

21stC Cybersecurity Trends

"CyberVision: 2015-2025"

- Integrated, Adaptive & Intelligent Security -

Dr David E. Probert

CyberVision : 2015 - 2025

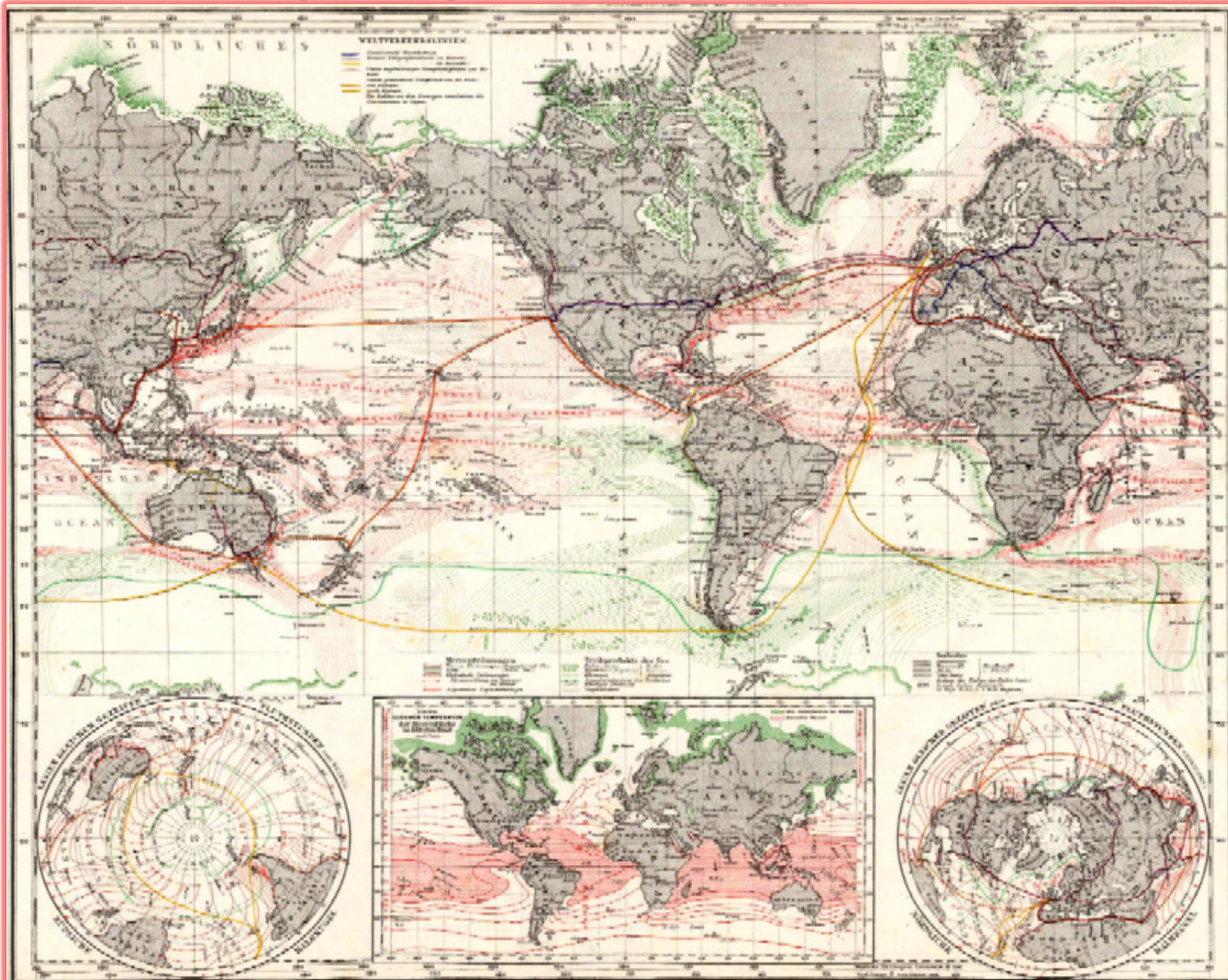
***** 21stC Cybersecurity Trends *****
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

“CyberVision: 2015 – 2025”

- **My Vision:** My Personal “CyberVision” develops practical scenarios for the next 10 Year Evolution of Cybersecurity
- **World Transition:** From 20thC Physical to 21stC Cyber World
- **AI Evolution:** Integrated, Adaptive & Intelligent Security
- **Marketplace:** The Global Cybersecurity Business Sector is forecast to expand to more than \$250Billion/Yr by 2025
- **Cybersecurity** is at the Core of 21stC Society: ProActive Real-Time Defence against Worldwide 24/7 Threats from
*** CyberTerrorism, Cyber Crime & Cyber Warfare ***

... *We need to fully embed Intelligent & Adaptive Cybersecurity within the “Internet of Things”*

“Visualisation of Cyberspace”: *Global IP “WHOIS” Addresses*



...From 19thC Physical World To 21stC Intelligent World!

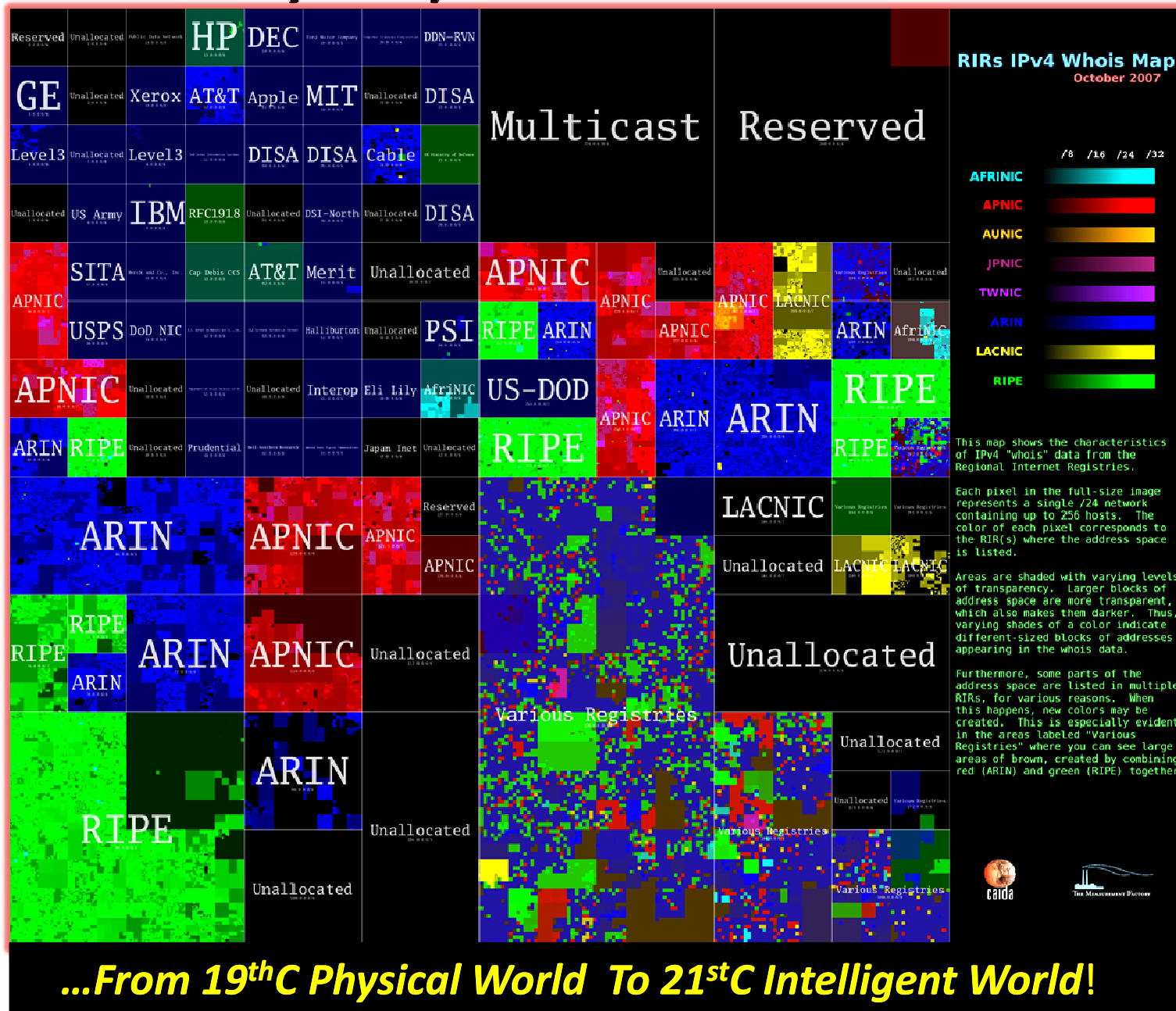
CyberVision : 2015 - 2025

***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

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

“Visualisation of Cyberspace”: *Global IP “WHOIS” Addresses*



CyberVision : 2015 - 2025

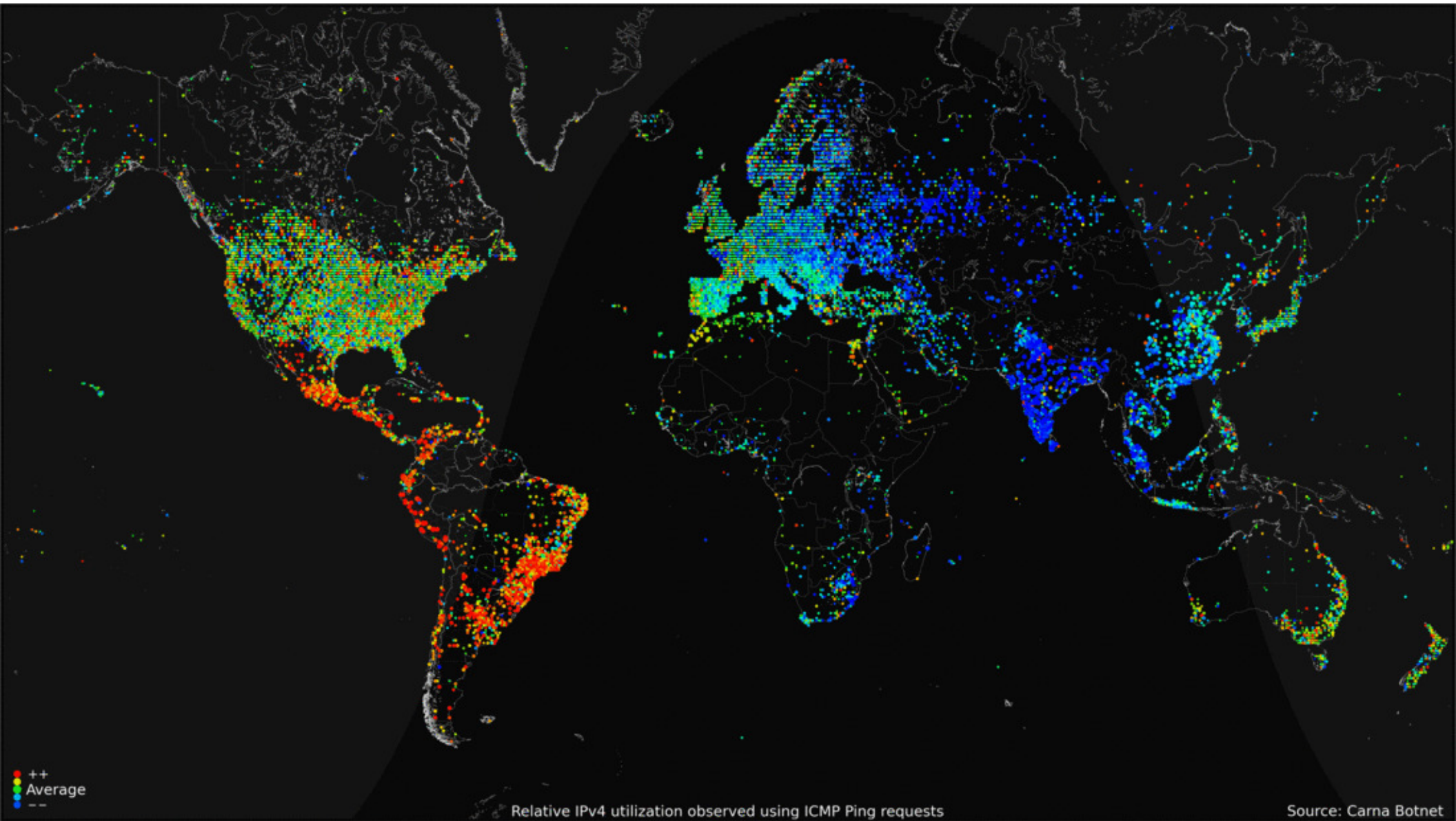
*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

GeoVision 24/7 Internet Connectivity

- “Worldwide Internet Census 2012” -



CyberVision : 2015 - 2025

*** 21st Century Cybersecurity Trends ***

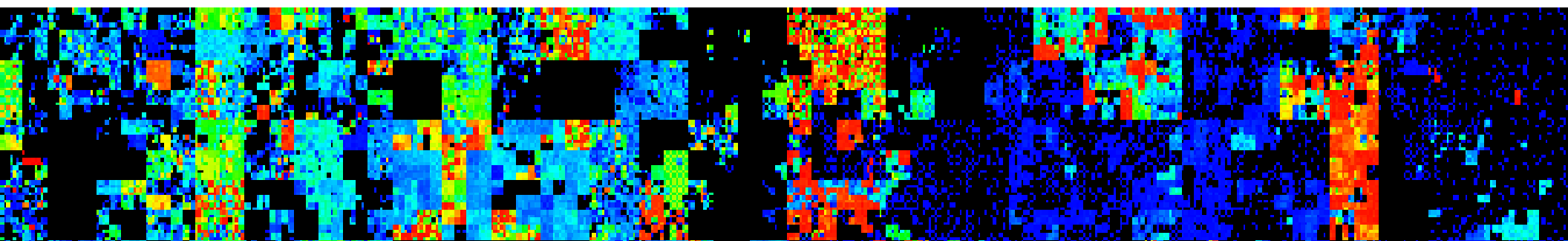
London, UK :: 15th December 2015

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

21stC Cybersecurity Trends: 2015 - 2025



1 – Background: “21st Security Landscape”	2 – Cybersecurity: Players & Threats	3 – Cyber Market Structure, Size & Growth
4 – CSO: C-Suite Security Integration “Integrated”	5 – Scenario 2020: Internet of Things (IoT) “Adaptive”	6 – Scenario 2025: AI & Machine Learning “Intelligent”
7 – CyberSecurity Ventures (Old and New)	8 – Mergers, Acquisitions & VC Funds	9 – YOUR Actions Plan for 21stC Cyber!....



CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

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)***

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”
- Evolution of Smart Devices, Cities, Economy & Society
- Dramatic increase in Cyber Crime & Cyber Terrorism

Cybersecurity Market Sectors

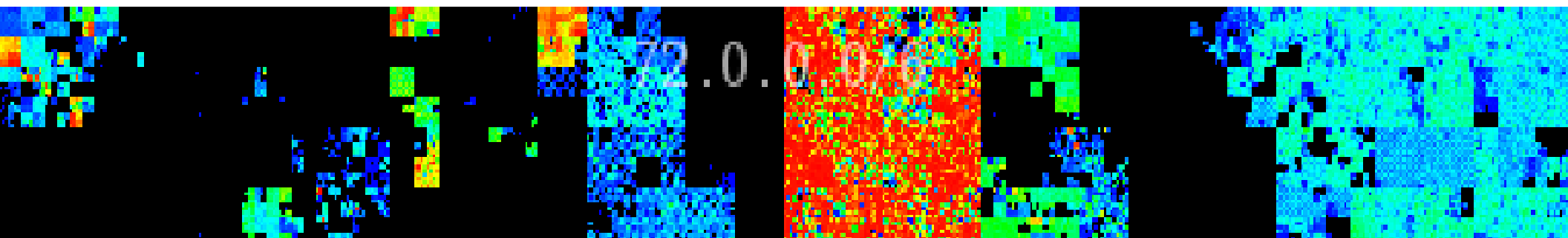
- Anti-Virus/Firewall
- ID Authentication
- Encryption/Privacy
- Risk & Compliance
- Mobile Device Security
- Anti-Fraud Monitoring
- Website Protection
- S/W Code Verification
- AI & Machine Learning
- Enterprise IoT Security
- Cloud Security Services
- Big Data Protection
- RT Log/Event Analytics
- 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”!***

21stC Cybersecurity Trends: 2015 - 2025



1 – Background: 21stC Security Landscape	2 – Cybersecurity – Players & Threats	3 – Cyber Market Structure, Size & Growth
4 – CSO: C-Suite Security Integration “Integrated”	5 – Scenario 2020: Internet of Things (IoT) “Adaptive”	6 – Scenario 2025: AI & Machine Learning “Intelligent”
7 – CyberSecurity Ventures (Old and New)	8 – Mergers, Acquisitions & VC Funds	9 – YOUR Actions Plan for 21stC Cyber!....



NEWS

Home

UK

World

Business

Politics

Tech

Science

Health

Education

Entertainment

England

N. Ireland

Scotland

Alba

Wales

Cymru

Friday 23rd Oct 2015

TalkTalk boss 'sorry for cyber-attack'

The head of TalkTalk says she is "very sorry" after personal details of up to four million customers were accessed by hackers in a major cyber-attack.

🕒 29 minutes ago | **UK**

Could this be an extortion attack?

LIVE TalkTalk hack reaction

▶ We're acting speedily - TalkTalk

How to stress test cybersecurity

Estimated \$\$\$ Loss = **\$55** Million



Major **Cyber-Attack** UK Internet Service Provider

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

17th Nov 2015: “Islamic State is Plotting Deadly Cyber-Attacks”: *George Osborne*



£1.9bn Cybercrime Budget
UK National Cyber Centre
National Cyber Crime Unit

CyberVision : 2015 - 2025

***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

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

Typical Global “*Botnet*” Cyber Attack



Wired Magazine – Summer 2007

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

Command & Control (C2) *Malware* Servers

- “Global 21st Century *Cyber-Colonisation*” -

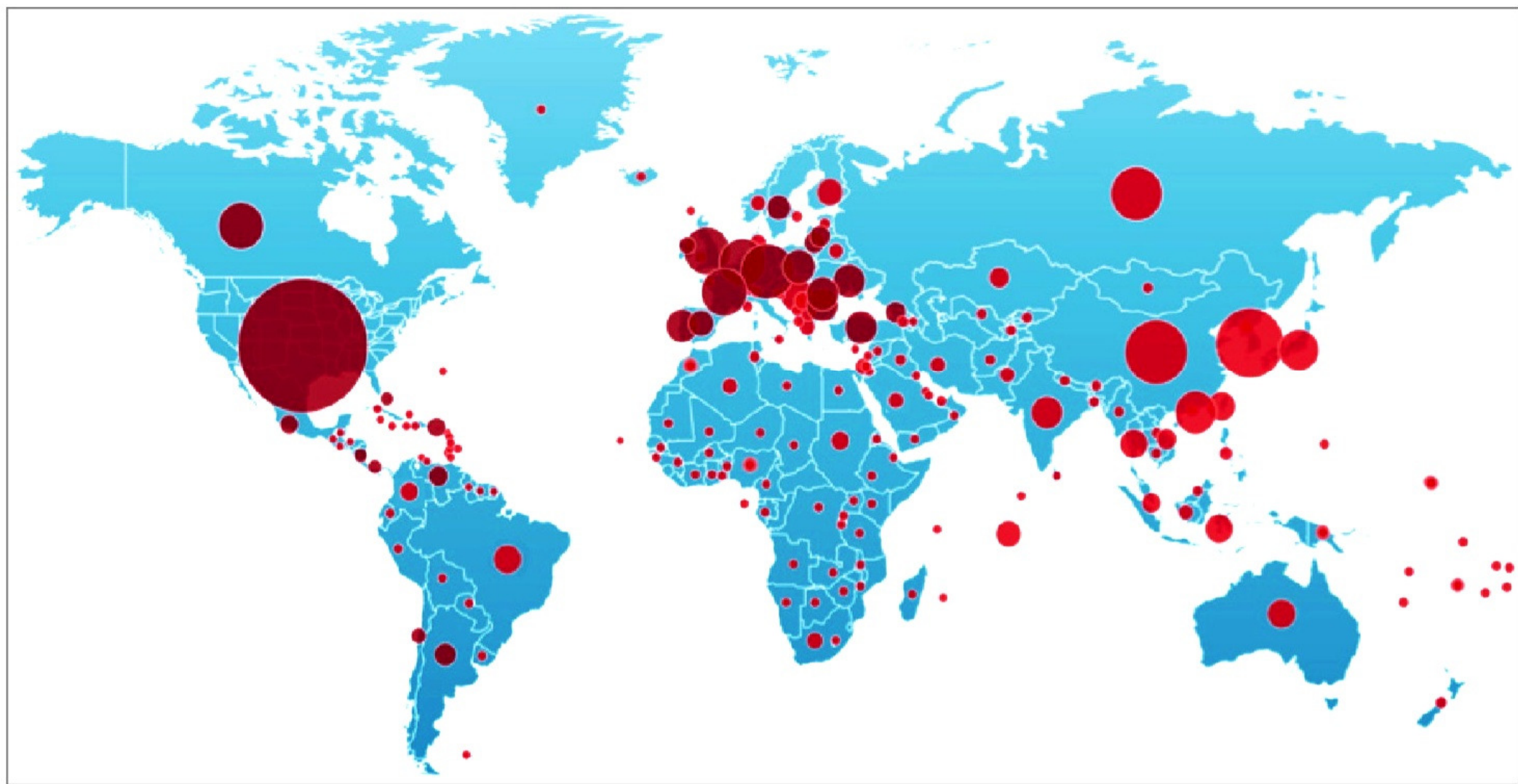


Image: www.fireeye.com – FireEye Inc (c)

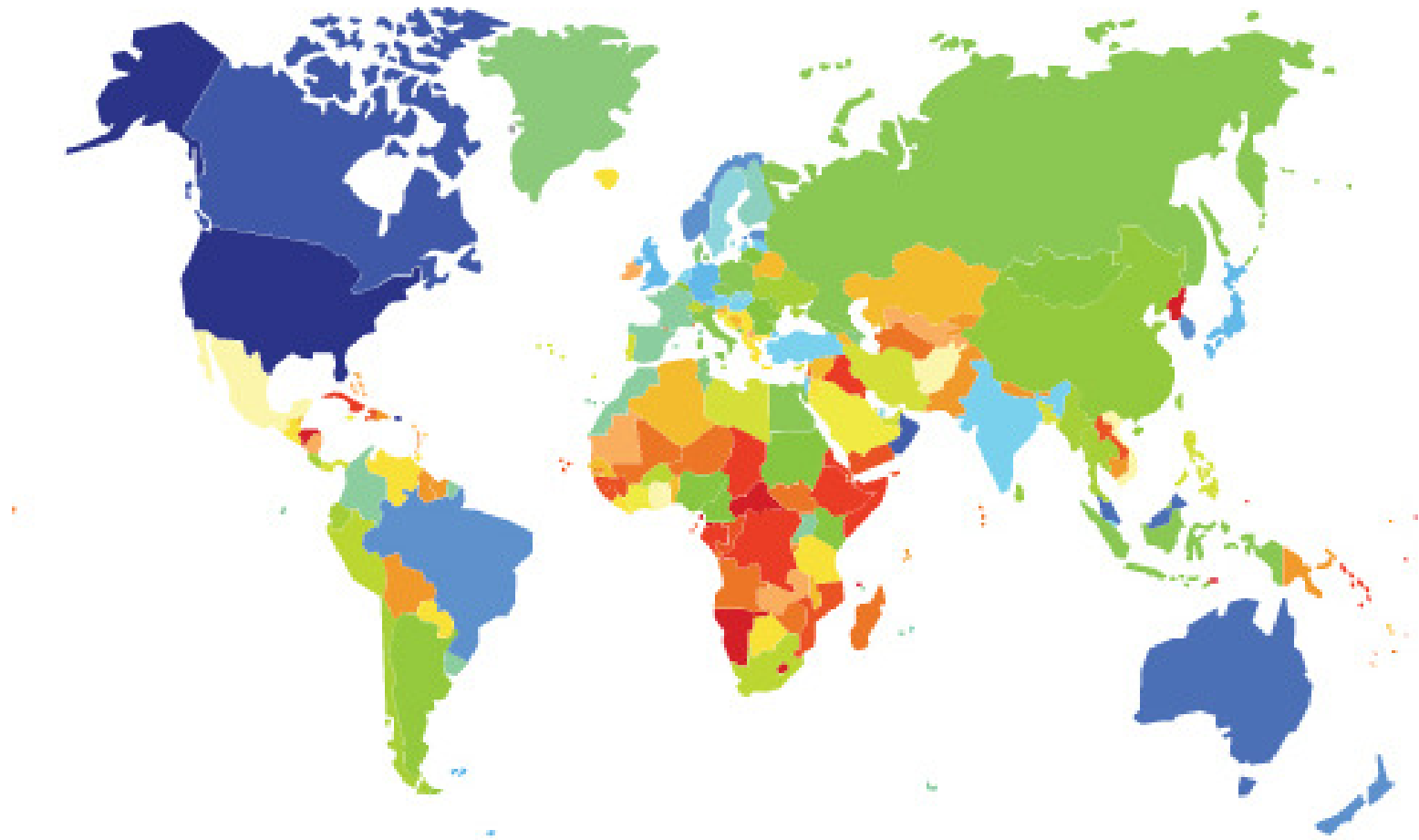
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

UN/ITU – Global Cybersecurity Index (Dec 2014)



ABIresearch[®]



