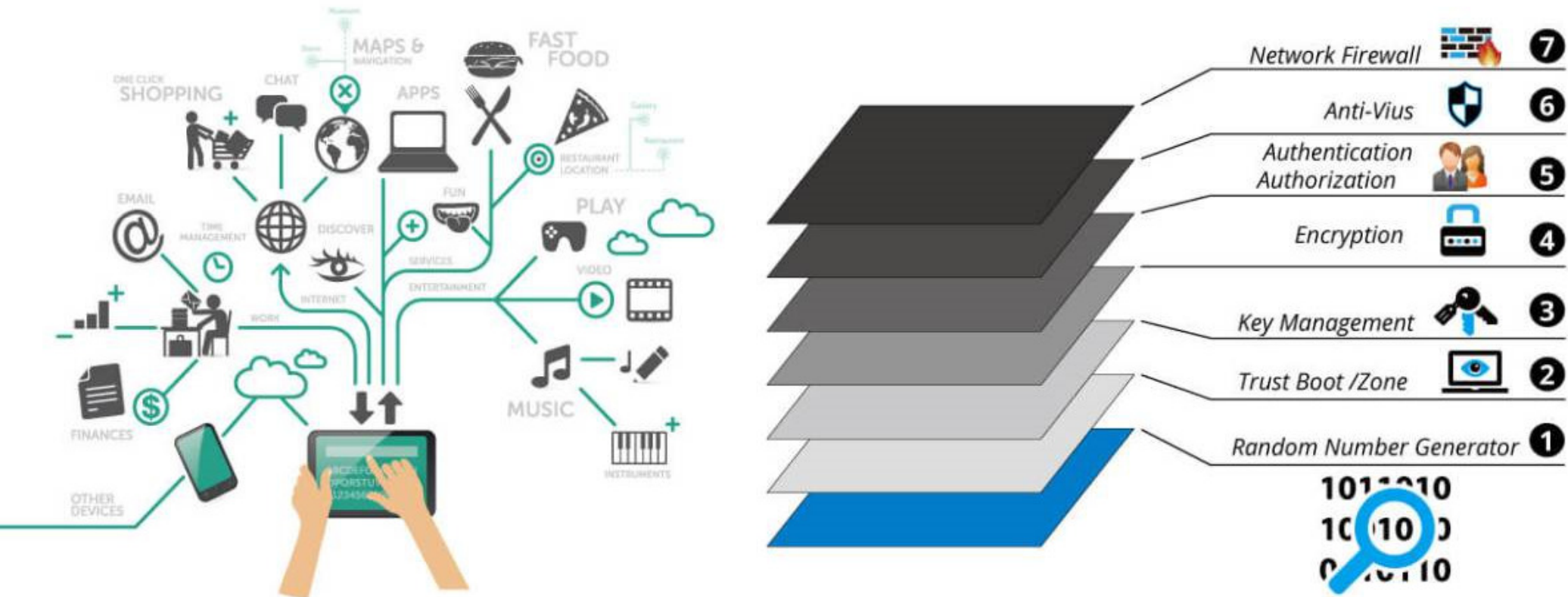
"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st-22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



IoT Cybersecurity: *7-Level Architecture*



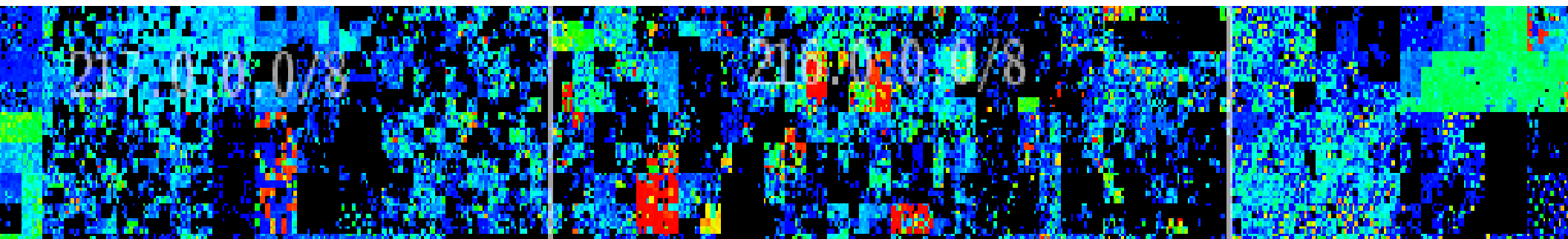
Cyber Security - 7 Security Layers Structure



