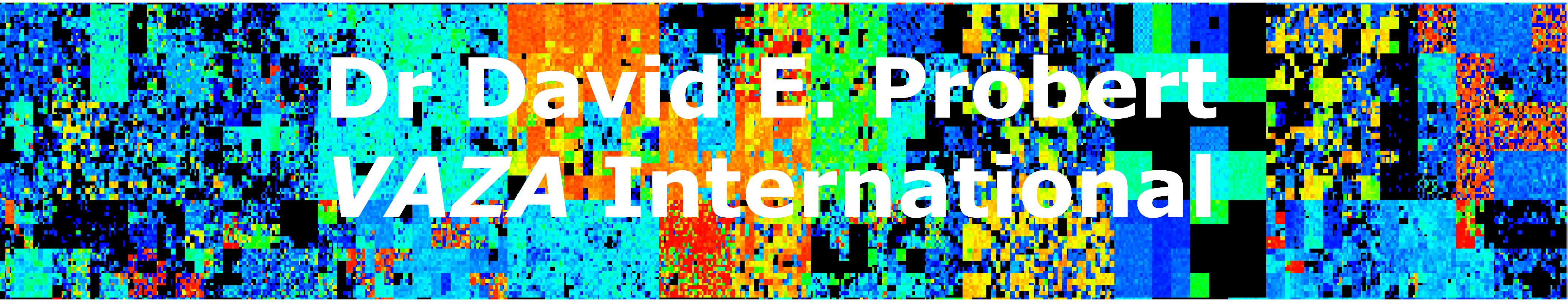
CyberSecurity Vision: ***2017 – 2027***



Dr David E. Probert

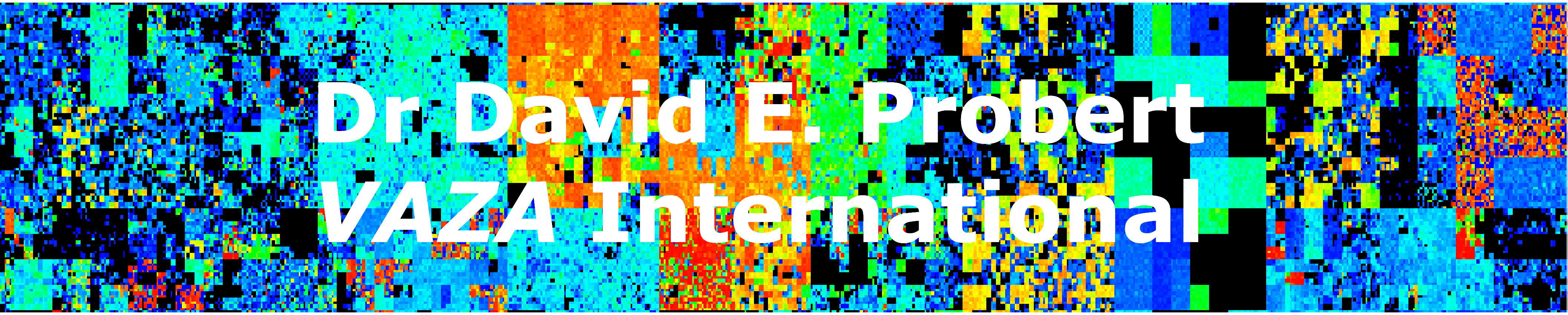
VAZA International

Dedicated to Grand-Sons: Ethan, Matthew, Roscoe & Hugh – *Securing YOUR Future!*

34th International East/West Security Conference

Видение Кибербезопасности

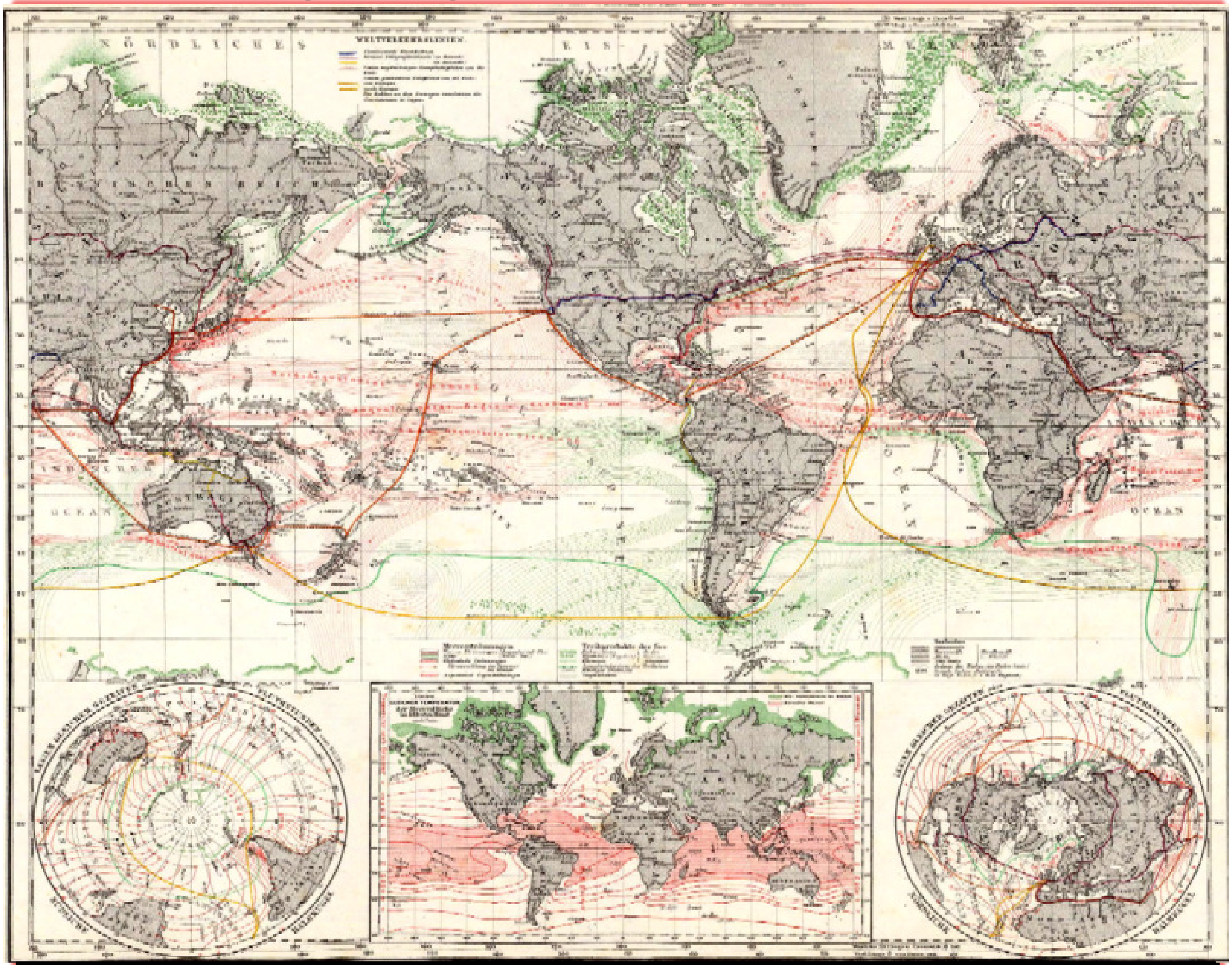
*** 2017 – 2027 ***



Dr David E. Probert

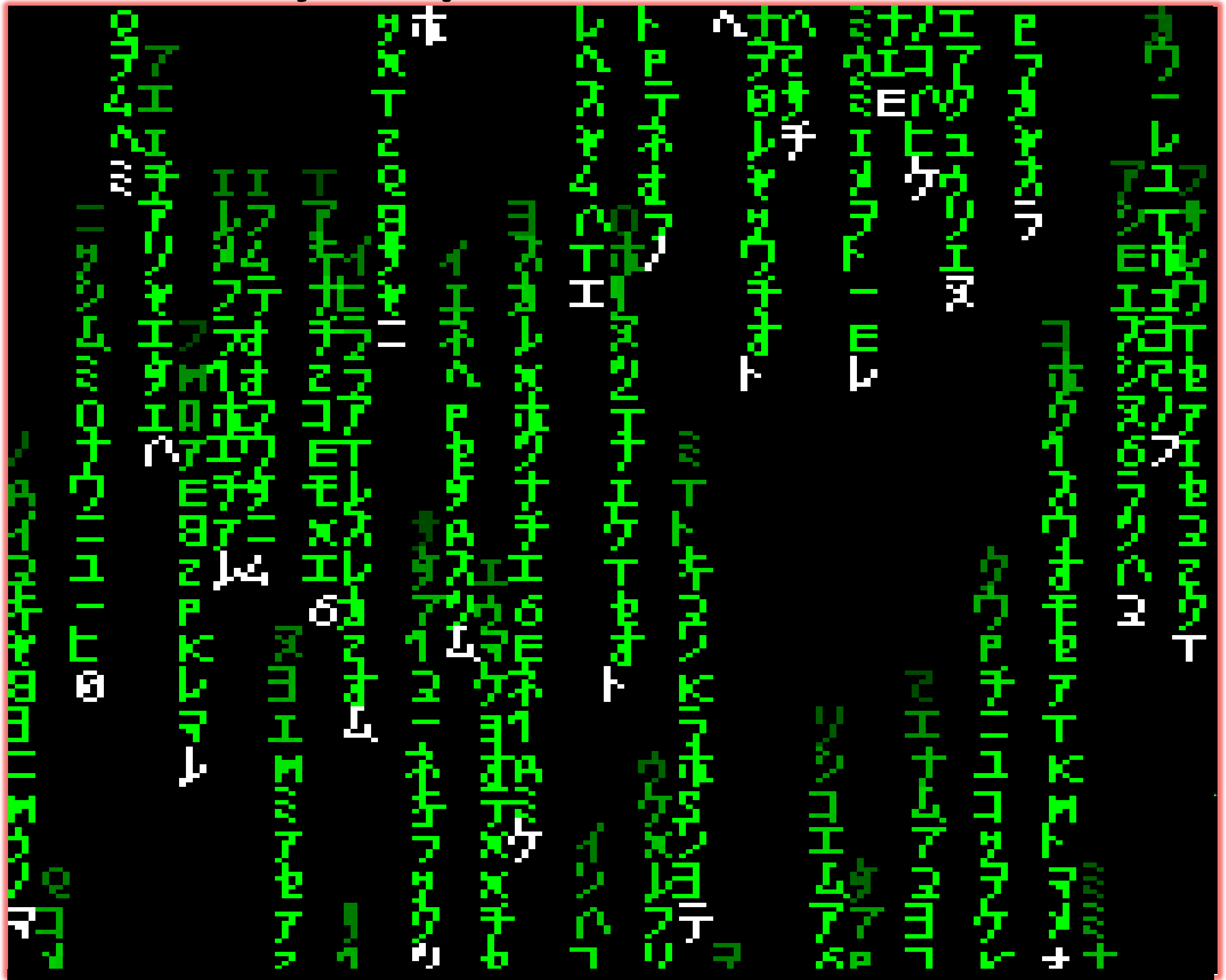
***VAZA* International**

"Visualisation of Cyberspace": *Global IP "WHOIS" Addresses*



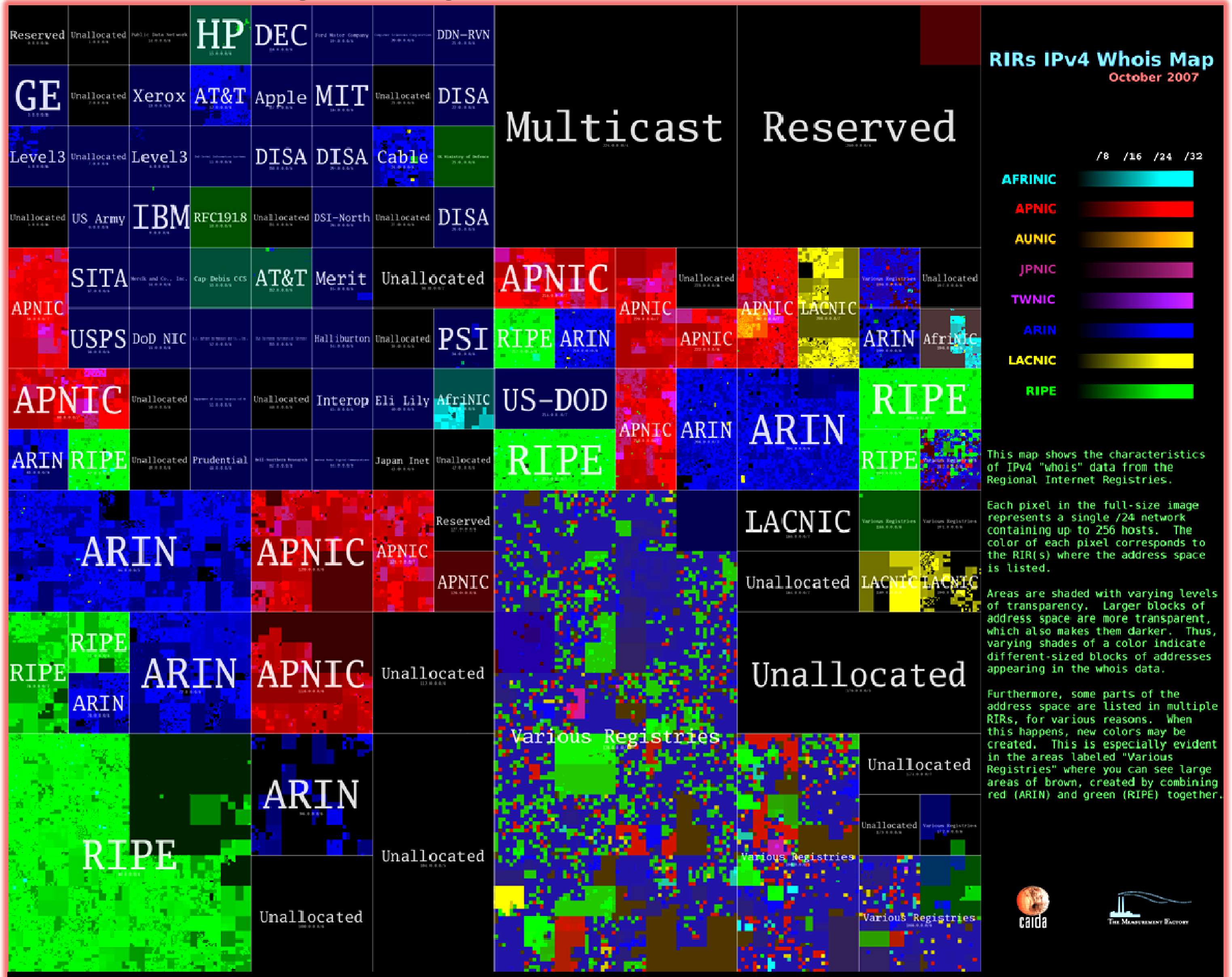
…From 19thC Physical World To 21stC Intelligent World

"Visualisation of Cyberspace": *Global IP "WHOIS" Addresses*



…From 19thC Physical World To 21stC Intelligent World

"Visualisation of Cyberspace": *Global IP "WHOIS" Addresses*



This map shows the characteristics of IPv4 "whois" data from the Regional Internet Registries.

Each pixel in the full-size image represents a single /24 network containing up to 256 hosts. The color of each pixel corresponds to the RIR(s) where the address space is listed.

Areas are shaded with varying levels of transparency. Larger blocks of address space are more transparent, which also makes them darker. Thus, varying shades of a color indicate different-sized blocks of addresses appearing in the whois data.

Furthermore, some parts of the address space are listed in multiple RIRs, for various reasons. When this happens, new colors may be created. This is especially evident in the areas labeled "Various Registries" where you can see large areas of brown, created by combining red (ARIN) and green (RIPE) together.

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

"Smart Cybersecurity": *Dual Themes*

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

"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

*"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 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

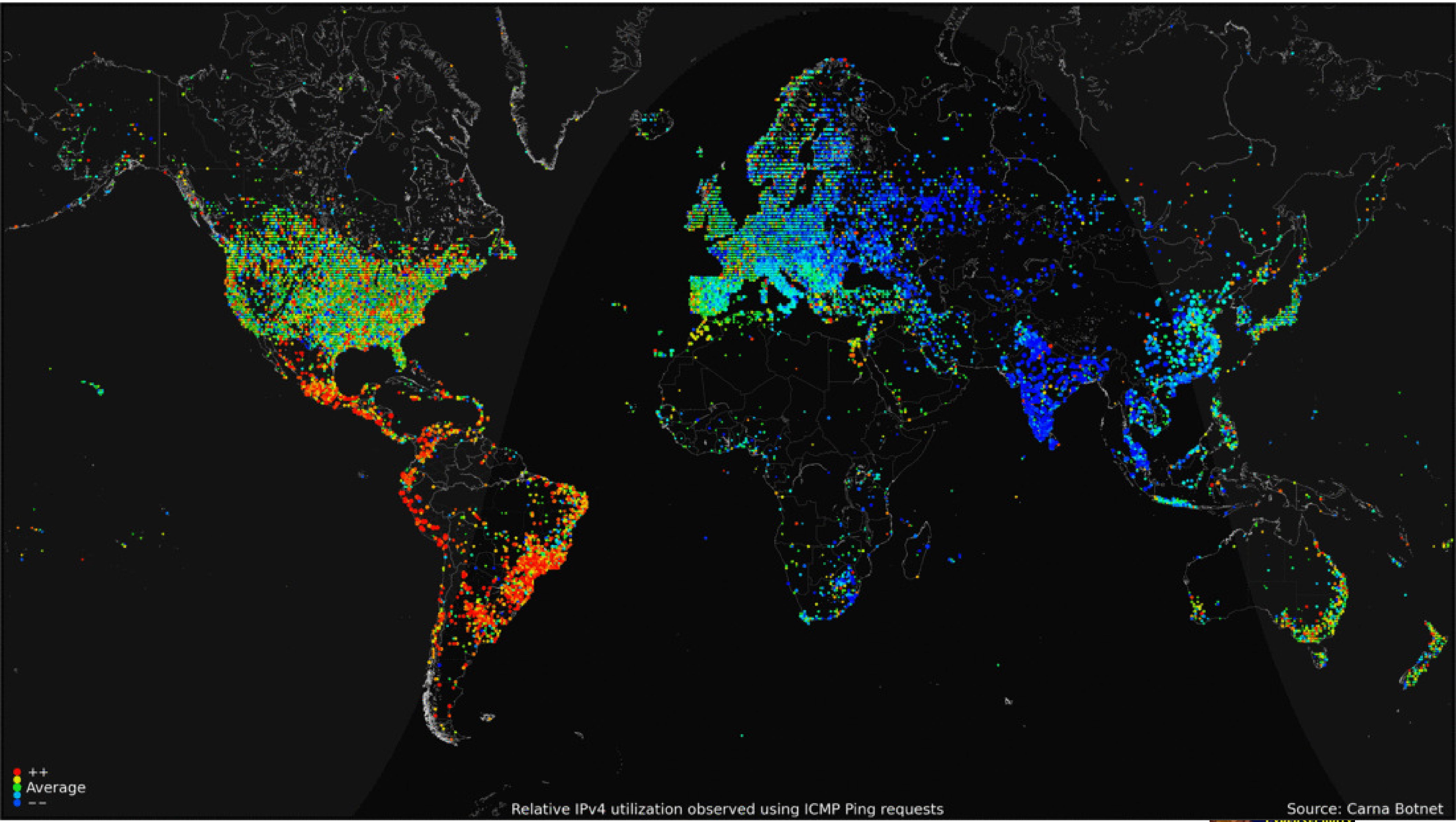
CyberSecurity is becoming transformed with Real-Time Cyber Tools based upon Artificial Intelligence & Machine Learning. These are ***Essential*** to win the war against CyberCrime and CyberTerrorism

"Intelligence": "ADAPTIVE Self-Learning CyberSecurity for IoT" ***09:00 22nd Nov 2016***