Global
Cybersecurity
Index

National Cybersecurity Commitment



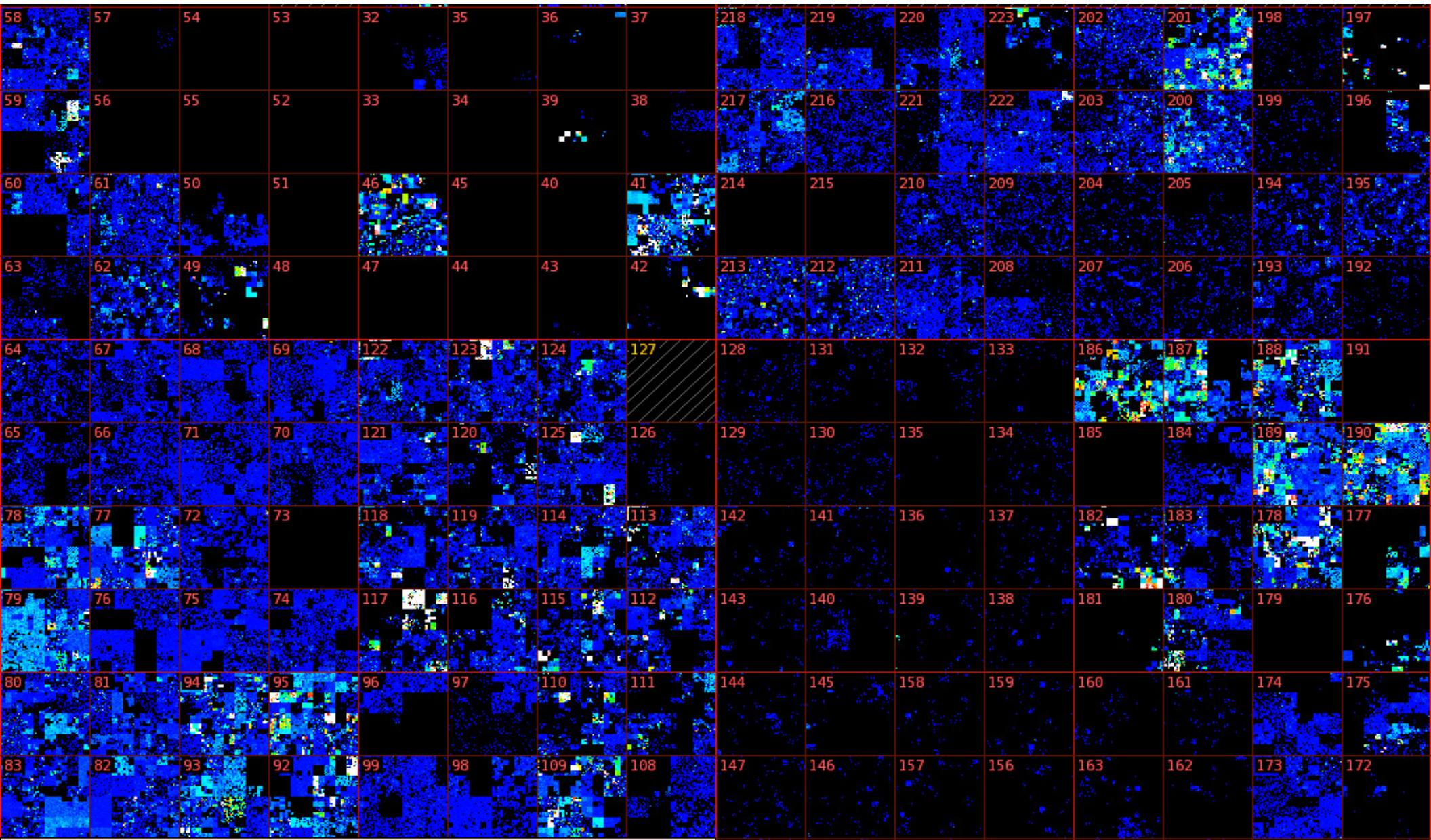
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

Map of *Recent* Malicious Activity in “*Cyberspace*”



www.team-cymru.org : - **Malicious Activity over 30 days - Sept 2014**

*** 21stC Cybersecurity Trends ***

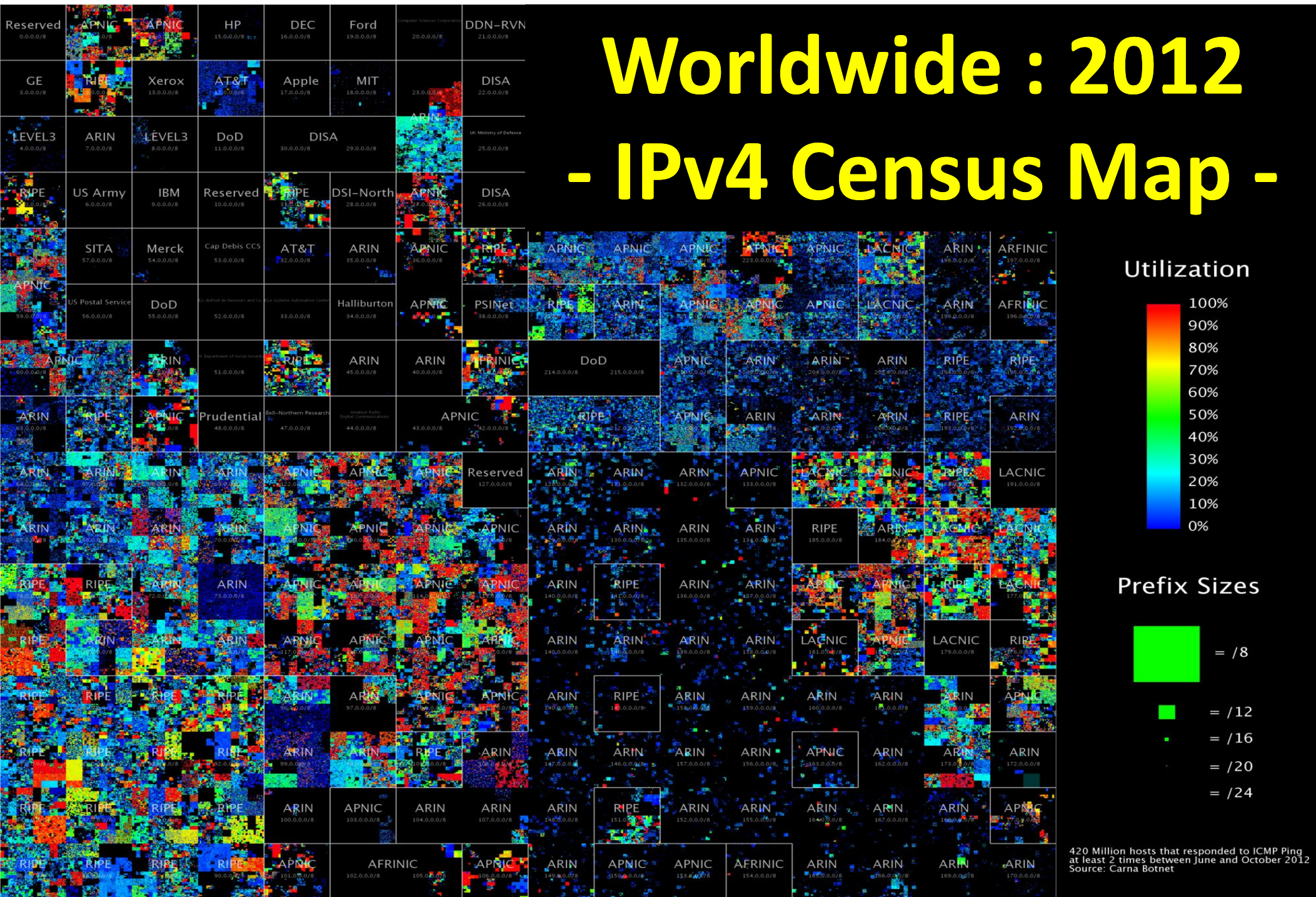
London, UK :: 15th December 2015

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

CyberVision : 2015 - 2025

Worldwide : 2012

- IPv4 Census Map -



*** 21stC Cybersecurity Trends ***

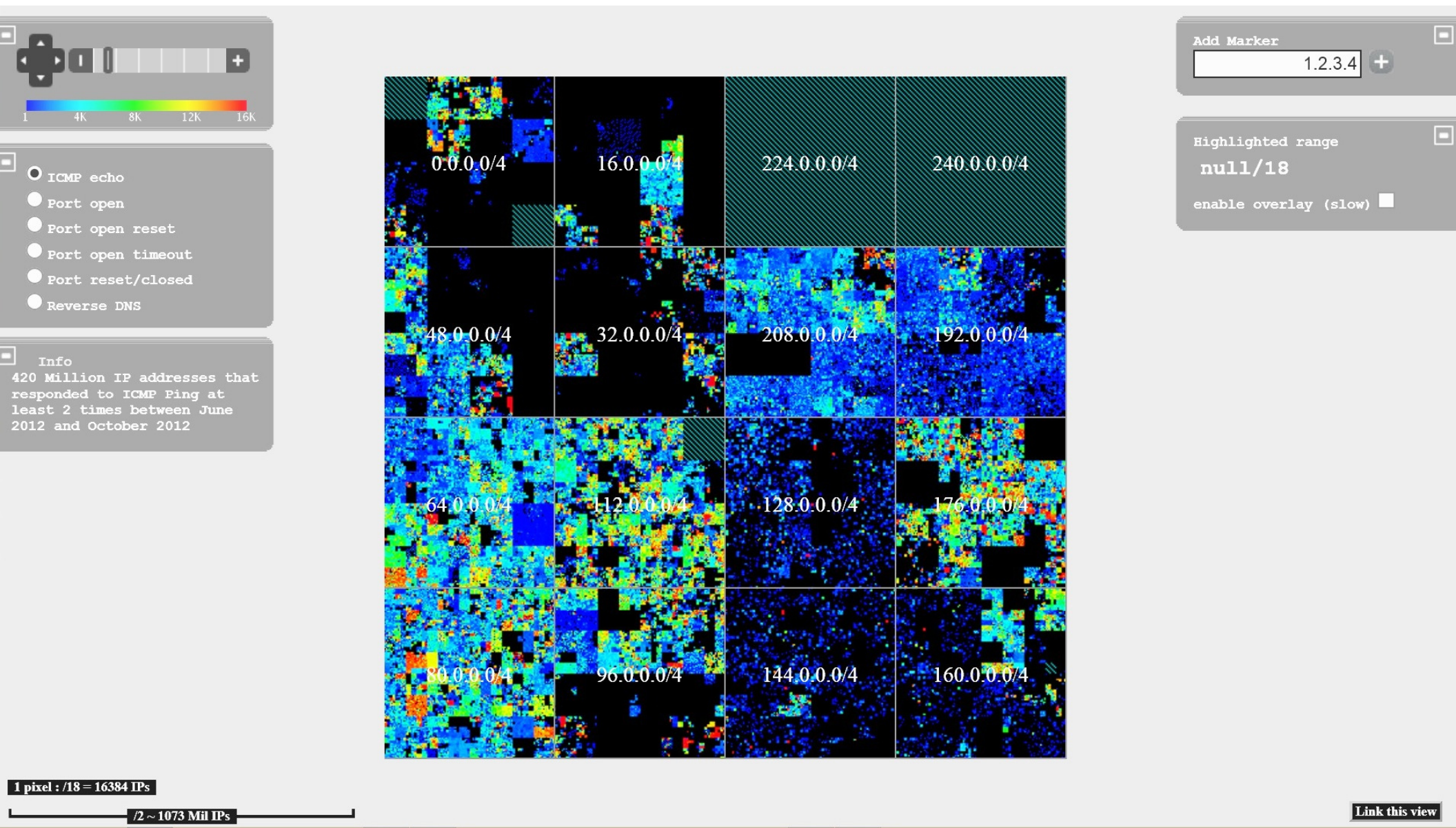
London, UK :: 15th December 2015

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

17

CyberVision : 2015 - 2025

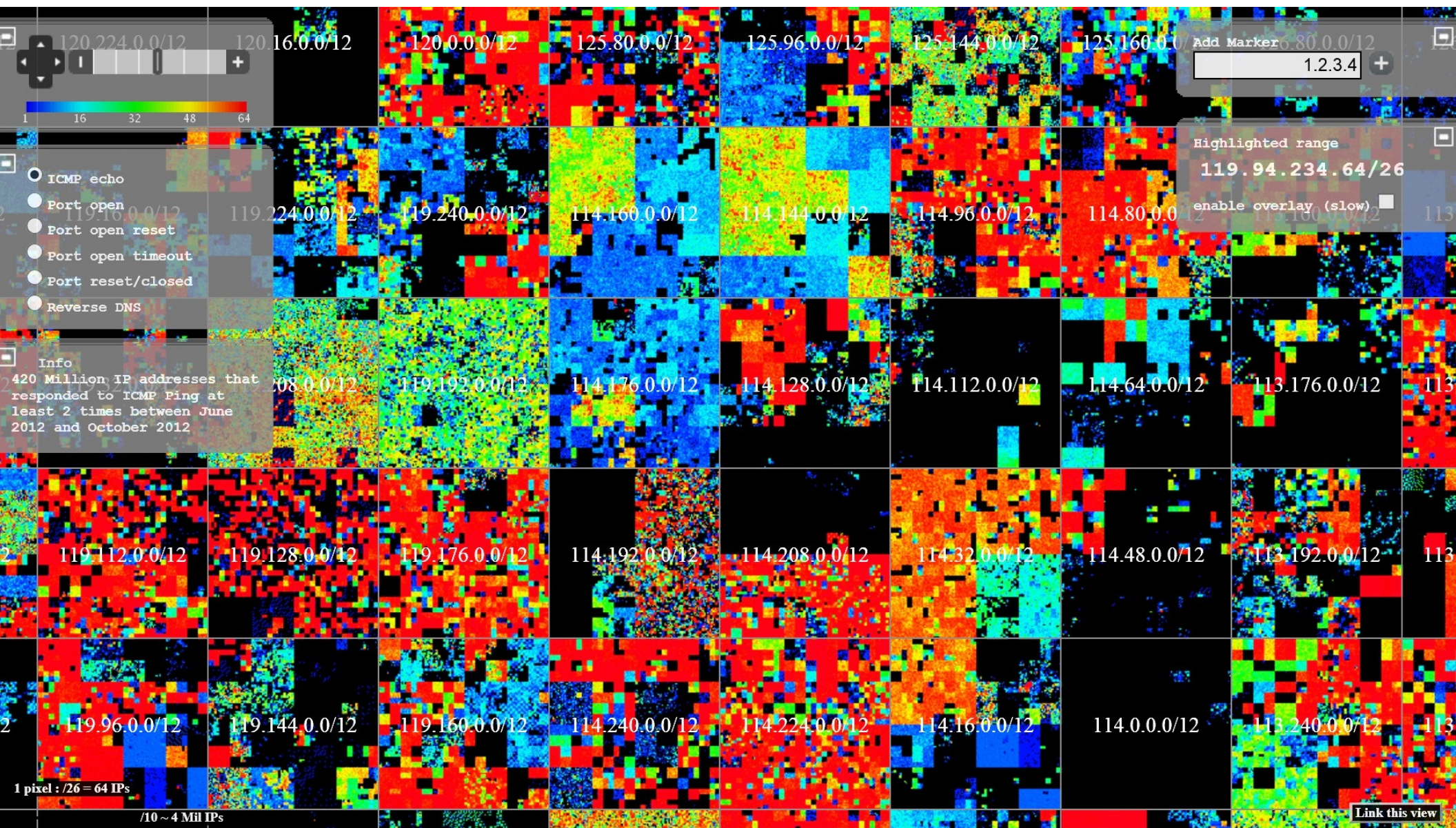
Cyberspace Browser: *Internet Census 2012*



CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

Cyberspace (Hilbert Map): *Browser Zoom(1)*



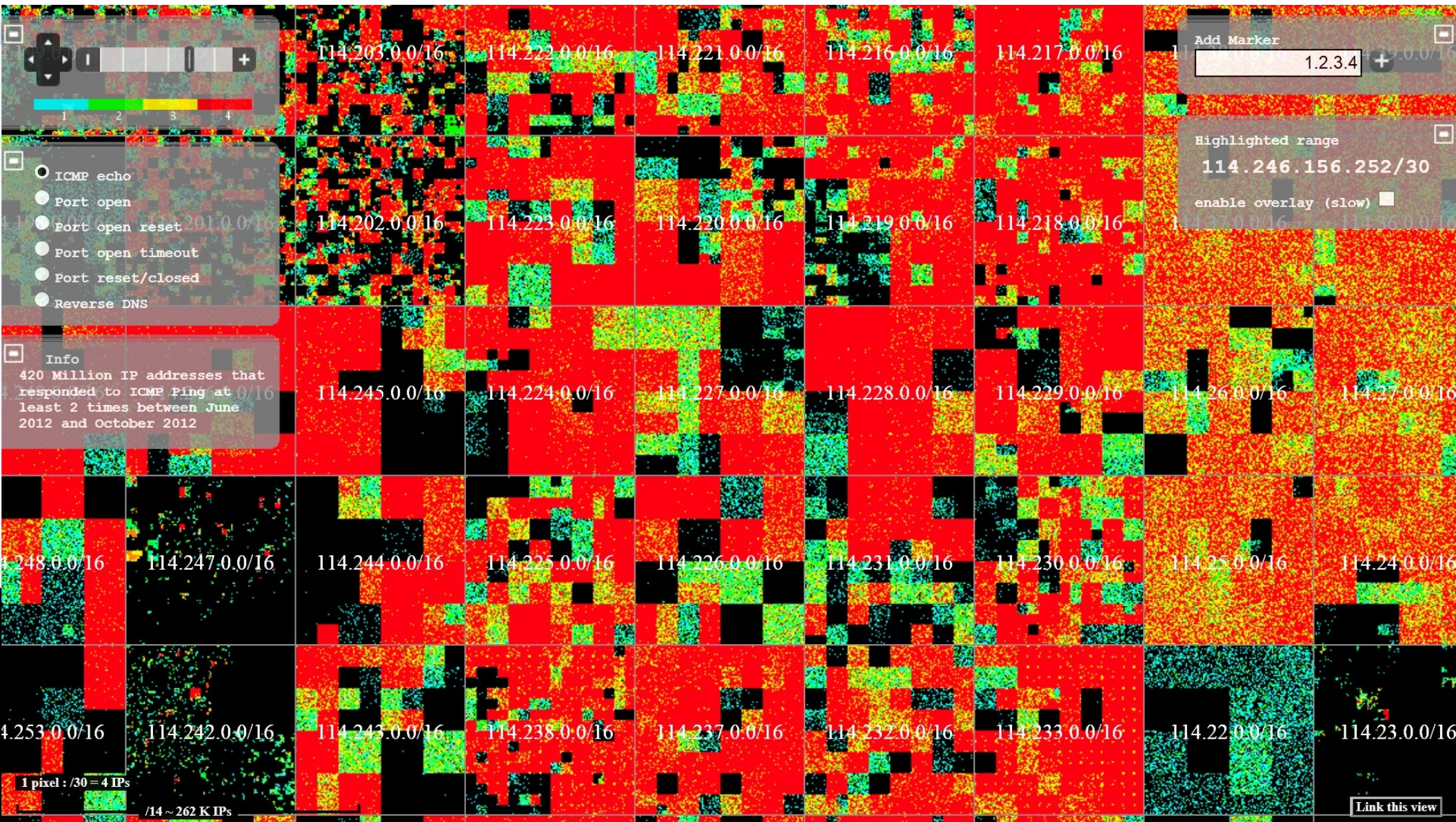
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

Cyberspace (Hilbert Map): *Browser Zoom(2)*



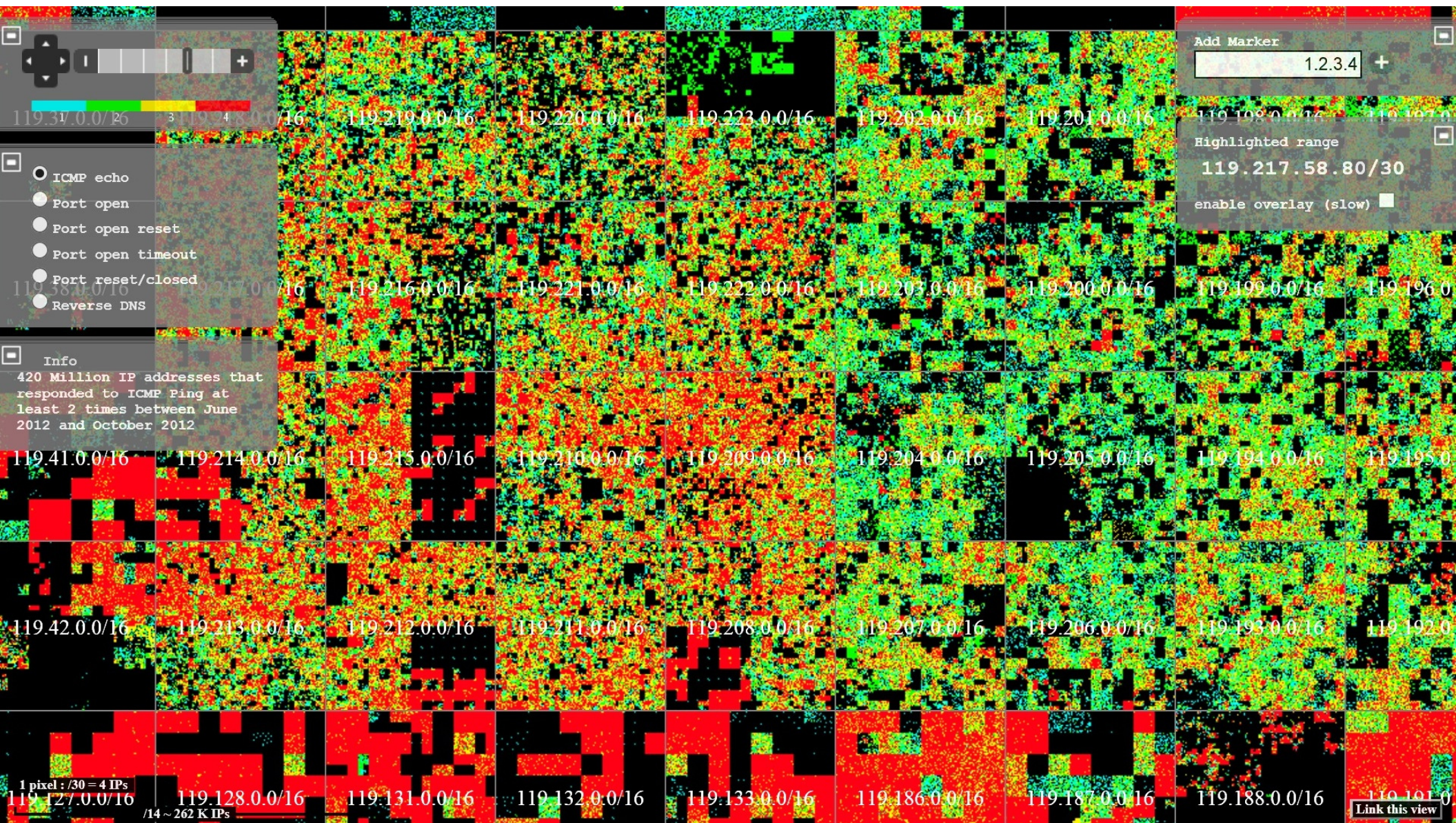
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

Cyberspace (Hilbert Map): *Browser Zoom(3)*



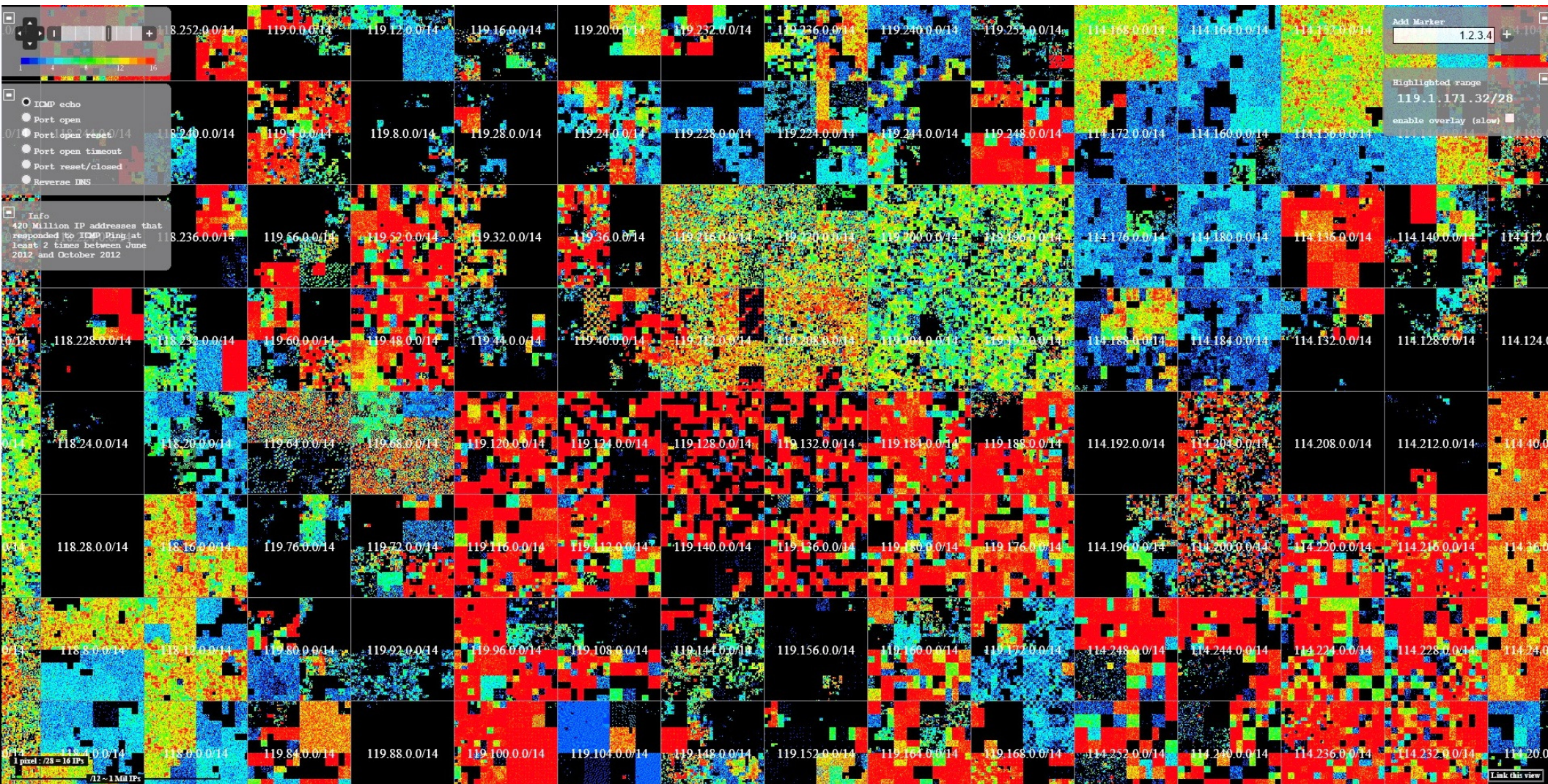
*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

CyberVision : 2015 - 2025

Cyberspace (Hilbert Map): *Browser Zoom(4)*



Link: internetcensus2012.bitbucket.org/hilbert/

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

22

2015-2025: Migration from IPv4 to IPv6



20thC – 1st Gen: **IPv4** – 2^{32} = 10^9 + Devices (*IP Address Space almost fully assigned*)
21stC – 2nd Gen: **IPv6** – 2^{128} = 10^{38} + Devices (*Networking “Internet of Things – IoT”*)
- Expanded IP Address Space for “IoT” sets new “**Cybersecurity Challenges**”! -

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

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
- Direct
- Padlocks & Keys
- Convergent
- Hierarchical
- Carbon Life
- Tanks & Missiles
- Mass Media

Cyber World = “Time”

- Bottom-Up
- Self-Organising
- Transparency
- Global – “Real-Time”
- Citizen Power
- Freedom
- Proxy
- Passwords & Pins
- Divergent
- Organic
- Silicon Life
- Cyber Weapons & “Botnets”
- Social Media

“Smart Security” will require Embedded Networked Intelligence in ALL future IoT devices

CyberVision : 2015 - 2025

***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

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

21stC Cybersecurity ***“Threats & Trends”***

- ***20 Year*** Evolution of Cyber Crime & Cyber Terror: ***1995-2015***
- ***“21st Century Colonisation”*** of Worldwide Internet by eCriminals, Hacktivists and CyberTerrorist Organisations
- ***Global Connectivity*** of Critical National Infrastructure (CNI) significantly increases CyberTerror Risks for ALL Nations!
- ***High Security Risks:*** Most Governments & Businesses are currently not well secured against Cyber Attacks & eCrime

.....and the “Bad Guys” are currently winning!