"Smart Security": 21stC Business Architectures



1 – Background: "21 st C Security Landscape"	2 – Basic "Smart Security" Concepts	3 – Integrated Cyber-Physical Security
4 - Towards "Smart Security" Architectures	5 – "Smart Security" for <i>YOUR</i> Business!	6 – Security Scenarios: Critical Sectors
7 – Smart Security for "Internet of Things"	8 – Practical "Smart Security" Operations	9 – <i>YOUR</i> TOP 3 Actions & RoadMap!



(8) Practical *CyberSecurity* Strategies

- Successful Cyber Strategies are Scaled from:
Device->User->Business->City->Country->Global
 - a) Device:** Secure ALL devices connected to “IoT”
 - b) User:** Bio-ID, Real-Time Behaviour Modelling
 - c) Business:** CSO-Led, Professional Cyber Team
 - d) City:** Secure Transit Hubs, Culture & Sports Sites
 - e) Country:** Secure CNI, Profile & Track “Bad Guys”
 - f) Global:** Deploy UN/ITU CyberSecurity Agenda....Upgrade **ALL** your Legacy Security Tools & Inject ***Cyber Solutions*** to ***YOUR*** Business Operations!...

Practical *“Smart Security”* Operations

- **CSO Action:** Develop & Communicate Board Level Security Strategy spanning Cyber/On-Line & Physical Operations
- **Audit & Upgrade** each Business Unit & Function: Sales, Marketing, HR, Finance, R&D, Production...
- **Top Security Priorities:** IT Networks, Data Bases, ALL IT Devices/BYOD, Building Access & Control, Staff, Contractors & Guests, Wi-Fi/Mobile Access...
- **Security Tools:** “AI/ML Cyber”, CCTV Video Analytics, Biometrics, RFID, ANPR, DB/Mail/Media Monitoring...
- **Authorise Security Audits** to check company-wide compliance including Real-Time “Cyber” Monitoring!

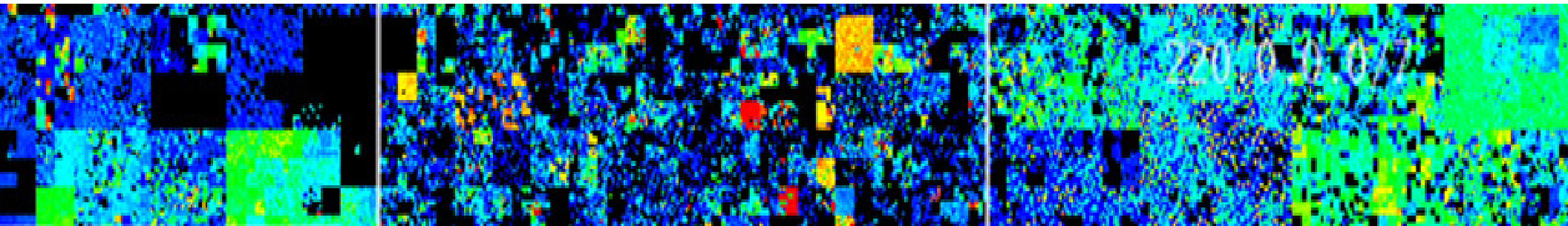
Benefits of “Smart” Cyber – Physical Security