Download Slides: *www.valentina.net/Rome2016/*

GeoVision 24/7 Internet Connectivity

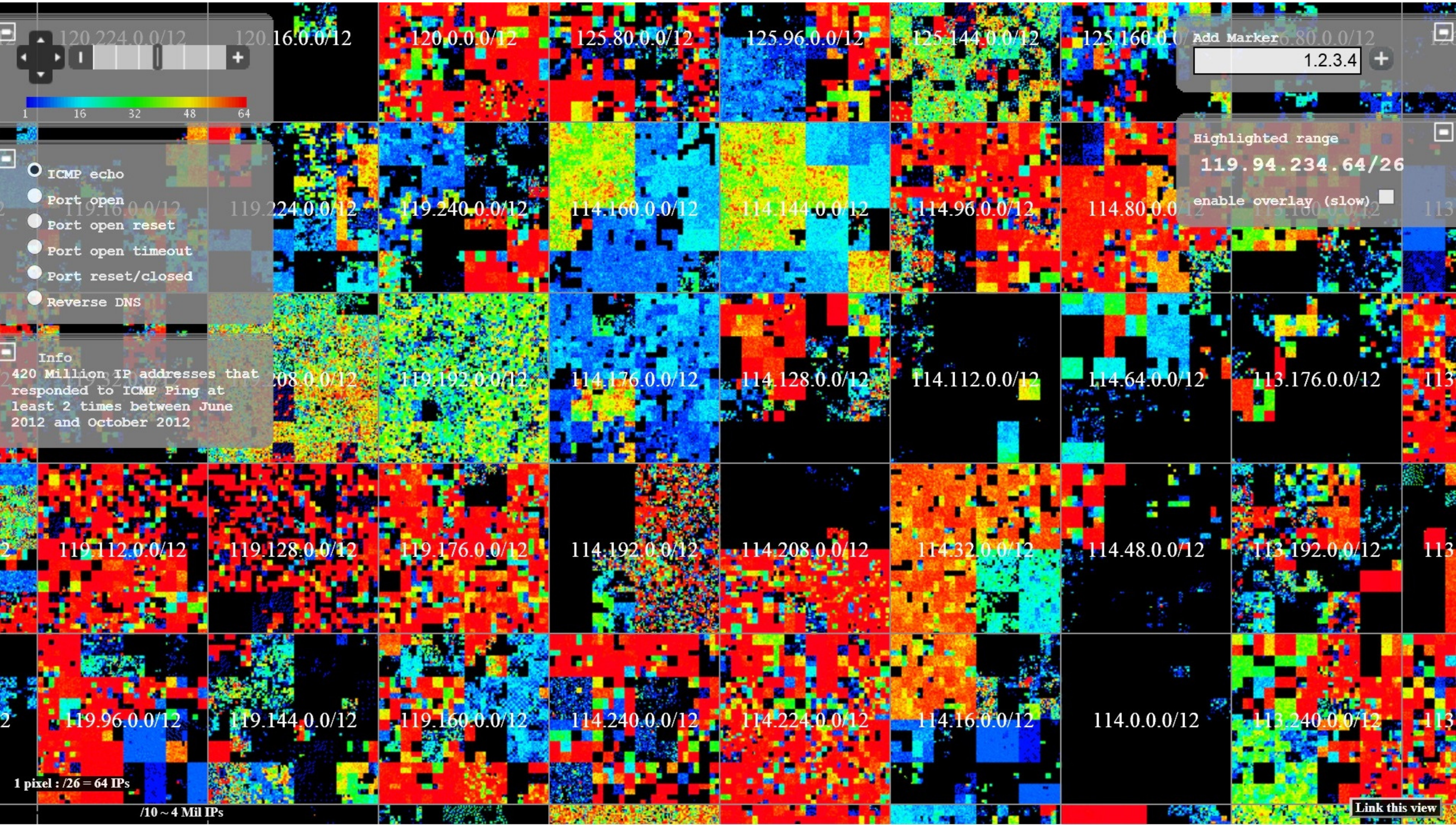
- “Worldwide Internet Census 2012” -



Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet

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



Add Marker

1.2.3.4

Highlighted range

119.94.234.64/26

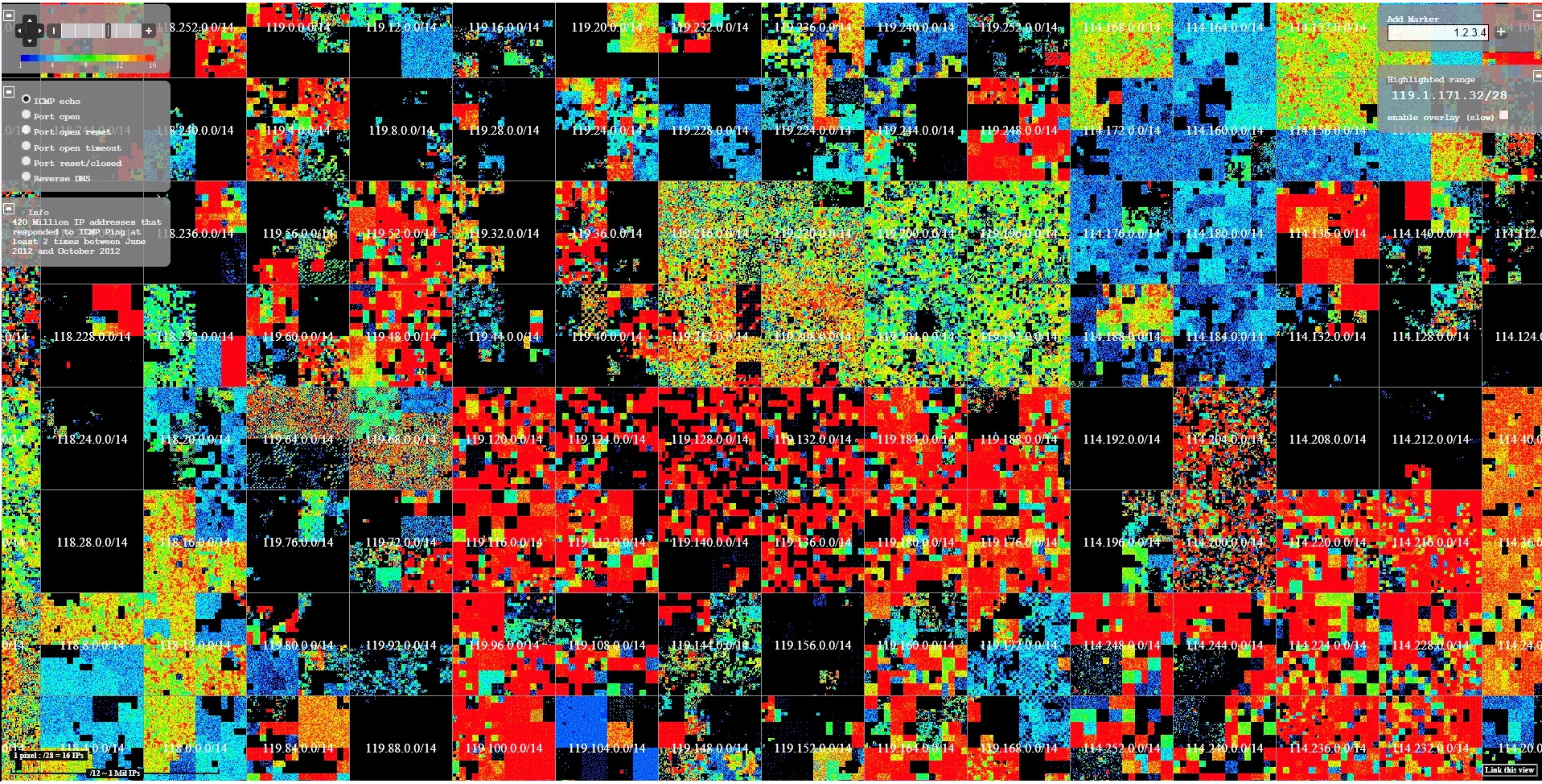
enable overlay (slow) □

● ICMP echo
○ Port open
○ Port open reset
○ Port open timeout
○ Port reset/closed
○ Reverse DNS

Info

420 Million IP addresses that responded to ICMP Ping at least 2 times between June 2012 and October 2012

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



● ICMP echo
○ Port open
○ Port open reset
○ Port open timeout
○ Port reset/closed
○ Reverse DNS

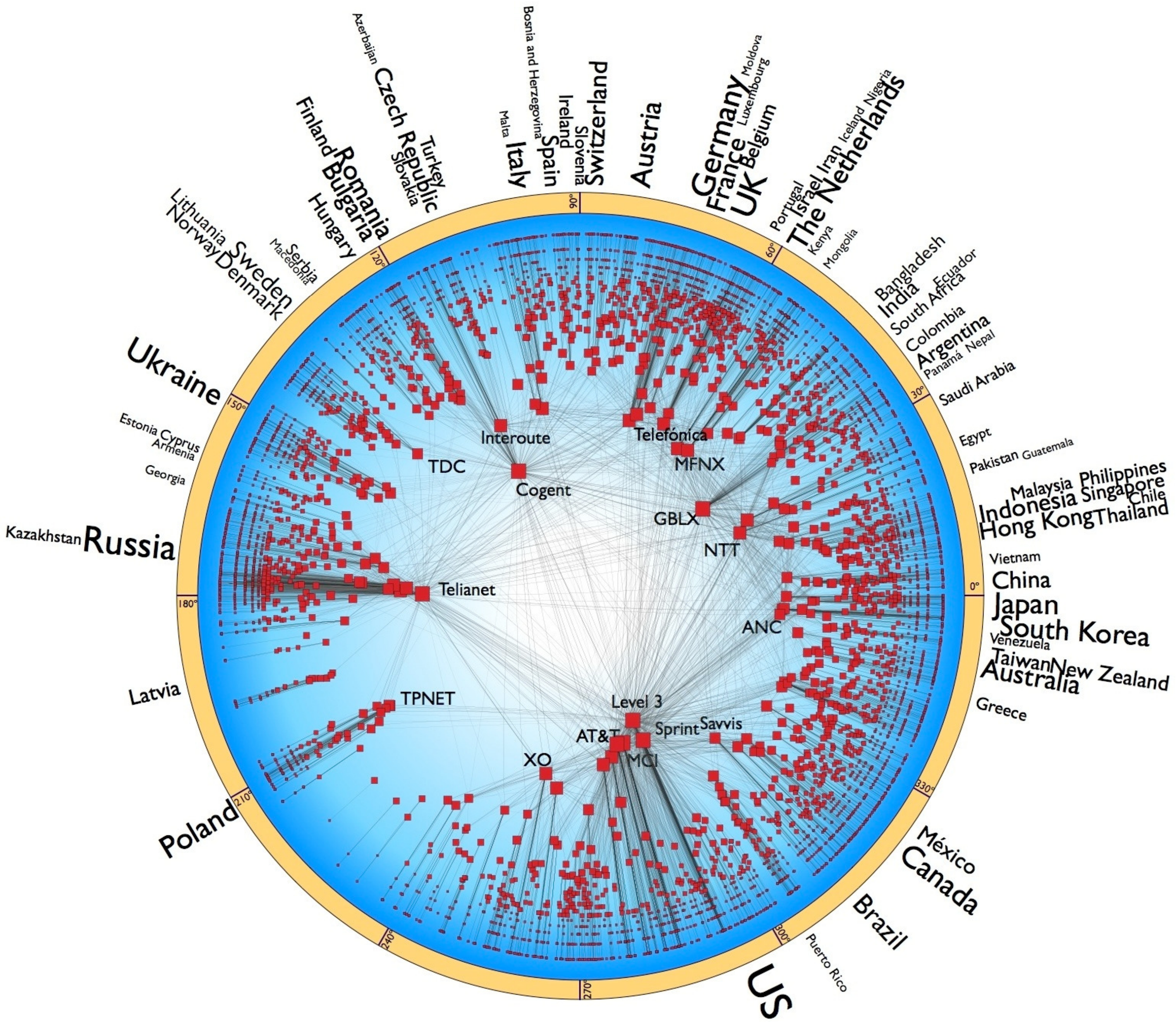
Info
420 Million IP addresses that responded to ICMP Ping at least 2 times between June 2012 and October 2012

Add Marker
1.2.3.4

Highlighted range
119.1.171.32/28

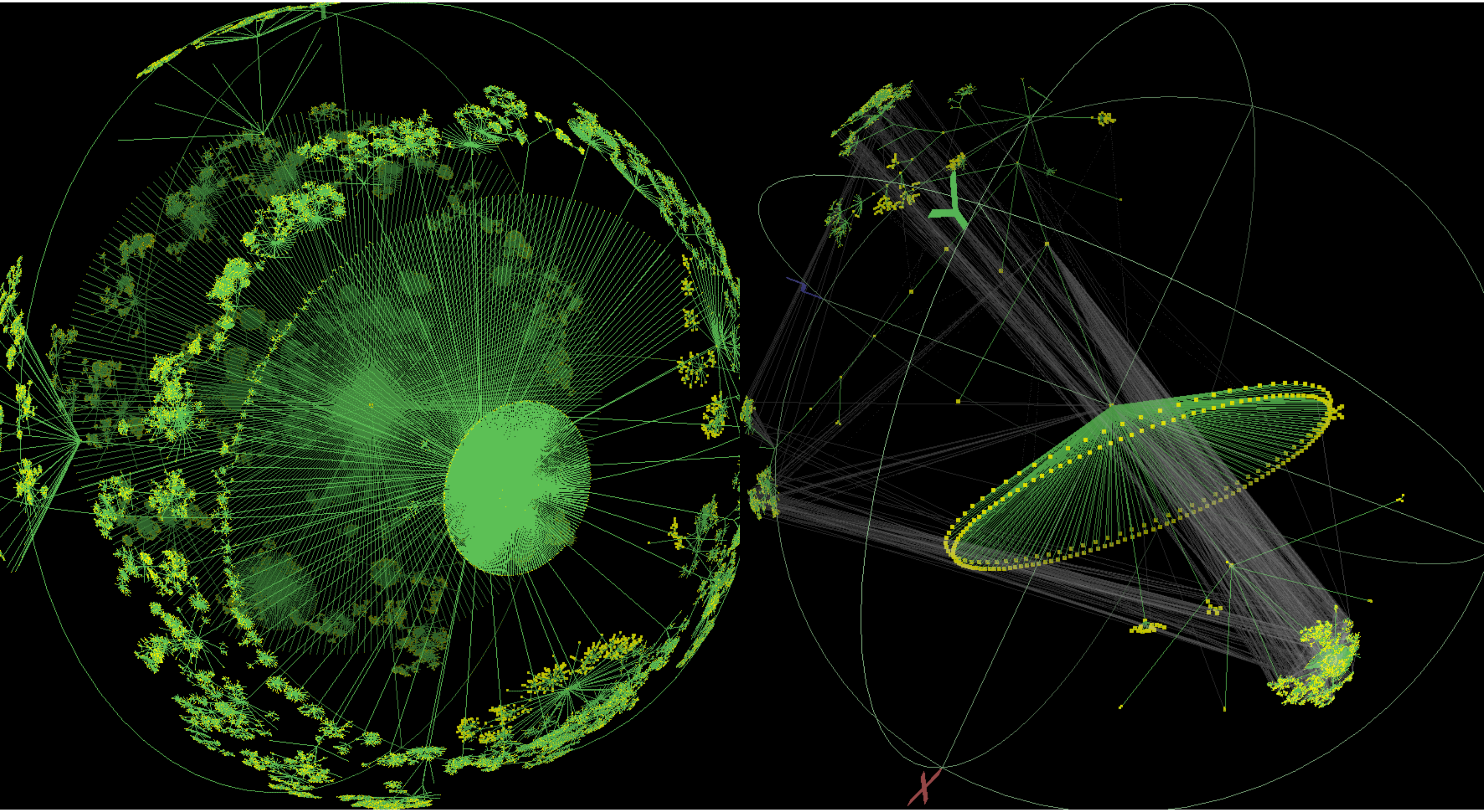
enable overlay (slow) □

Link: internetcensus2012.bitbucket.org/hilbert/



Worldwide Hyperbolic Map of ***Internet Connectivity*** **- Link: *www.CAIDA.org***

Worldwide *Hyperbolic Models* of Internet

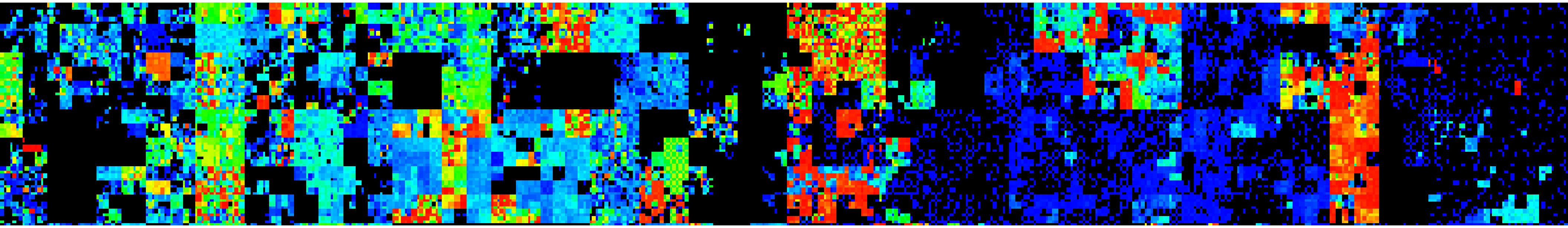


Link: www.CAIDA.org **:** *Center for Applied Internet Data Analysis*

- University of California - San Diego Supercomputer Center -

"CyberSecurity Vision": *2017–2027 & Beyond!*

1 –*"Cyber Crime, Cyber Terror & Cyber War"*	2 – CyberVision: 21stC Players & Threats	3 – CyberSecurity: 21stC Radical Innovation
4 – Scenario 2018 - CSO: C-Suite Integration **"Integrated"**	5 –Scenario 2020 – Internet of Things(IoT) **"Adaptive"**	6 – Scenario 2025 - AI & Machine Learning **"Intelligent"**
7 – In-Depth: Critical Sector Scenarios"	8–From CyberVision to Business Reality!	9 –*YOUR* Action Plan for 21stC Cyber!...



"CyberVision: 2017 – 2027"

- **My Vision:** My Personal "CyberVision" develops practical scenarios for the next 10-15 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: Pro-Active Real-Time Defence against Worldwide 24/7 Threats from *** Cyber Crime, Cyber Terrorism & Cyber Warfare ***

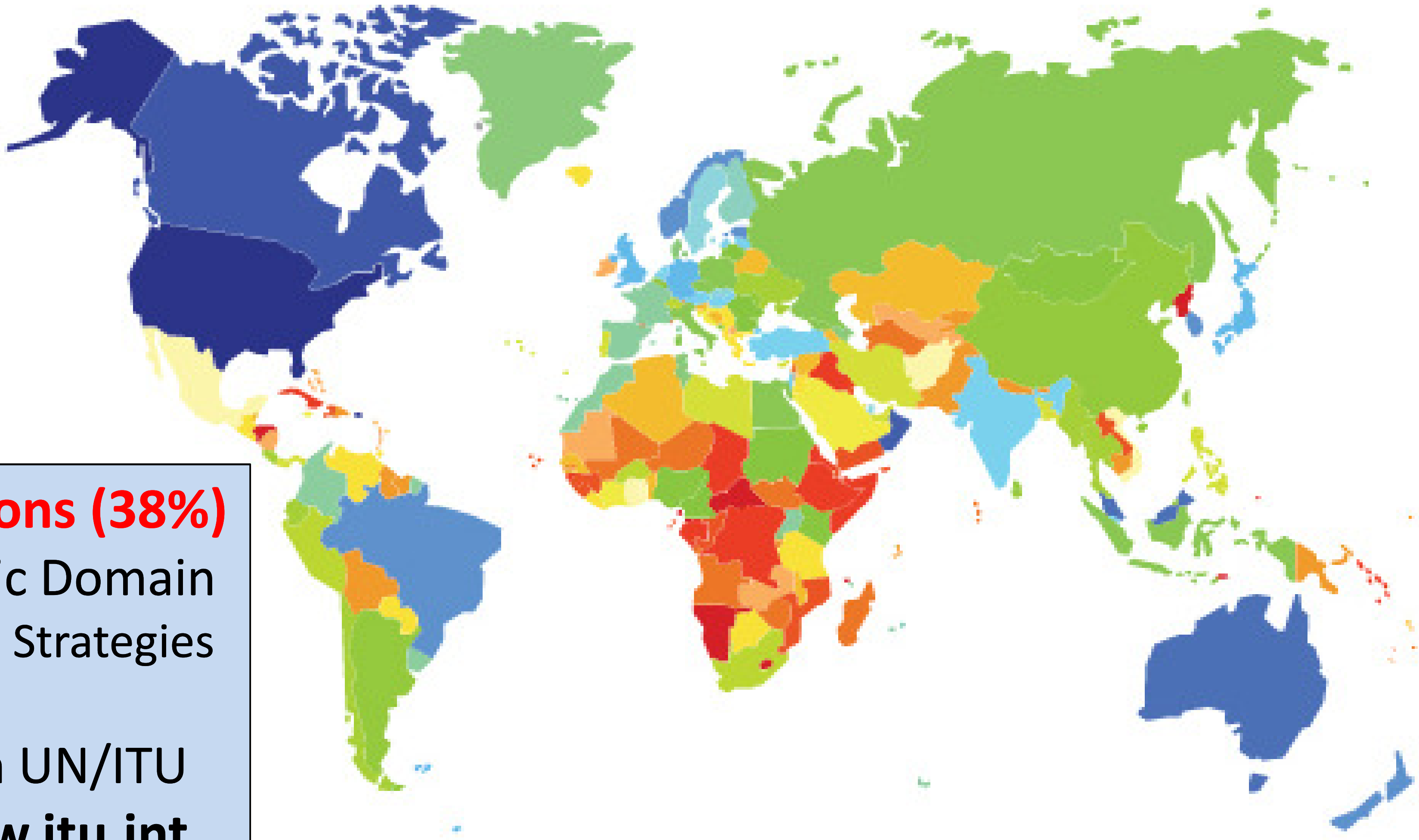
... *We need to fully embed Intelligent & Adaptive Cybersecurity within the **"Internet of Things"***

Cyber Crime, *Cyber* Terror & *Cyber* War!

- **21stC *Cyber* Security:** New security threats & attacks hit our media screens EVERY Day!
- **Hybrid *Cyber*-Physical:** The "Bad Guys" now exploit hybrid weapons with hybrid cyber-physical attacks on critical info infrastructure
- **25 Year *Cyber* Vision:** Business & Government need to Urgently deploy New Generation AI/ML Security Solutions to "Win" the "War"

Our *"**Cyber**Vision"* provides the basis for designing practical Strategies, Action Plans and Roadmaps to combat ***Cyber**Crime*, ***Cyber**Terror* & ***Cyber**War* for ***YOUR*** Business!