21stC Cybersecurity ***“Threats & Trends”***

- ***20 Year*** Evolution of Cyber Crime & Cyber Terror: ***1995-2015***



.....and the “Bad Guys” are currently winning!

Image: David Shankbone: Occupy Wall Street – Sept 2011
CyberVision : 2015 - 2025

*** **21stC Cybersecurity Trends** ***
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

Main *Cyber* Players and their Motives

- ***Cyber Criminals:*** Seeking commercial gain from hacking banks & financial institutions as well as phishing scams & computer ransomware
- ***Cyber Terrorists:*** Mission to penetrate & attack critical assets, and national infrastructure for aims relating to political power & “branding”
- ***Cyber Espionage:*** Using stealthy IT Malware to penetrate both corporate & military data servers in order to obtain plans & intelligence
- ***Cyber Hackivists:*** Groups such as “Anonymous” with Political Agendas that hack sites & servers to virally communicate the “message” for specific campaigns

Cyber-Physical Threat Scenarios

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

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

Anonymous-Hacktivist declare *“Total War”* on ISIS after Paris Attacks – 16th Nov 2015



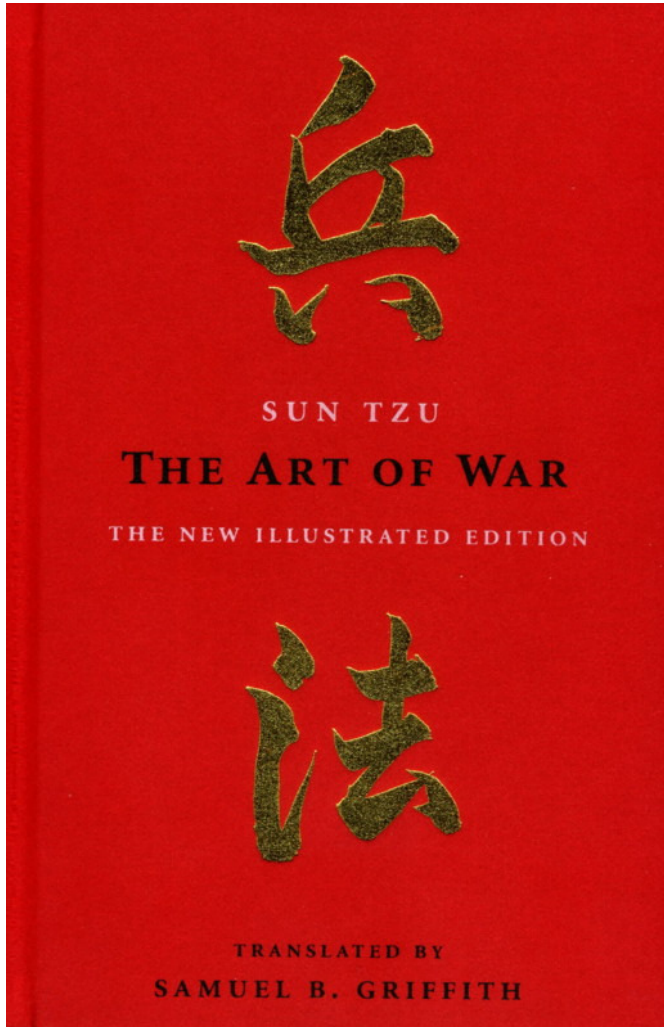
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

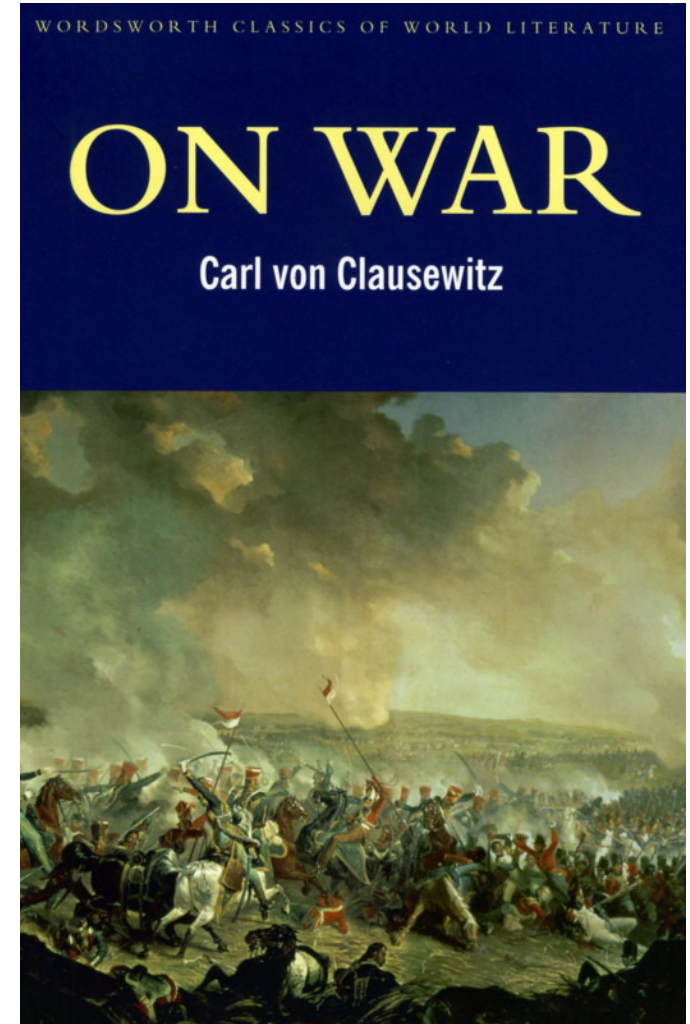
London, UK :: 15th December 2015

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

“CyberWar” Strategies & Models from Classic Works!



Recommended
“Bedtime
Reading”
for
Cybersecurity
Specialists!



Classic Works on “War” are as relevant today for Cybersecurity as pre-21stC!

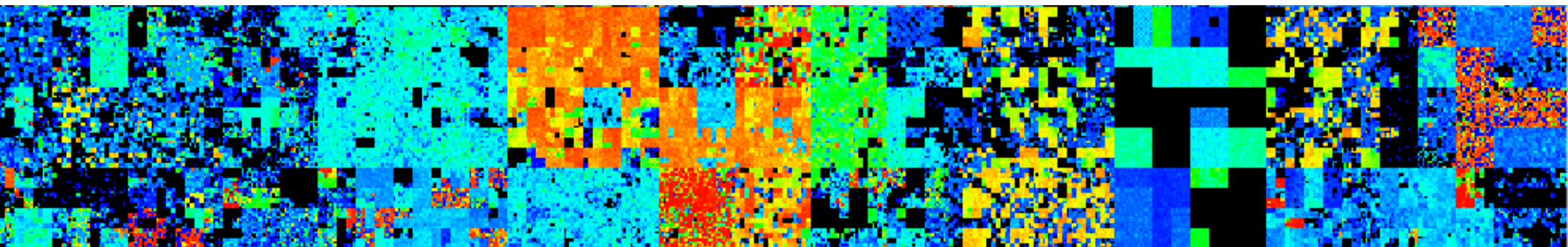
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

21stC Cybersecurity Trends: 2015 - 2025



1 – Background: 21stC Security Landscape	2 – Cybersecurity: Players & Threats	3 – Cyber Market Structure, Size & Growth
4 - CSO: C-Suite Security Integration “Integrated”	5 – Scenario 2020: Internet of Things (IoT) “Adaptive”	6 – Scenario 2025: AI & Machine Learning “Intelligent”
7 – CyberSecurity Ventures (Old and New)	8 – Mergers, Acquisitions & VC Funds	9 – YOUR Actions Plan for 21stC Cyber!....



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%)

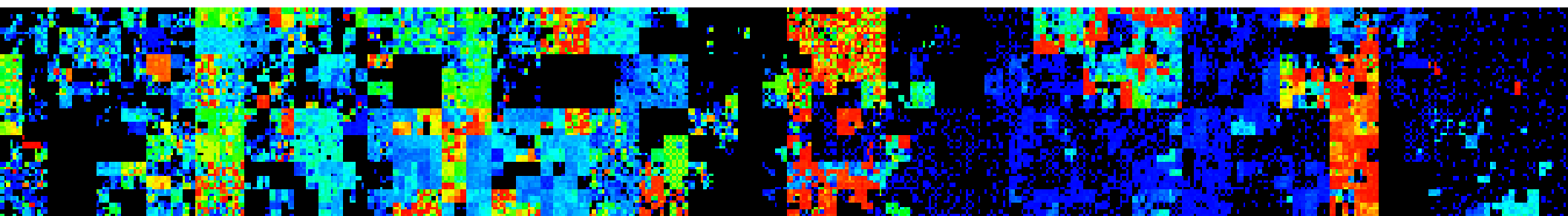
(**Sources:** “Micro Market Monitor” & “Markets and Markets” –
Estimated and Extrapolated from projections for 2014 – 2019)

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

21stC Cybersecurity Trends: 2015 - 2025



1 – Background: 21stC Security Landscape	2 – Cybersecurity: Players & Threats	3 – Cyber Market Structure, Size & Growth
4 – CSO: C-Suite Security Integration “Integrated”	5 – Scenario 2020: Internet of Things (IoT) “Adaptive”	6 – Scenario 2025: AI & Machine Learning “Intelligent”
7 – CyberSecurity Ventures (Old and New)	8 – Mergers, Acquisitions & VC Funds	9 – YOUR Actions Plan for 21stC Cyber!....



CSO: *Board Level Security Integration*

- **20thC Legacy Model:** Physical and IT Security managed with minimal common operations
- **21stC CSO Model:** Business & Government urgently need to manage TOTAL Cyber-Physical Operations at C-Suite Board Level
- **Investment Plan:** CSOs need professional team & Investment Budget to manage physical & cyber security risks, threats and attacks!

Cyber Integration with *Physical Security Operations*

- **Cybersecurity** for Government, Business & Critical Sectors can now be integrated with operational physical security solutions including:
 - 1) **Advanced CCTV** Camera Surveillance of the Secure Government & Critical Facilities
 - 2) **Exterior ANPR** (Automatic Number Plate Recognition) Systems for Traffic & Parking
 - 3) Integration of the Cyber **CERT/CSIRT** with CCTV & Alarm Control Centres
 - 4) **Personnel RFID** and **Biometrics** for Office, Warehouse & Campus Access Controls
 - 5) Professionally trained **Security Personnel & Guards** – 24/7 – for top security facilities
 - 6) Implemented facility **Security Policy** for staff, visitors and contractors
 - 7) **Intelligent Perimeter** security controls for campuses and critical service facilities such as airports, power stations, refineries, hospitals and government institutions
 - 8) **On-Line Audit trails** and Electronic Log-Files for secure Physical Facilities
 - 9) Focus upon in-depth **Access Control** for computer server rooms & data storage

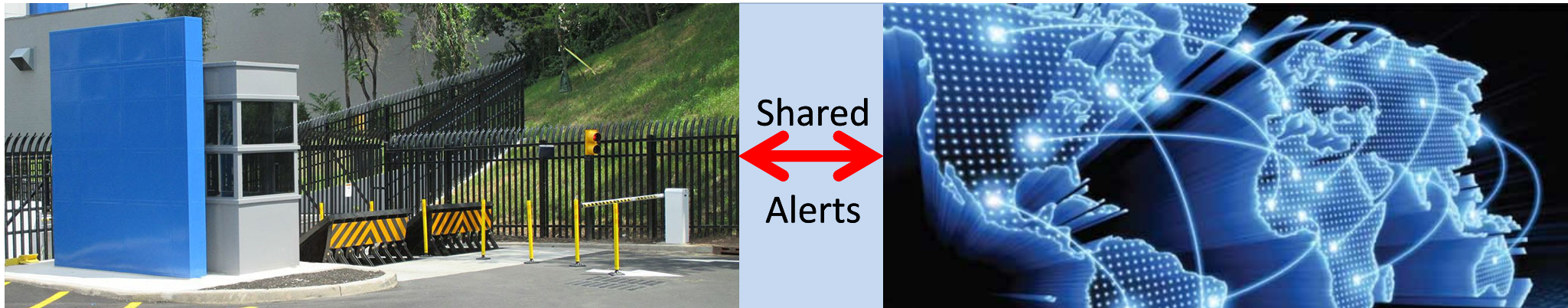
“Integrated Real-Time Cyber-Physical Security Operations”
“SMART SECURITY”

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

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

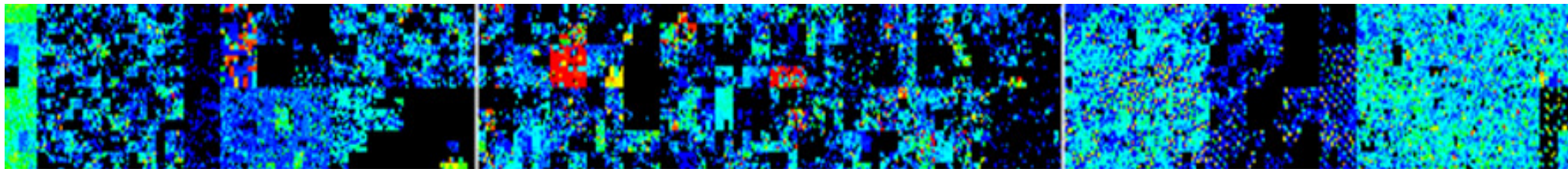
London, UK :: 15th December 2015

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

21stC Cybersecurity Trends: 2015 - 2025



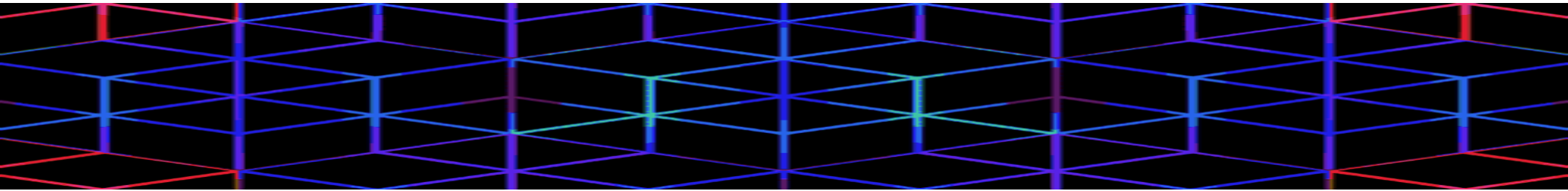
1 – Background: 21stC Security Landscape	2 – Cybersecurity: Players & Threats	3 – Cyber Market Structure, Size & Growth
4 – CSO: C-Suite Security Integration “Integrated”	5 – Scenario 2020: Internet of Things (IoT) “Adaptive”	6 – Scenario 2025: AI & Machine Learning “Intelligent”
7 – CyberSecurity Ventures (Old and New)	8 – Mergers, Acquisitions & VC Funds	9 – YOUR Actions Plan for 21stC Cyber!....



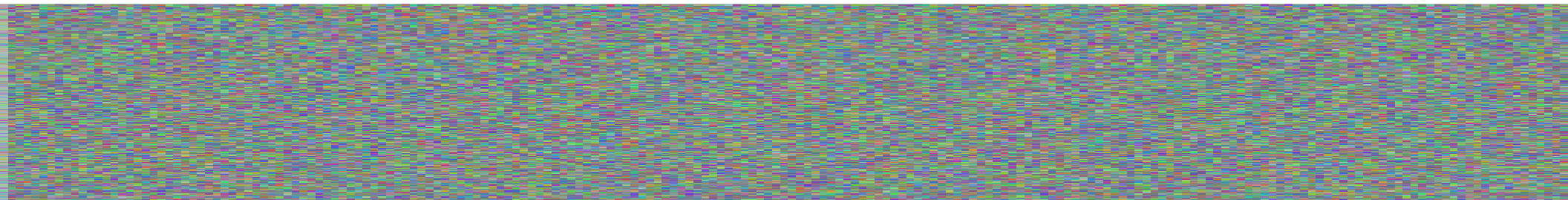
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

Our CyberVision: **2020 - 2025**



- **Scenario 2020 – *Adaptive Security-IoT***: Managed Integration of IoT, *Cyber* & Physical Ops under CSO
- **Scenario 2025 – *Intelligent Security***: Transition to Real-Time Artificial Intelligence & Machine Learning based Enterprise Cybersecurity Tools & Solutions



Scenario **2020**: Adaptive Security - **IoT**

-5 Year Time Window - **2010 <- 2015 -> 2020**
- Integrated **Cyber-Physical Security** deployed & managed by Board Level Chief Security Officer
- **International Standards** for “IoT” APIs, Net Interface, Security Standards & Operations
- **Distributed Security** for “**Legacy**” Network Assets & Devices for the “Internet of Things”
- Trial Deployment of **Advanced AI-based** Intelligent & Adaptive Cybersecurity Tools

Enterprise *“Internet of Things”*- IoT

- **Cyber-Enterprise:** During the next 5-10 years of Cyber Evolution the Internet will extend to practically ALL our IT enabled devices within cars, homes, offices, power stations & retail products! This is defined as the “Internet of Things” – IoT.
- **Extended Security:** ALL IoT connected devices, nodes & servers must be secured against attack!
- **CSO Challenge:** The IoT is the next Cyber Conflict Zone and Security Challenge for Enterprise CSOs!

Internet of Things: *Phases of Evolution*

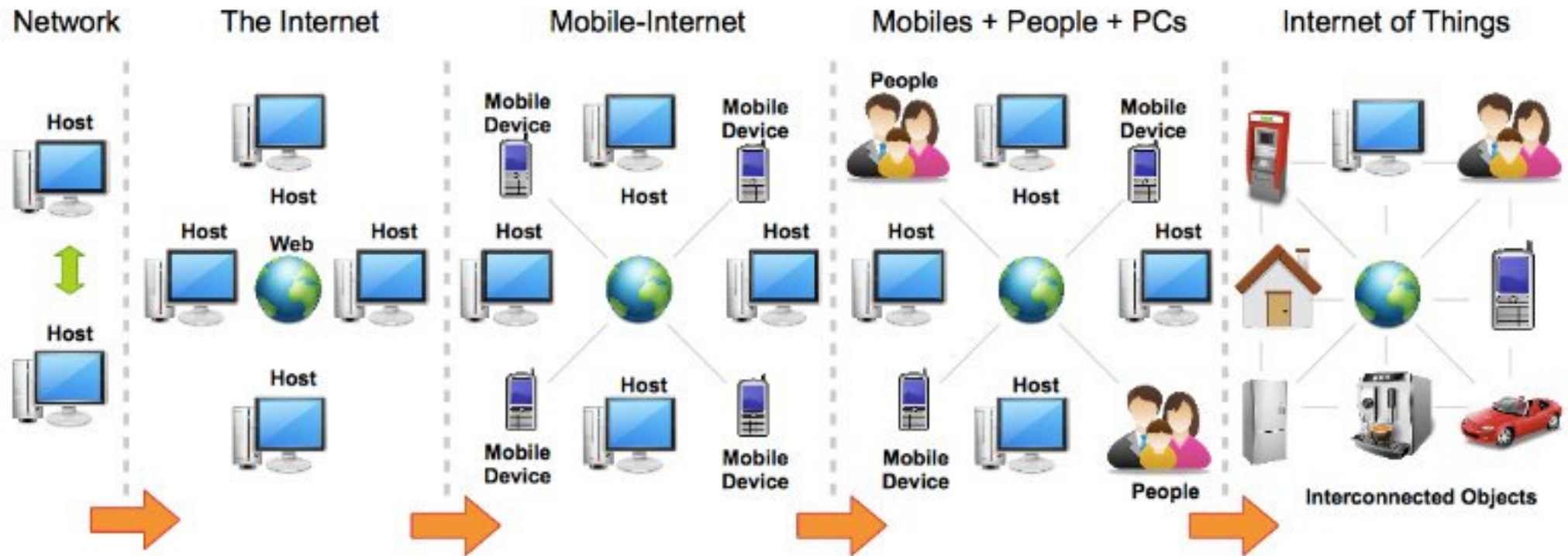
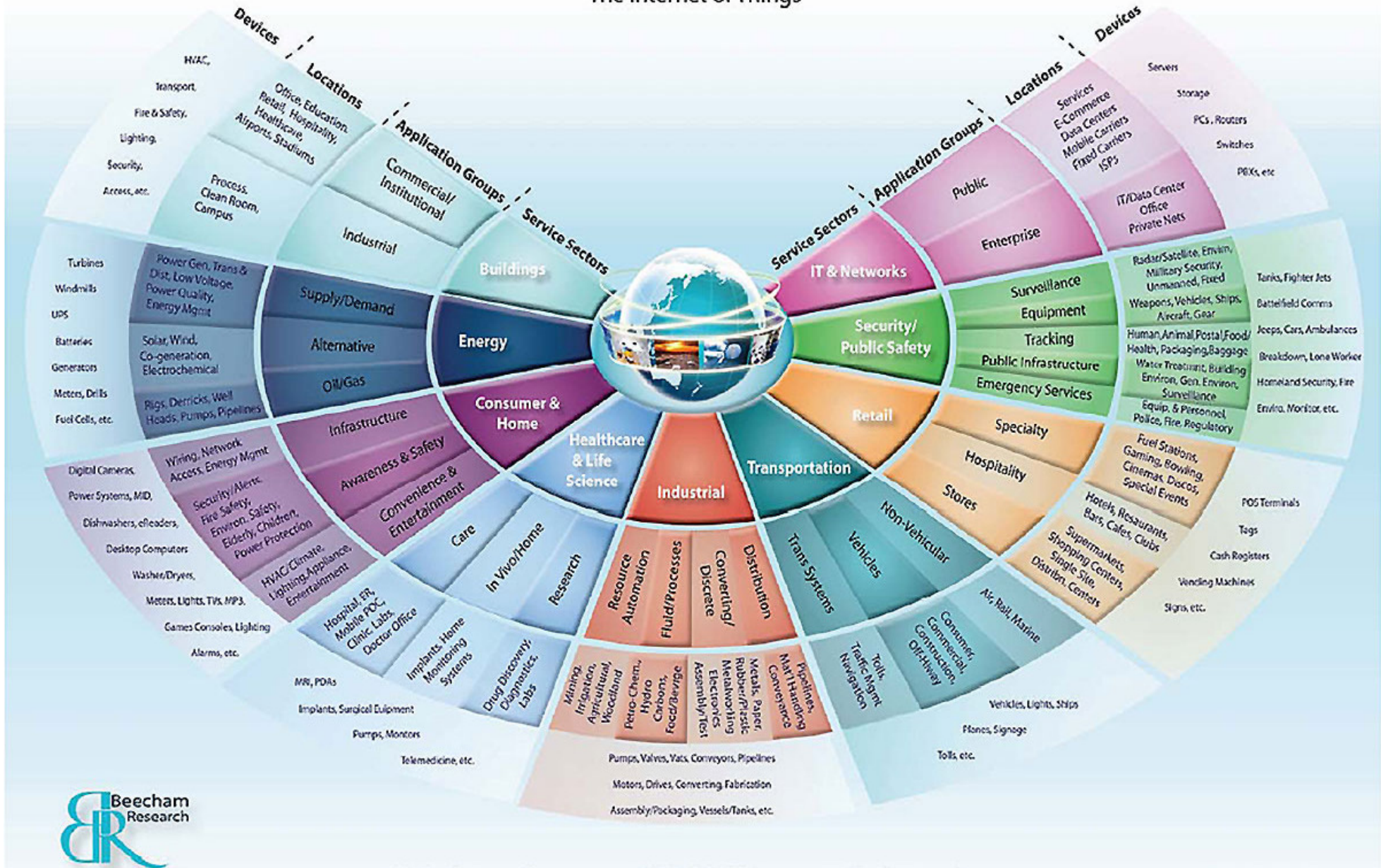


Fig. 1. Evolution of the Internet in five phases. The evolution of Internet begins with connecting two computers together and then moved towards creating World Wide Web by connecting large number of computers together. The mobile-Internet emerged by connecting mobile devices to the Internet. Then, peoples' identities joined the Internet via social networks. Finally, it is moving towards Internet of Things by connecting every day objects to the Internet.

Internet of Things: *Spans ALL Sectors*

The Internet of Things



*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

CyberVision : 2015 - 2025

Cyber-Physical Threats from the “IoT”

- **ALL Networked Devices** are at risk from Cyber-Hacking, Penetration & 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 controls are still inherently INSECURE against cyberattacks!

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.