- Some of the key benefits from integrating Cybersecurity solutions with physical operational processes and policies are:
 - *Reduced Operational Costs*, through “Single CSO-led Security Organisation”
 - *Early Warning* of both Physical & Cyber Penetration through RT surveillance
 - *Extended Protection* of ALL Critical Physical and On-Line Assets
 - *Focused Security Policy* for Government, Businesses and Citizens
 - *Risks*: Reduced “Open World” Security Risks from Smart Devices
 - *CyberCrime*: Comprehensive Management and Control of Cybercrime
 - *CNI*: Critical Infrastructure such as Banks & Airports are protected
 - *National Defence: Nations* now need hi-protection in “cyber” & “physical”
-In summary, the practical 21st approach to *integrated “smart” security* is a combination of *technological* solutions together with strong *operational* procedures, all implemented to international *ISO/IEC* security standards

"Smart Security": 21stC Business Architectures



1 – Background: "21 st C Security Landscape"	2 – Basic "Smart Security" Concepts	3 – Integrated Cyber-Physical Security
4 – Towards "Smart Security" Architectures	5 – "Smart Security" for <i>YOUR</i> Business!	6 – Security Scenarios: Critical Sectors
7 – Smart Security for "Internet of Things"	8 – Practical "Smart Security" Operations	9 – <i>YOUR</i> TOP 3 Actions & RoadMap!