UN/ITU – Global Cybersecurity Index



Only 73 Nations (38%) Publish Public Domain CyberSecurity Strategies

Available on UN/ITU Website: **ww.itu.int**

ABIresearch

ITU

Global Cybersecurity Index

National Cybersecurity Commitment HIGHEST LOWEST

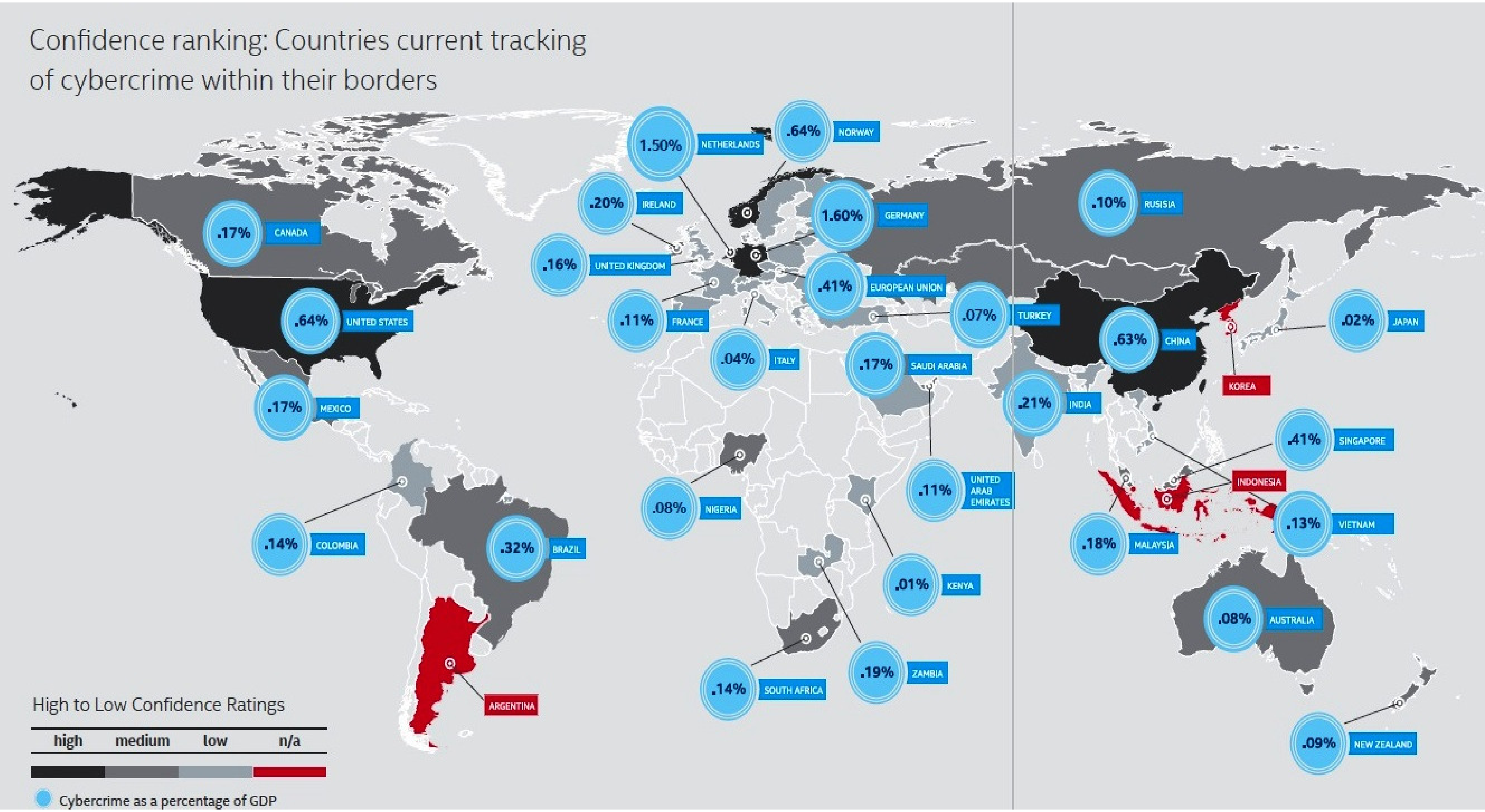
UN/ITU: National Cybersecurity Strategies

EGTI
Estratégia Geral de Tecnologia da Informação
2013 / 2015
SISP
Versão 1.0
Islamic Republic of Afghanistan
Ministry of Communications and IT
National Cyber Security Strategy of Afghanistan (NCSA)
Ministry of Defence
THE DEFENCE CYBER STRATEGY
NORWEGIAN MINISTRIES
Strategy
Cyber Security Strategy for Norway
SINGAPORE'S CYBERSECURITY STRATEGY
Federal Ministry of the Interior
Cyber Security Strategy for Germany
NATIONAL CYBER SECURITY STRATEGY
GOVERNMENT OF JAMAICA
وزارة الاتصالات وتقنية المعلومات
Ministry of Communications and Information Technology
Developing National Information Security Strategy for the Kingdom of Saudi Arabia
NISS, Draft 7
National Information Security Strategy
Gov
CYBER SECURITY
NATIONAL ICT STRATEGY AND PLAN NICI - 2015
THE DOD CYBER STRATEGY
THE DEPARTMENT OF DEFENSE

www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

World Economic Forum: Global CyberCrime

- $445Billion (Intel Research : June 2014) -



Confidence ranking: Countries current tracking of cybercrime within their borders

High to Low Confidence Ratings

high	medium	low	n/a
■	■	■	🟥

● Cybercrime as a percentage of GDP

World Economic Forum: Global CyberCrime

- $445Billion (Intel Research : June 2014) -

Net Losses:
Estimating the Global Cost of Cybercrime

Economic impact of cybercrime II

Center for Strategic and International Studies
June 2014

Confidence ranking: C
of cybercrime within t
.17%
CA
.17
.14
High to Low Confidence Ratings
high
medium
low
n
Cybercrime as a percentage of GDP
SISIA
.02%
JAPAN
CHINA
KOREA
.41%
SINGAPORE
INDONESIA
.13%
VIETNAM
YSIA
.08%
AUSTRALIA
.09%
NEW ZEALAND

World Economic Forum: Global CyberCrime

- $445Billion (Intel Research : June 2014) -

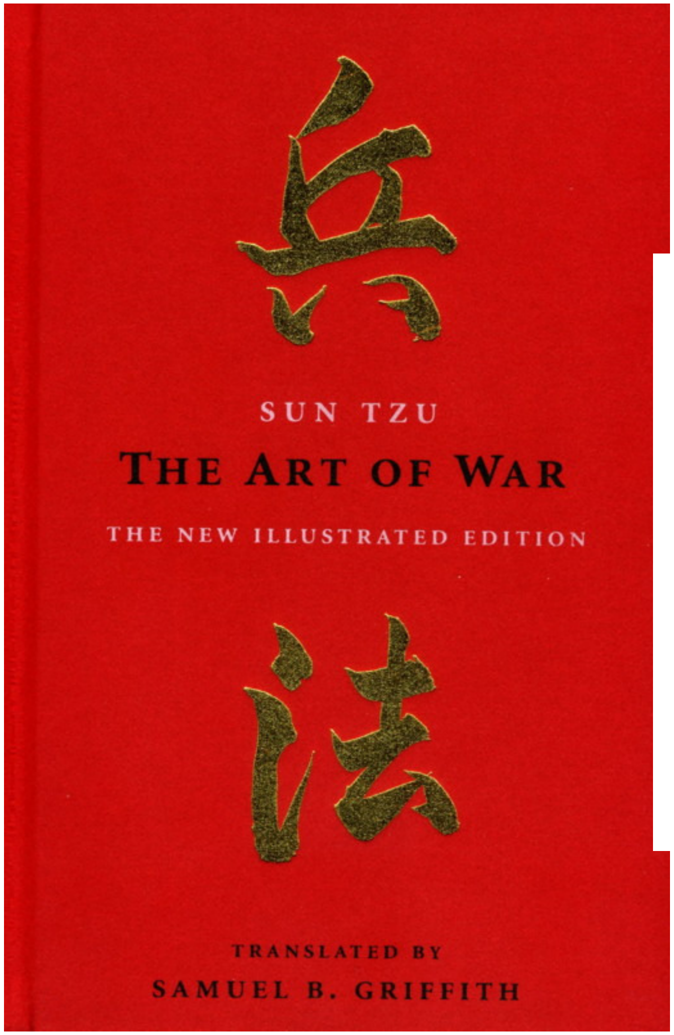
Red Alert!

– In-Coming Cyber Attack! –

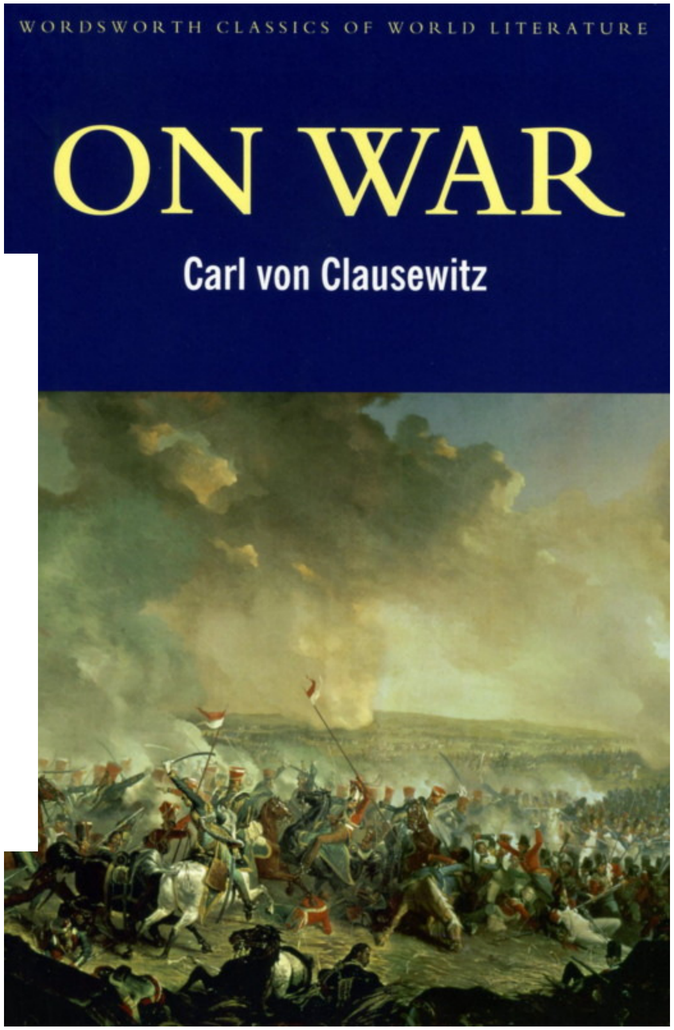
17th Nov 2015: "Islamic State is Plotting Deadly Cyber-Attacks": *George Osborne*

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

"CyberWar" Strategies & Models from *Classic Works*!

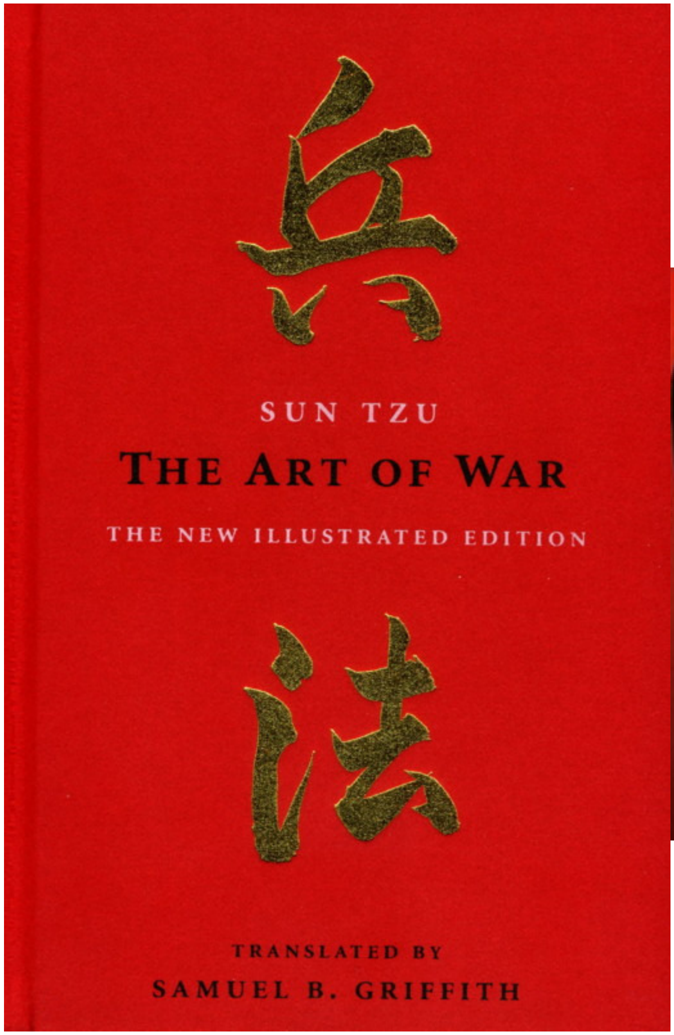


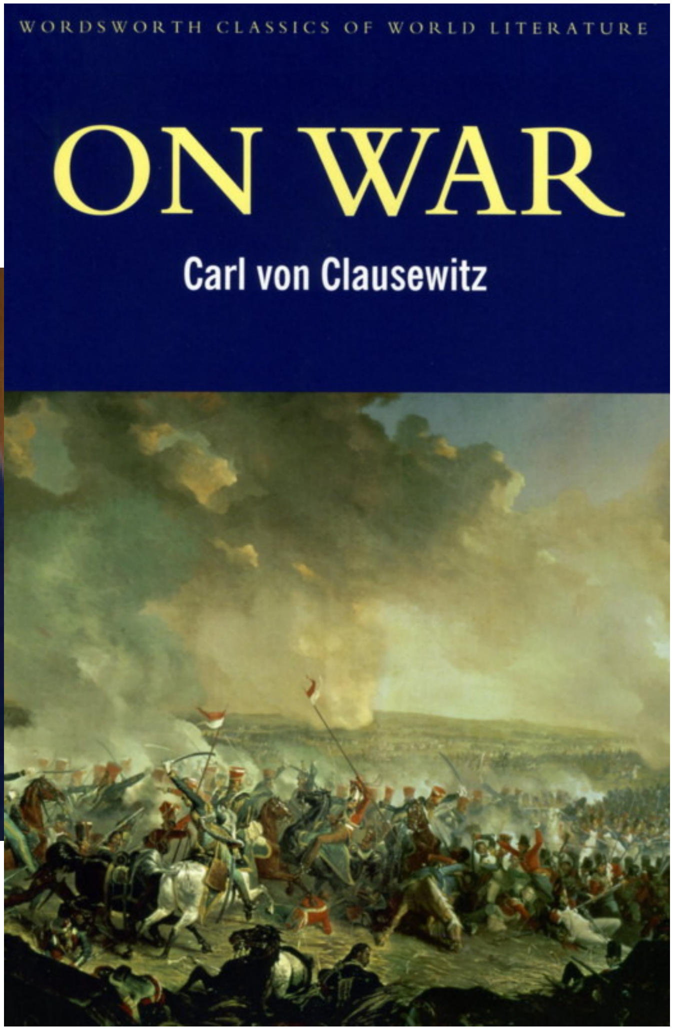
Recommended "Bedtime Reading" *for* Cybersecurity Specialists!



Classic Works on "War" are as relevant today for Cybersecurity as Pre-21stC!

"CyberWar" Strategies & Models from *Classic Works*!

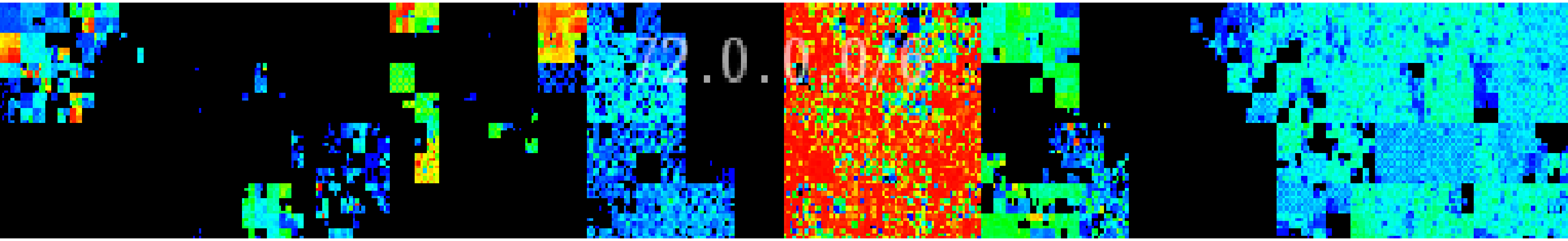




Classic Works on "War" are as relevant today for Cybersecurity as Pre-21stC!

“CyberSecurity Vision”: *2017–2027 & Beyond!*

1 – Cyber Crime, Cyber Terror & Cyber War	**2 – CyberVision: 21stC Players & Threats!**	3 – CyberSecurity: 21stC Radical Innovation
4 –Scenario 2018 - CSO: C-Suite Integration **“Integrated”**	5 –Scenario 2020 – Internet of Things(IoT) **“Adaptive”**	6 –Scenario 2025 - AI & Machine Learning **“Intelligent”**
7 – In-Depth: Critical Sector Scenarios“	8 – From CyberVision to Business Reality!	9 – YOUR TOP 10 Actions & RoadMap



CyberVision: *"21stC Players & Threats"*

- ***Cyber Criminals:*** Seeking commercial gain from hacking banks & financial institutions as well as phishing scams through Email, Social Media & Encryption *Ransom Ware*.
- ***Cyber Terrorists:*** Mission to penetrate & attack critical business assets, and *national infrastructure* for aims relating to *"political power", "shock"* & *"terror branding".*
- ***Cyber Espionage:*** Using stealthy IT "*Malware & Bots*" to penetrate both corporate & military data servers in order to obtain plans & intelligence.
- ***Cyber Hacktivists:*** Groups such as *"Anonymous"* with Political Agendas that hack sites & servers to virally communicate the "message" for specific campaigns.

...**ALL** these **"Bad Guys"** have access to IT/Computing Professionals , and launch attacks with **"Intelligent Bots"**, **"Self-modifying Malware"** & **Cyber Tools Kits**

21stC Cybersecurity *"Threats & Trends"*

- ***20 Year*** Evolution of Cyber Crime & Cyber Terror: ***1997-2017***

- ***"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"*

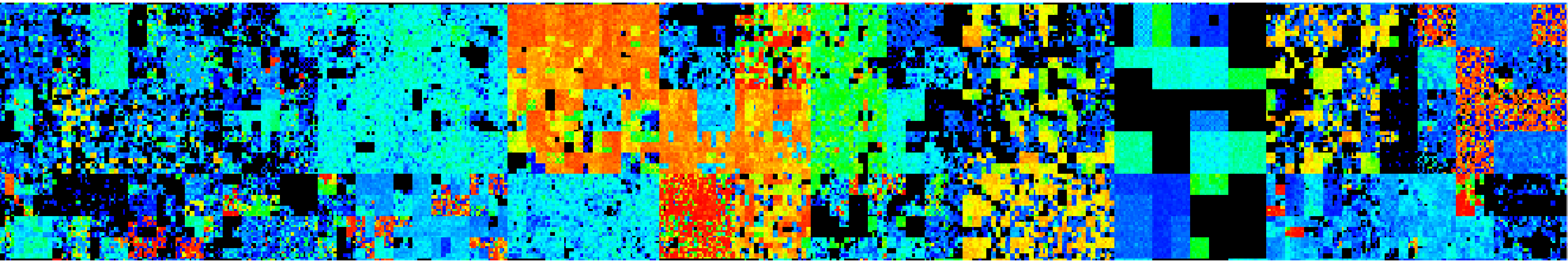
- ***20 Year*** Evolution of Cyber Crime & Cyber Terror: ***1997-2017***

.......and the "Bad Guys" are currently winning!

Image: **David Shankbone**: Occupy Wall Street – Sept 2011

“CyberSecurity Vision”: *2017–2027 & Beyond!*

1 – Cyber Crime, Cyber Terror & Cyber War	2 – CyberVision: 21stC Players & Threats	**3 – Cyber-Physical Threat Scenarios**
4 –Scenario 2018 - CSO: C-Suite Integration **“Integrated”**	5 –Scenario 2020 – Internet of Things(IoT) **“Adaptive”**	6 –Scenario 2025 - AI & Machine Learning **“Intelligent”**
7 – In-Depth: Critical Sector Scenarios“	8 – From CyberVision to Business Reality!	9 – YOUR TOP 10 Actions & RoadMap

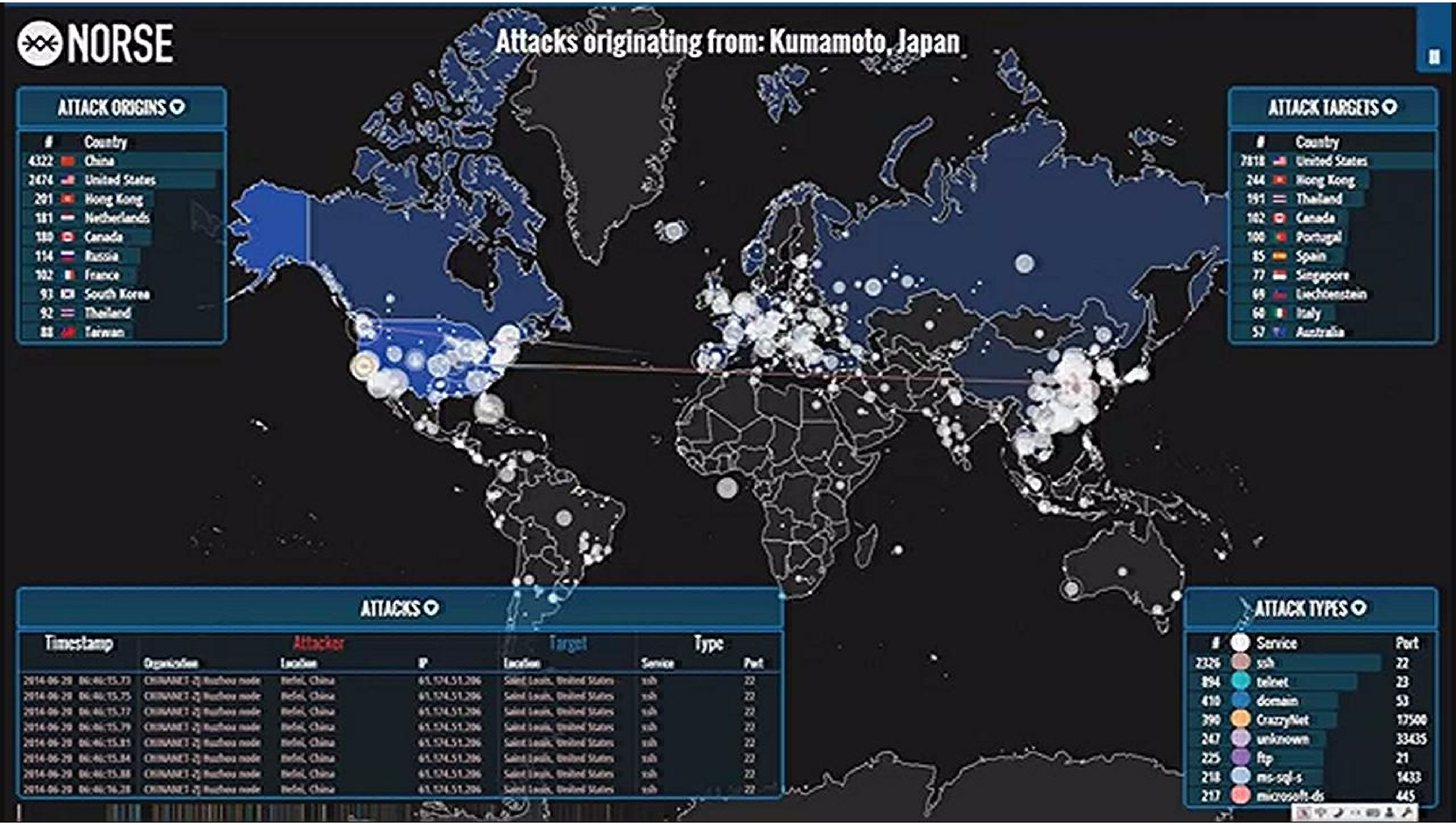


Cyber-Physical Threat Scenarios

- **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**

Global *“Real-Time”* DarkWeb CyberAttacks



ATTACK ORIGINS

#		Country
4322	🟥	China
2474		United States
201		Hong Kong
181		Netherlands
180		Canada
114		Russia
102		France
93		South Korea
92		Thailand
88		Taiwan