Internet of Things: *Business Alliances*

Handbook: Internet of Things Alliances and Consortia



CC Attribution: Postscapes.com - Version 1.0 Updated March 2015

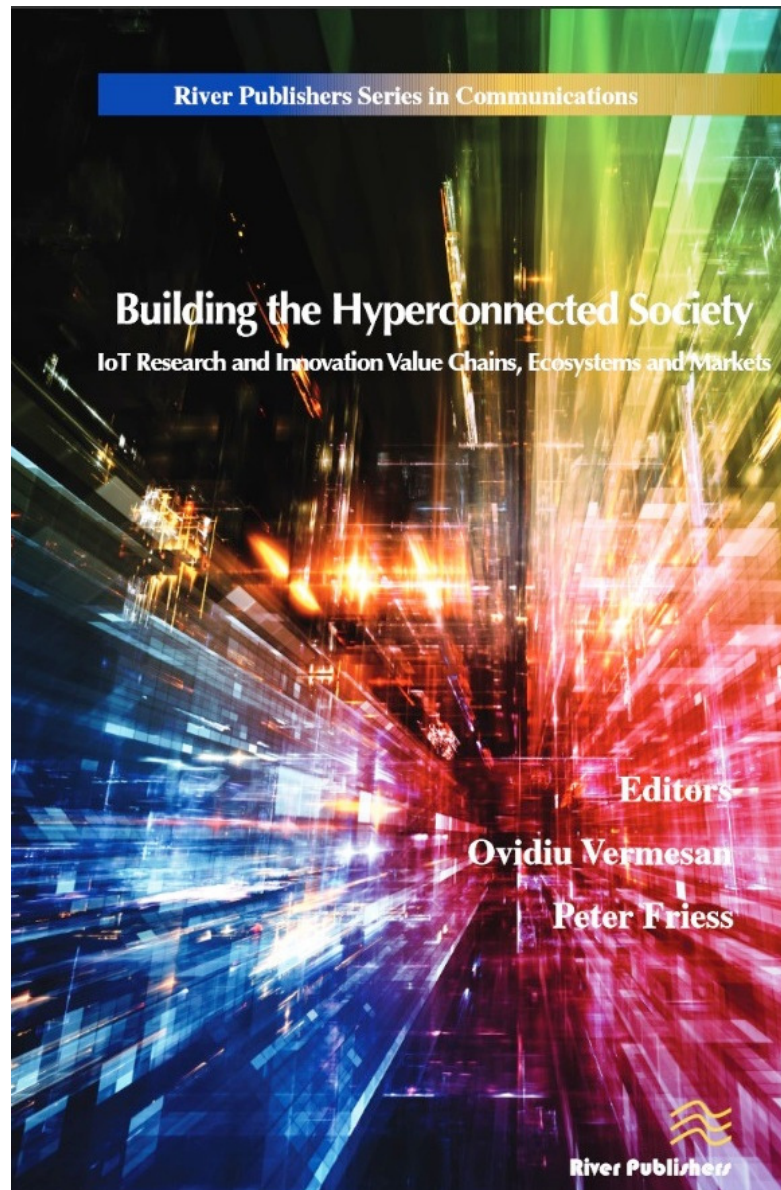
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

- 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

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

CyberVision : 2015 - 2025

Cyber-Physical Systems as Basis of “IoT”



Cyber-Physical City System

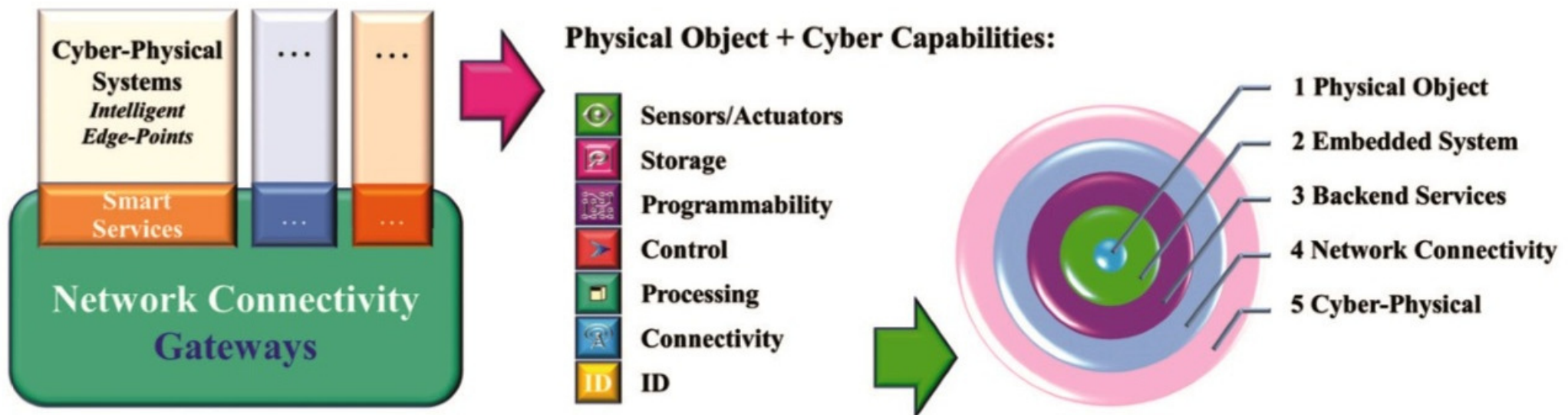
Edge Intelligent Systems

Cyber-Physical System

*Embedded System with Communication Capabilities
Intelligent Edge-Point*

Internet of Things

Complex Internetworked Intelligent Systems



CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

EU “IoT” Programme Visions for 2015 and 2020



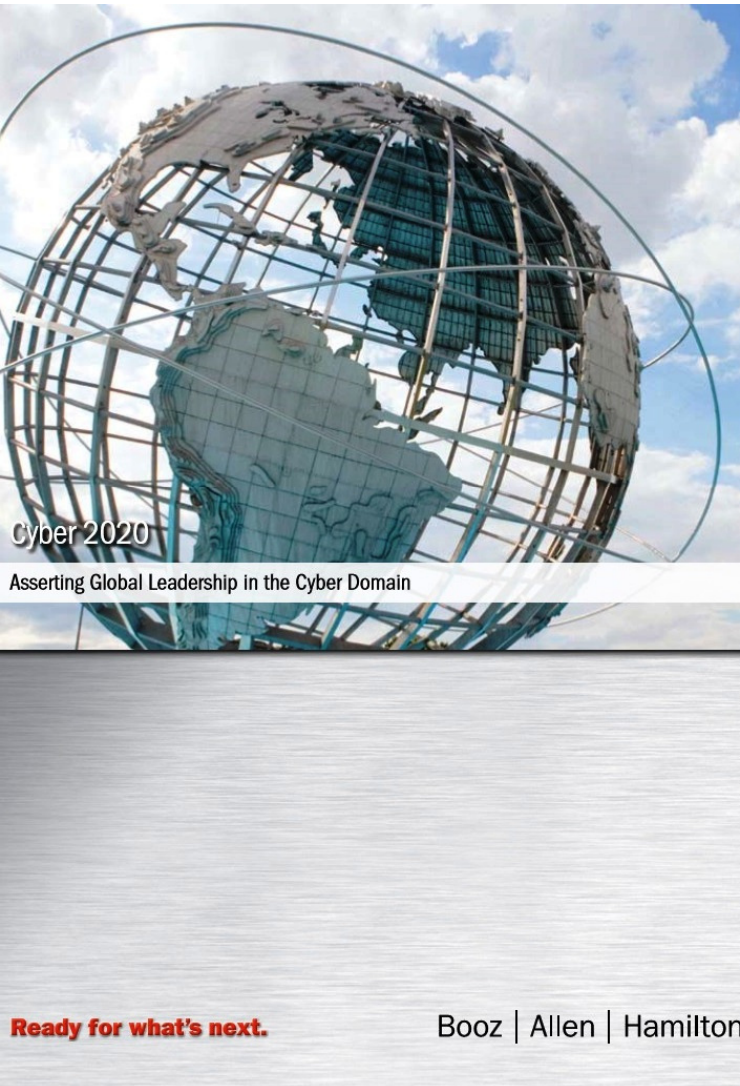
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

Cyber 2020 Visions: Booz, Allen & Hamilton and The Australian Government (Defence)



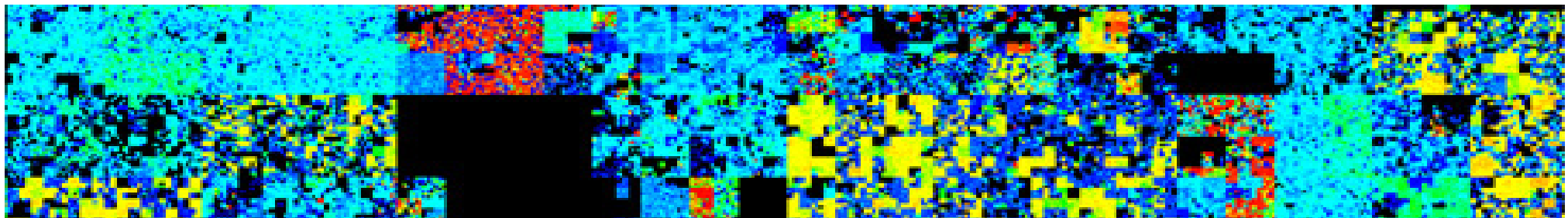
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

21stC Cybersecurity Trends: 2015 - 2025



1 – Background: 21stC Security Landscape	2 – – Cybersecurity: Players & Threats	3 – Cyber Market Structure, Size & Growth
4 – CSO: C-Suite Security Integration “Integrated”	5 – Scenario 2020: Internet of Things (IoT) “Adaptive”	6 – Scenario 2025: AI & Machine Learning “Intelligent”
7 – CyberSecurity Ventures (Old and New)	8 – Mergers, Acquisitions & VC Funds	9 – YOUR Actions Plan for 21stC Cyber!....



Scenario **2025**: Intelligent Security

- ..10 Year Time Window - **2005 <- 2015 -> 2025**
- Transition & Full Deployment of Enterprise-Wide AI-based **Intelligent** “Cyber” Tools
- Real-Time **Behavioural Modelling** of ALL aspects of Net Traffic, System/Event Logs, Net Nodes, Servers, Databases, Devices & Users
- Trial Deployment of **Autonomous Real-Time** “Cyber” Alerts that integrate both traditional & advanced AI-based “Cybersecurity Tools”

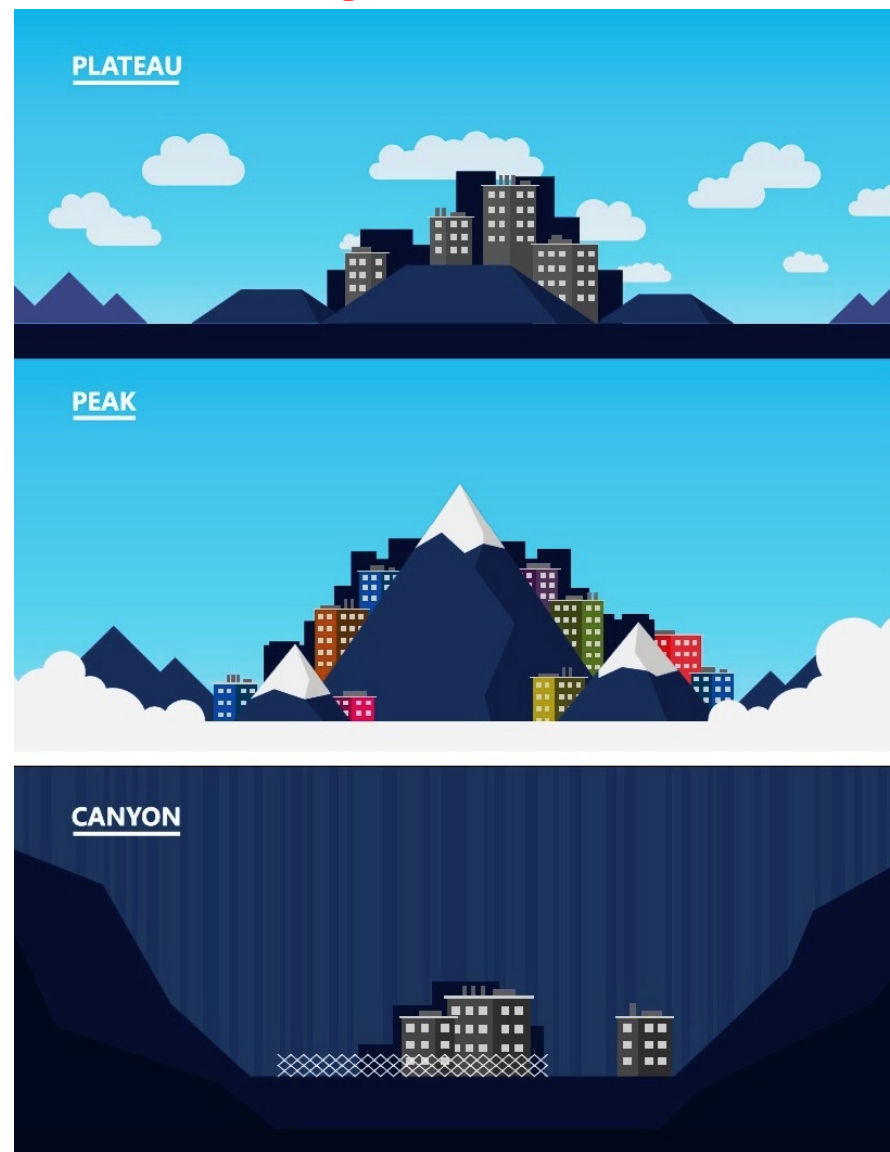
Cyberspace **2025**: *Microsoft Scenarios*

***** Plateau – Peak – Canyon *****



JUNE 2014

CyberVision : 2015 - 2025



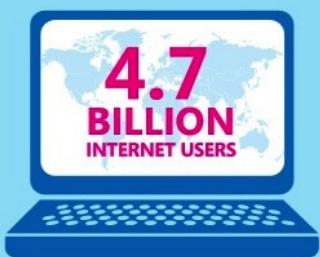
***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

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

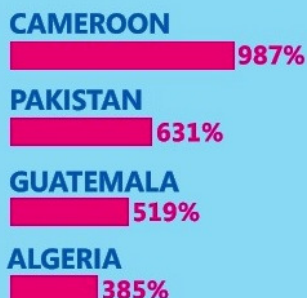
QUANTIFYING THE WORLD IN 2025

HOW MANY INTERNET USERS WILL THERE BE IN 2025?



Percentage from emerging economies

COUNTRIES EXPECTED TO SEE THE GREATEST INCREASE IN INTERNET USERS FROM 2012



WILL THE WORKFORCE KEEP UP WITH THE GROWING DEPENDENCE ON TECHNOLOGY?

ANNUAL STEM GRADUATES



By 2025, emerging economies will produce nearly 16 million graduates in science, technology, engineering, and mathematics (STEM) fields annually, which will be nearly 5 times greater than the 3.3 million per year from developed countries.

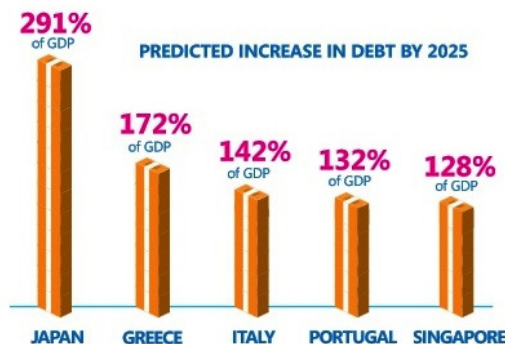
COUNTRIES WITH THE STRONGEST GROWTH IN STEM GRADUATES FROM 2013 (PERCENTAGE OF GROWTH)



HOW WILL THE WORLD MANAGE GROWING PUBLIC DEBT?

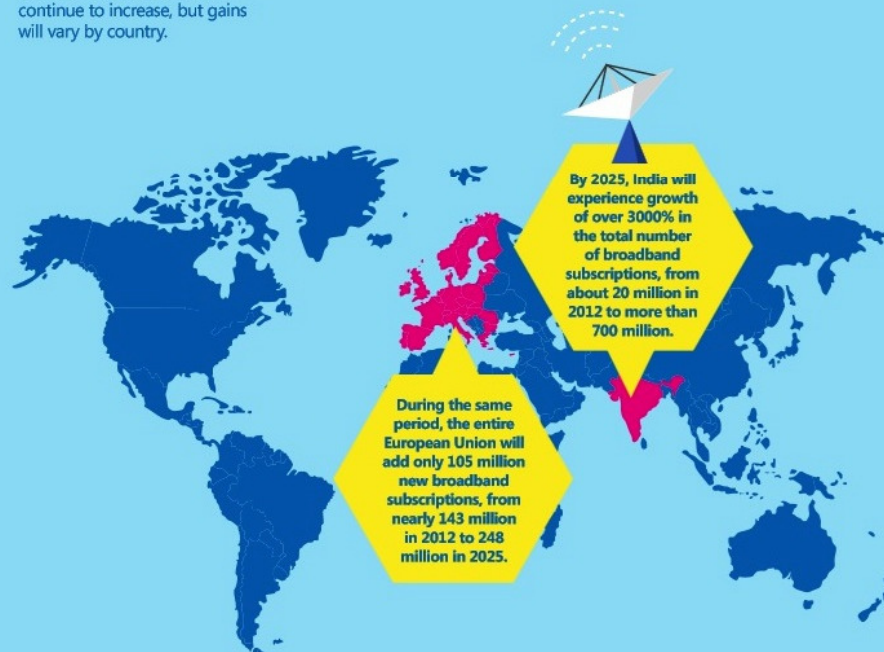


National debt as a percentage of GDP will average just over 10 percent worldwide, but some countries/regions will carry greater debt.



CAN THE WORLD DELIVER CONNECTIVITY FOR EVERYONE?

Broadband penetration will continue to increase, but gains will vary by country.



Microsoft 2025: Cyberspace Scenarios

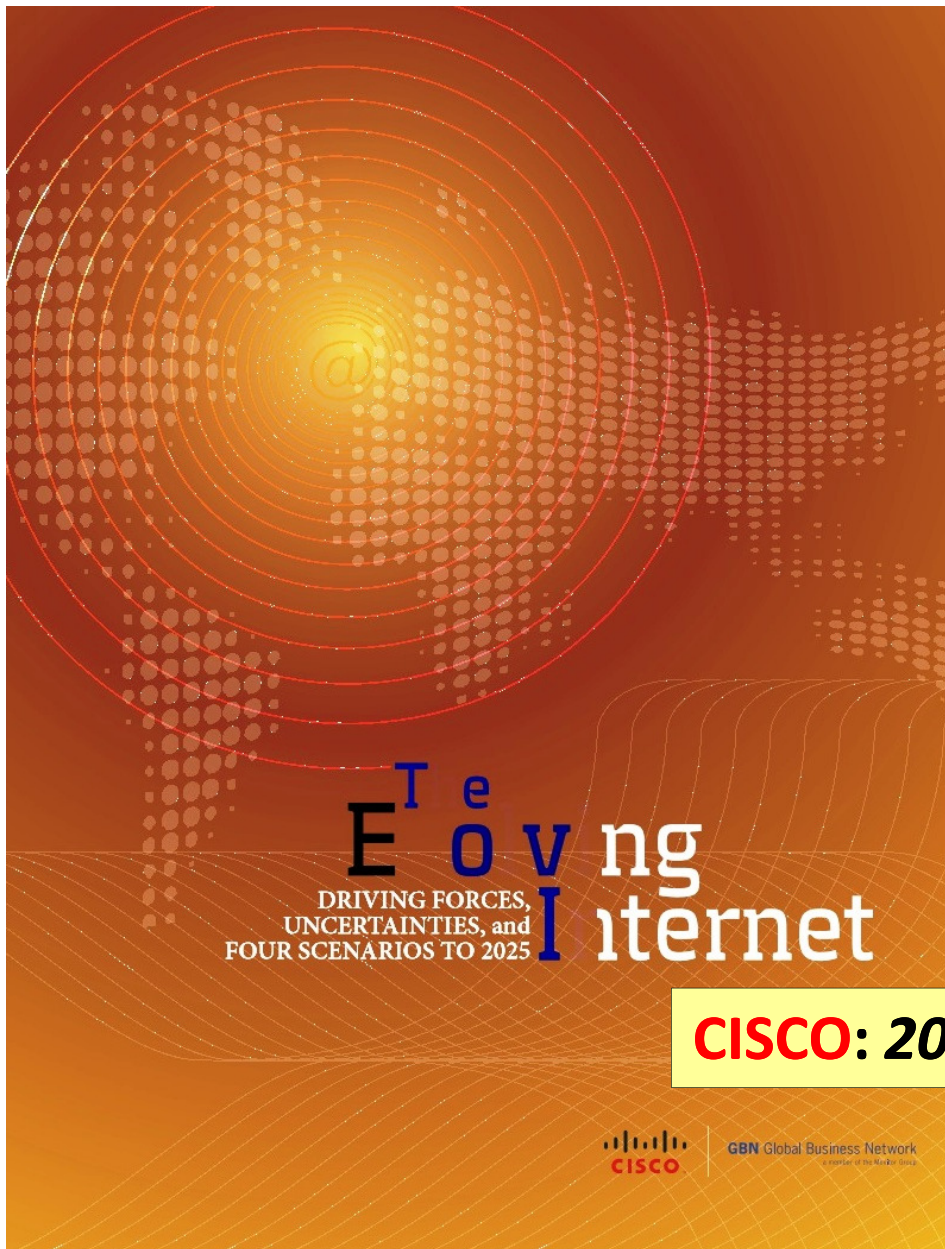
*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

CyberVision : 2015 - 2025

Technology Visions: **Scenario 2025**



➔ **The Future Internet in 2025**

Open paradigms for personal data and platforms?

M14117MRA – November 2014

CISCO: 2025 Scenarios: IDATE

••• This document is a part of our "Telecom & Over-The-Top" category which includes in 2014:
- a dataset in Excel,
- a state-of-the-art report in PowerPoint,
- six market reports in Word, each with its synopsis in PowerPoint
- Privileged access to our lead OTT analysts

www.idate.org



***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

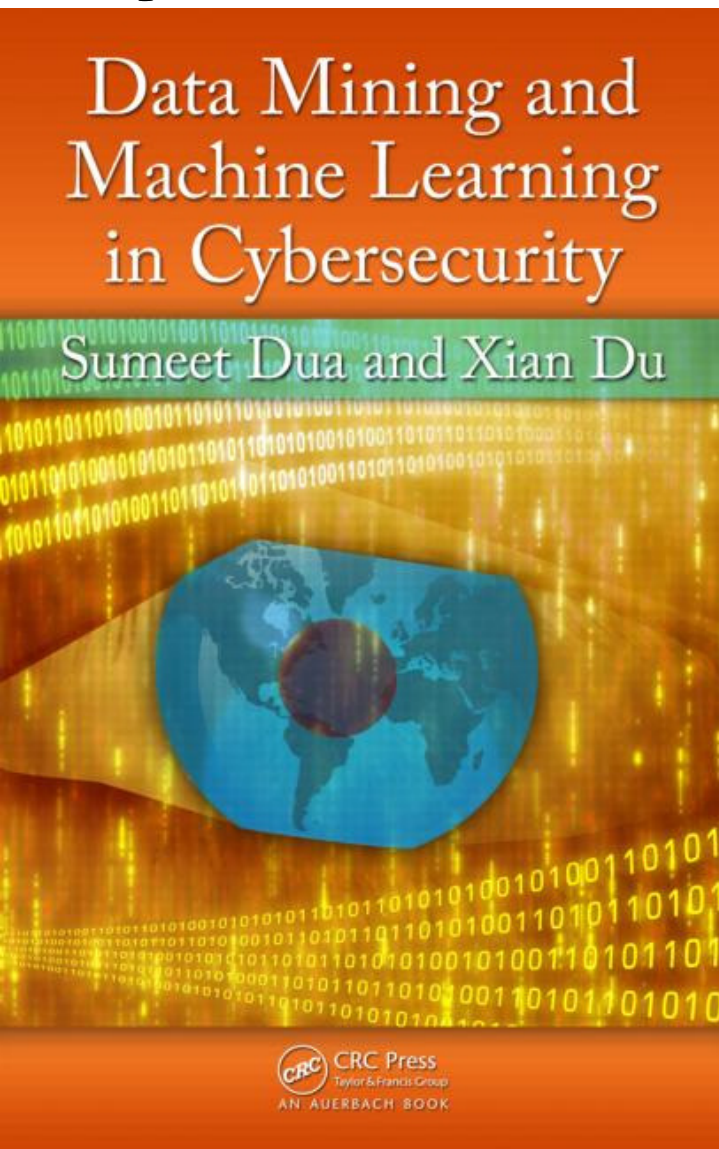
© Dr David E. Probert : www.VAZA.com ©

CyberVision : 2015 - 2025

AI & Machine Learning as *Cyber Tools*

- **Artificial Intelligence (AI)** : Developed during 1960s/70s : Neural Networks, Expert Systems, Self-Organising Automata, Adaptive Stochastic Learning, Algorithms, Robotics, Autonomous Systems, Augmented Reality
- **Behavioural Modelling**: AI can be applied to real-time modelling of ALL Network Traffic, Log & Audit Files, Net Nodes, Servers and all “Smart IoT” Devices
- **Zero-Day Attacks**: AI modelling can mitigate risks of new malware that can no defined “signature”.
- **Advanced Persistent Threats (APTs)**: Adaptive Learning Algorithms can detect the step-by-step penetration of APT malware (Phishing, Trojans, Adware, Botnets...)
- **Insider Threats & Attacks**: Enterprise AI Traffic Modelling can quickly expose the malicious activities of malicious “insiders”!

....“Machine Learning Methods” for Cybersecurity developed from 2010...



Information Systems Technology & Design / iTrust

SUTD
SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN
Established in collaboration with MIT

DATE
23 Sept 2013 (Mon)

TIME
11:00 - 12:00PM

VENUE
SUTD LT4


Cyber Security Meets Machine Learning

ABSTRACT

Computer and communication systems are constantly the target of cyber security attacks. Given the number of vulnerabilities discovered each day, the introduction of new attack schemes and the ever expanding use of the Internet, it is not surprising that the field of cyber security has grown in importance in recent years. Attacks are currently so pervasive that many institutions (large financial firms in particular) now spend over 10% of their information and communication technology (ICT) budget on cyber security alone. Developments, including changes in the type of attacks, such as the introduction of Advanced Persistent Threats (APTs), and the identification of new vulnerabilities and attack vectors, have resulted in a highly dynamic cyber threat landscape that cannot be handled by traditional security methods.