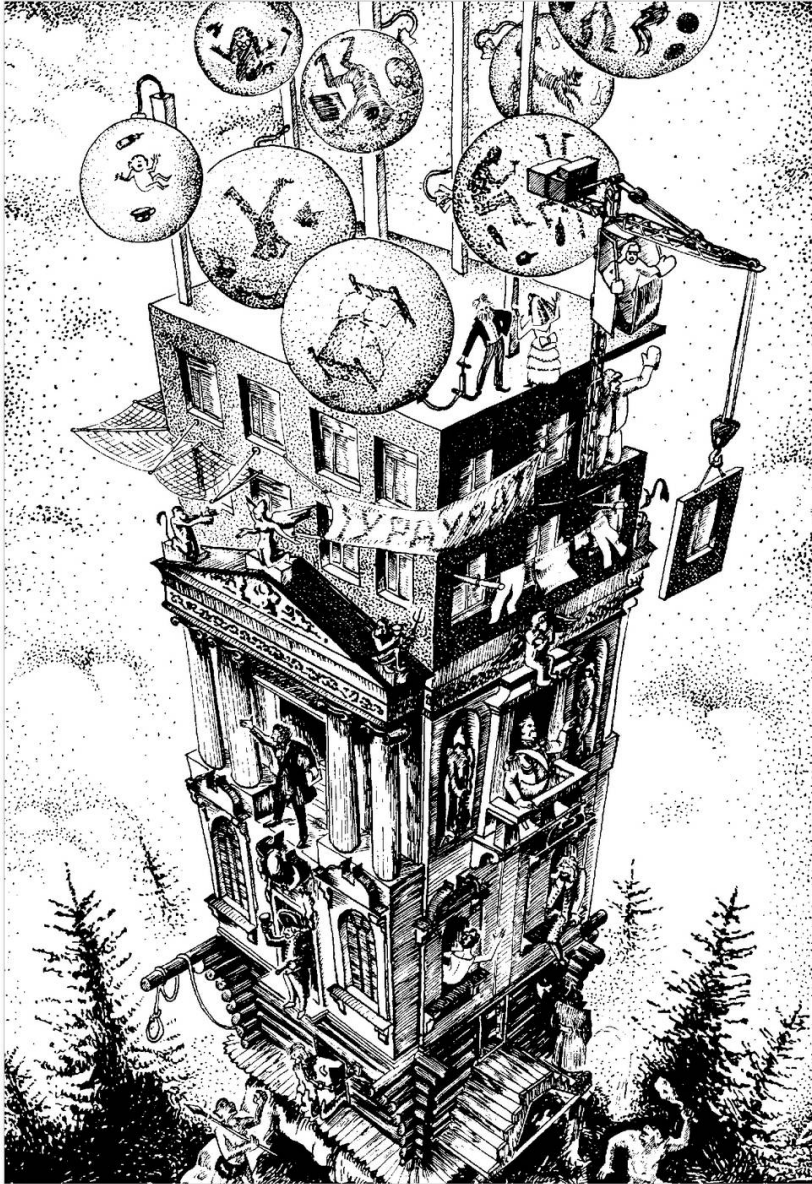


YOUR TOP 3 Actions & RoadMap

- **Action 1:** Board-Level Review & Audit of current Cybersecurity Tools & Operations – 60 days
- **Action 2:** Highlight security issues & insecure legacy net assets, devices & processes – 30 days
- **Action 3:** Develop Multi-Year Plan, Budget & Roadmap for Advanced “Cyber” to include:
 - a) CSO-Led “**Cyber-Physical**” Operational Integration
 - b) “**IoT Security**” for Legacy & New Network Assets
 - c) Training and Testing of “**AI/ML**” Cyber Solutions.

Tomorrow Morning @ **09:00** we'll explore **Future Scenarios** for “**Smart Security**” in our **CyberVision 2017 – 2027** and Beyond!

“Design & Deploy 21stC Smart Security Architectures for YOUR Business”



“Integrated & Intelligent
Security Architectures
provide Real-Time
Defence for Business,
Government and
Critical Sectors”

“History of Architecture”

- From *Baroque* to *Bubbles* -

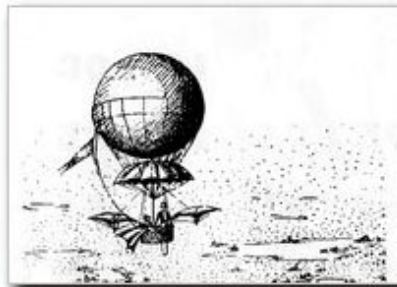
Pen & Ink Drawing by

Dr Alexander Rimski-Korsakov

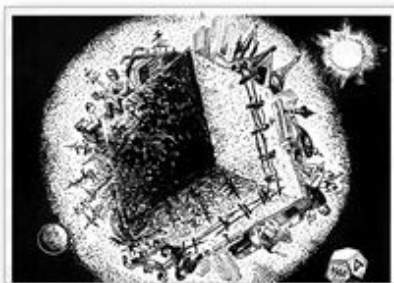
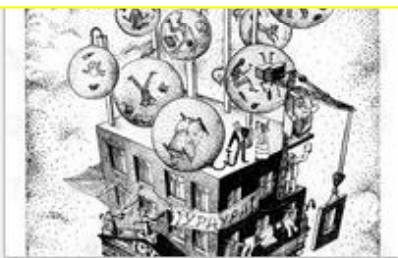
- Celebrated **80th** Birthday – 2016 -

“21stC Smart Security Architectures”
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©





The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov



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

34th International East/West Security Conference

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
 - Rome, Italy, 21st-22nd November 2016 -
 © Dr David E. Probert : www.VAZA.com ©





“Smart Security”: *21stC Business Architectures*

International East-West Security Conference: Rome

Download Presentation Slides:
www.Valentina.net/Rome2016/

“Smart Security”: 21stC Business Architectures

International East-West Security Conference: Rome

Thank-You!

Download Presentation Slides:
www.Valentina.net/Rome2016/

East-West Security Conference – Rome 2016

- “Smart CyberSecurity” - Slides (PDF) -



“Smart Security” Architectures for **YOUR** Business!