ATTACK TARGETS

#		Country
7818		United States
244		Hong Kong
191		Thailand
102		Canada
100		Portugal
85		Spain
77		Singapore
69		Liechtenstein
60		Italy
57		Australia

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-20 06:46:15.73	CHINANET-Zj Huzhou node	Hefei, China	61.174.51.206	Saint Louis, United States	ssh	22
2014-06-20 06:46:15.75	CHINANET-Zj Huzhou node	Hefei, China	61.174.51.206	Saint Louis, United States	ssh	22
2014-06-20 06:46:15.77	CHINANET-Zj Huzhou node	Hefei, China	61.174.51.206	Saint Louis, United States	ssh	22
2014-06-20 06:46:15.79	CHINANET-Zj Huzhou node	Hefei, China	61.174.51.206	Saint Louis, United States	ssh	22
2014-06-20 06:46:15.81	CHINANET-Zj Huzhou node	Hefei, China	61.174.51.206	Saint Louis, United States	ssh	22
2014-06-20 06:46:15.84	CHINANET-Zj Huzhou node	Hefei, China	61.174.51.206	Saint Louis, United States	ssh	22
2014-06-20 06:46:15.88	CHINANET-Zj Huzhou node	Hefei, China	61.174.51.206	Saint Louis, United States	ssh	22
2014-06-20 06:46:16.28	CHINANET-Zj Huzhou node	Hefei, China	61.174.51.206	Saint Louis, United States	ssh	22

ATTACK TYPES

#		Service	Port
2326	●	ssh	22
894	●	telnet	23
410	●	domain	53
390	●	CrazyNet	17500
247	●	unknown	33435
225	●	ftp	21
218	●	ms-sql-s	1433
217	●	microsoft-ds	445

Link: map.norsecorp.com - Norse Corporation

20th June 2014 : Global CyberAttacks @ *“Speed of Light”*

Typical C2 *Malware* Signatures

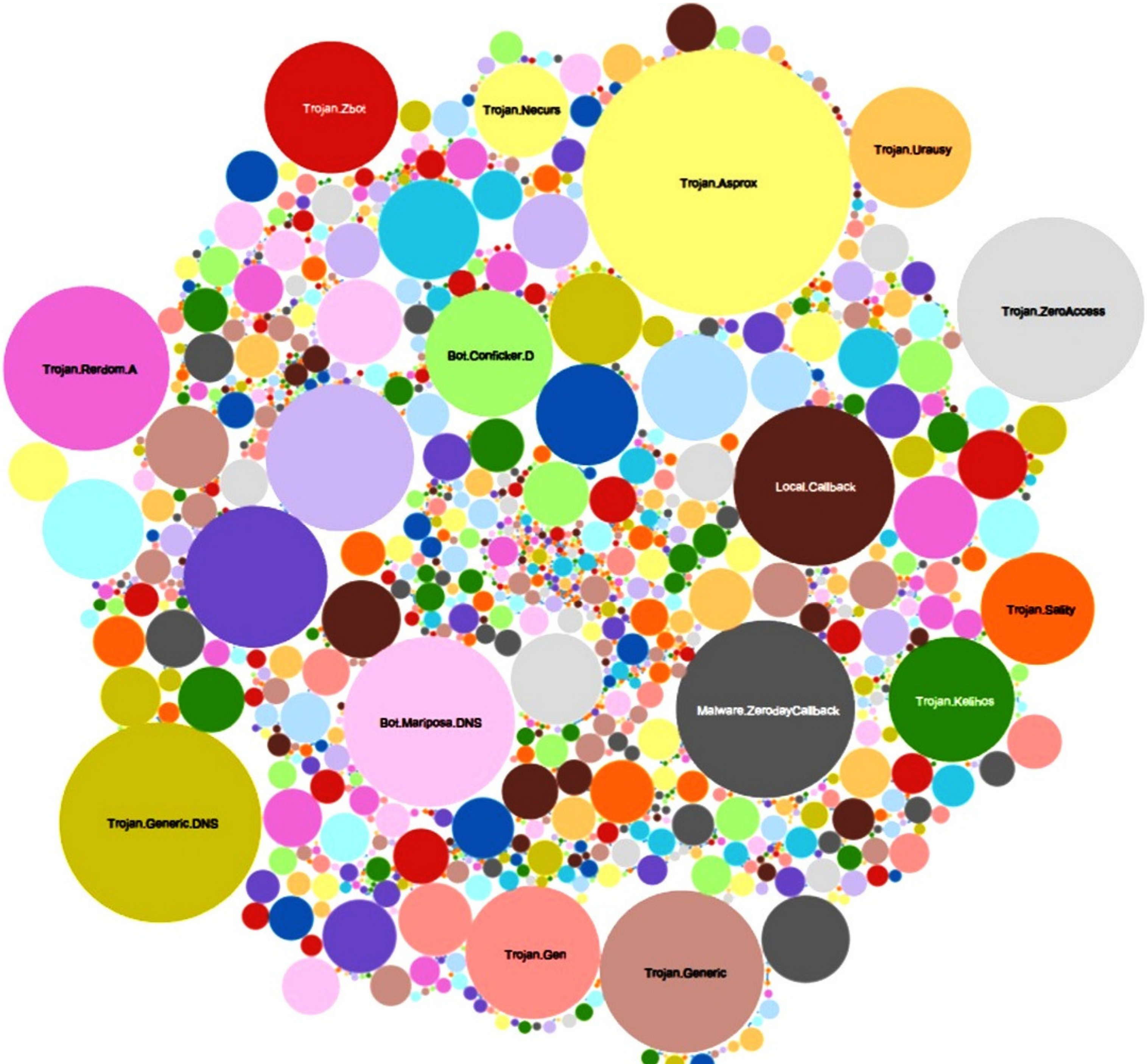


Image: www.fireeye.com – FireEye Inc (c)

2017-2027: Migration from IPv4 to IPv6

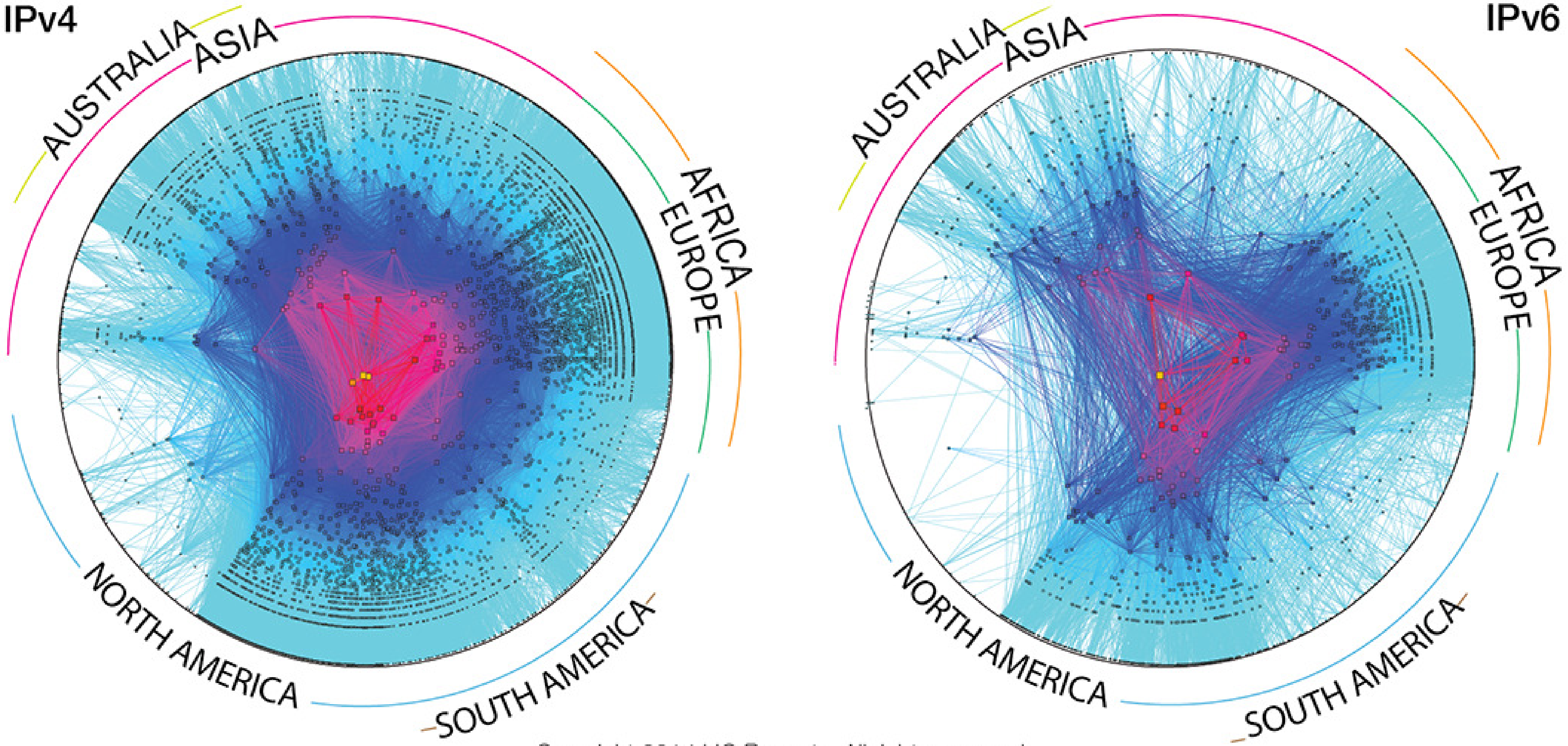
20thC – 1st Gen: IPv4 – 2^{32} = 10^{9}+ Devices (*IP Address Space almost fully assigned*)

21stC – 2nd Gen: IPv6 – 2^{128} = 10^{38}+ Devices (*Networking "Internet of Things – IoT"*)

- Expanded IP Address Space for "IoT" sets new "Cybersecurity Challenges"! -

WW Internet Connections – IPv4 & IPv6

CAIDA's IPv4 & IPv6 AS Core
AS-level INTERNET Graph
Archipelago January 2014

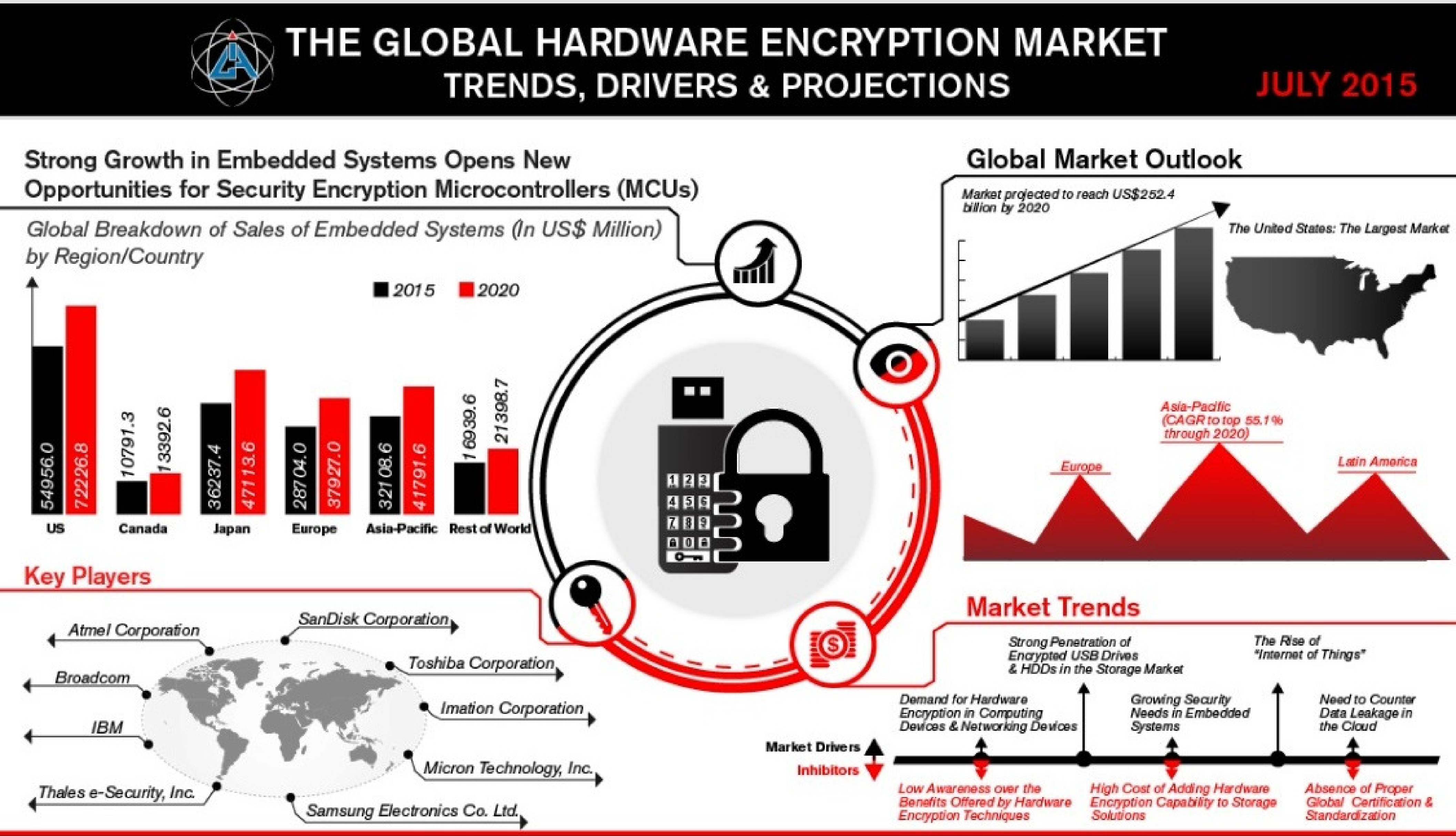


Copyright 2014 UC Regents. All rights reserved.

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



THE GLOBAL HARDWARE ENCRYPTION MARKET

TRENDS, DRIVERS & PROJECTIONS

JULY 2015

Strong Growth in Embedded Systems Opens New Opportunities for Security Encryption Microcontrollers (MCUs)

Global Breakdown of Sales of Embedded Systems (In US$ Million) by Region/Country

Global Market Outlook

Market projected to reach US$252.4 billion by 2020

The United States: The Largest Market

Key Players

Market Trends

Market Drivers
Inhibitors
Demand for Hardware Encryption in Computing Devices & Networking Devices
Strong Penetration of Encrypted USB Drives & HDDs in the Storage Market
Growing Security Needs in Embedded Systems
The Rise of "Internet of Things"
Need to Counter Data Leakage in the Cloud
Low Awareness over the Benefits Offered by Hardware Encryption Techniques
High Cost of Adding Hardware Encryption Capability to Storage Solutions
Absence of Proper Global Certification & Standardization

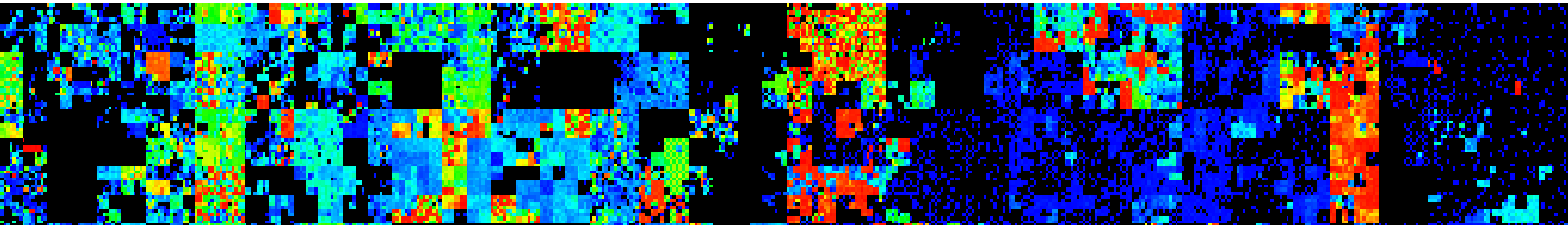
2020: Hardware Encrypted Systems - **$252 Bn - 55%** CAGR (Hard Disks, USB, Custom)

2020 : Software Encrypted Systems - **$6 Bn – 21%** CAGR (Cloud, Mobile, Database)

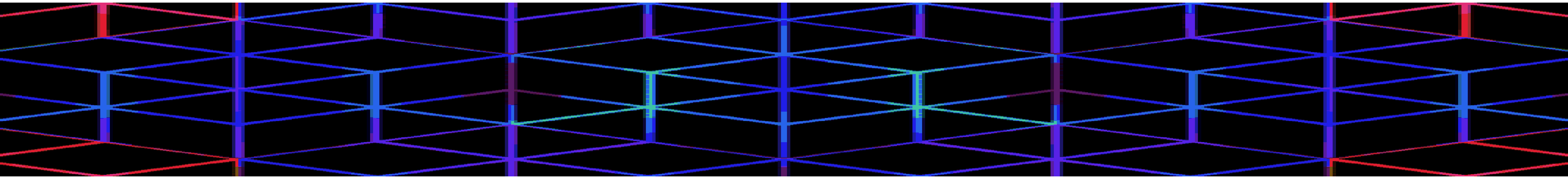
Source: (1) Global Industry Analysts Inc (H/W) – (2) Markets and Markets (S/W)

"CyberSecurity Vision": *2017–2027 & Beyond!*

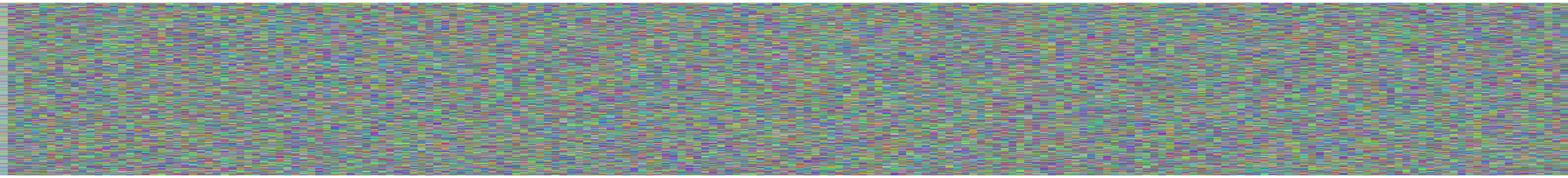
1 – Cyber Crime, Cyber Terror & Cyber War	2 – CyberVision: 21stC Players & Threats	3 – CyberSecurity: 21stC Radical Innovation
4 –Scenario 2018 – CSO: C-Suite Integration "Integrated"	5 –Scenario 2020 – Internet of Things(IoT) "Adaptive"	6 –Scenario 2025 - AI & Machine Learning "Intelligent"
7 –In-Depth: Critical Sector Scenarios"	8 – From CyberVision to Business Reality!	9 – YOUR TOP 10 Actions & RoadMap



Our CyberVision: *2017 to 2025*



- **Scenario 2018 – *Integrated Security*:** Managed "Smart" *Cyber* & *Physical* Operations under ***"CSO"***
- **Scenario 2020 – *Adaptive Security-IoT:*** Distributed "Smart Security" for networked ***"Internet of Things"***
- **Scenario 2025 – *Intelligent Security:*** Transition to Real-Time ***"AI/ML"*** Cybersecurity Tools & Solutions



Scenario 2018 – *CSO: C-Suite 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 - *"CSO - Chief Security Officer!"*
- **Investment Plan:** CSOs need full Professional Teams & Investment Budget to manage both Physical & Cyber security risks, threats and attacks!

.....Corporate Security now requires Strategic Management, Budget @ Board Director Level!