Machine learning (ML) techniques incorporating induction algorithms which explore data in order to discover patterns have proved effective in responding to the growing challenges to cyber security. I will discuss lessons learned from our ongoing research and experience developing ML-based solutions to various cyber security threats, such as unknown malware detection, the detection of unknown network security attacks and mobile device anomaly detection. I will conclude my talk by focusing on emerging new fields of research, such as big data security analytics and trusted monitoring.

BIOGRAPHY



Prof. Yuval Elovici is the director of the Telekom Innovation Laboratories at Ben-Gurion University, head of the Cyber Security Research Center and a Professor at the Department of Information Systems Engineering of Ben-Gurion University. He holds B.Sc and M.Sc degrees in Computer and Electrical Engineering from the Ben-Gurion University, and Ph.D in Information Systems from Tel-Aviv University. He served as the head of the Software Engineering program at Ben-Gurion University for two and a half years.

Prof. Elovici also professionally consults in the area of the cyber security. In the last eight years he has lead the cooperation between Ben-Gurion University and Deutsche Telekom. In addition, he has published more than 50 refereed journal papers in leading journals, published over 80 papers in various refereed conferences and co-authored a book on social network security and a book on information leakage detection and prevention. His main research interests are Computer and Network Security, Cyber Security, Web Intelligence, Information Warfare, Social Network Analysis and Machine Learning.

Since 2010, leading Cybersecurity Specialists have explored
AI & Machine Learning to mitigate cyber threats & attacks!

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

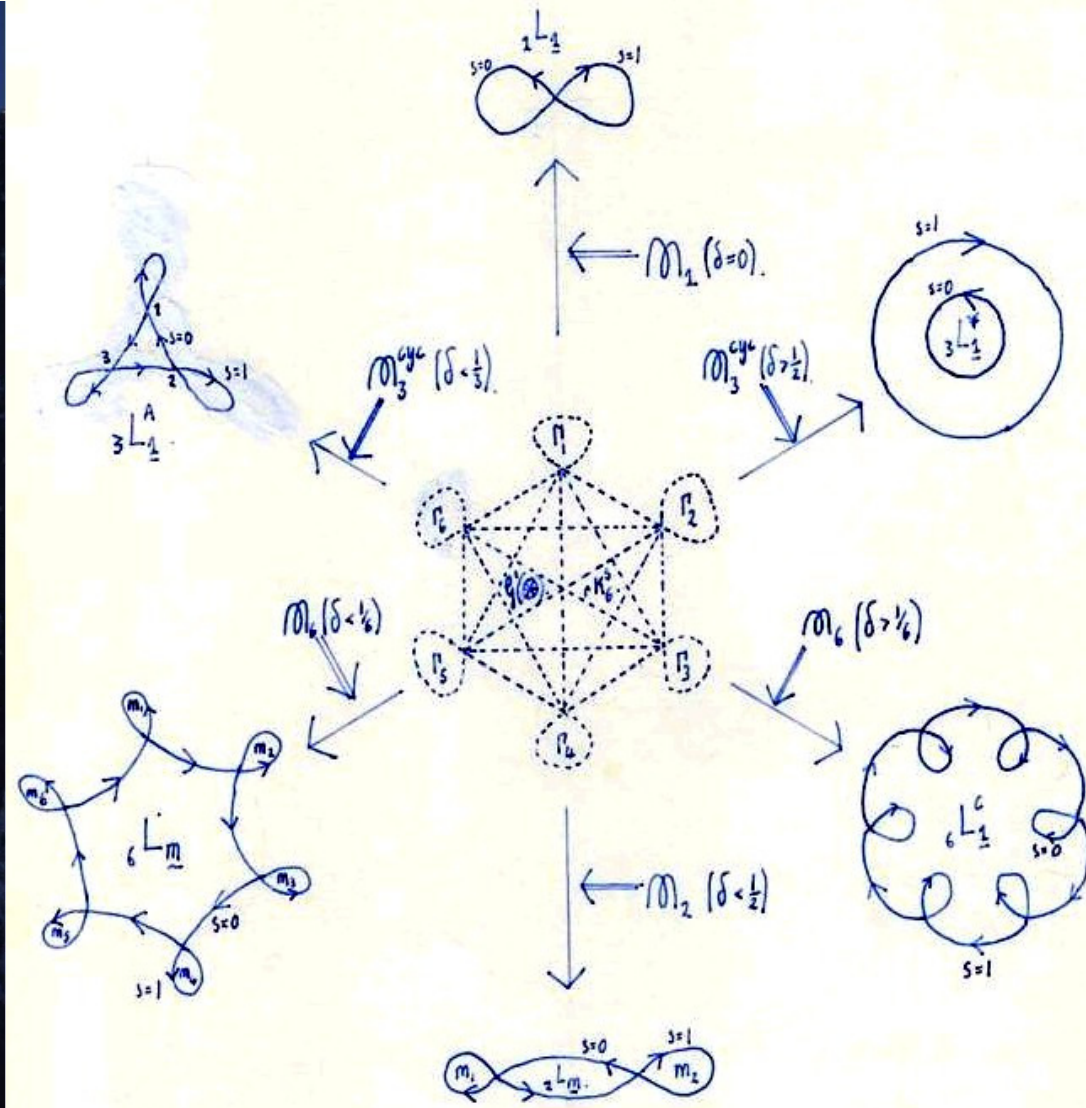
© Dr David E. Probert : www.VAZA.com ©

Evolution of Stochastic Automata – *Cambridge, June '76*

The Evolution of Stochastic Automata

David Eric Probert - 1976
Churchill College, Cambridge

Self-Organisation & Adaptation Of Stochastic Learning Automata To Dynamic Environments



Frontispiece:-

"The Adaptation of Automaton
in Environments M_n ".

$q'(0)$

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

- Dept of Mathematics & Statistics - Cambridge University : 1973 - 1976



Cambridge University Statistical Laboratory - **David E Probert** - Summer 1974

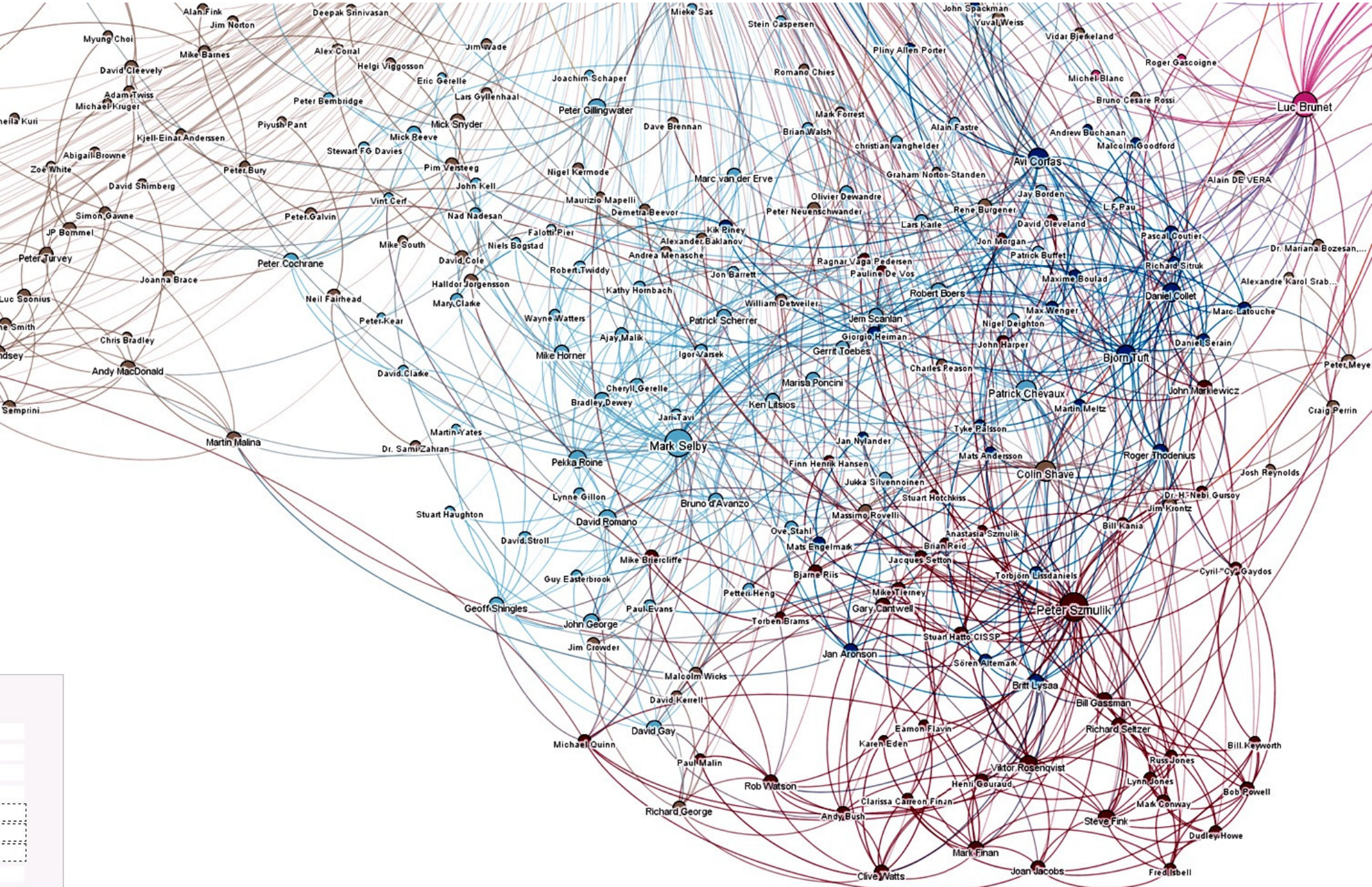
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

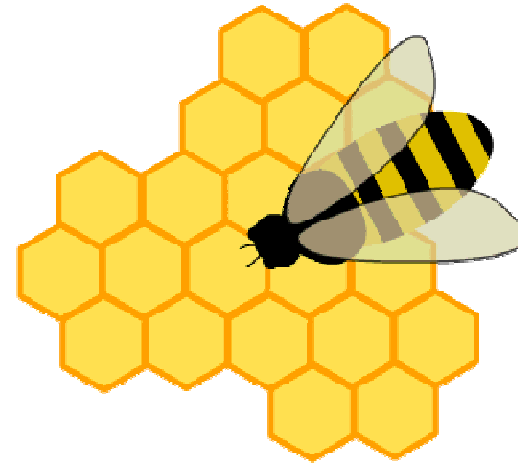
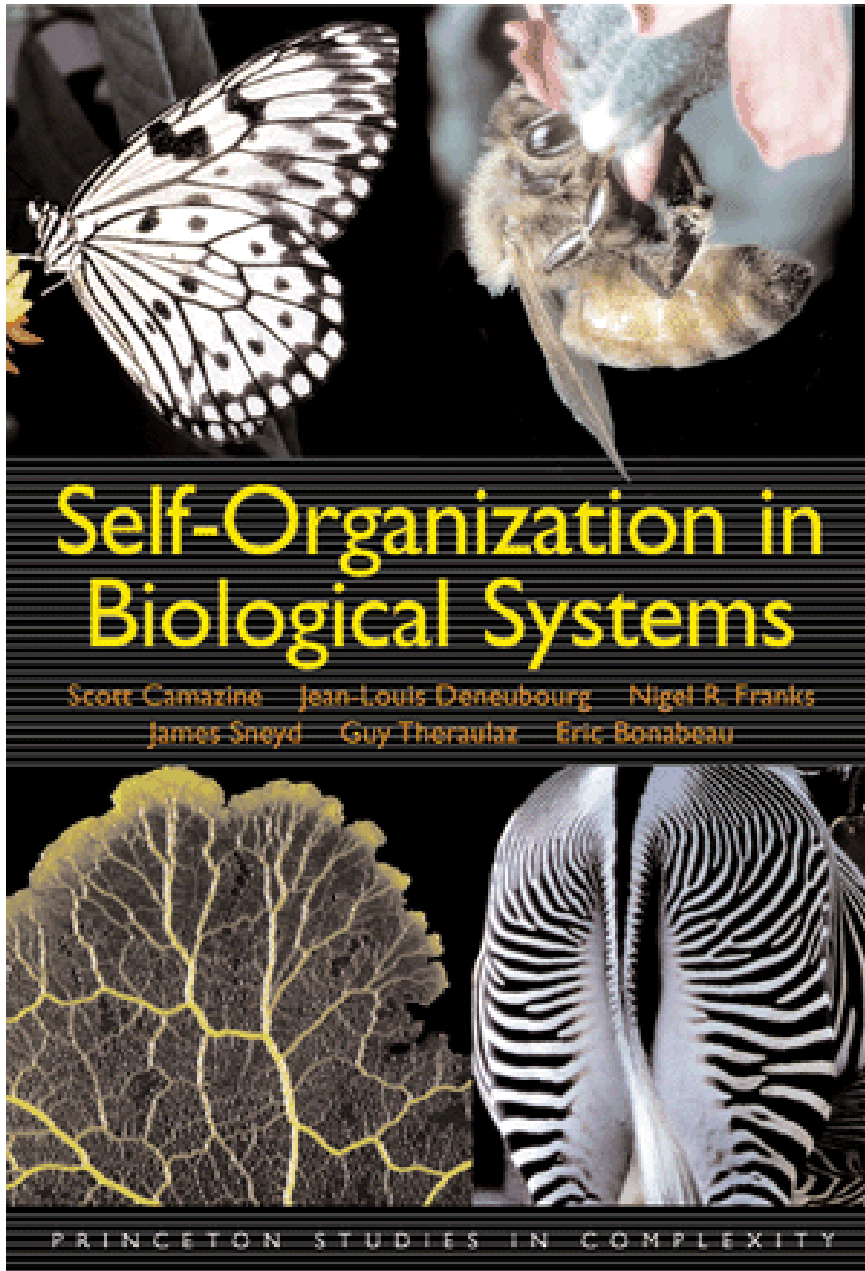
Mapping 21stC Social Media Networks: *LinkedIn (Probert)*



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
-”Effective Security for the **IoT** will also be based upon the principles of self-organisation & self-learning”*

Self-Organisation in “*Bio-Systems*”



CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

- *Smart Sustainable Security in the Wild!* -



The Sociable Weaver Bird

“World’s largest Bird Nests”

*** Southern Africa ***



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

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

CyberVision : 2015 - 2025

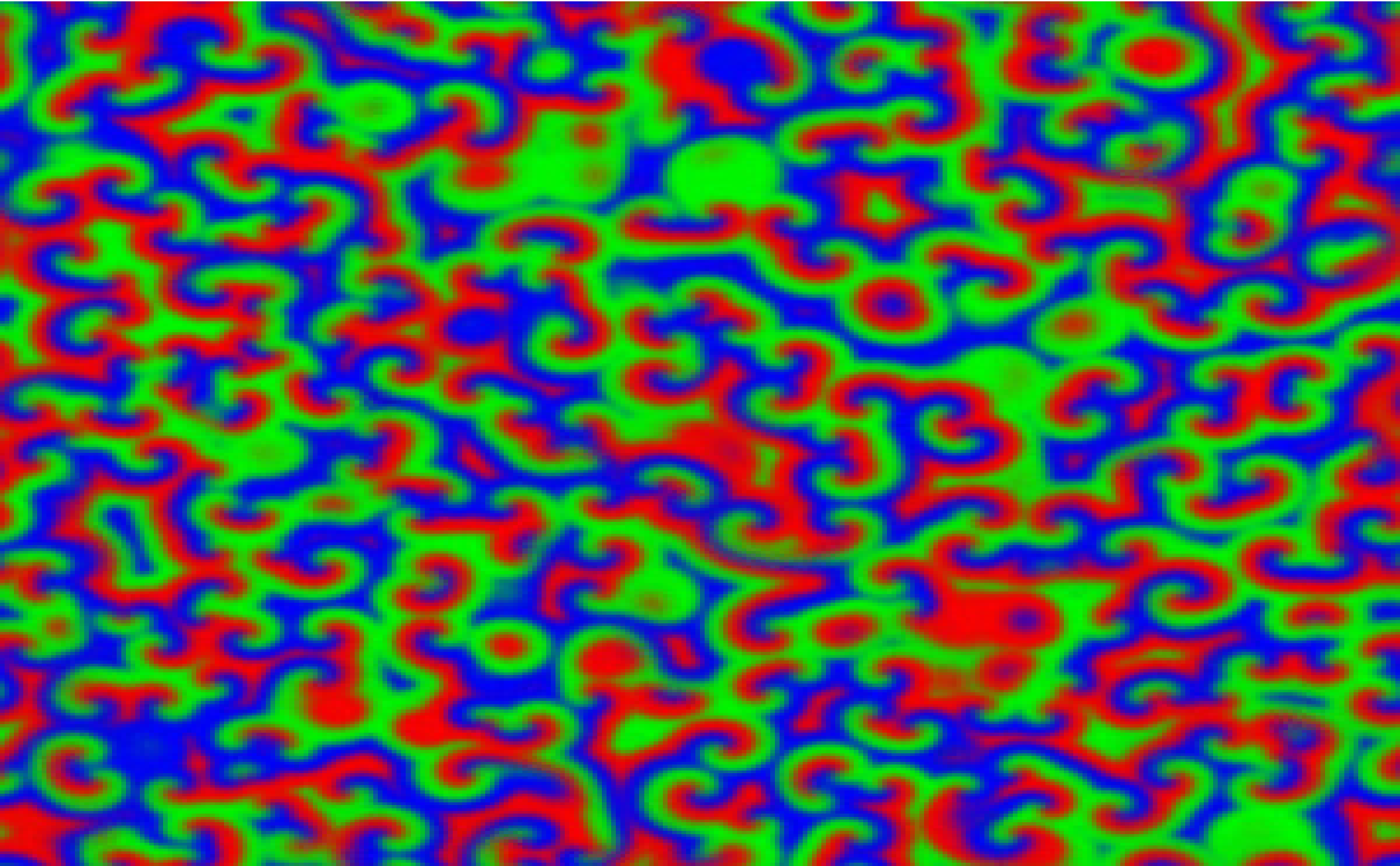
*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

“Smart” Autonomous Chemical Oscillator:

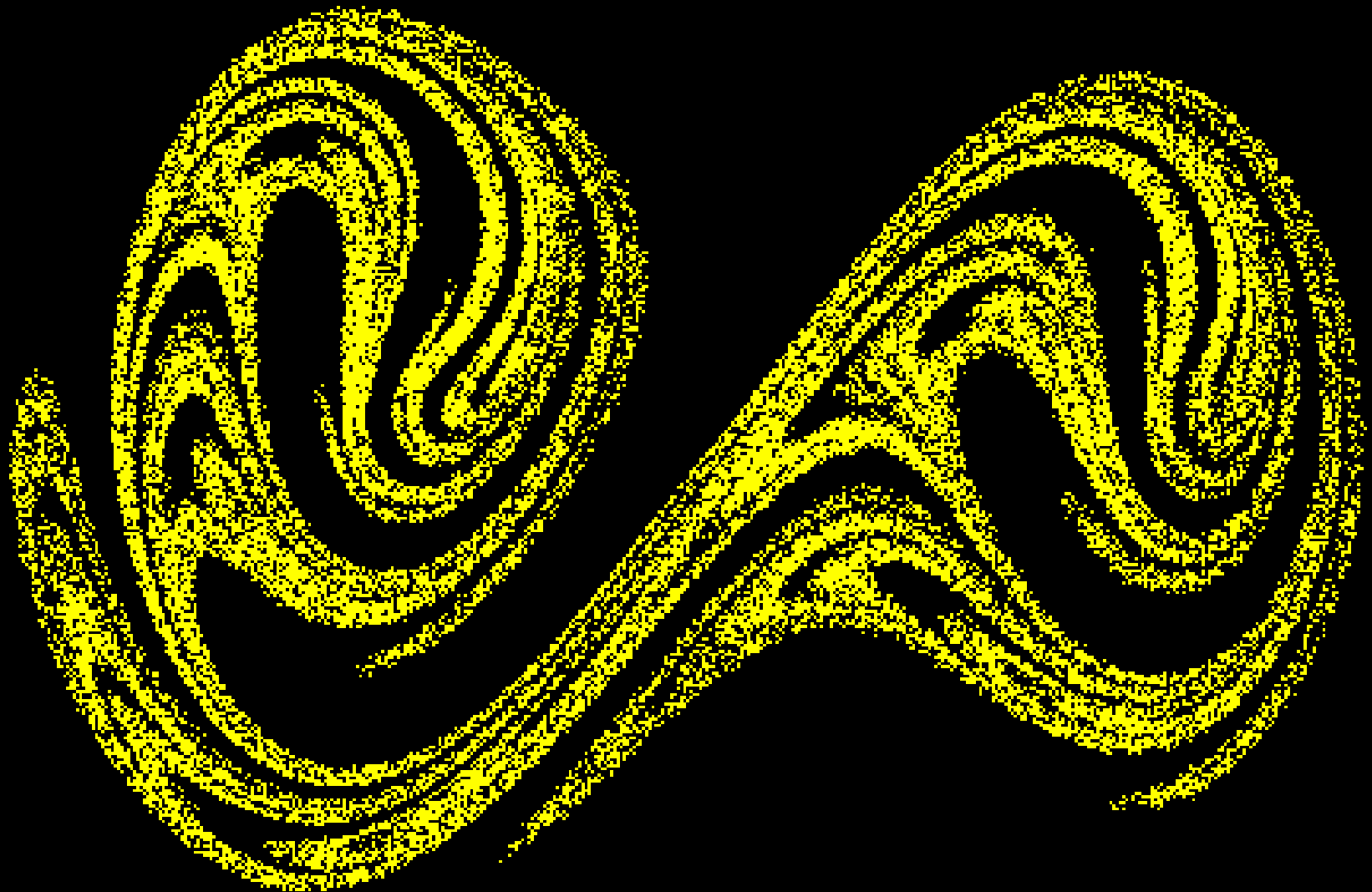
- Belousov–Zhabotinsky Reaction (BZ) -*



Chaotic Attractor: *Duffing Oscillator*

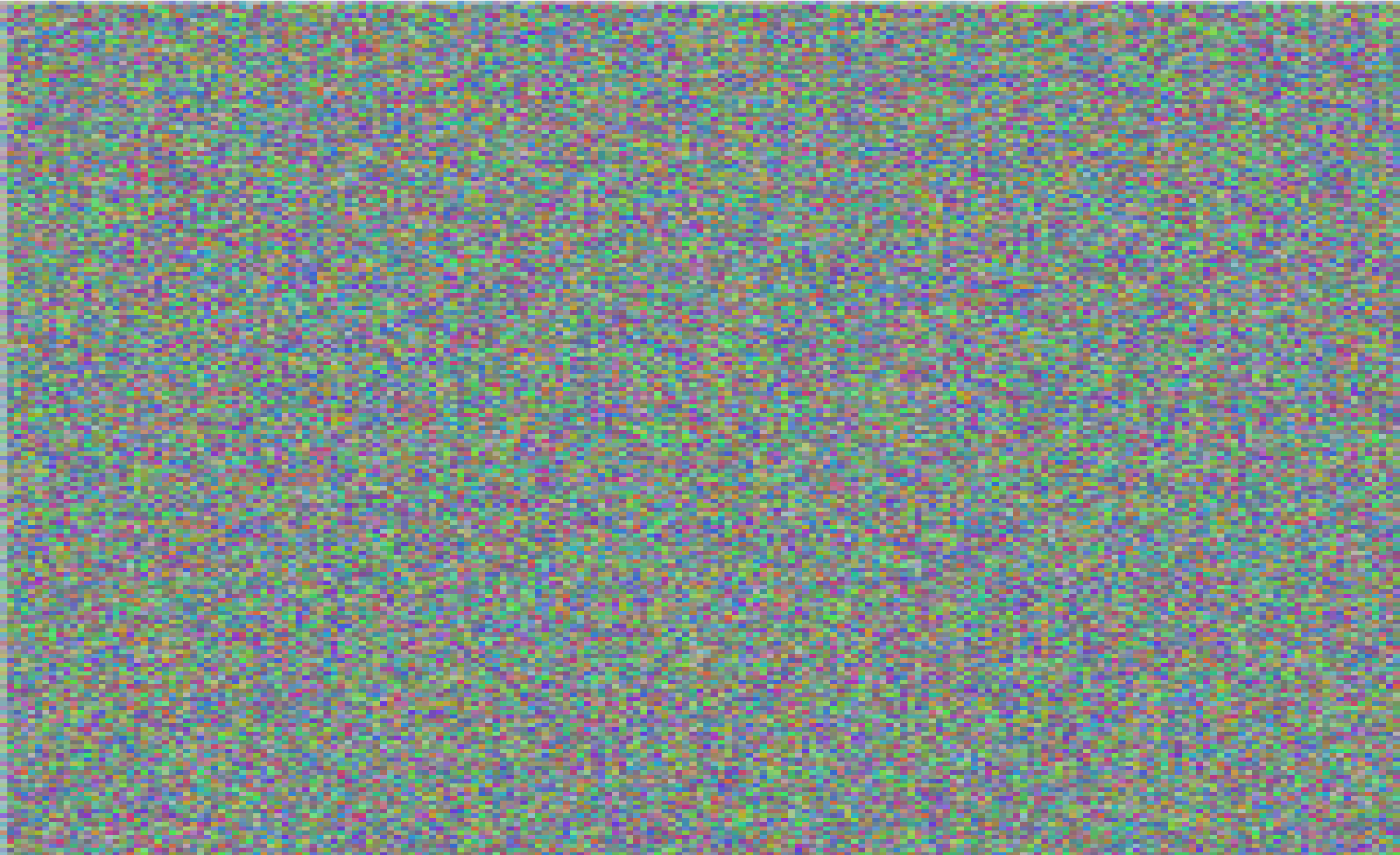
....*"Chaos" is common in "Smart Systems" and "Cyber Communities"*

Dynamic Duffing Equation: $\ddot{x} + \delta\dot{x} + \alpha x + \beta x^3 = \gamma \cos(\omega t)$ - Exhibits Chaotic Behaviour