Dr David E. Probert
VAZA International

Dedicated to Grand-Daughters – Abigail, Alice & Tatiana – Securing YOUR Life!
34th International East/West Security Conference
“21stC Smart Security Architectures”
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



1

Theme (1) – “21stC Smart Security”



CyberSecurity Vision: ***2017 – 2027***

Dr David E. Probert
VAZA International

Dedicated to Grand-Sons: Ethan, Matthew, Roscoe & Hugh – Securing YOUR Future!
34th International East/West Security Conference
CyberSecurity Vision: 2017 – 2027 & Beyond
“Integrated, Adaptive & Neural Security”
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



1

Theme (2) – “CyberVision: 2017-2027”

Download Link: www.valentina.net/Rome2016/

34th International East/West Security Conference

“21stC Smart Security Architectures”
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©



103

Download Presentation Slides:
www.Valentina.net/Rome2016/



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
Jamaica: Cybersecurity Technology- Slides	Jamaica: Cybersecurity Strategy- Slides	"Short Professional Bio"	ITU/CITEL: Cybersecurity in the Americas	ITU/CITEL: Cybersecurity Skills Building

Link: www.valentina.net/vaza/CyberDocs

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
 - Rome, Italy, 21st-22nd November 2016 -
 © Dr David E. Probert : 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 1st Multi-Media and e-Commerce Web-Site for the World's 1st Supersonic Car – ThrustSSC – for the World Speed Record.
- **Secure Wireless Networking** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.
- **Networked Enterprise Security** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional engineers & a diverse portfolio of hi-tech security products.
- **Republic of Georgia** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament.
- **UN/ITU** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

Dr David E. Probert is a Fellow of the Royal Statistical Society, IEEE Life Member and 1st 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: 2007-2017 Editions.

“Master Class”: Armenia - *DigiTec2012*

- *Smart Security, Economy & Governance* -

 <p>Smart Solutions: "Master Class" – Part 1</p> <p>- Defining Smart Solutions & Business Architectures -</p> <p>Dr David E. Probert VAZA International</p> <p>digtectbusiness12</p>	 <p>Smart Solutions: "Master Class" – Part 2</p> <p>- Smart Solutions in Practice for 21stC Armenia -</p> <p>Dr David E. Probert VAZA International</p> <p>digtectbusiness12</p>	 <p>Smart Solutions: "Master Class" – Part 3</p> <p>- Designing & Engineering Smart Solutions -</p> <p>Dr David E. Probert VAZA International</p> <p>digtectbusiness12</p>
"Master Class - Smart Theory"	"Master Class - Smart Practice"	"Master Class - Smart Design"
 <p>- Armenia: Smart Economy -</p> <p>"Smart Business Architectures for Intelligent Economic Development"</p> <p>Dr David E. Probert VAZA International</p> <p>digtectbusiness12</p>	 <p>- Smart Sustainable Security -</p> <p>"Integrating Cyber & Physical Operations"</p> <p>Dr David E. Probert VAZA International</p> <p>digtectbusiness12</p>	 <p>- Smart Governance -</p> <p>"Stimulating Innovation & Economic Growth"</p> <p>Dr David E. Probert VAZA International</p> <p>digtectbusiness12</p>
"Armenia: Smart Economy"	"Armenia: Smart Sustainable Security"	"Armenia: Smart Governance"

Download: www.valentina.net/DigiTec2012/

34th International East/West Security Conference

"21stC Smart Security Architectures"
- Real-Time Cyber-Physical Integration -
 - Rome, Italy, 21st-22nd November 2016 -
 © Dr David E. Probert : www.VAZA.com ©