Cyber Integration with *Physical Security Operations*

- ***Cybersecurity*** for Government, Business & Critical Sectors can now be integrated with operational security solutions (PSIM&SIEM) 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"=Cyber+PSIM+SIEM

Key Cybersecurity Ventures - USA

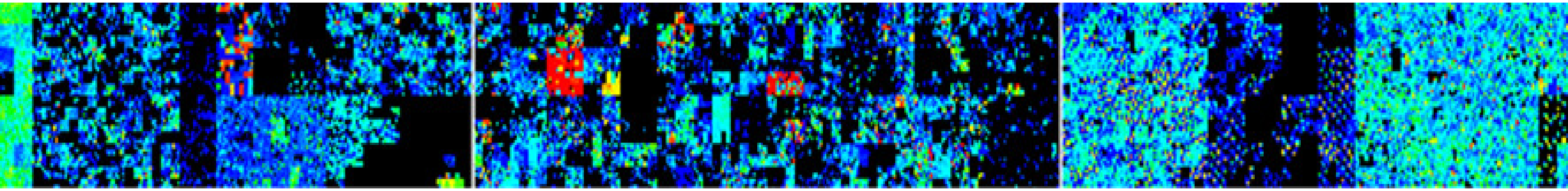
- **FireEye –** Next Generation Security
- **Norse –** In-Depth Real-Time Intel
- **Cylance –** AI/ML Threat Detection
- **DB Networks –** Real-Time ML Defence
  LanCope – Security Threat Intelligence
- **AlienVault –** Intelligent Security
- **RSA –** Big Data & Cloud Security
- **VeraCode –** Secure Code Analytics
- **Palo Alto Networks –** Next Gen Cyber
- **Resilient Systems –** Auto Threat Alert
- **Prelert –** Machine Learning Solutions
- **Barracuda Networks** – Firewalls+

- **Palantir** –Analytics & Fraud
- **Daon** – Biometics & 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

"CyberSecurity Vision": *2017–2027 & Beyond!*

1 – Cyber Crime, Cyber Terror & Cyber War	2 – CyberVision: 21stC Players & Threats	3 – CyberSecurity: 21stC Radical Innovation
4 –Scenario 2018 - CSO: C-Suite Integration "Integrated"	5 –Scenario 2020 – Internet of Things(IoT) "Adaptive"	6 –Scenario 2025 - AI & Machine Learning "Intelligent"
7 –In-Depth: Critical Sector Scenarios"	8 – From CyberVision to Business Reality!	9 – YOUR TOP 10 Actions & RoadMap



Scenario 2020: *"Internet of Things"*

- **Cyber-Enterprise:** During the next 3-5 years of Cyber Evolution, the Internet will extend to practically ALL our IT enabled devices within *Cars, Homes, Business, and Cities*! This is defined as the "Internet of Things - IoT"

- **Extended Security:** ALL IoT connected devices, nodes & servers (*Legacy & New*) must be secured against attack!

- **CSO Challenge:** The IoT is *already* the next 21stC Cyber Conflict Zone and Security Challenge for Enterprise CSOs!

.... ***Cyber DDoS Attacks*** *(Mirai BotNet on DYN Inc)* during Sept/Oct 2016 demonstrate the *Vulnerability* of "IoT"

Internet of Things: *Phases of Evolution*

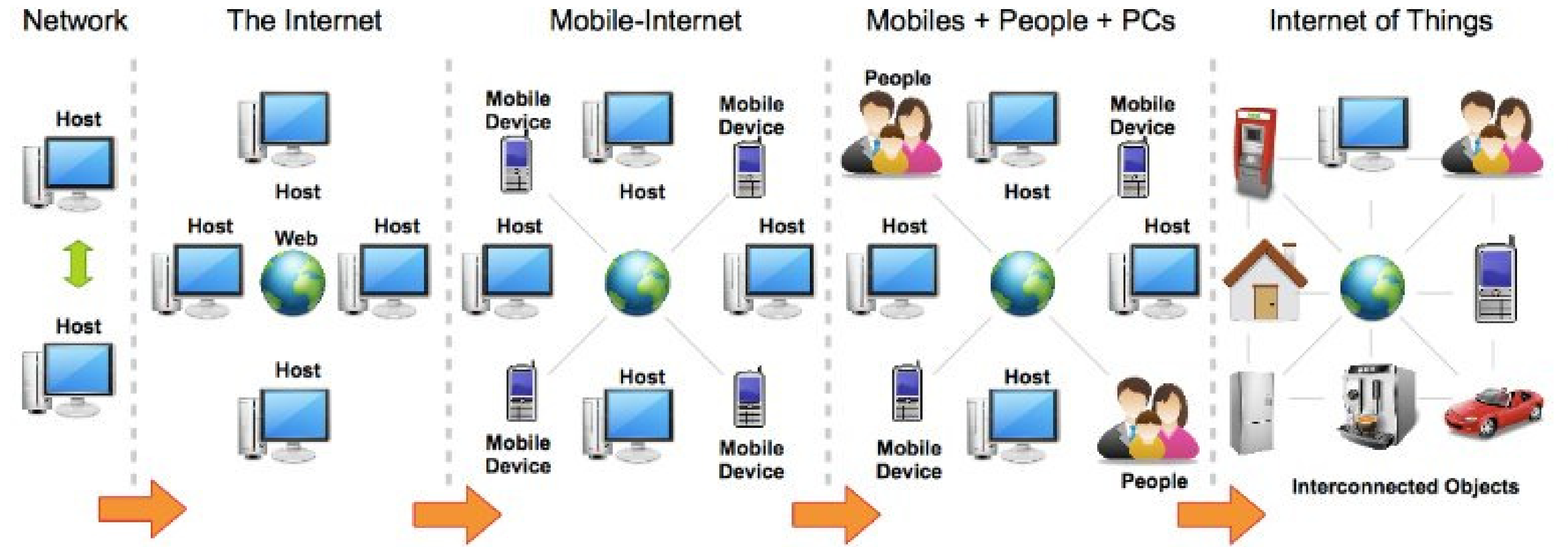
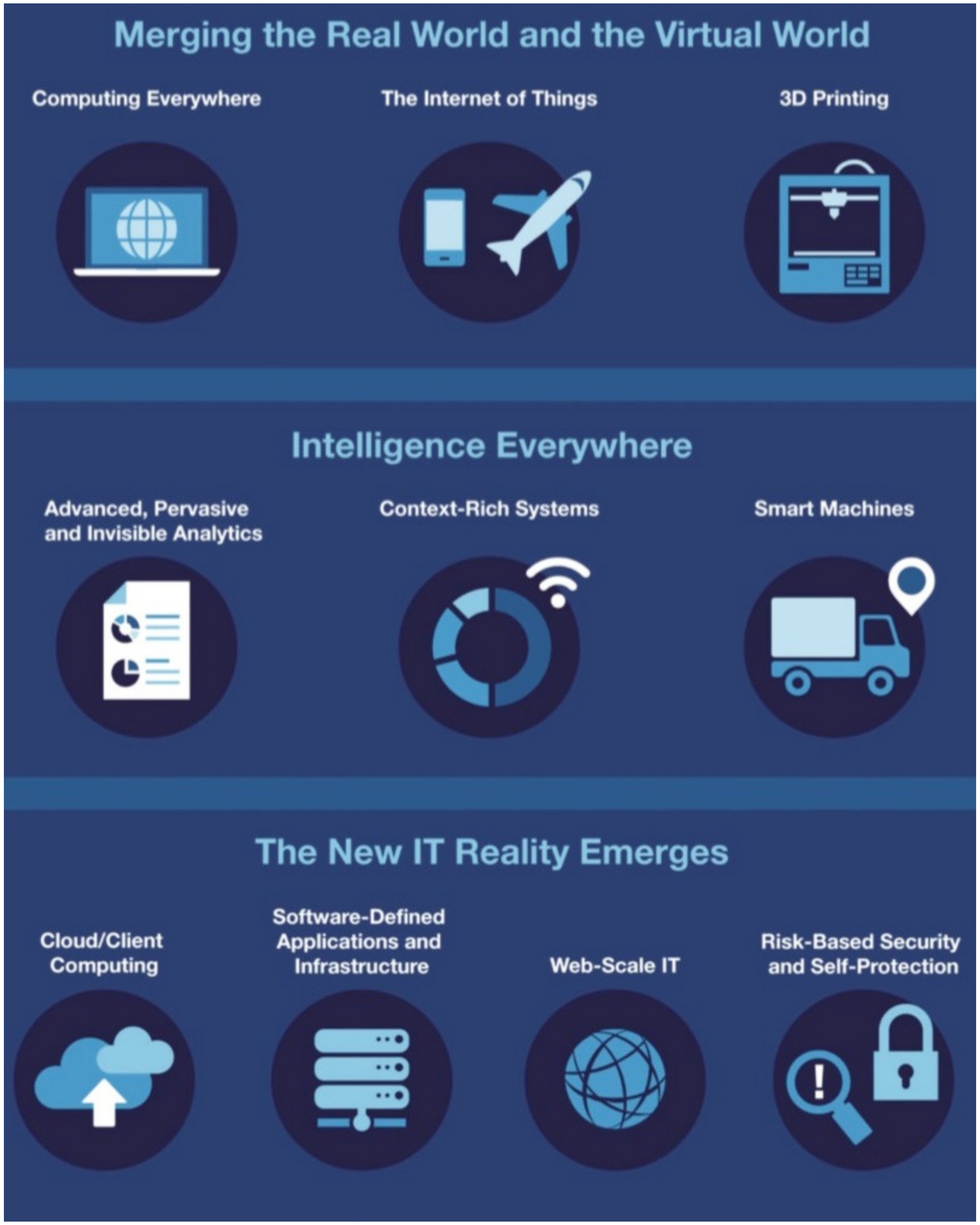
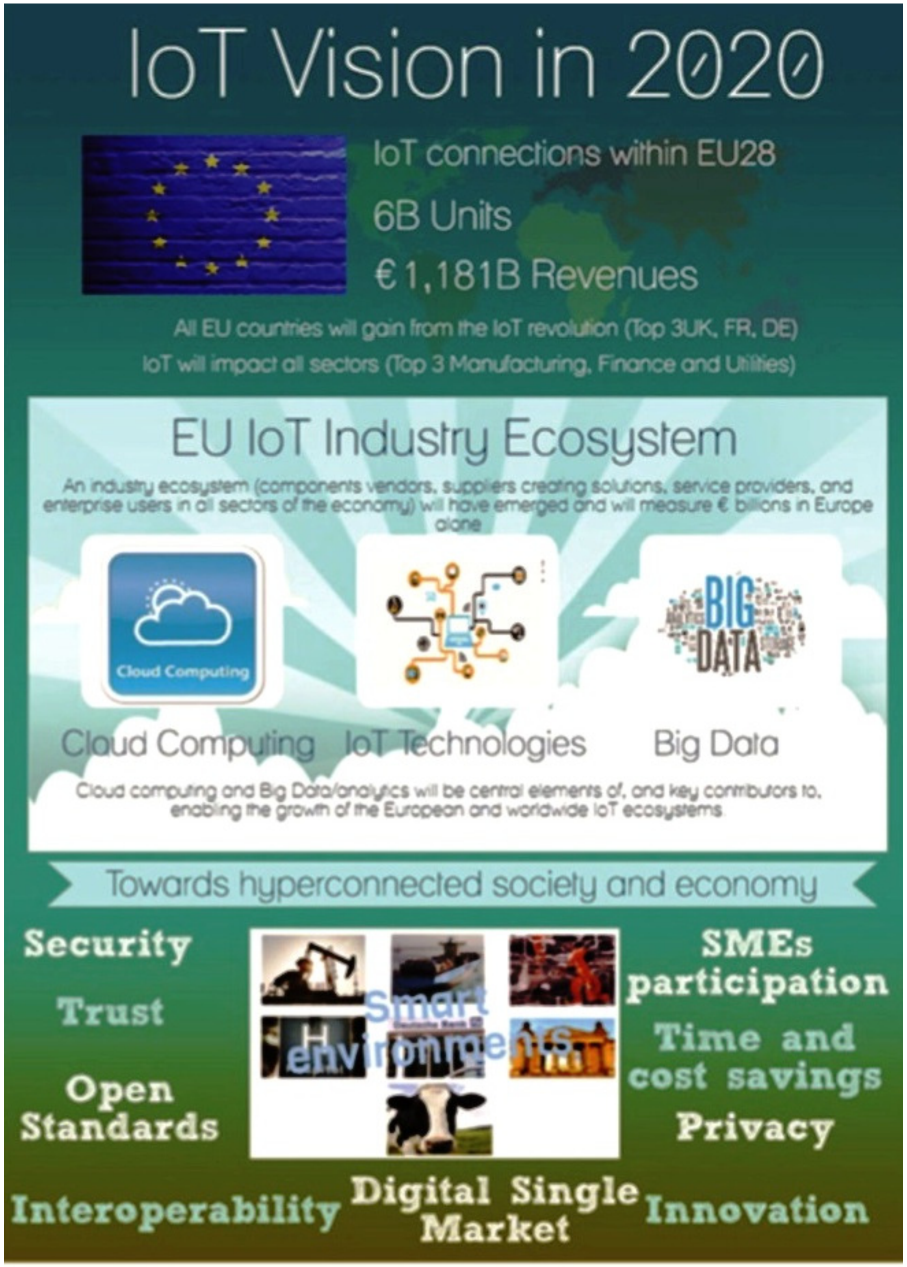


Fig. 1. Evolution of the Internet in five phases. The evolution of Internet begins with connecting two computers together and then moved towards creating World Wide Web by connecting large number of computers together. The mobile-Internet emerged by connecting mobile devices to the Internet. Then, peoples'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

EU "IoT" Programme Visions for "NOW" & 2020


Merging the Real World and the Virtual World
Computing Everywhere
The Internet of Things
3D Printing
Intelligence Everywhere
Advanced, Pervasive and Invisible Analytics
Context-Rich Systems
Smart Machines
The New IT Reality Emerges
Cloud/Client Computing
Software-Defined Applications and Infrastructure
Web-Scale IT
Risk-Based Security and Self-Protection



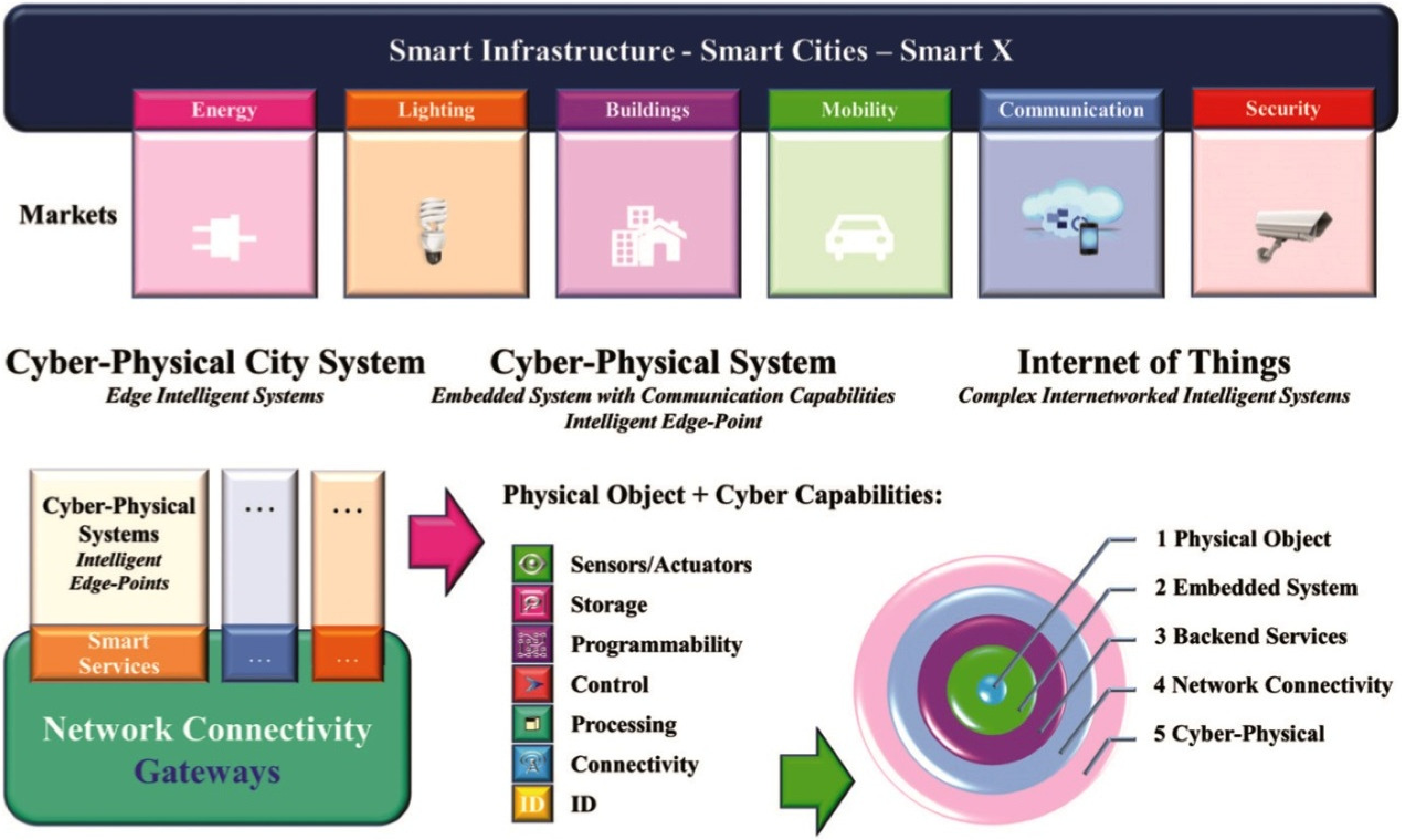
All EU countries will gain from the IoT revolution (Top 3UK, FR, DE)

IoT will impact all sectors (Top 3 Manufacturing, Finance and Utilities)

An industry ecosystem (components vendors, suppliers creating solutions, service providers, and enterprise users in all sectors of the economy) will have emerged and will measure € billions in Europe alone

Cloud computing and Big Data/analytics will be central elements of, and key contributors to, enabling the growth of the European and worldwide IoT ecosystems.

Cyber-Physical Systems as Basis of *"IoT"*



Smart Infrastructure - Smart Cities – Smart X

Markets

Energy	Lighting	Buildings	Mobility	Communication	Security

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

Cyber-Physical Systems *Intelligent Edge-Points*

Smart Services

...

Network Connectivity

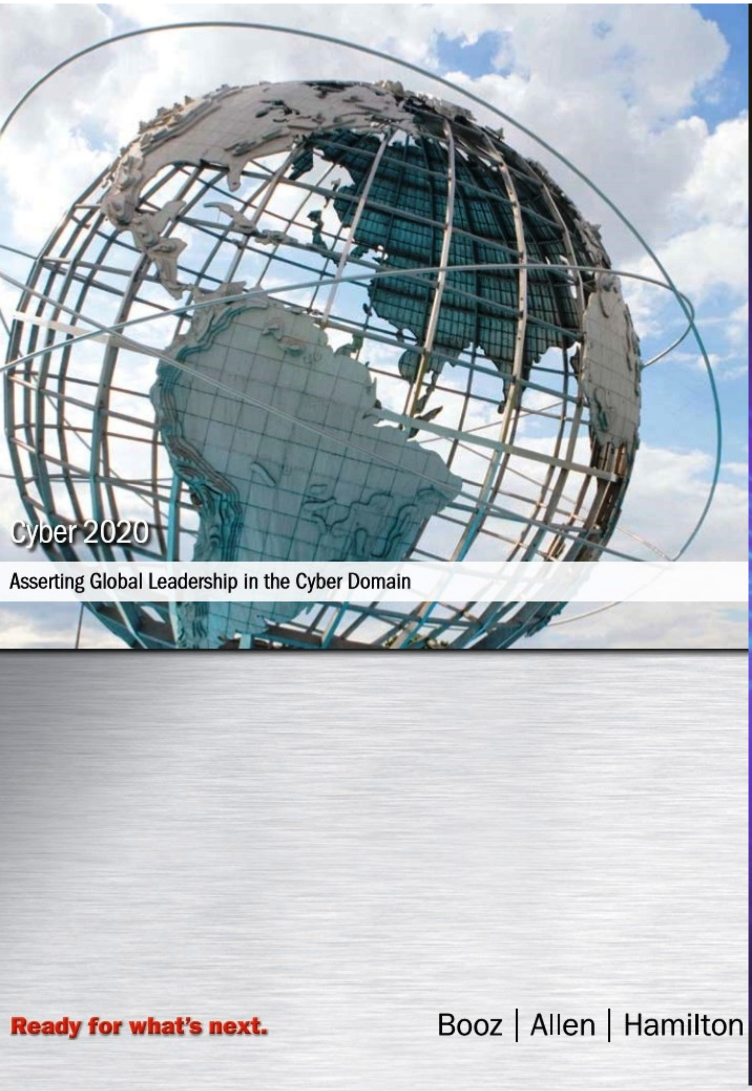
Gateways

Physical Object + Cyber Capabilities:

- Sensors/Actuators
- Storage
- Programmability
- Control
- Processing
- Connectivity
- ID

1 Physical Object
2 Embedded System
3 Backend Services
4 Network Connectivity
5 Cyber-Physical

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

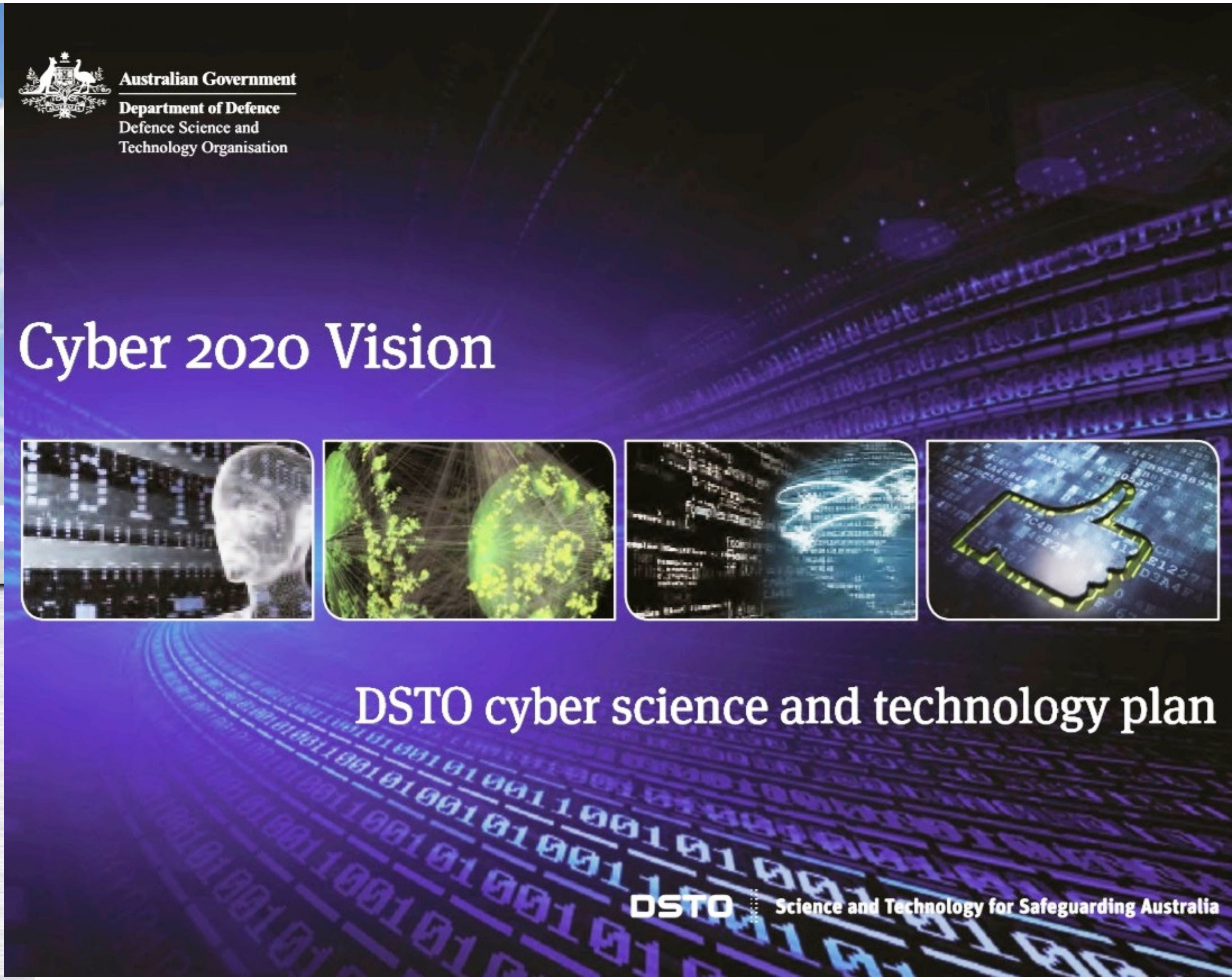


Cyber 2020

Asserting Global Leadership in the Cyber Domain

Ready for what's next.