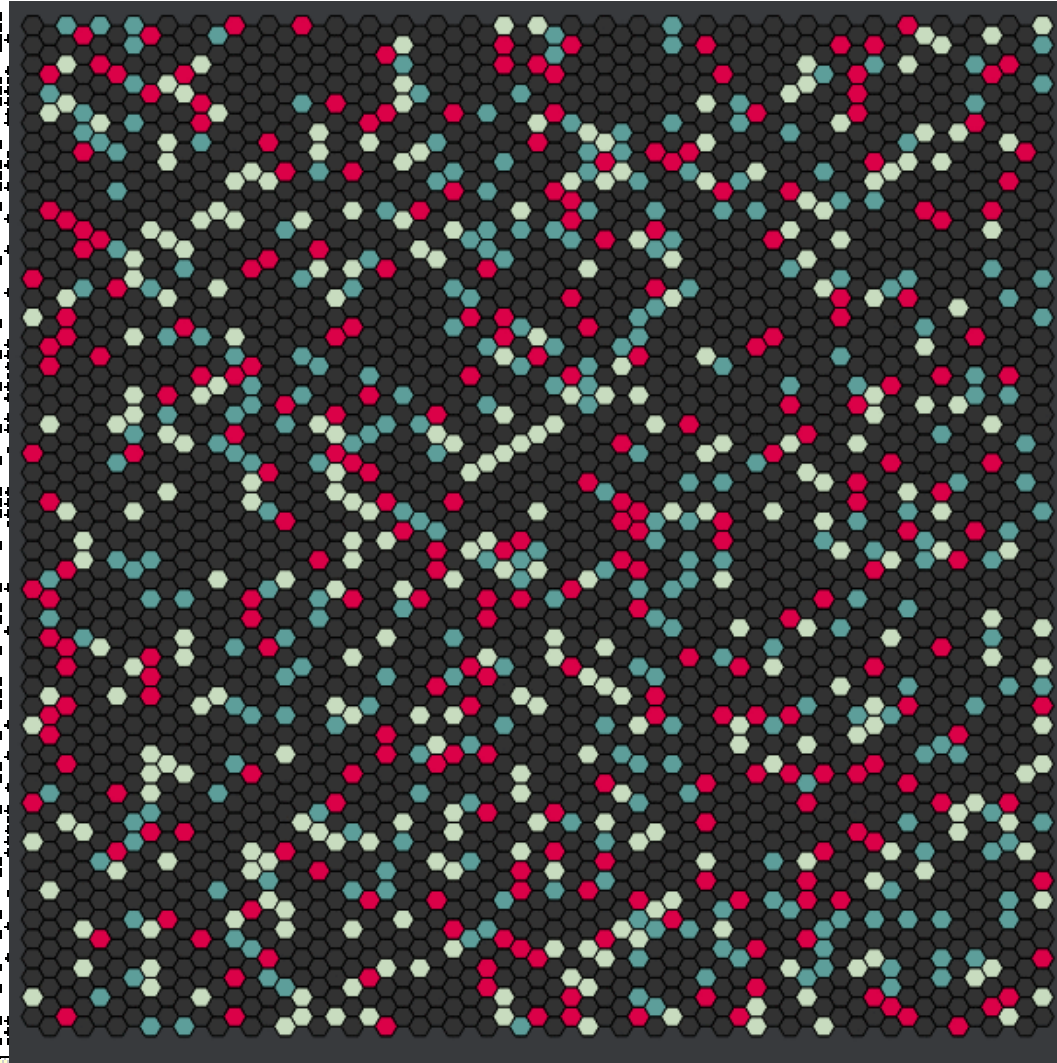
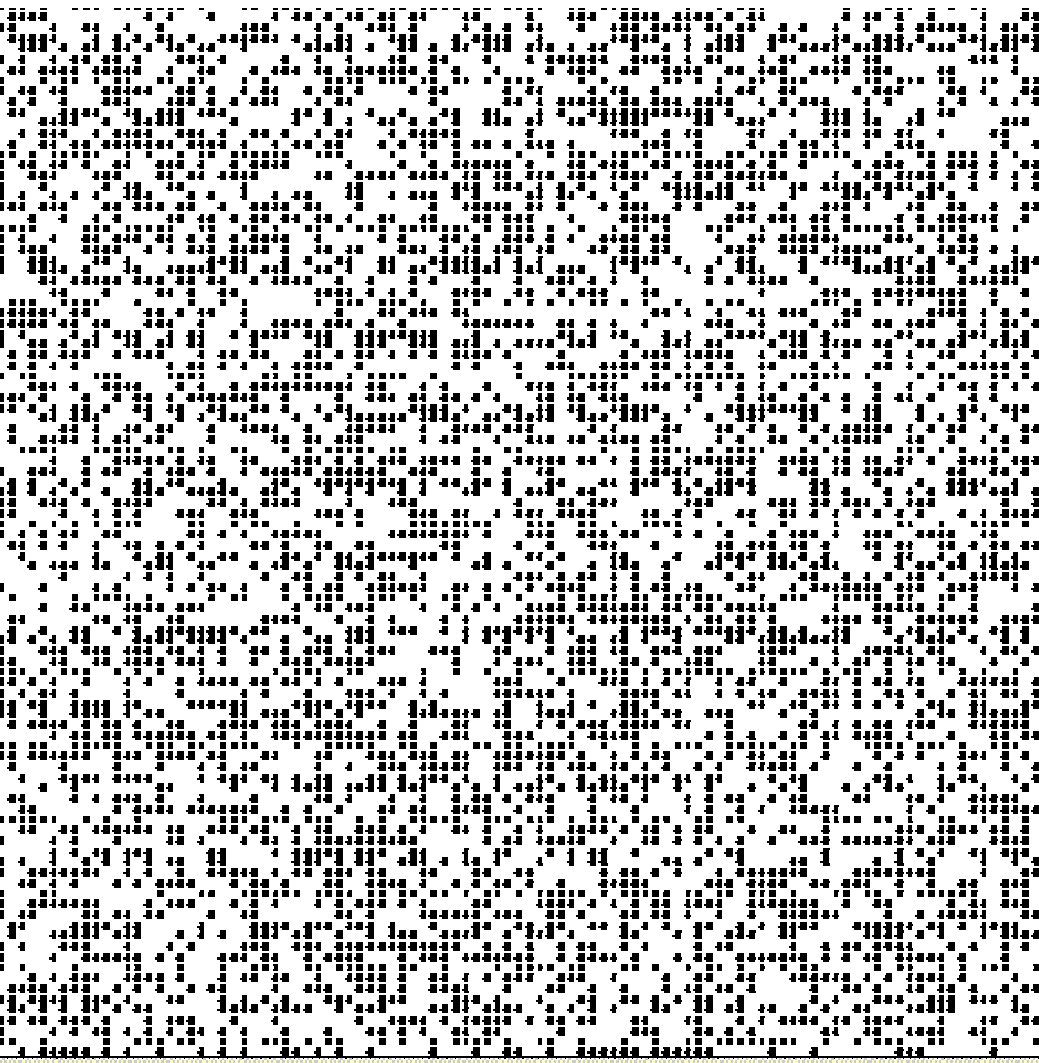


2D Super-Cyclic Cellular Automaton:

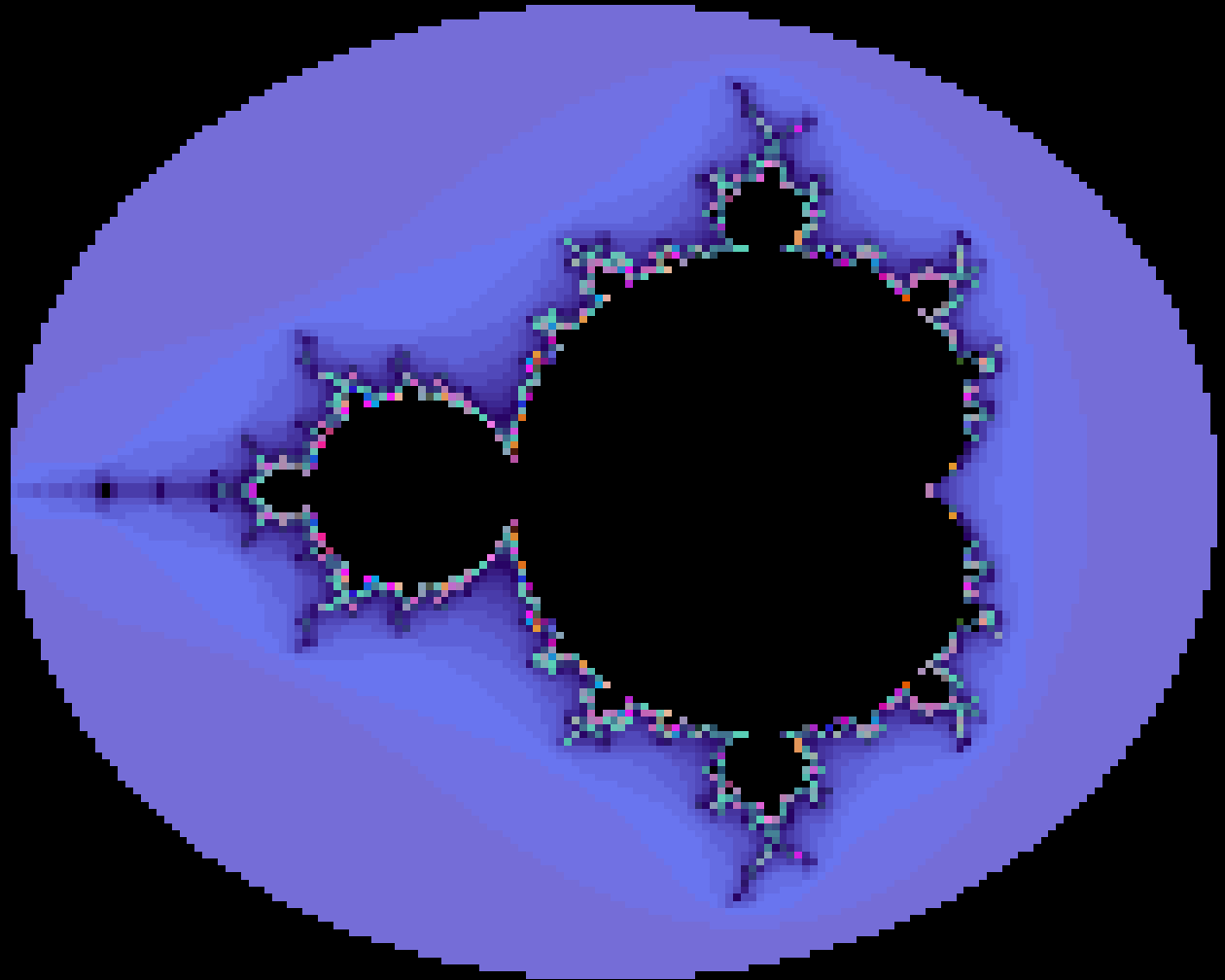
- *Emergence of Patterns from Random Chaos* -



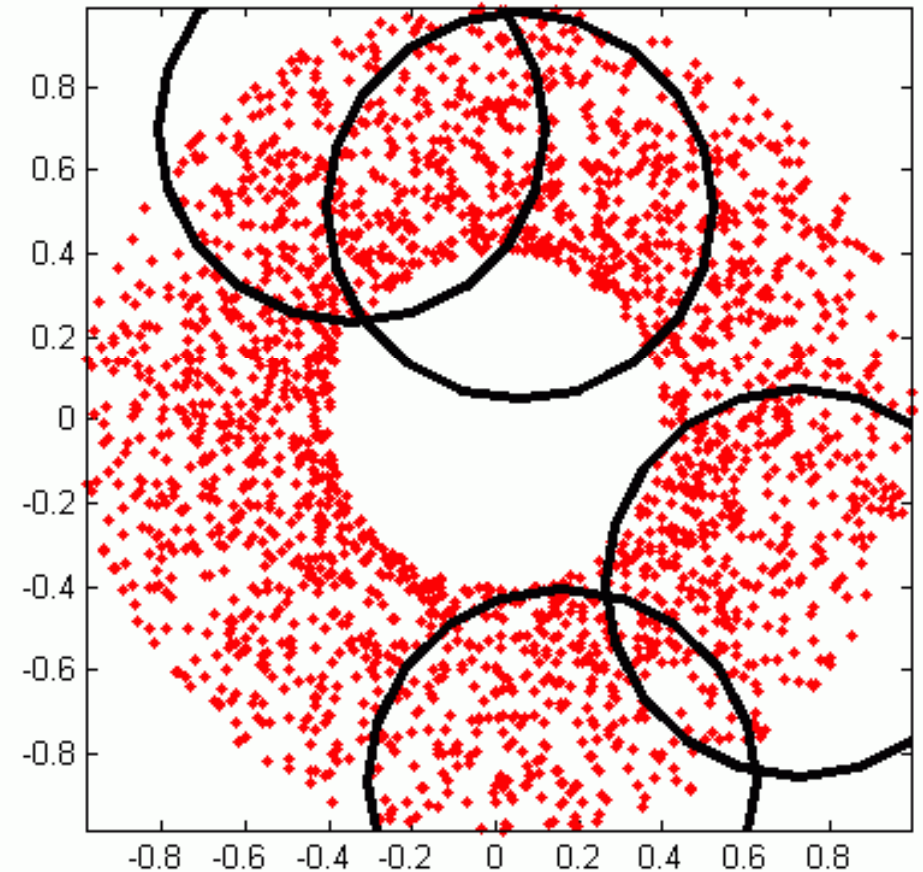
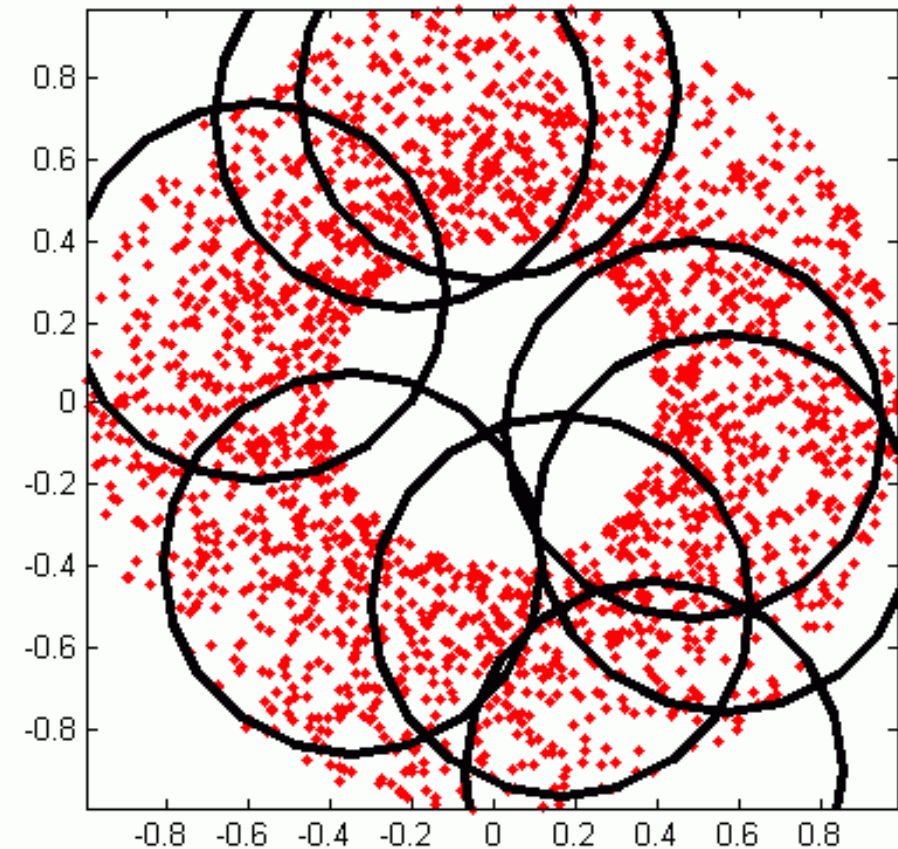
Cellular Automata: *“Games of Life”*



“Smart Scaling”: Fractal Mandelbrot Set

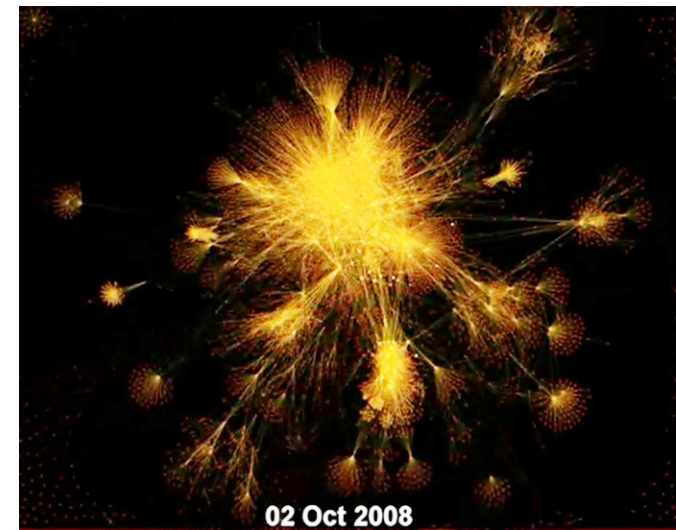
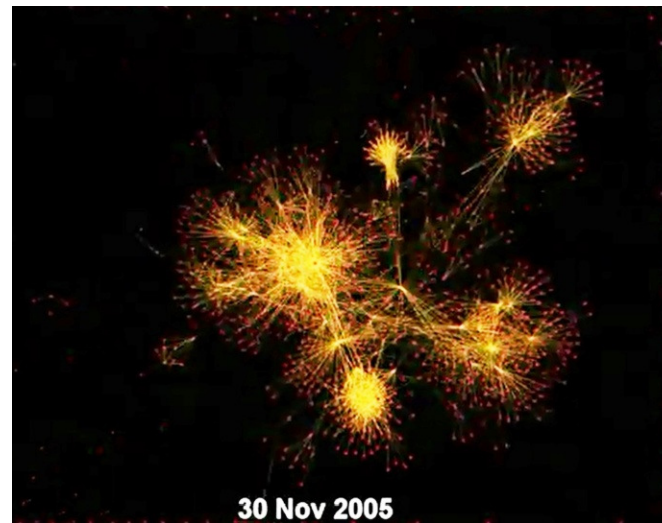
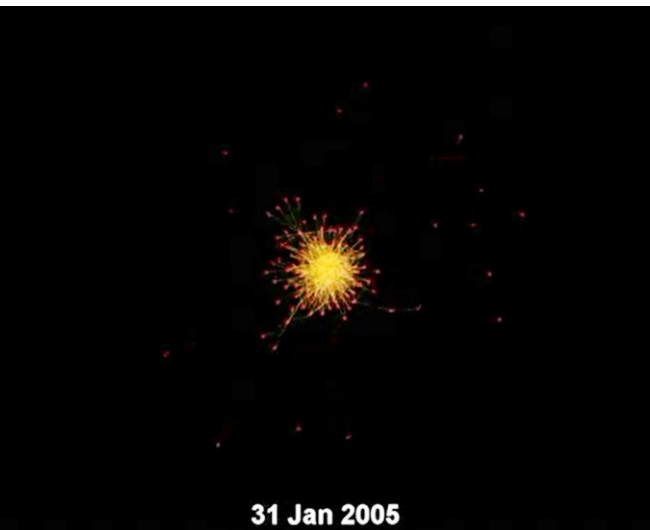


“Machine Learning Algorithms”



Multi-Year Evolution of Wiki-Web

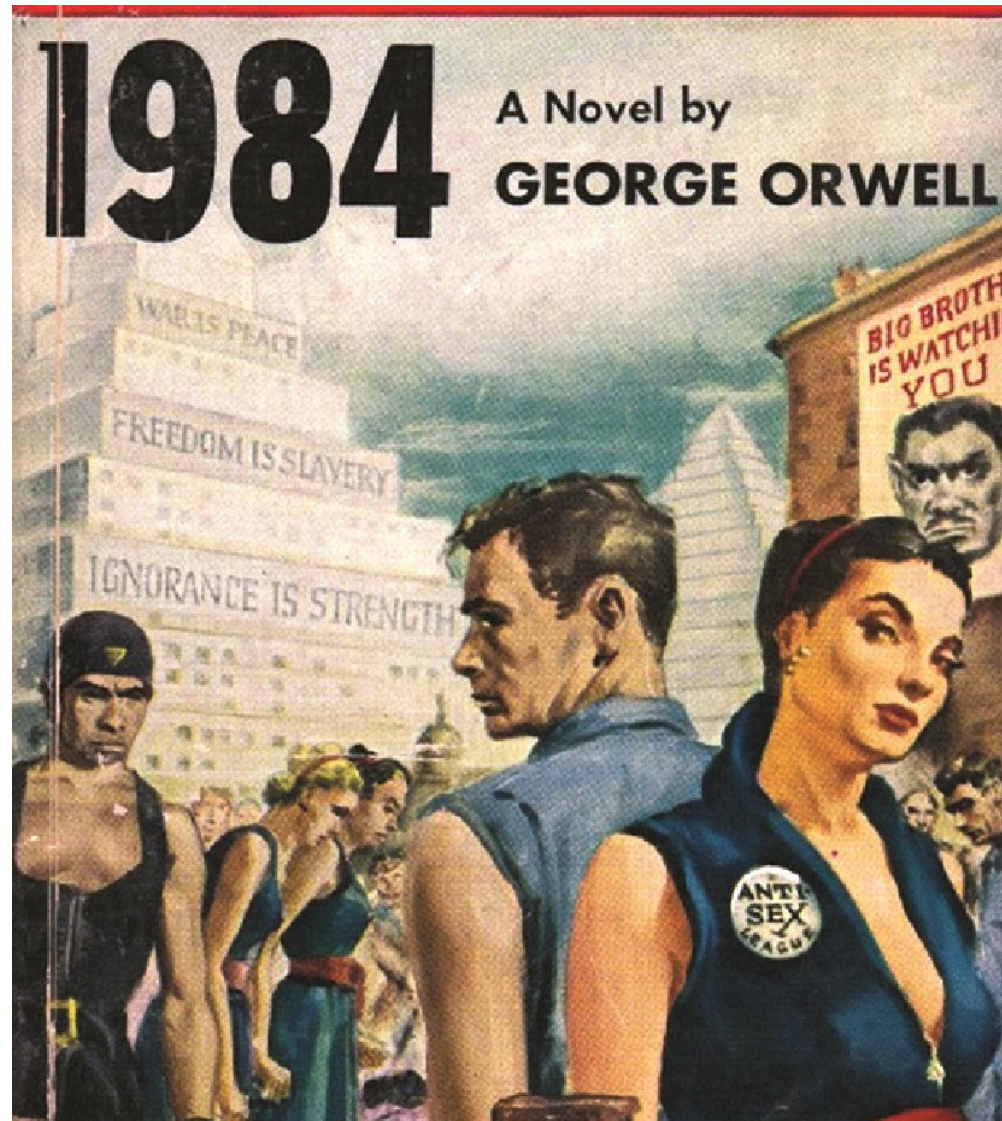
Complex Adaptive System : “Wiki.tudelft.nl”



Delft University of Technology - Netherlands
CyberVision : 2015 - 2025

*** **21stC Cybersecurity Trends** ***
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

1984: “Birth” of Intelligent Networks and *“Death” of Personal Privacy ?*



CyberVision : 2015 - 2025

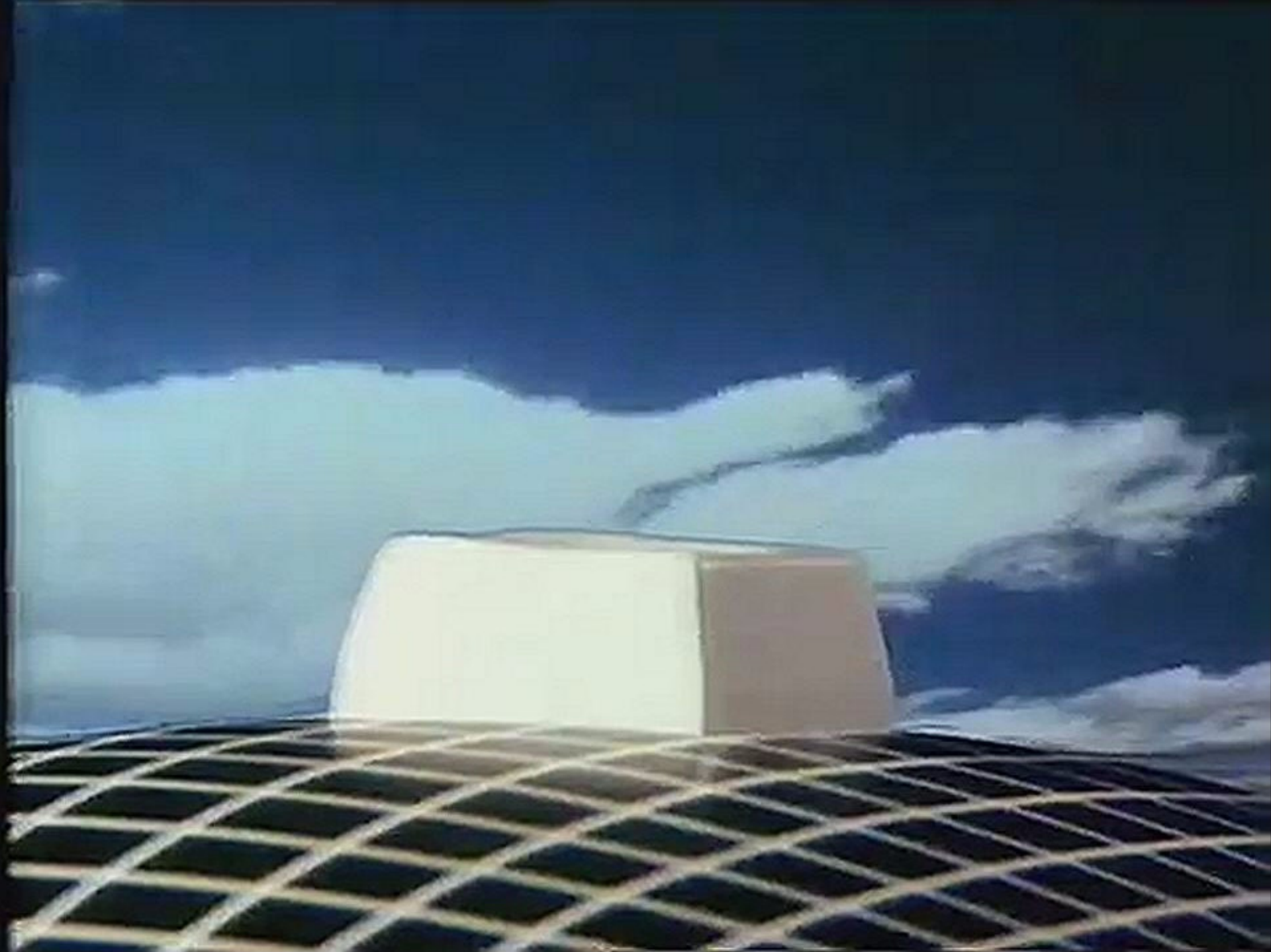
***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