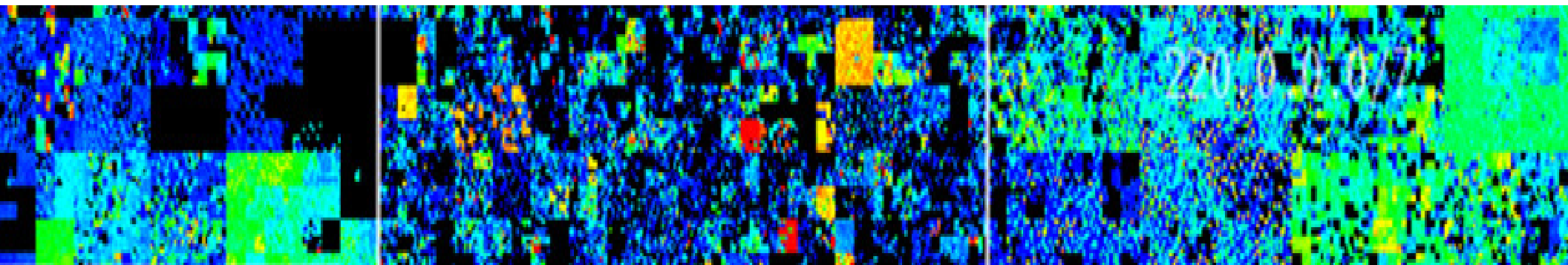


“Smart Security”: *21stC Business Architectures*

34th International East-West Security Conference: Rome, Italy



BACK-UP SLIDES

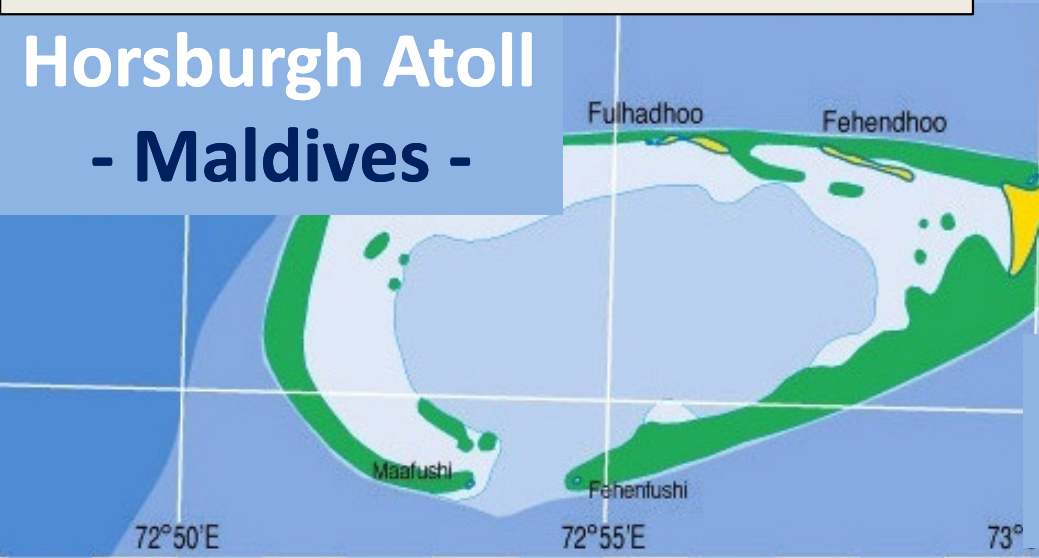


- **Secure** Navigation in the “*Southern Seas*” - “**Captain James Horsburgh**” (1762 – 1836)

Charting the “*Southern Seas*”
-“**The India Directory**”(1809) -
for “**The East India Company**”