Booz | Allen | Hamilton



Australian Government

Department of Defence
Defence Science and
Technology Organisation

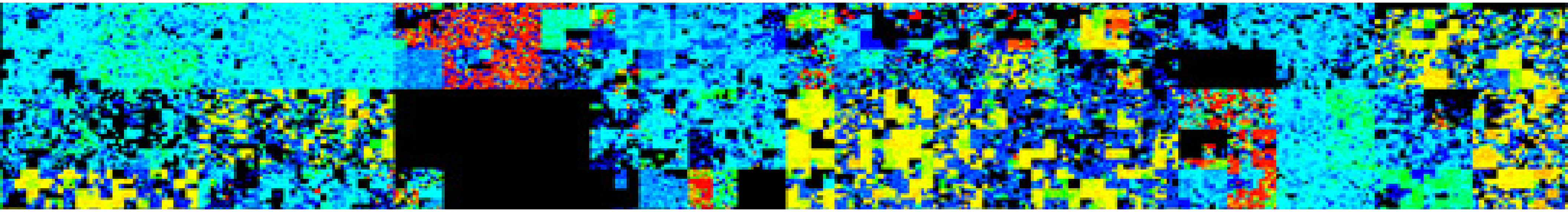
Cyber 2020 Vision

DSTO cyber science and technology plan

DSTO Science and Technology for Safeguarding Australia

"CyberSecurity Vision": *2017–2027 & Beyond!*

1 – Cyber Crime, Cyber Terror & Cyber War	2 – CyberVision: 21stC Players & Threats	3 – CyberSecurity: 21stC Radical Innovation
4 – Scenario 2018 - CSO: C-Suite Integration **"Integrated"**	5 –Scenario 2020 – Internet of Things(IoT) **"Adaptive"**	6 – Scenario 2025 – AI & Machine Learning **"Intelligent"**
7 – In-Depth: Critical Sector Scenarios"	8 – From CyberVision to Business Reality!	9 – YOUR TOP 10 Actions & RoadMap



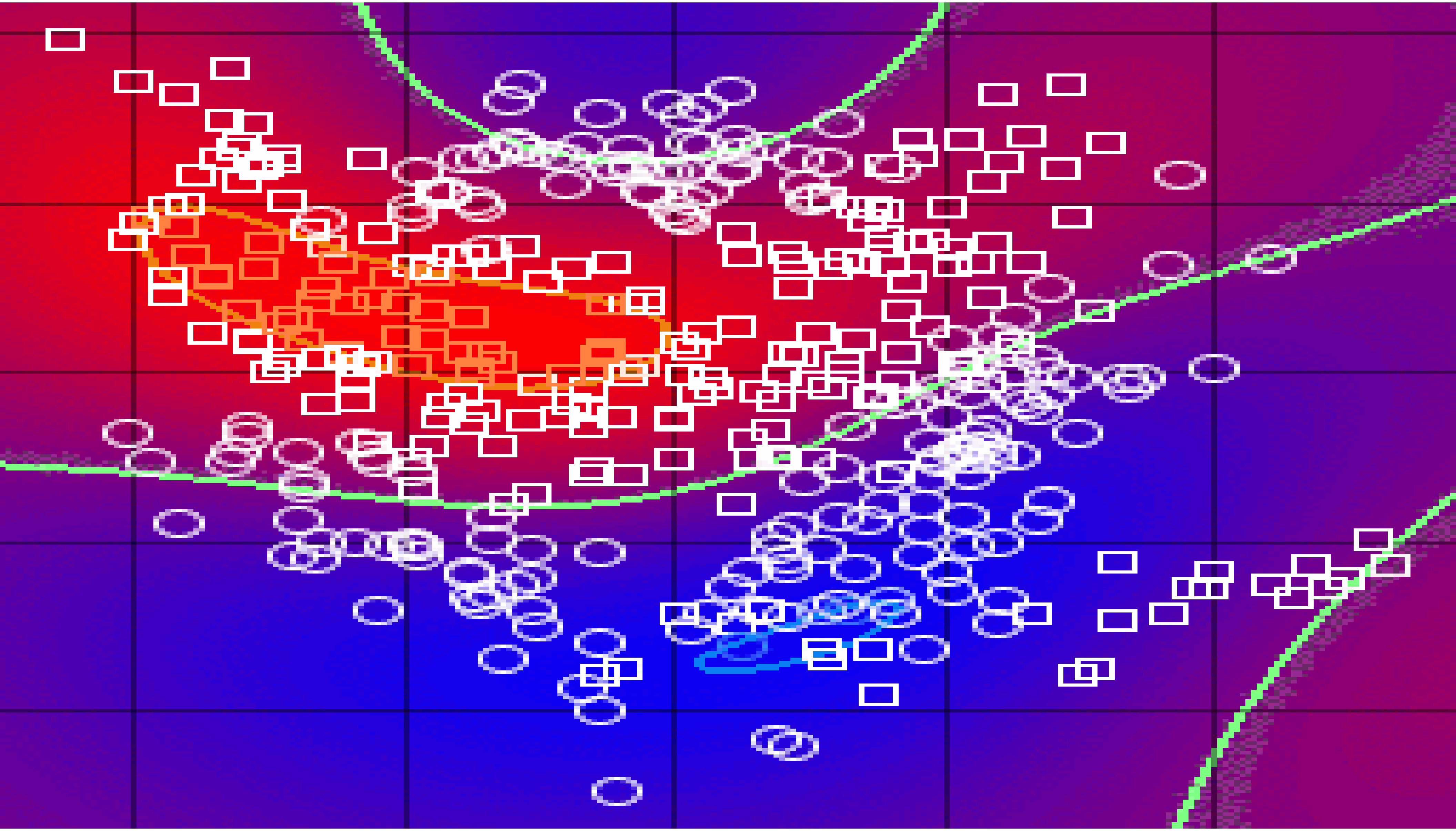
Scenario 2025: *"Intelligent Security"*

- Transition & Full Deployment of Enterprise-Wide AI/ML-based **Intelligent** "CyberSecurity" Tools
- Real-Time **Behavioural Modelling** of ALL aspects of Net Traffic, System/Event Logs, Net Nodes, Servers, Databases, Devices & Users
- Focus on **AI/ML Modelling** of the **"Known Good"** to augment Classic Detection using **"Known Bad",** and hence provide New Generation **"Defence In-Depth"**
- Trial Deployment of **Autonomous Real-Time** "Cyber" Alerts that integrate both Traditional & Advanced AI/ML "Cybersecurity Tools"

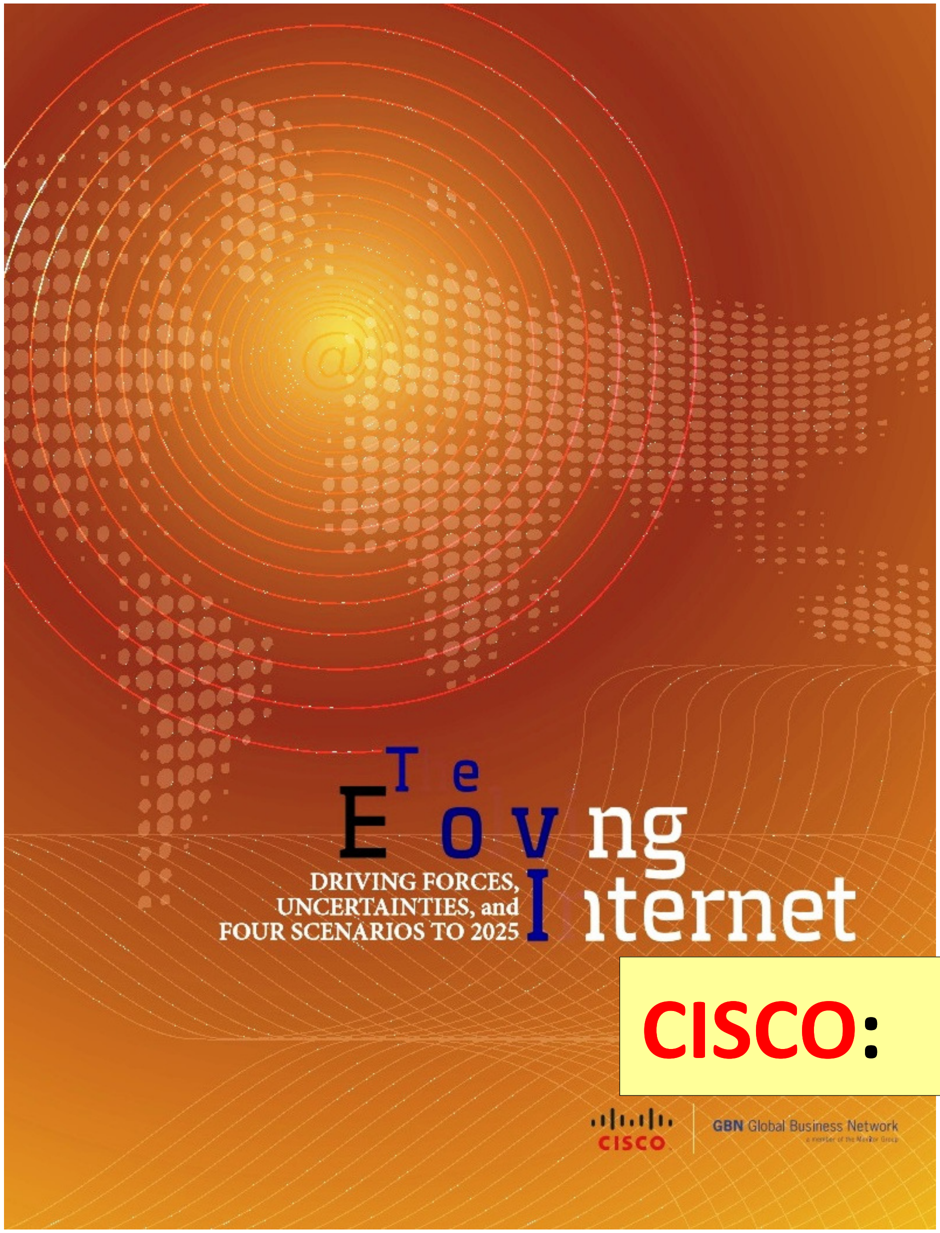
AI & Machine Learning as *Cyber Tools*

- **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/ML 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 & Machine Learning can mitigate risks of new malware that have no prior "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"!

Typical "Machine Learning" Algorithm



Technology Visions: Scenario 2025



The Evolving Internet

DRIVING FORCES, UNCERTAINTIES, and FOUR SCENARIOS TO 2025

CISCO

GBN Global Business Network

IDATE Research

Understanding the Digital World

Telecom & Over-The-Top

The Future Internet in 2025

Open paradigms for personal data and platforms?

M14117MRA – November 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

DIGIWORLD by IDATE

CISCO: 2025 Scenarios: IDATE

Cyberspace 2025: *Microsoft Scenarios*

*** Plateau – Peak – Canyon ***

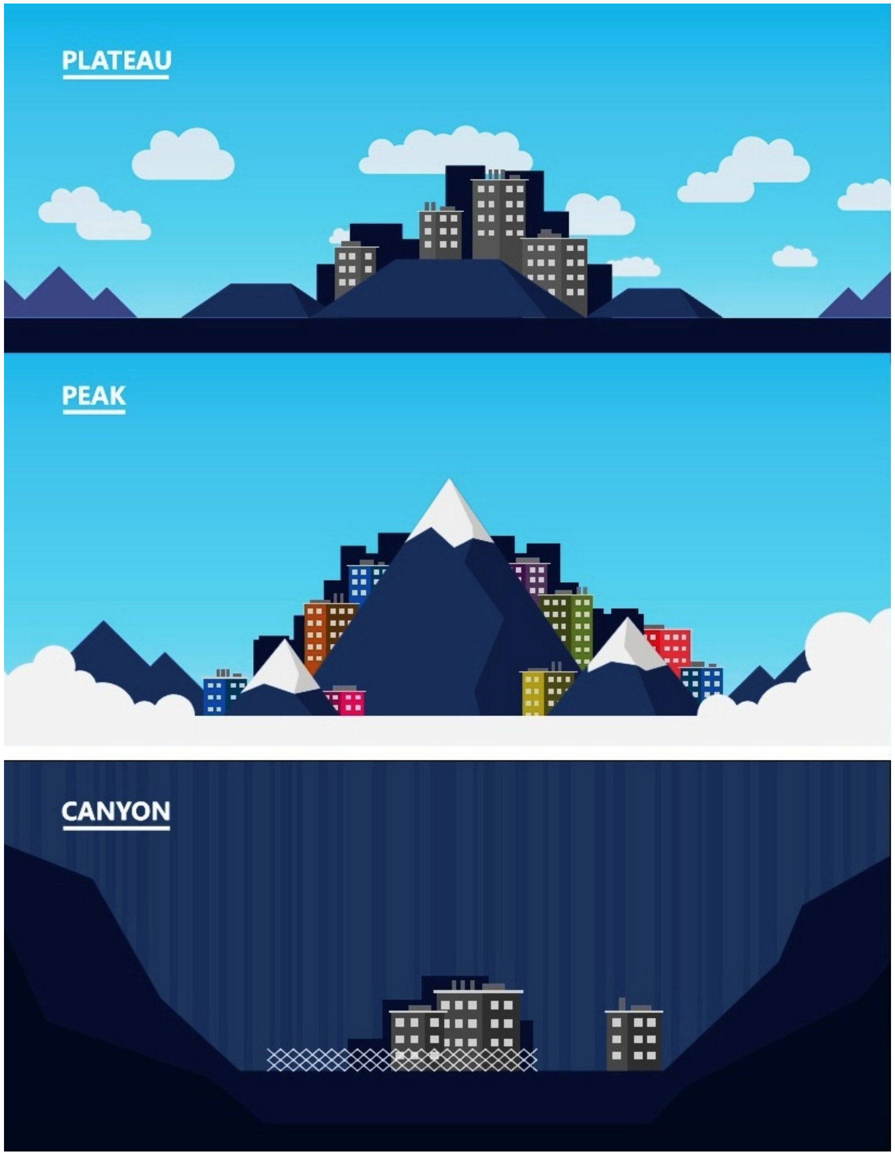
Microsoft

CYBERSPACE 2025 TODAY'S DECISIONS, TOMORROW'S TERRAIN

NAVIGATING THE FUTURE OF CYBERSECURITY POLICY

AUTHORS
David Burt
Aaron Kleiner
J. Paul Nicholas
Kevin Sullivan

JUNE 2014



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 => 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.

Scenario 2025 Business will evolve to "Smart" –Hybrid– Security Operations!

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)

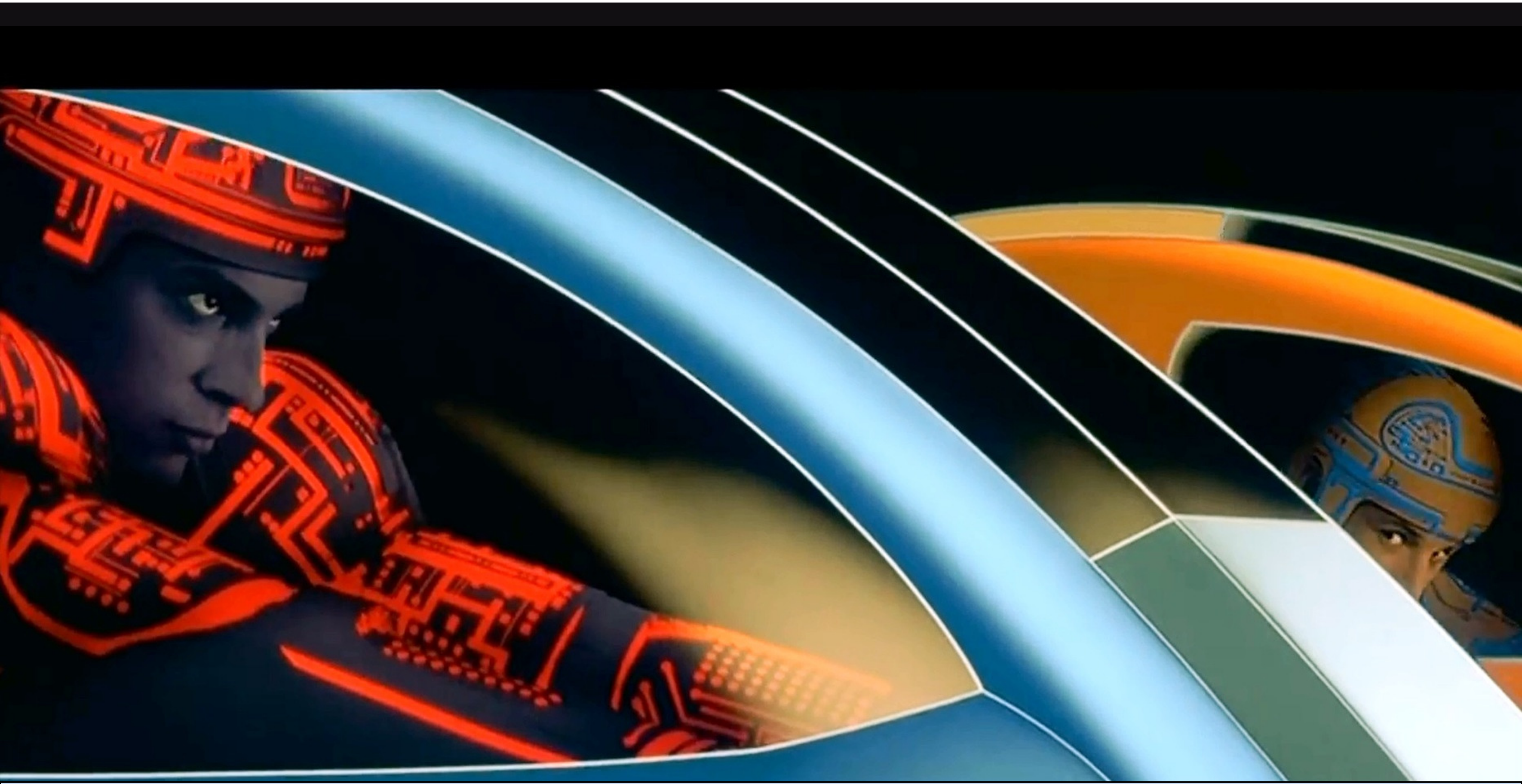
  2) ***Smart Decision Principles (D-Genes):*** Space, Time & Decision Focus

  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!*

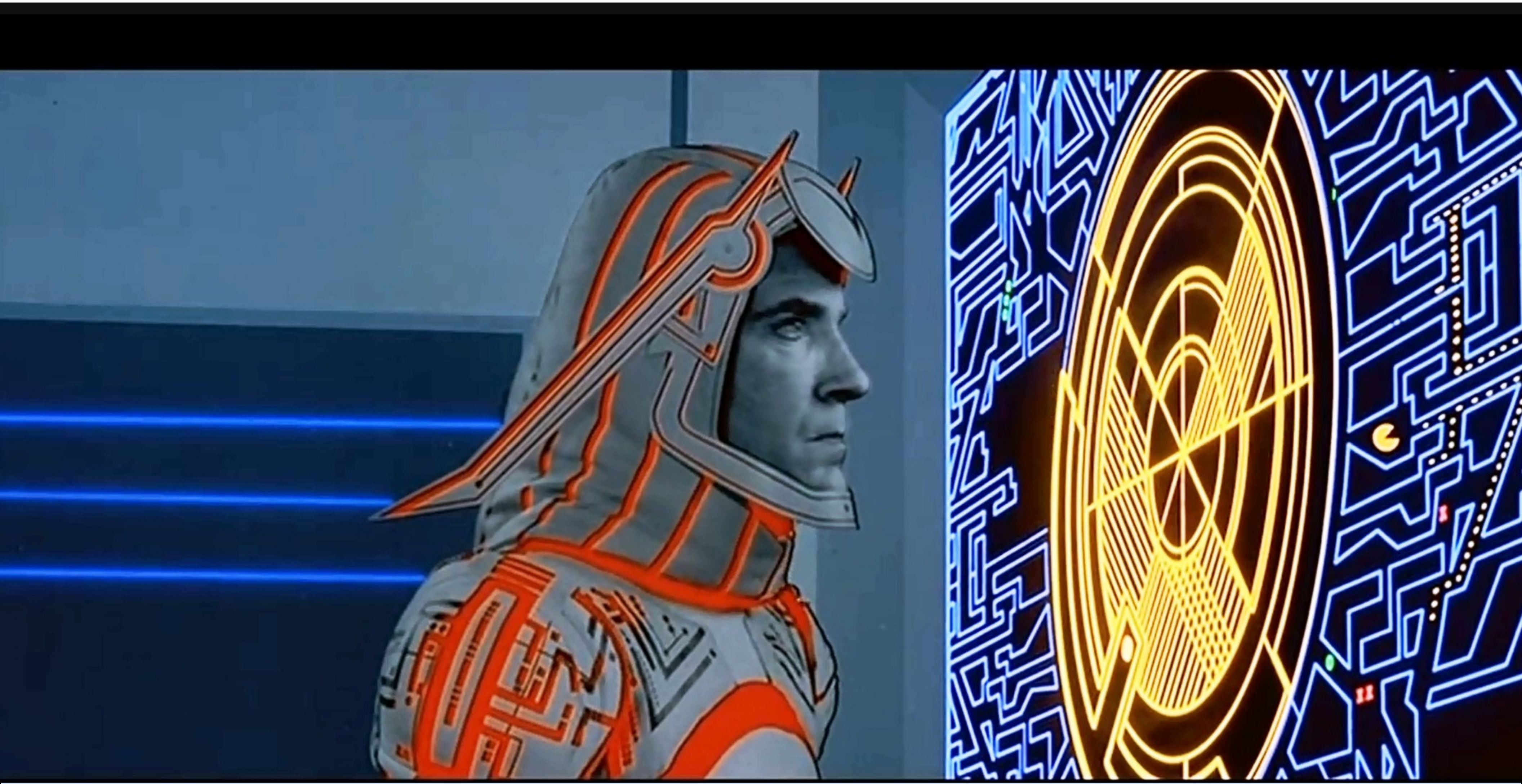
Scenario 2025: “Intelligent Defence Bots”



1982 < -Review Past 34 years-> 2016 <- Explore Future 34 years-> 2050

TRON (1982): Sci-Fi Security Perspective!