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

- City Business Systems – British Telecom –

Launch of Real-Time Financial Trading: 1984



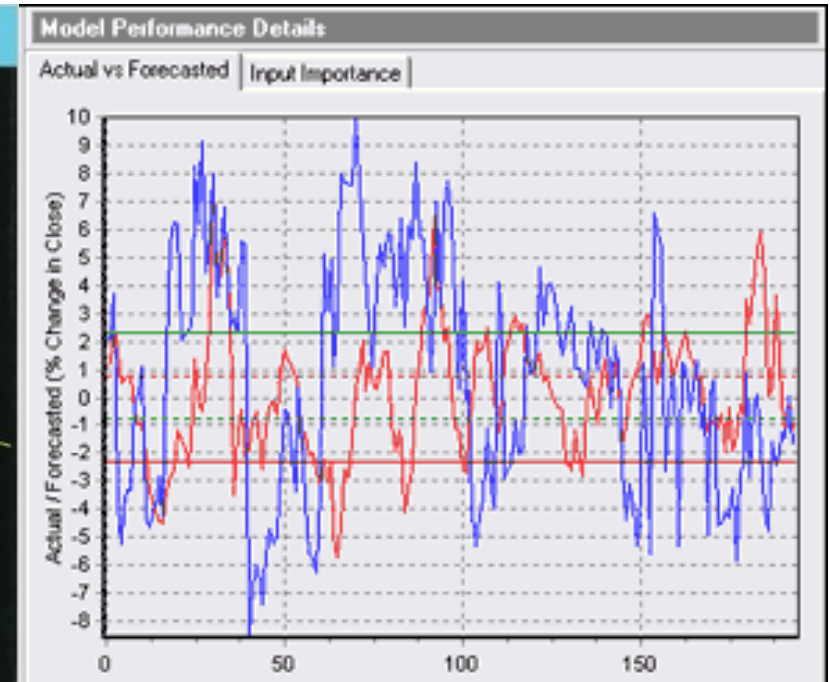
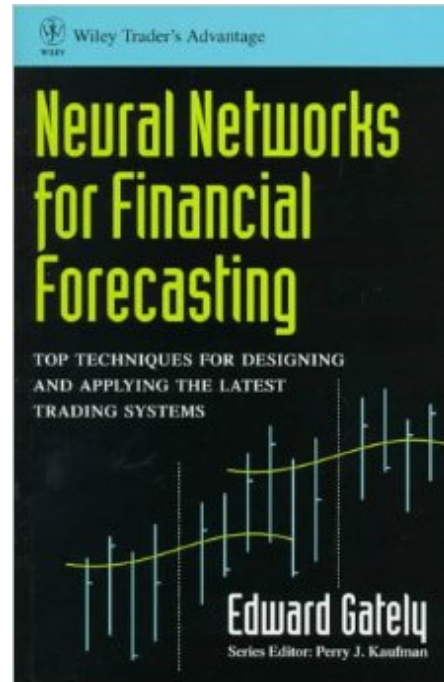
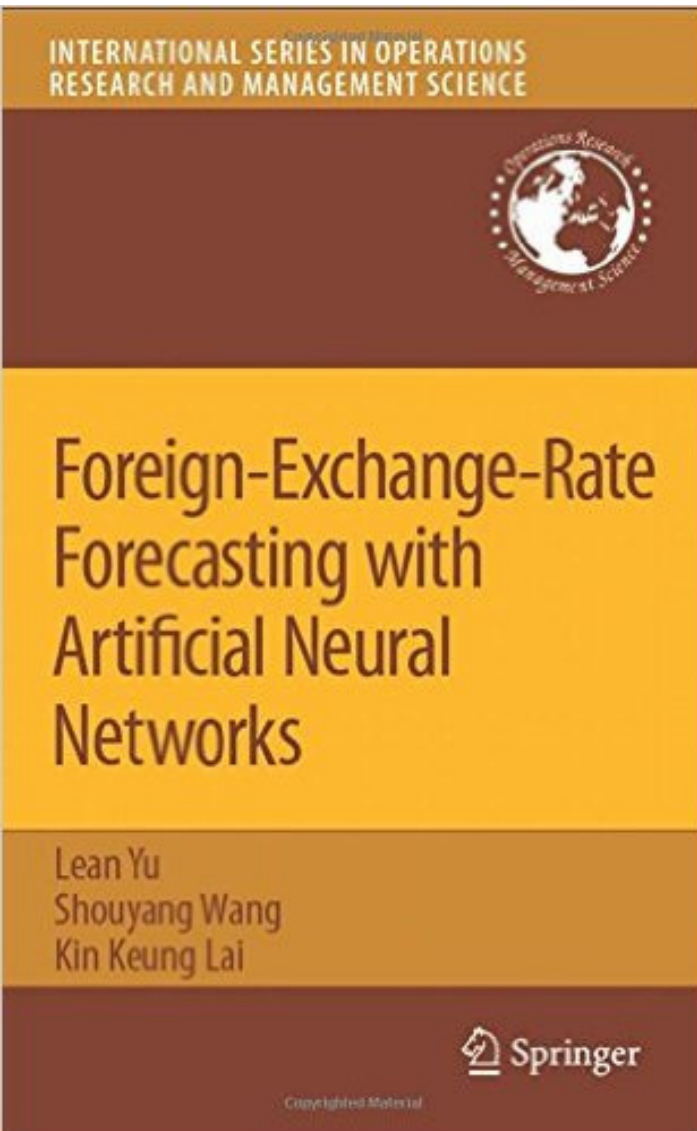
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

Artificial Neural Networks applied to **Real-Time Foreign Exchange Dealing**



**Algorithmic Computer Trading using Real-Time Neural Nets
& Statistical Maths Tools have been used for 20+ Years!**

***.....Now they are being applied to provide intelligent
real-time forecasts for Enterprise Cybersecurity Threats!***

CyberVision : 2015 - 2025

***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

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

Worldwide Real-Time Financial Trading

@Light Speed – 24/7 – Global Networks



CyberVision : 2015 - 2025

***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

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

Towards 2025 : ***“Smart Security Solutions”***

- The Application of Artificial Intelligence and Machine Learning allows us to develop ***“Smart Security Solutions”*** as follows:

.....***“Smart Security Solutions”*** typically possess the following features:

- 1) ***Space-Time Awareness:*** Location (GPS) & Real-Time Clocks
- 2) ***Learning, Adaptation & Self-Organisation:*** Real-Time Intelligence
- 3) ***Massive Memory & Storage:*** Local & Remote Cloud Storage
- 4) ***Sustainability:*** Embedded Security – *Everywhere in the Network!*
- 5) ***Scalable Networked Architecture:*** Smart Architectures will need to scale in space & time from micro cells to macro solutions
- 6) ***Decision Focus:*** “Knowledge Lens” for Data Mining & “Big Data” from Global Social Networks, Search & On-Line Trade & Commerce
- 7) ***Systems Integration:*** Cyber and Physical Solutions & Operations

.....Now we'll consider how ***“AI & Machine Learning”*** principles are being engineered into ***21stC Cybersecurity Solutions & Services...***

Building our 2025 **Smart Security** Toolkit

(1) *Smart **Decision** Principles - “D-Genes”*

- **Business Decisions** require focusing & filtering of Big Data sources in *Space-Time* to create local knowledge (Data Mining). Hence a useful metaphor is the **“Knowledge Lens”**:
 - Smart Decision **“Genes”** = Space, Time and Information Focus
 - Conceptual **“Knowledge Lens”** can filter and focus information in “Space” from searching Big Data Sets to a Small focused Short-List
 - The **“Knowledge Lens”** can focus information & present in real-time, possibly as an stream of multi-media news or market intelligence
- **“Knowledge Lens”**: This concept can be a useful architectural principle in the design of **Smart Security**, Smart Business & Smart Governance

....21stC *Cyber Attacks* occur in Real-Time @Optical Speeds
so ultra fast analysis, decisions and action is a must!

Building our 2025 **Smart Security** Toolkit

(2) *Smart Learning Principles - “L-Genes”*

- **Smart Learning** requires: Self-Organisation, Adaptation, Memory and Scalable Architecture. The Decision “Genes” are relatively traditional whilst these new Learning “Genes” lie at the heart of Smart Security.
 - **Self-Organisation** & Adaptation are essential principles of living systems and communities which include the well known self-organisation of insect roles in communities such as ants & bees.
 - **Cellular Automata** demonstrate relatively complex behaviour from simple mathematical rules, as in Conway’s “Game of Life”
 - **Simple Dynamic Recursive Maps** such as $x \Rightarrow 4x(1-x)$ also result in complex chaotic behaviour as found in real world insect populations
 - **Scalable Architecture** is also an essential feature of plants & animal life & Mandelbrot’s theory of Fractal Curves provides vivid examples.
-**Current Trends:** Research into AI, Machine Learning, Self-Organisation & Adaptation remains highly active in both Universities & Commercial R&D Labs

Hybrid 21stC Business Organisation

- *Hierarchical & Organic* -

- **Transition** from 20thC to 21stC Business, Governance & Security requires fundamental re-structuring of operations:
 - **20thC Industrial Organisations:** Hierarchical Bureaucracies (Pyramids) to manually process data/information.
 - **21stC Intelligent Organisations:** Networked Peer-to-Peer Business & Agencies with data processed in “**Cyber Clouds**”
- **Living Systems**, such as Mammals, use Hybrid Organisation of their extended nervous system (**Brain & Body**) to optimise real-time learning and effective environmental adaptation!
- **Smart Security Solutions** will also require **Hybrid** organisation to optimise real-time response to **Cyber & Physical** Attacks.

2025 : Designing “*Smart Security*”

- **Smart Security Solutions** all use combinations of these Basic ICT Learning & Decision “genes” shared with Intelligent Living Systems:
 - 1) **Hybrid Organisation:** Hierarchical (Pyramid) & Organic (Networked)
 - 2) **Smart Decision Principles (D-Genes):** Space, Time & Decision Focus
 - 3) **Smart Learning Principles (L-Genes):** Memory, Scaling & Adaptation
 - 4) **Smart Security Solutions and Services:** Integration of Decision and Learning “Genes”, within Secure & Resilient Systems Environment

.....Using “**AI & Machine Learning**”, 21stC Cyber Ventures are now marketing “Smart” **Self-Learning Cybersecurity** Tools to secure Enterprises, Government & Critical Information Infrastructure!

BBC Worldwide Internet Scenario: 2040



Sign in

News

Sport

Weather

iPlayer

TV

Radio

More

Search



This website is made by BBC Worldwide. BBC Worldwide is a commercial company that is owned by the BBC (and just the BBC.) No money from the licence fee was used to create this website. Instead this website is supported by advertising outside the UK. The profits we make from it go back to BBC programme-makers to help fund great new BBC programmes

future

Home

Tech

Science

Health

About us

DISCOVER:

The Genius Behind

THE HUMAN MIND

Secrets of the brain

World-Changing Ideas | Internet | World Wide Web

What will the internet look like in 2040?

In 25 years, will life online be bright or bleak? Chris Baraniuk analyses competing visions for the future of the internet.

Related Stories



CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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



MINISTRY OF DEFENCE

Scenario 2040: Cyber Defense: UK Ministry of Defence - MOD

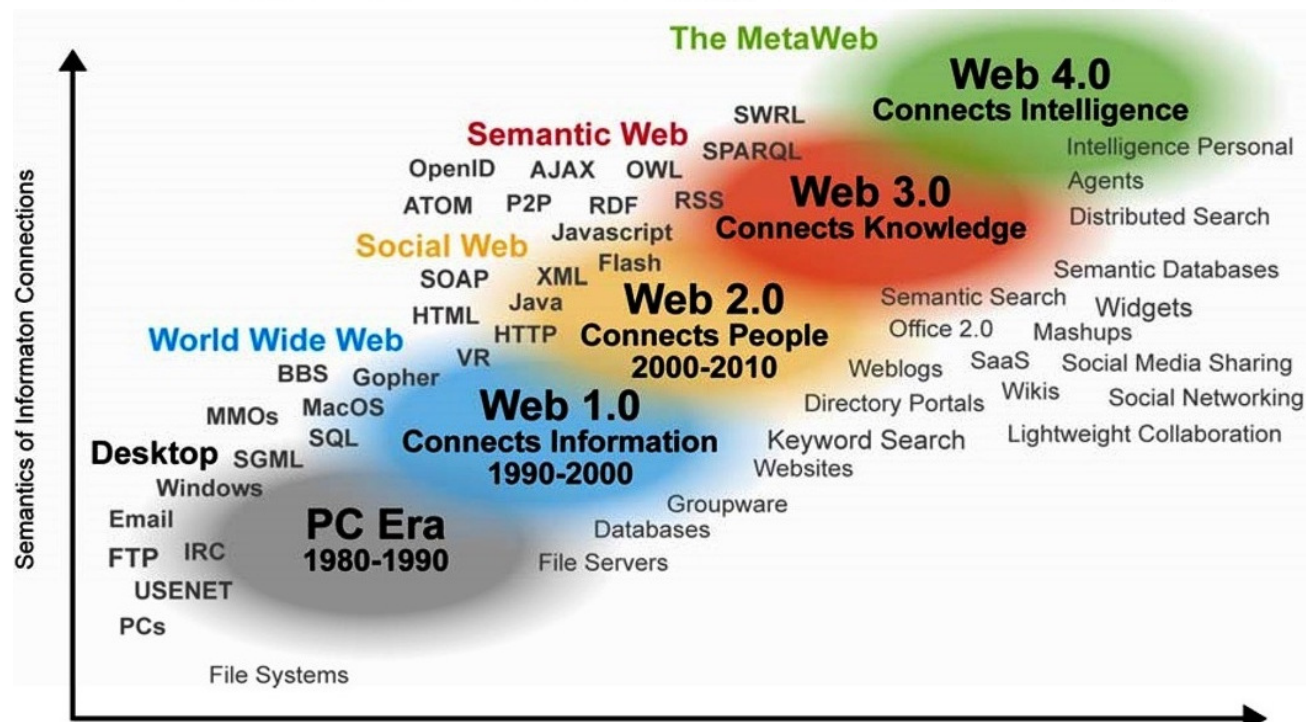
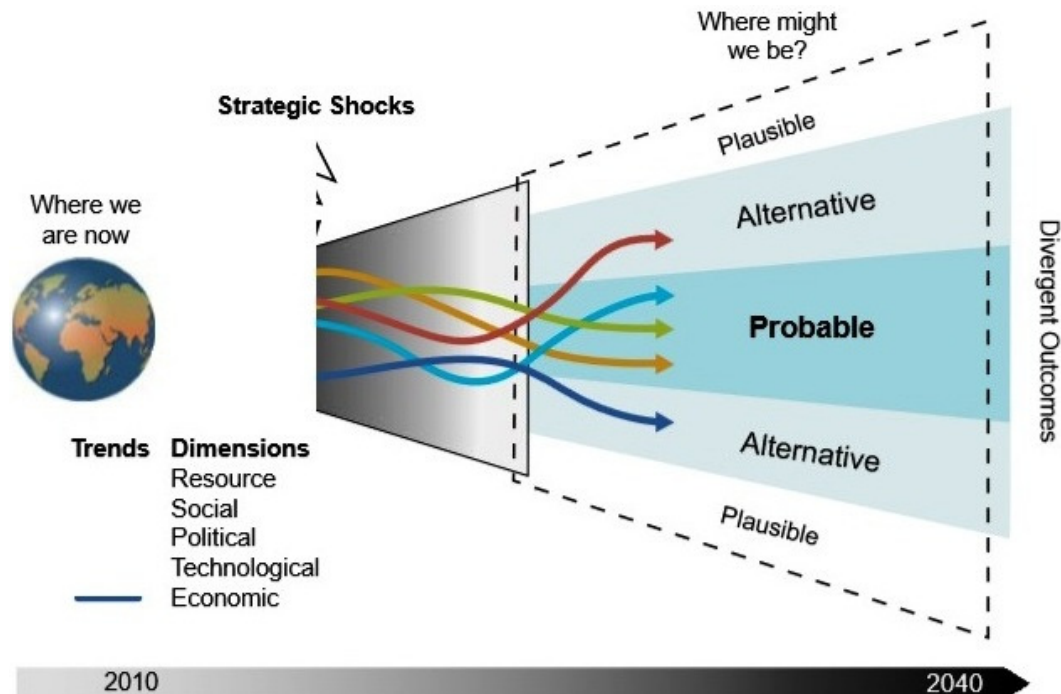
Ministry of Defence

Strategic Trends Programme Global Strategic Trends - Out to 2040

Fourth Edition



D C D C



*** 21st Century Cybersecurity Trends ***

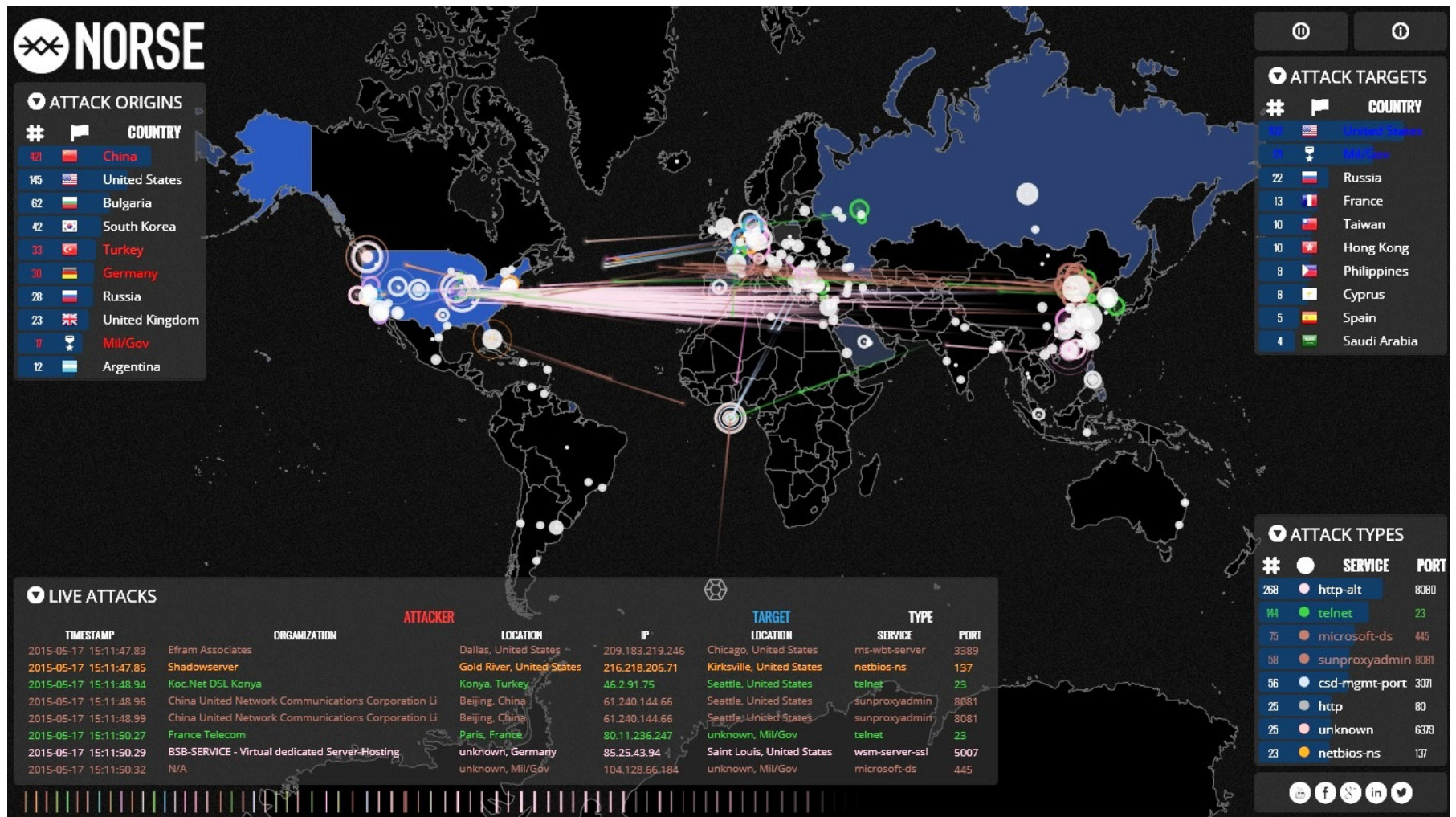
London, UK :: 15th December 2015

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

CyberVision : 2015 - 2025

The **Cybersecurity** Industry 10 Year Challenge:

- **Apply AI Apps for Real-Time Cyber Defence** -



Deploy **Light-Speed "AI-Neural Security"** against the 24/7 Attacks from **"Bad Cyber Guys"**

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

The **Cybersecurity** Industry 10 Year Challenge:

- *Apply AI Apps for Real-Time Cyber Defence* -



Deploy *Light-Speed "AI-Neural Security"* against the 24/7 Attacks from *"Bad Cyber Guys"*

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

Scenario 2040: Cyber Defense – NATO & Canada

The Future Security Environment 2013-2040



Canada National Defence / Défense nationale

Canada

CyberVision : 2015 - 2025

2011 3rd International Conference on Cyber Conflict
C. Czosseck, E. Tyugu, T. Wingfield (Eds.)
Tallinn, Estonia, 2011 © CCD COE Publications

Permission to make digital or hard copies of this publication for internal use within NATO, and for personal or educational use done for non-profit or non-commercial purpose is granted providing that copies bear this notice and a full citation on the first page. Any other reproduction or transmission requires prior written permission.

Artificial Intelligence in Cyber Defense

Enn Tyugu
R&D Branch
Cooperative Cyber Defense Center of Excellence (CCD COE)
and Estonian Academy of Sciences
Tallinn, Estonia
tyugu@ieee.org

Abstract- The speed of processes and the amount of data to be used in defending the cyber space cannot be handled by humans without considerable automation. However, it is difficult to develop software with conventional fixed algorithms (hard-wired logic on decision making level) for effectively defending against the dynamically evolving attacks in networks. This situation can be handled by applying methods of artificial intelligence that provide flexibility and learning capability to software. This paper presents a brief survey of artificial intelligence applications in cyber defense (CD), and analyzes the prospects of enhancing the cyber defense capabilities by means of increasing the intelligence of the defense systems. After surveying the papers available about artificial intelligence applications in CD, we can conclude that useful applications already exist. They belong, first of all, to applications of artificial neural nets in perimeter defense and some other CD areas. From the other side – it has become obvious that many CD problems can be solved successfully only when methods of artificial intelligence are being used. For example, wide knowledge usage is necessary in decision making, and intelligent decision support is one of yet unsolved problems in CD.

Keywords: applied artificial intelligence; intelligent cyber defense methods; neural nets in cyber defense; expert systems in cyber defense.

*** 21stC Cybersecurity Trends ***

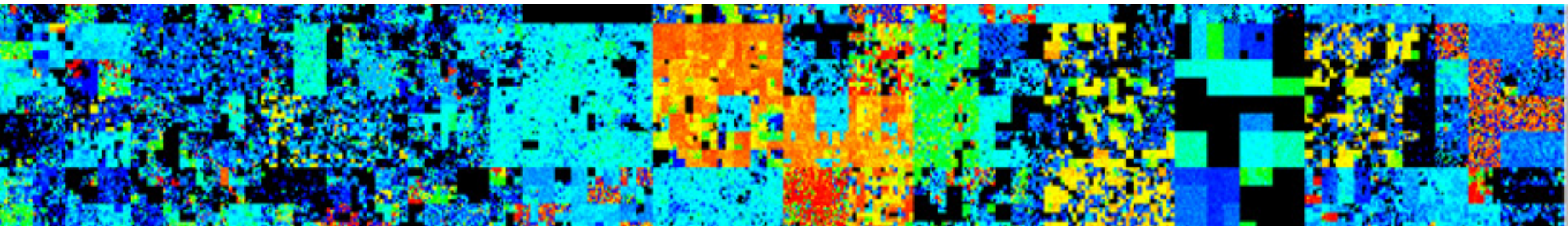
London, UK :: 15th December 2015

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

21stC Cybersecurity Trends: 2015 - 2025



1 – Background: 21stC Security Landscape	2 – Cybersecurity: Players & Threats	3 – Cyber Market Structure, Size & Growth
4 – CSO: C-Suite Security Integration “Integrated”	5 – Scenario 2020: Internet of Things (IoT) “Adaptive”	6 – Scenario 2025: AI & Machine Learning “Intelligent”
7 – Cybersecurity Ventures (Old and New)	8 – Mergers, Acquisitions & VC Funds	9 –YOUR Actions Plan for 21stC Cyber!....