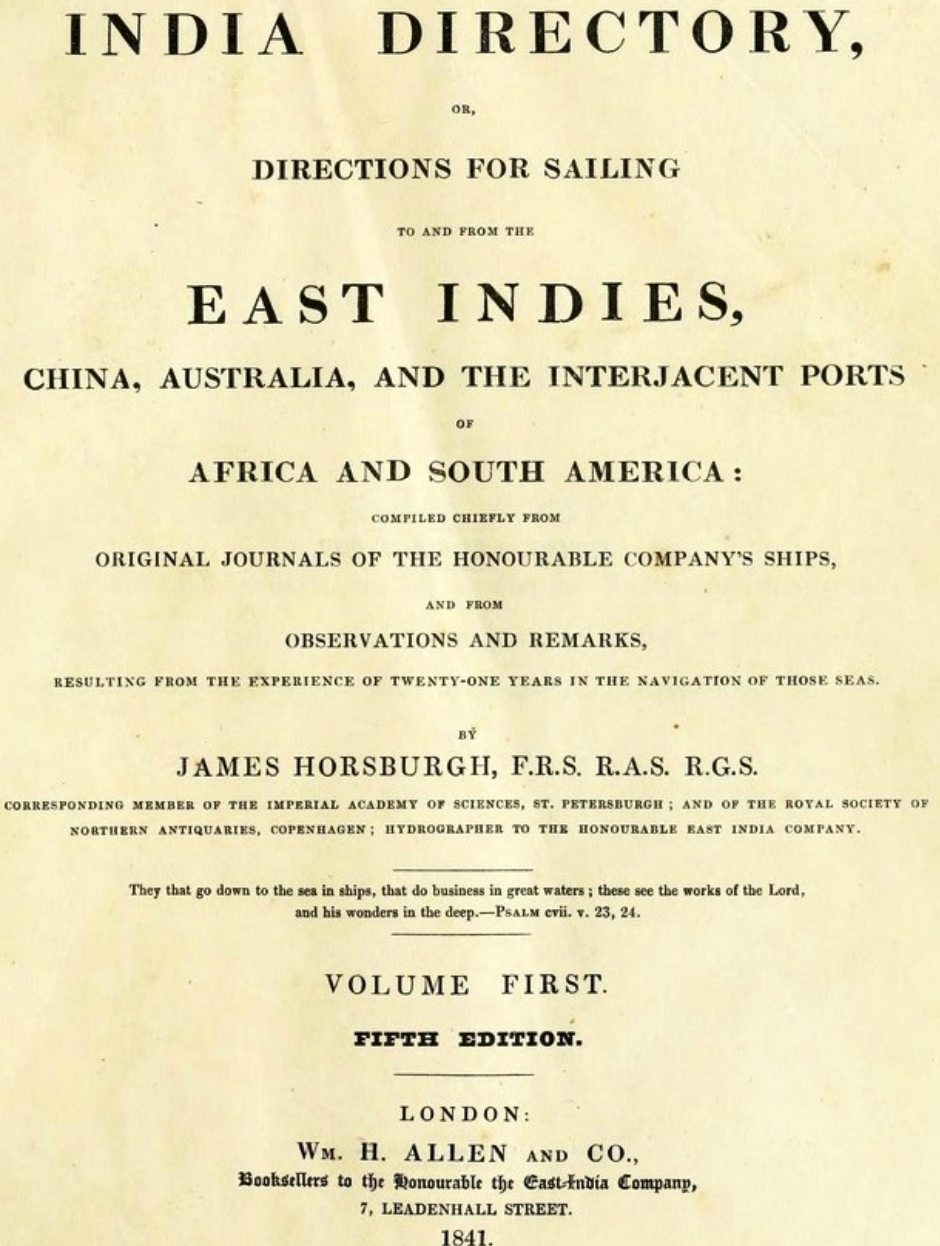
- 1) **Horsburgh Island: Cocos/Keeling Is**
- 2) **Horsburgh Lighthouse: Singapore**
- 3) **Horsburgh/Goidhoo Atoll: Maldives**

Horsburgh Atoll
- **Maldives** -



From “**Smart Navigation**” to “**Smart Security**”!