Scenario 2025: "Intelligent Defence Bots"



1982 < -Review Past 34 years-> 2016 <- Explore Future 34 years-> 2050

TRON (1982): Sci-Fi Security Perspective!

Transition from "Cyber Now - 2017" to "Intelligent AI/ML Cyber - 2025"

2017 - "Cyber Now"

- "Signature" Detection
- Multi-DMZ Firewalls
- Anti-Virus & Malware
- Supervised Learning
- Zero-Day Attacks
- Objects & Assets
- **"Known BAD!"**

2025 - AI/ML Cyber

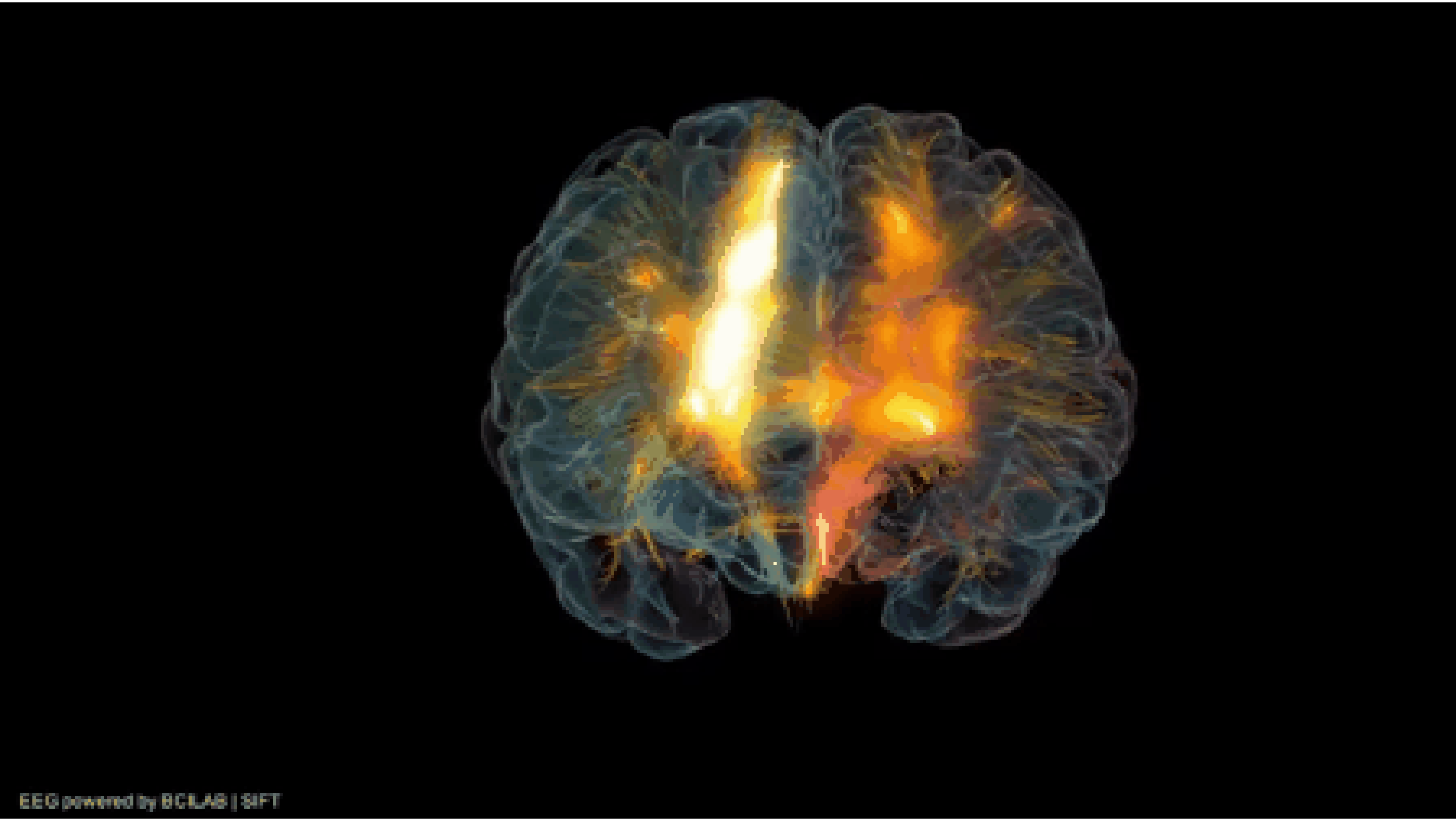
- Behaviour Modelling
- Learning the Baseline
- "Smart Security"
- Unsupervised Learning
- Zero-Second Attacks
- Events & Experience
- **"Known GOOD!"**

Scenario 2025: Defence In-Depth requires Augmentation of **Traditional " Cyber" Tools** to include **Intelligent AI/ML Security Tools** that model **BOTH "Known GOOD & BAD!"**

Scenario 2040+: *“Neural Security”*

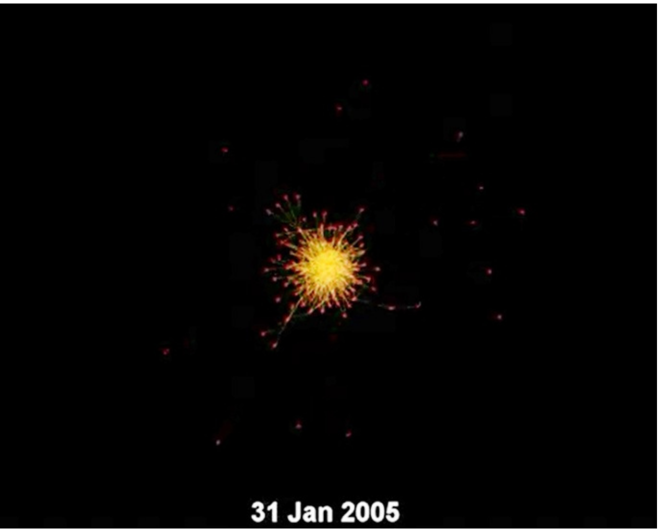
- Full Implementation of Intelligent & Adaptive Cybersecurity across the ***Extended Enterprise***
- ***Autonomous “Alerts”*** and Real-Time AI/ML-based Cyber Event, Traffic & User Modelling
- New Scaled Architectures and Operational Standards for ***“Smart Systems”*** – Smart Devices, Business, Cities, Government, Economy & Society
- Cybersecurity Operations transition to become Ultra-Intelligent – ***“Neural Security”*** – through Embedded “AI-Security Bots” for Real-Time Defence

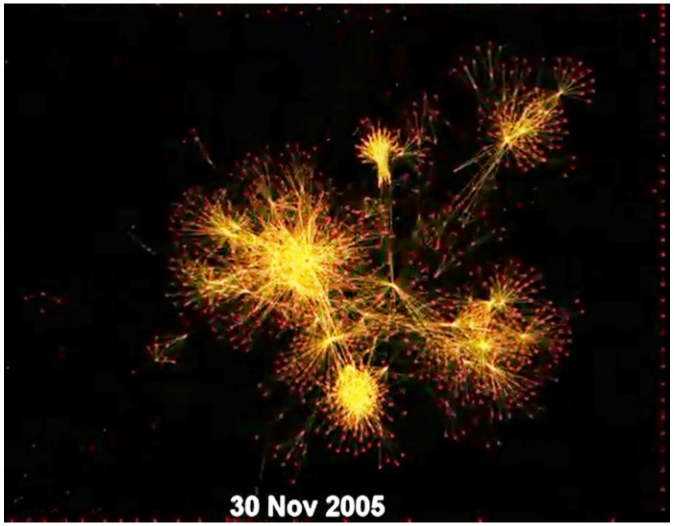
Scenario 2040+: *“Neural Security”*

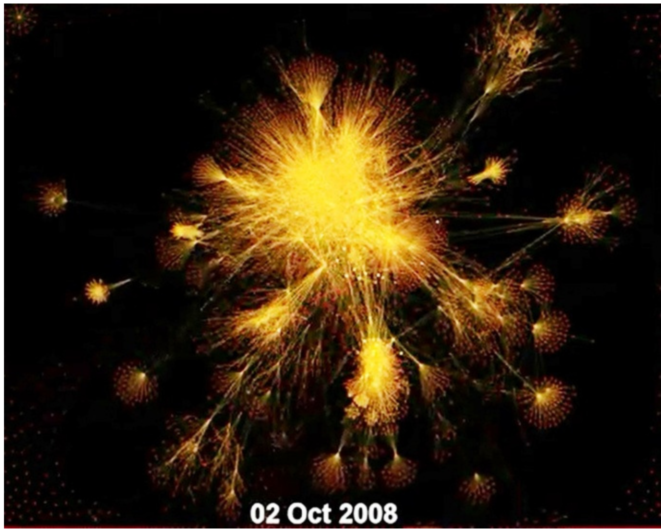


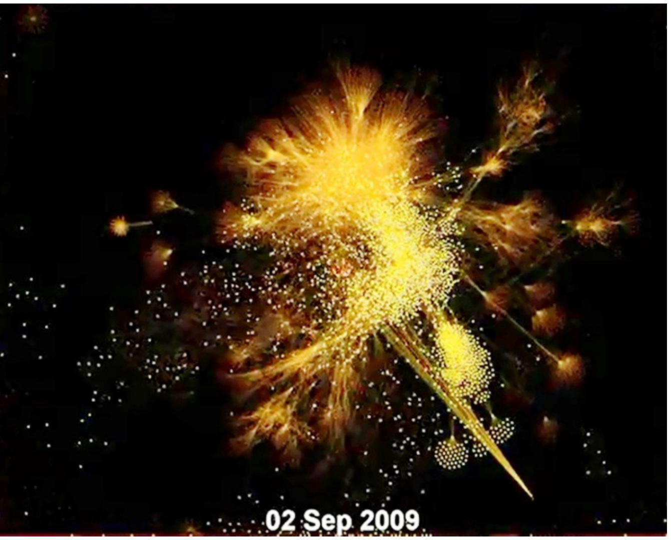
Multi-Year Evolution of Wiki-Web

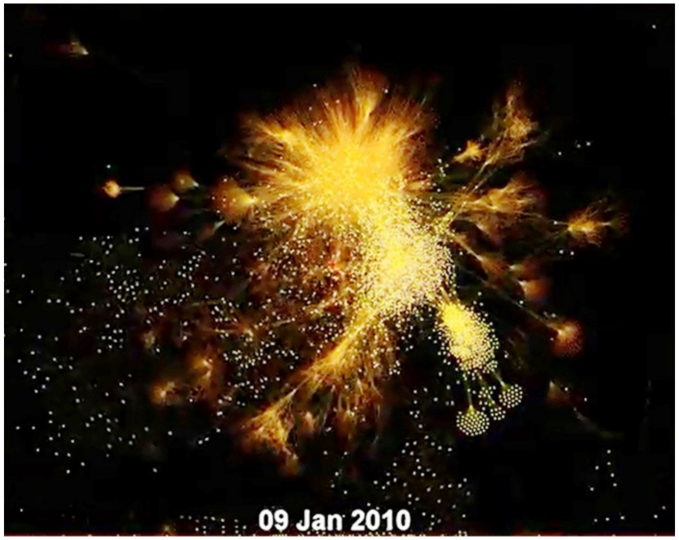
Complex Adaptive System : “Wiki.tudelft.nl”

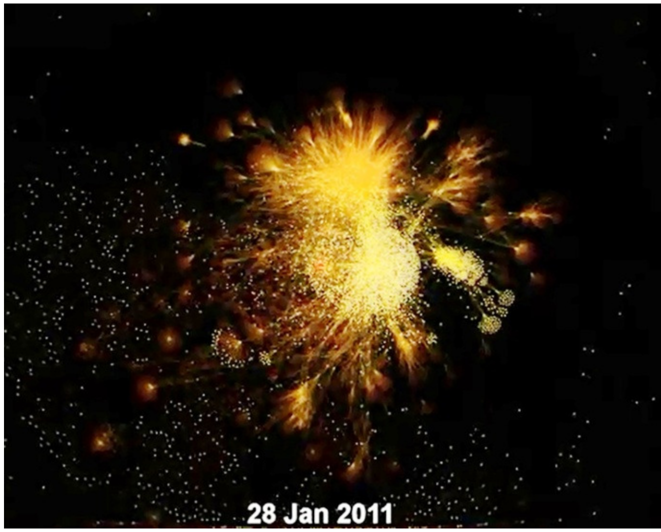










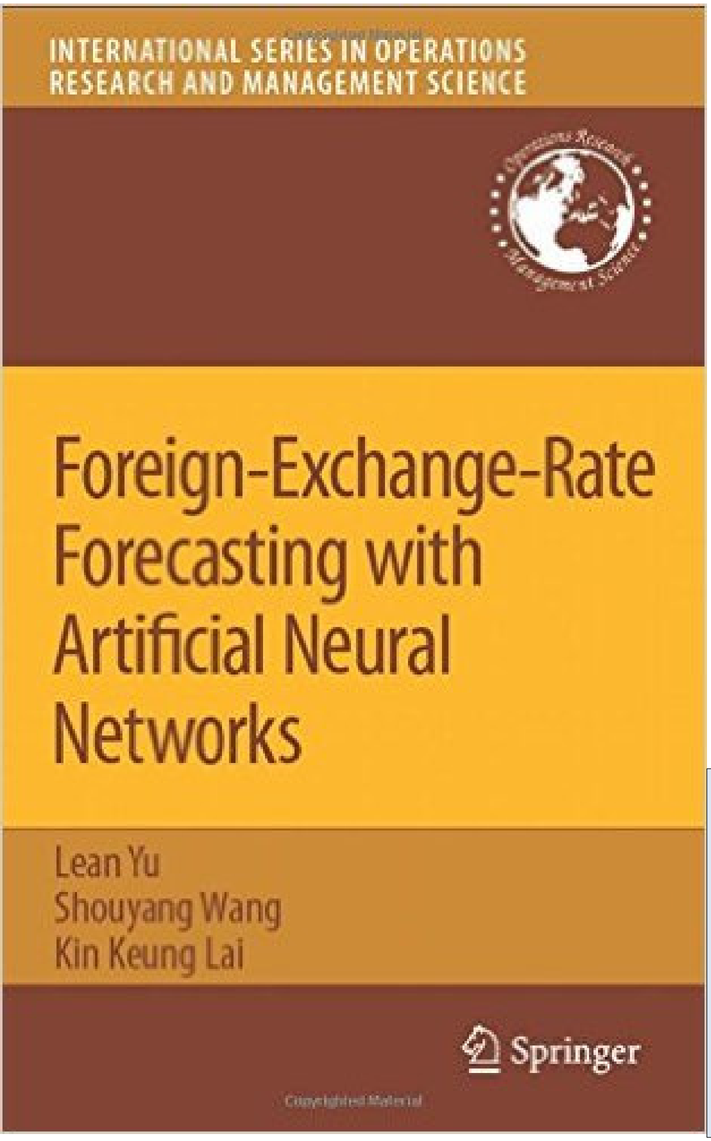


Delft University of Technology - Netherlands

Security Futures: *Towards "Neural Society"*

- ***Real-Time Security Operations:***
  - Secure and monitor every cyber asset and critical physical asset through IP Networking, RFID Tagging & communication of status to operations centre
- ***Augmented & Immersive Reality:***
  - Multimedia virtual world overlays on data from the real physical world, through head-up displays & other forms of embedded sensors & displays
- ***Bio Neural Metaphors:***
  - Further developments of self-organising and autonomous systems for monitoring and responding to cyber alerts & attacks in real-time
- ***3D Adaptive Simulation & Modelling:***
  - Adaptive 3D computer modelling of physical buildings, campuses & cities, as well as dynamic models of extended enterprises networks. The aim is to visualise, model & respond to security alerts with greater speed & precision
- ***"Smart Security" Architectures:***
  - Effective integrated security requires management through hybrid hierarchical and "peer-to-peer" organisational architectures. Living organic systems also exploit hybrid architectures for optimal command & control

Artificial Neural Networks applied to Real-Time Foreign Exchange Dealing

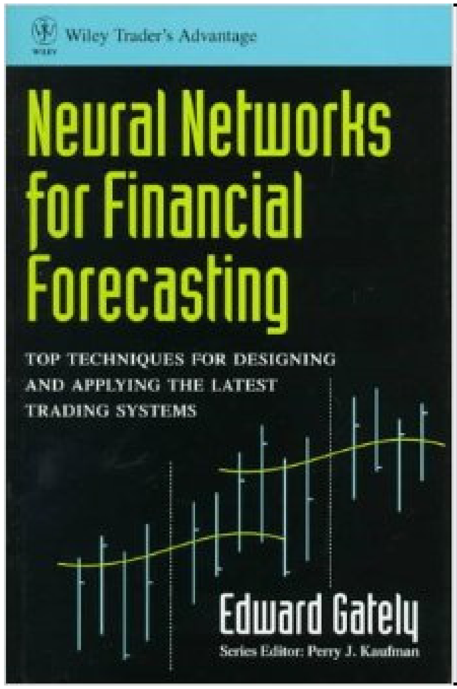


INTERNATIONAL SERIES IN OPERATIONS RESEARCH AND MANAGEMENT SCIENCE

Foreign-Exchange-Rate Forecasting with Artificial Neural Networks

Lean Yu
Shouyang Wang
Kin Keung Lai

Springer



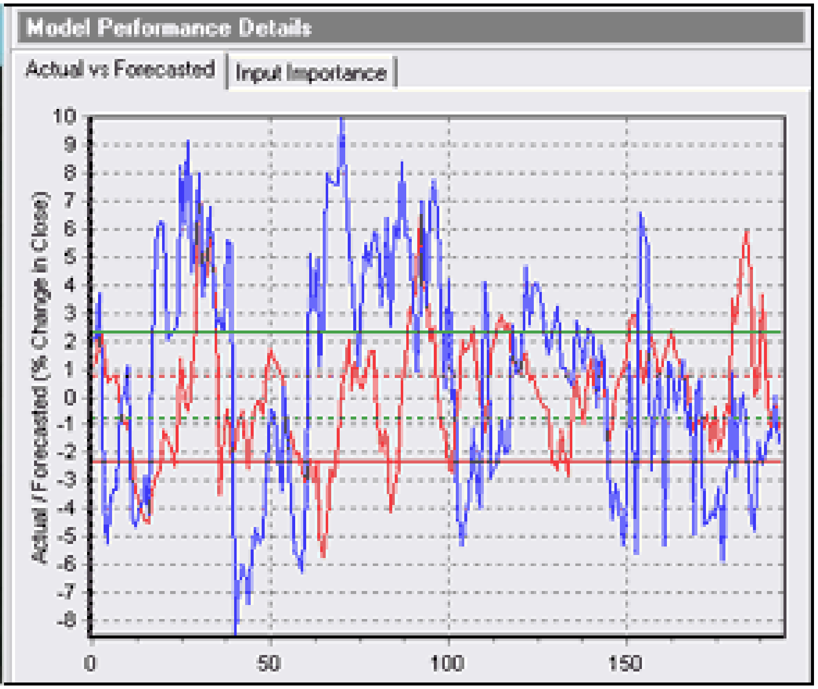
Wiley Trader's Advantage

Neural Networks for Financial Forecasting

TOP TECHNIQUES FOR DESIGNING AND APPLYING THE LATEST TRADING SYSTEMS

Edward Gately

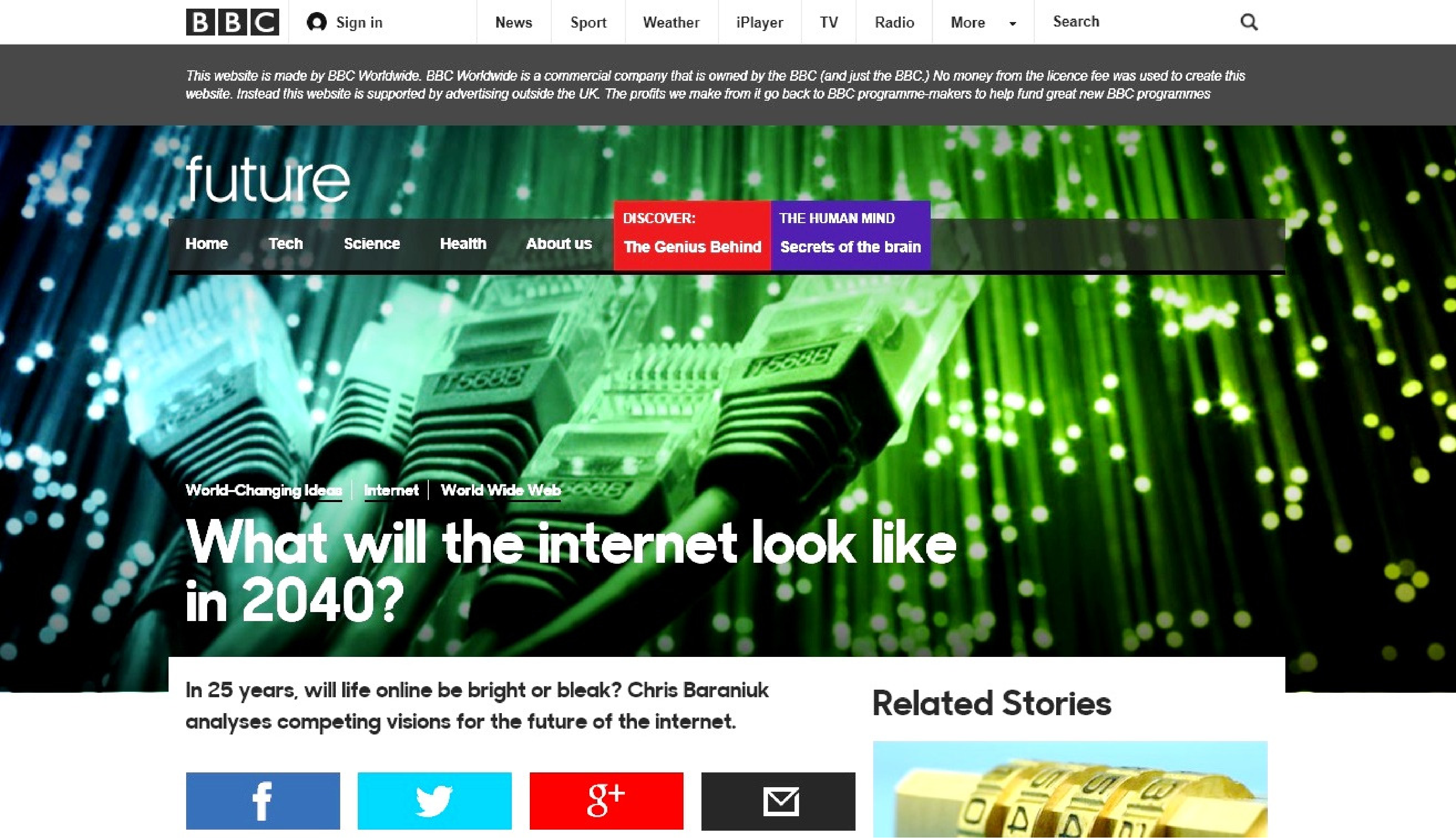
Series Editor: Perry J. Kaufman



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!