CyberVision : 2015 - 2025

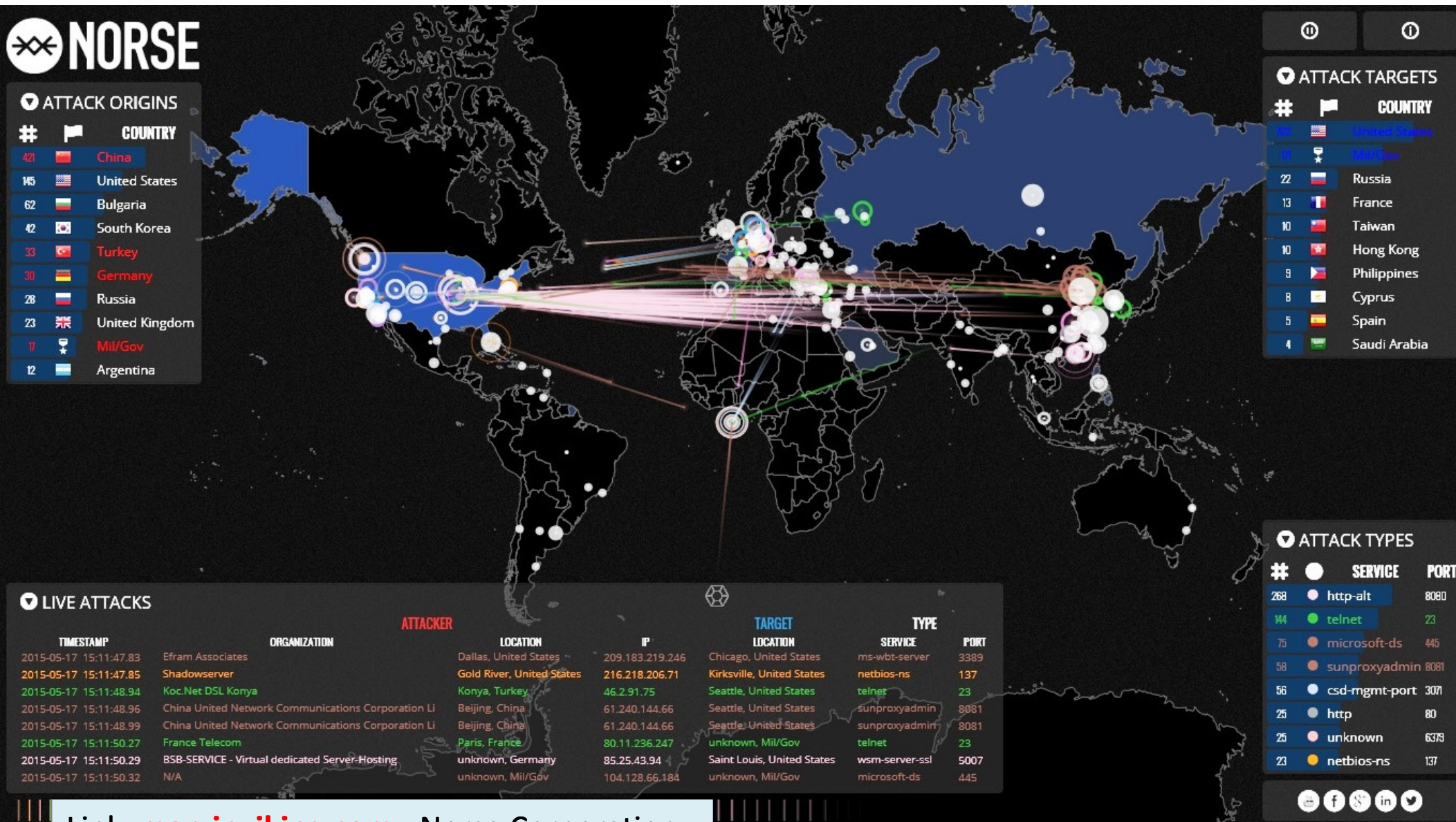
*** 21stC Cybersecurity Trends ***
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

Cybersecurity Companies - USA

- **FireEye** – Next Generation Security
- **Norse** – In-Depth Real-Time Intel
- **Cylance** – AI/ML Threat Detection
- **DB Networks** – Real-Time ML Defence
- **LanCope** – Security Threat Intelligence
- **AlienVault** – Intelligent Security
- **RSA** – Big Data & Cloud Security
- **VeraCode** – Secure Code Analytics
- **Palo Alto Networks** – Next Gen Cyber
- **Resilient Systems** – Auto Threat Alert
- **Prelert** – Machine Learning Solutions
- **Barracuda Networks** – Firewalls+
- **Palantir** – Analytics & Fraud
- **Daon** – Biometrics & ID Mgt
- **Akamai** – Cloud & Mobile
- **Qualys** – Cloud Security
- **Blue Coat** – Business Assurance
- **Arbor Networks** – DDoS Attack
- **Zscaler** – Security Services
- **Sonatype** – Enterprise Security
- **Okta** – Identity Management
- **Skybox Security** – Risk Analytics
- **LogRhythm** – Log Mgt Analytics
- **PKWare** – Data Encryption

USA/Canada is estimated to be **38% (\$37Bn)** of Global **CyberSecurity** Marketplace

Norse Corporation: *Intelligence Service*



Link: map.ipviking.com - Norse Corporation

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

New Cybersecurity Companies - **UK**

- **DarkTrace** – Machine Learning
- **Avecto** – Endpoint Security
- **Acunetix** – Vulnerability Scanner
- **PortSwigger** – Web Security
- **Wandera** – Secure Mobile Portal
- **SentryBay** – Mobile, IoT Security
- **Citicus** – Risk & Compliance Mgt
- **Protectimus** - 2-Factor Security
- **Clearswift** – Big Data Security
- **SiloBreaker** – Risk Analytics
- **SentryBay** - Mobile & IoT
- **Swivel Secure** - Authentication
- **Digital Shadows** - Cyber Intel
- **Smooth Wall** - Threat Mgt
- **BeCrypt** - Mobile Data Security
- **Acuity** – Compliance & Risk Mgt

Cybersecurity Companies - *Israel*

- **CyberArk** –(NASDAQ – CYBR)
- **CheckPoint** –(NASDAQ–CHKP)
- **Elbit Systems** - (NASDAQ –ESLT)
- **CheckMarx** – Code Analytics
- **Seculert** – Attack Detection
- **Sentrix** – Cloud DMZ Firewall
- **TrapX** – “HoneyPot” Solutions
- **Skycure** – Real-Time Mobile
- **Radware** - (NASDAQ – RDWR)
- **Light Cyber** – Threat Detection
- **GreenSQL** – Secure Database
- **GuardiCore** – Server Security
- **CyActive** – Acquired by Paypal
- **Waterfall** – Control Security
- **6Scan** – Website Security
- **MinerEye** – Self-Learning Tool

- “*Innovative*” *Cybersecurity* Business - “*AI & Machine Learning Solutions*”

- **Darktrace (UK)** – Enterprise Immune System – Real-Time Modelling of Traffic, Nodes & Users
- **DB Networks (US)** – Real-Time Advanced Threat Database Analytics & Cybersecurity
- **Cylance (US)** – Next Generation Anti-Virus and Enterprise Advanced Threat Protection
- **Prelert (US)** – Behavioural Analytics Platform for Detection of Database Threats & Anomalies
- **MinerEye (Israel)** – “Self-Learning” Data Loss Prevention with In-Depth Intelligent Classification
- **LogRhythm (US)** – “Machine Learning” Log Forensics

Darktrace: *Cyber Intelligence Platform*

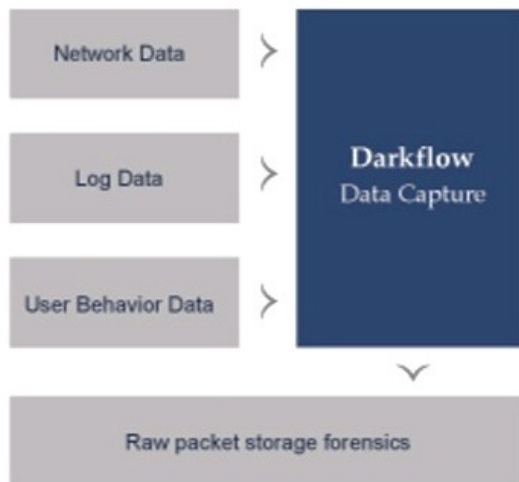
Darktrace Cyber Intelligence Platform (DCIP)



DARKTRACE CYBER INTELLIGENCE PLATFORM

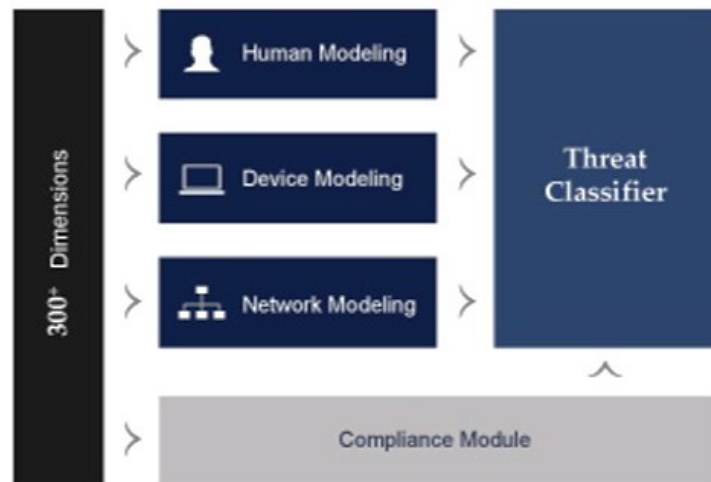
Data Capture & Interpretation

Real-time Total Network Immersion



Recursive Bayesian Estimation

Unsupervised real-time mathematical engines



Threat Visualizer

3D Topological Network Projection



Notifications & SIEM outputs

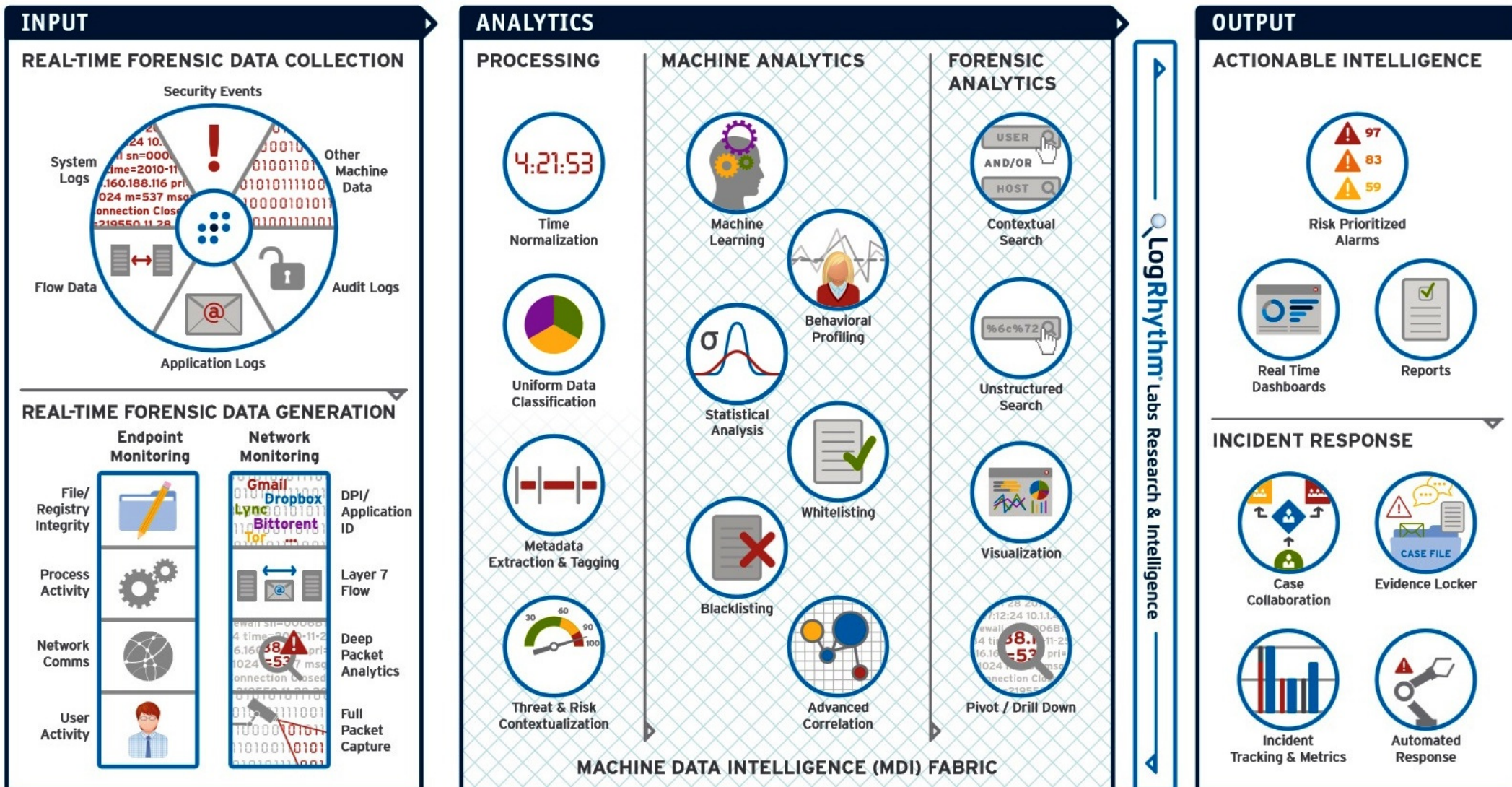
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

LogRhythm: *Machine Learning Forensics*



LogRhythm's *Security Intelligence Platform*

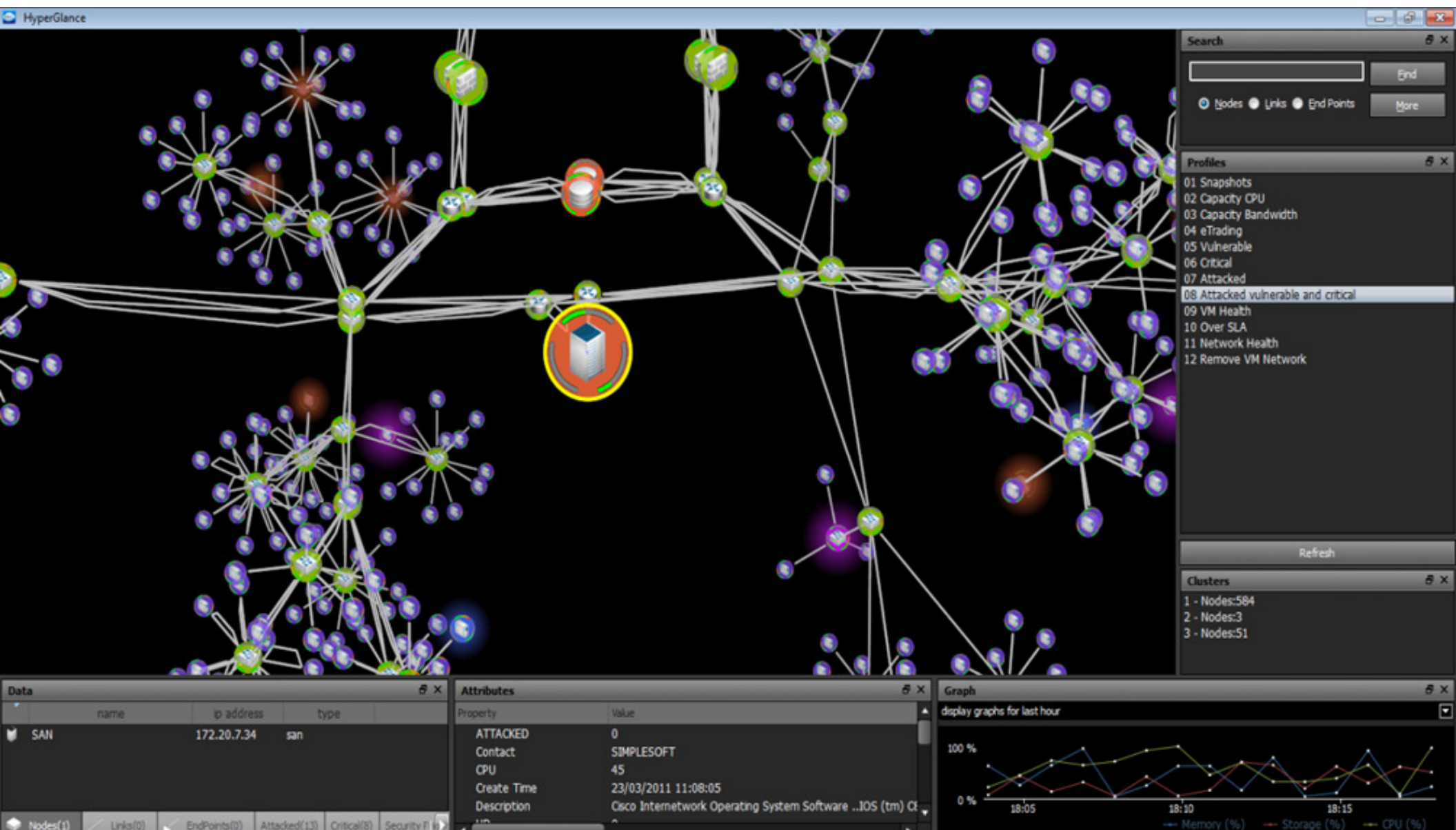
CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

Hyperglance:*Smart 3D Network Modelling*



Hyperglance Real-Time Visualisation Software: Real-Status.com - London, UK

CyberVision : 2015 - 2025

***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

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

“Smart Analysis Tools”: 4D Simulation Modelling for Hybrid Terror Alert & Disaster Management



CyberVision : 2015 - 2025

***** 21stC Cybersecurity Trends *****

London, UK :: 15th December 2015

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

Cyber Solutions from Corporations

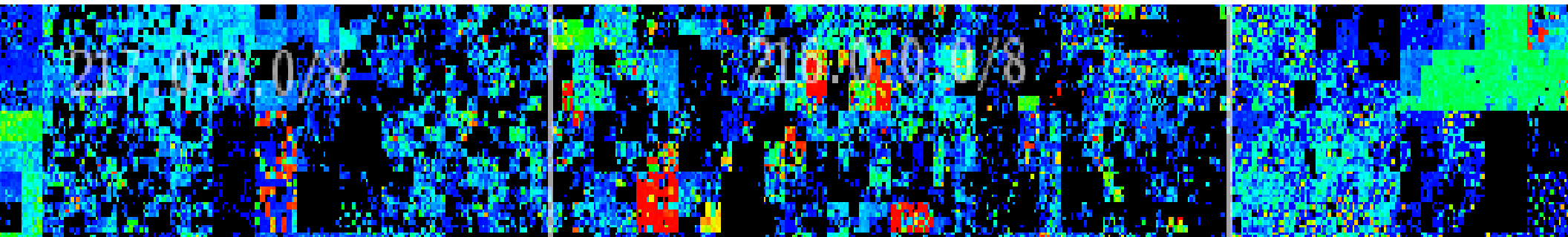
- Consultancy, Networking and Services -

- **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 Consultancy, Solutions & Services
- **Symantec (US)** – Security Solutions
- **Kaspersky Lab(RU)** – Security Solutions
- **BAE Systems** – Cyber Risk Management
- **IBM** – Enterprise 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

21stC Cybersecurity Trends: 2015 - 2025



1 – Background: 21stC Security Landscape	2 – Cybersecurity: Players & Threats	3 – Cyber Market Structure, Size & Growth
4 – CSO: C-Suite Security Integration “Integrated”	5 – Scenario 2020: Internet of Things (IoT) “Adaptive”	6 – Scenario 2025: AI & Machine Learning “Intelligent”
7 – CyberSecurity Ventures (Old and New)	8 – Mergers, Acquisitions and VC Funds	9 – YOUR Actions Plan for 21stC Cyber!....



Mergers & Acquisitions: 2014/2015

- Cybersecurity Business Sector -

- **PayPal:** CyActive-\$60m, Fraud Sciences - \$169m
- **Splunk:** Caspida - \$190m
- **Raytheon:** Websense-\$1.9Bn, and Blackbird Technologies - \$420m
- **Fortinet:** Meru - \$44m
- **Elbit Systems:** CyberBit
- **Bain Capital:** Blue Coat Systems - \$2.4Bn
- **BAE:** SilverSky - \$233m
- **Gemalto:** SafeNet - \$890m
- **Veritas:** Beyond Trust Software - \$310m
- **AVG:** Location Labs -\$220m
- **Singtel:** Trustwave - \$810m
- **GTT:** MegaPath-\$152m
- **IBM:** LightHouse Security
- **CISCO:** NeoHapsis

Venture Capital Investments

Cybersecurity Business: 2014-2015

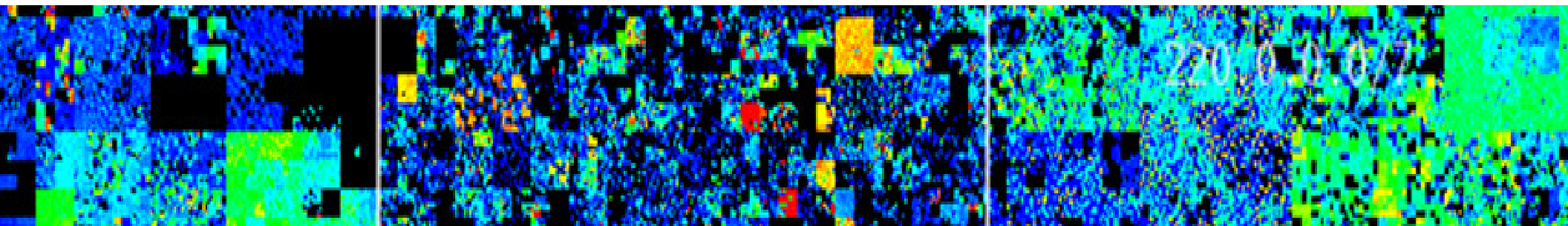
- **CrowdStrike:** \$100m
- **Cylance:** \$42m
- **Ziften:** \$24m
- **Checkmarx:** \$84m
- **Ionic Security:** \$140m
- **iSIGHT:** \$30m
- **DB Networks:** \$17m
- **ThreatStream:** \$22m
- **Darktrace:** \$18m
- **Illumio:** \$100m
- **Looking Glass:** \$20m
- **Ping Identity:** \$35m
- **Vector Nets:** \$25m
- **LookOut:** \$150m
- **vARMOUR:** \$21m
- **BitGlass:** \$25m
- **Skycure:** \$11m
- **Venafi:** \$39m

Around \$2Billion VC Funds Invested in *CyberSecurity Companies* – 2014/2015

21stC Cybersecurity Trends: 2015 - 2025



1 – Background: 21stC Security Landscape	2 – Cybersecurity: Players & Threats	3 – Cyber Market Structure, Size & Growth
4 – CSO: C-Suite Security Integration “Integrated”	5 – Scenario 2020: Internet of Things (IoT) “Adaptive”	6 – Scenario 2025: AI & Machine Learning “Intelligent”
7 – CyberSecurity Ventures (Old and New)	8 – Mergers, Acquisitions & VC Funds	9 – YOUR Action Plan for 21stC Cyber!....



CyberVision : 2015 - 2025

*** **21stC Cybersecurity Trends** ***
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

1990 <– 2015 –> 2040: *Next 25 Years*

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

.....Meet the Long Term Challenge of Deploying AI & Machine Learning Based Cybersecurity Tools across *YOUR Enterprise!*

10 Steps To Cyber Security



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

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

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

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

Maintain the Board's engagement with the cyber risk.

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

Establish an effective governance structure and determine your risk appetite.

Information Risk Management Regime

Produce supporting information risk management policies.

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

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

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

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

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



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

Link: www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

YOUR Action Plan for *Advanced “Cyber”*!

- **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) Cyber-Physical Operational Integration
 - b) IoT Security for both Legacy & New Assets
 - c) Training and Testing of AI-based “Cyber” Tools.

21stC Cybersecurity Trends



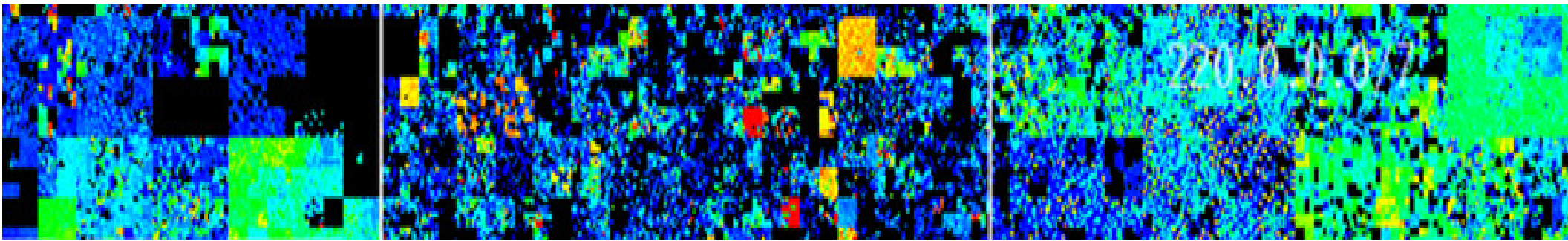
Thank you for your time!

21stC Cybersecurity Trends

"CyberVision: 2015-2025"



BACK-UP SLIDES



CyberVision : 2015 - 2025

***** 21stC Cybersecurity Trends *****
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

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

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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

“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>digitecbusiness12</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>digitecbusiness12</p>	 <p>Smart Solutions: "Master Class" – Part 3</p> <p>- Designing & Engineering Smart Solutions -</p> <p>Dr David E. Probert VAZA International</p> <p>digitecbusiness12</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>digitecbusiness12</p>	 <p>- Smart Sustainable Security -</p> <p>"Integrating Cyber & Physical Operations"</p> <p>Dr David E. Probert VAZA International</p> <p>digitecbusiness12</p>	 <p>- Smart Governance -</p> <p>"Stimulating Innovation & Economic Growth"</p> <p>Dr David E. Probert VAZA International</p> <p>digitecbusiness12</p>
"Armenia: Smart Economy"	"Armenia: Smart Sustainable Security"	"Armenia: Smart Governance"

Download: www.valentina.net/DigiTec2012/
CyberVision : 2015 - 2025

*** **21stC Cybersecurity Trends** ***
 London, UK :: 15th December 2015
 © 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 (Thrust SSC)** – 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 – Thrust SSC – for the World Speed Record.
- **Secure Wireless Networking** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.
- **Networked Enterprise Security** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional engineers & a diverse portfolio of hi-tech security products.
- **Republic of Georgia** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament.
- **UN/ITU** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

Dr David E. Probert is a Fellow of the **Royal Statistical Society**. He has a 1st Class Honours Degree in Mathematics (Bristol University) & PhD from **Cambridge University** in Self-Organising Systems (Evolution of Stochastic Automata), and his Full Professional Biography is featured in the Marquis Directory of **Who’s Who in the World: 2007-2016**.

CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***

London, UK :: 15th December 2015

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