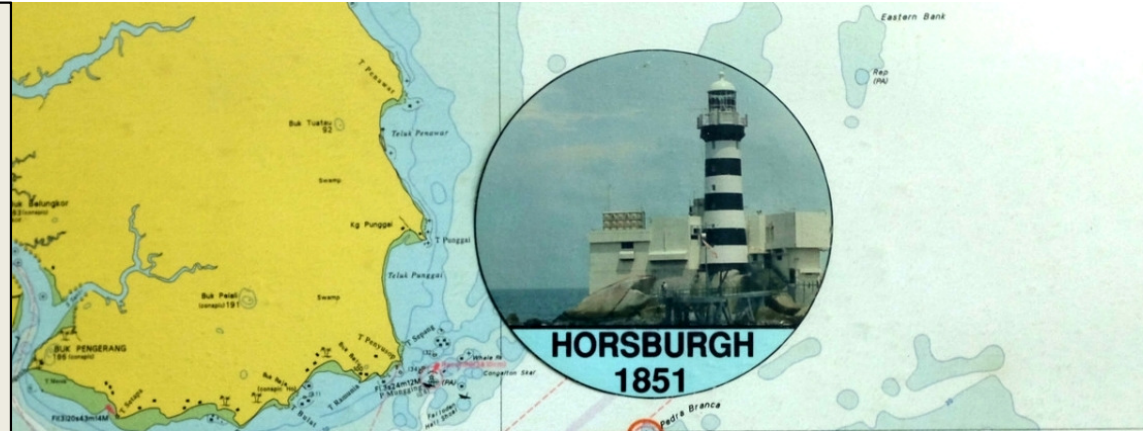
34th International East/West Security Conference



- **Secure** Navigation in the “*Southern Seas*” - “Captain James Horsburgh” (1762 – 1836)

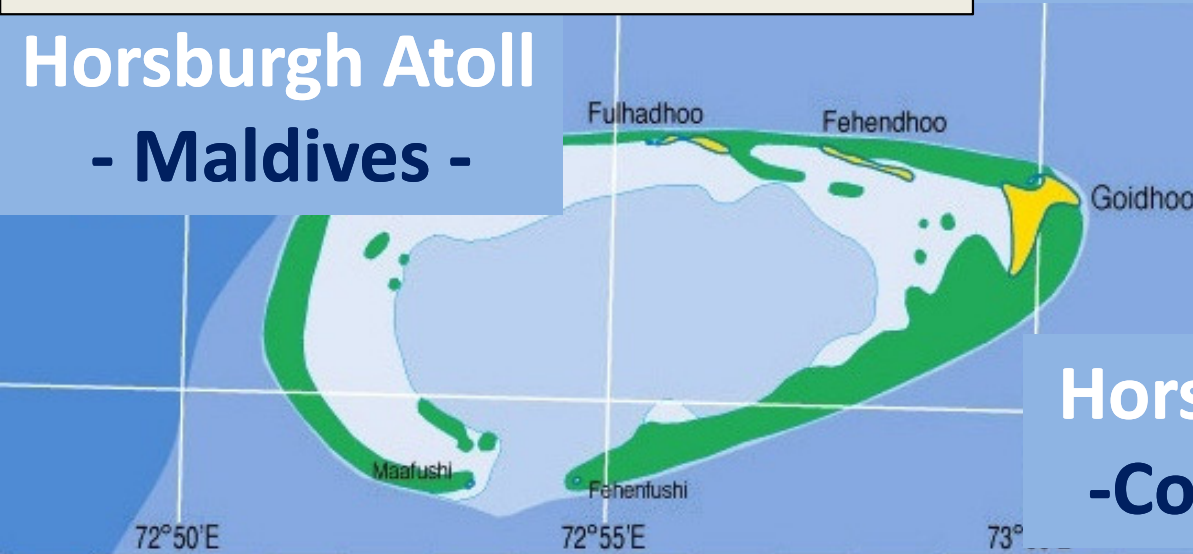
Charting the “*Southern Seas*”
- “The India Directory” (1809) -
for “The East India Company”

- 1) Horsburgh Island: Cocos/Keeling Is
- 2) Horsburgh Lighthouse: Singapore
- 3) Horsburgh/Goidhoo Atoll: Maldives



Horsburgh Lighthouse: Singapore

Horsburgh Atoll
- Maldives -



Horsburgh Island
- Cocos/Keeling -

From “**Smart Navigation**” to “**Smart Security**”!

34th International East/West Security Conference

Dedicated to Memory of Edward Michael Horsburgh (1923–2013)

“21stC Smart Security Architectures”
- Real-Time Cyber-Physical Integration -
- Rome, Italy, 21st–22nd November 2016 -
© Dr David E. Probert : www.VAZA.com ©