BBC Worldwide Internet Scenario: 2040

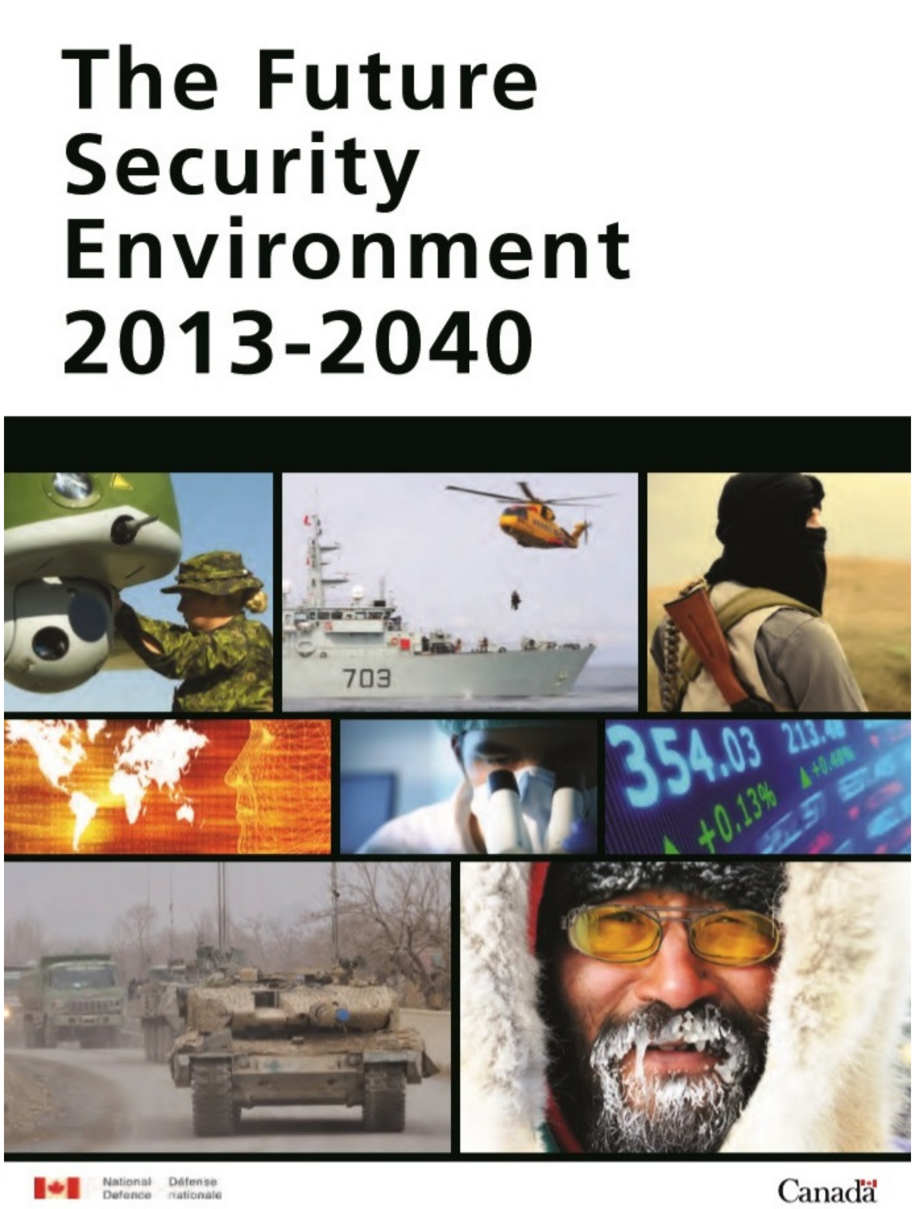


This website is made by BBC Worldwide. BBC Worldwide is a commercial company that is owned by the BBC (and just the BBC.) No money from the licence fee was used to create this website. Instead this website is supported by advertising outside the UK. The profits we make from it go back to BBC programme-makers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

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.

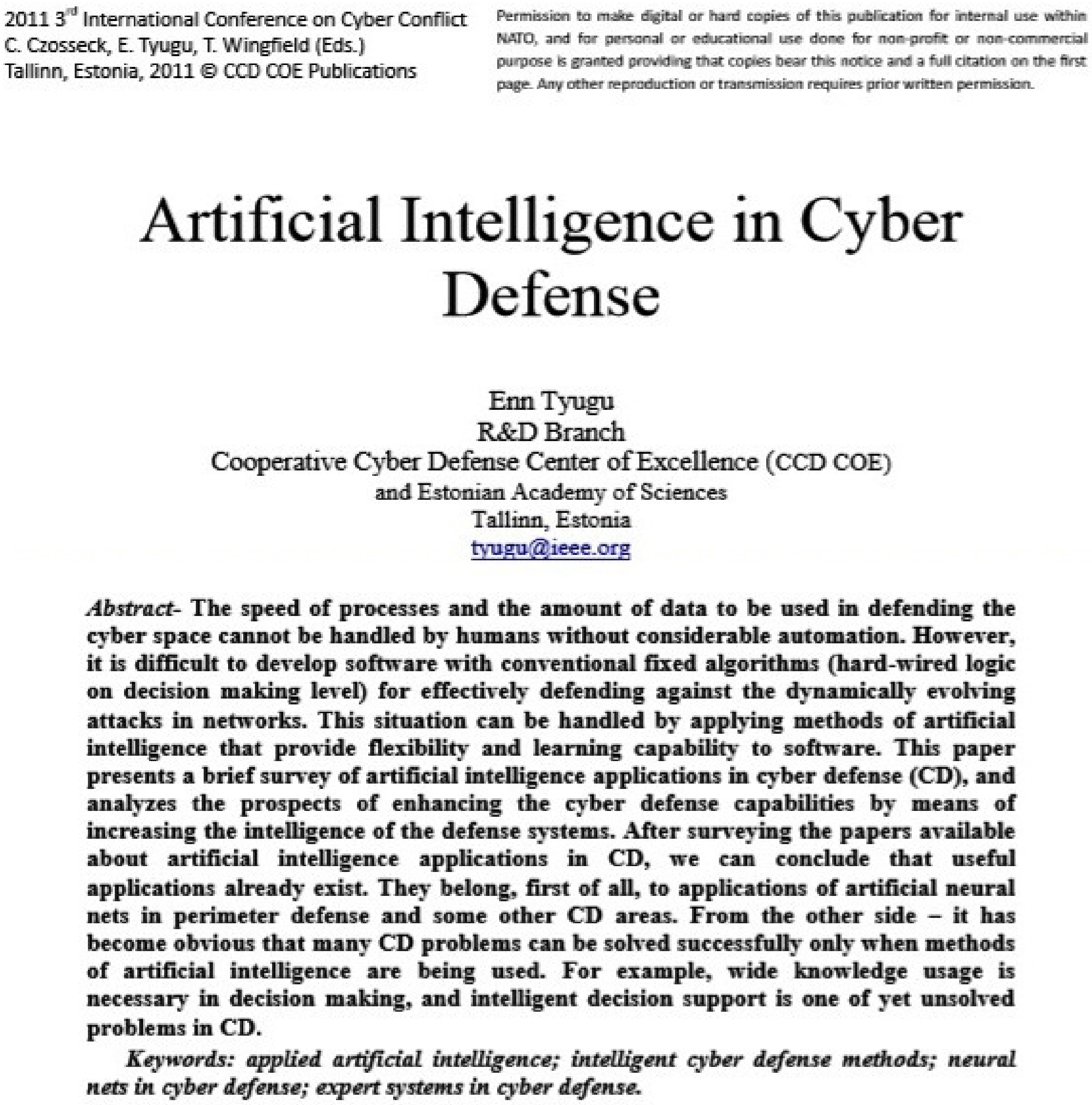
Scenario 2040: Cyber Defense – NATO & Canada



The Future Security Environment 2013-2040

National Defence Défense nationale

Canada



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

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.

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

MINISTRY OF DEFENCE

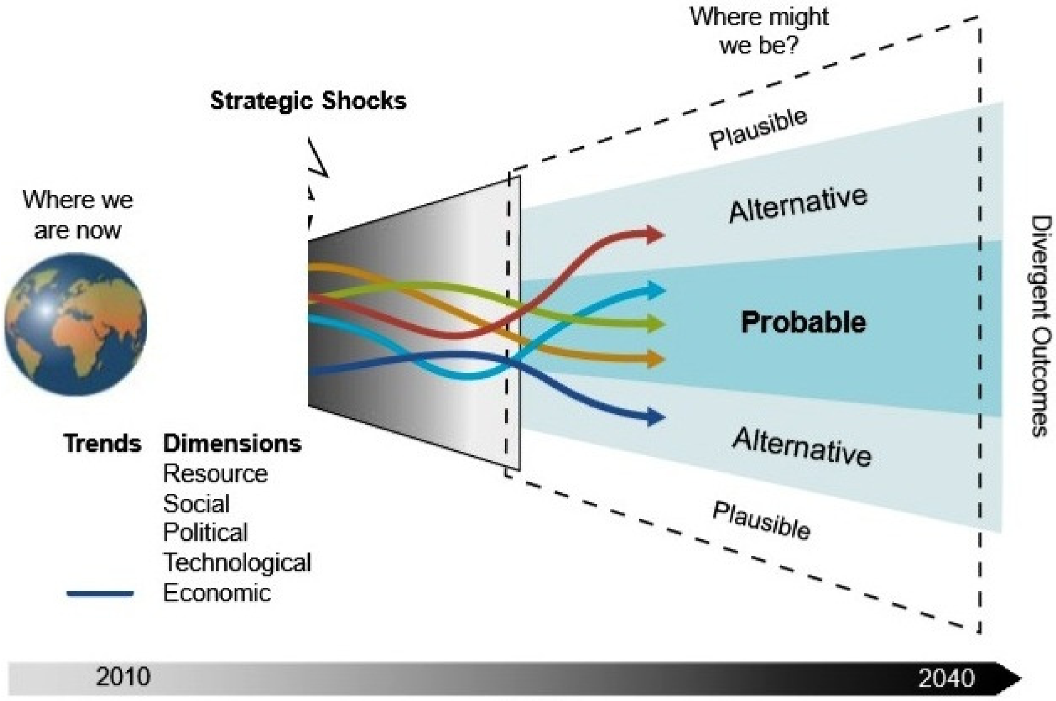
Ministry of Defence

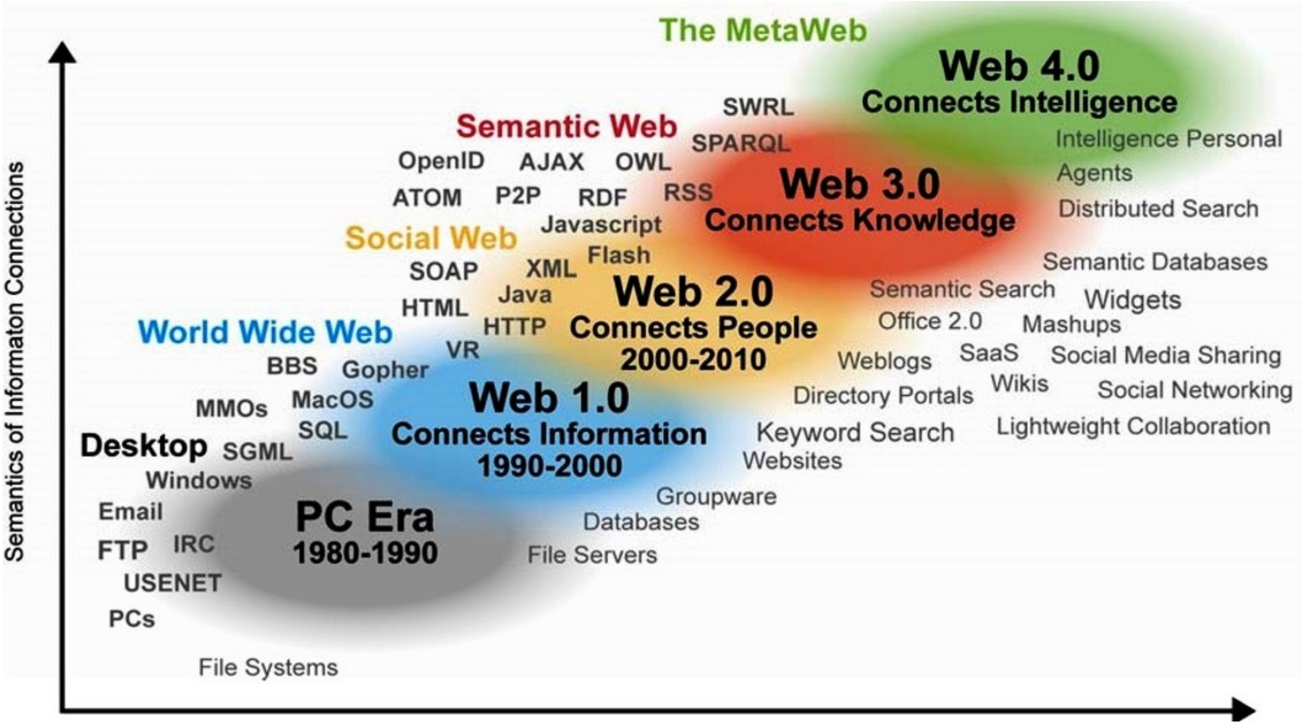
Strategic Trends Programme

Global Strategic Trends - Out to 2040

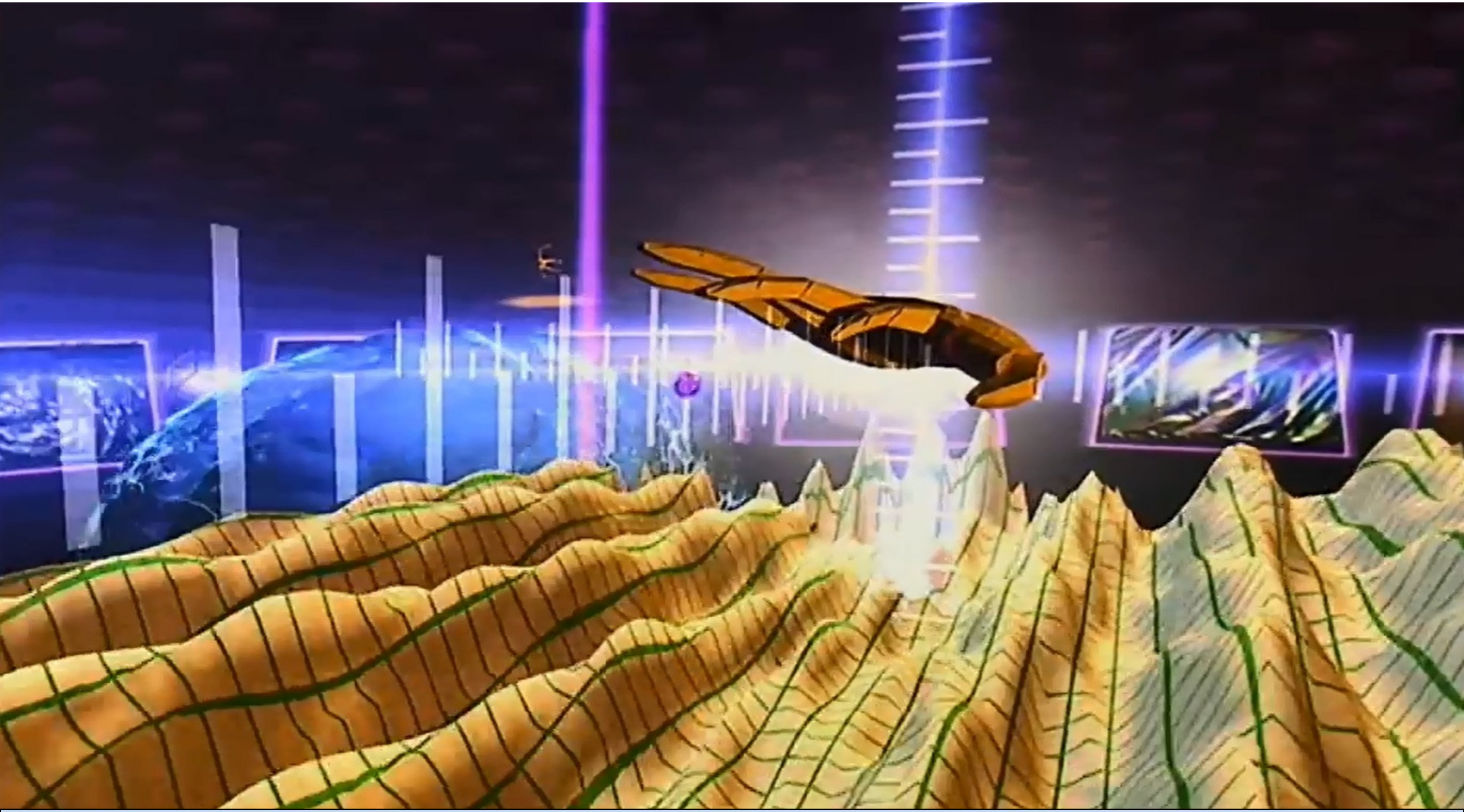
Fourth Edition

D C D C





Scenario 2040: “Neural Security & Society”



1992 < -Review Past 24 years-> 2016 <- Explore Future 24 years-> 2040

Lawnmower Man (1992): 3D VR Neural Futures!

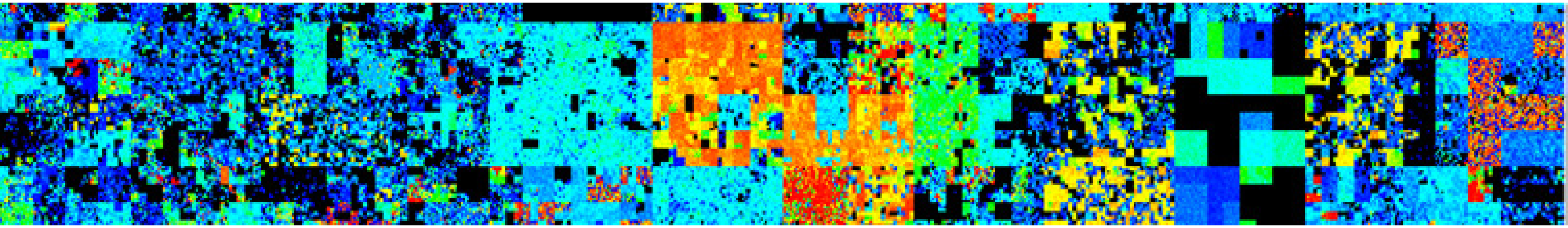
Scenario 2040: “Neural Security & Society”

1992 < -Review Past 24 years-> 2016 <- Explore Future 24 years-> 2040

[illegible]

“CyberSecurity Vision”: *2017–2027 & Beyond!*

1 – Cyber Crime, Cyber Terror & Cyber War	2 – CyberVision: 21stC Players & Threats	3 – CyberSecurity: 21stC Radical Innovation
4 – Scenario 2018 - CSO: C-Suite Integration **“Integrated”**	5 –Scenario 2020 – Internet of Things(IoT) **“Adaptive”**	6 – Scenario 2025 - AI & Machine Learning **“Intelligent”**
7 – In-Depth: Critical Sector Scenarios	8 – From CyberVision to Business Reality!	9 – YOUR TOP 10 Actions & RoadMap



7) Future Security Tools: *"Critical Sectors"*

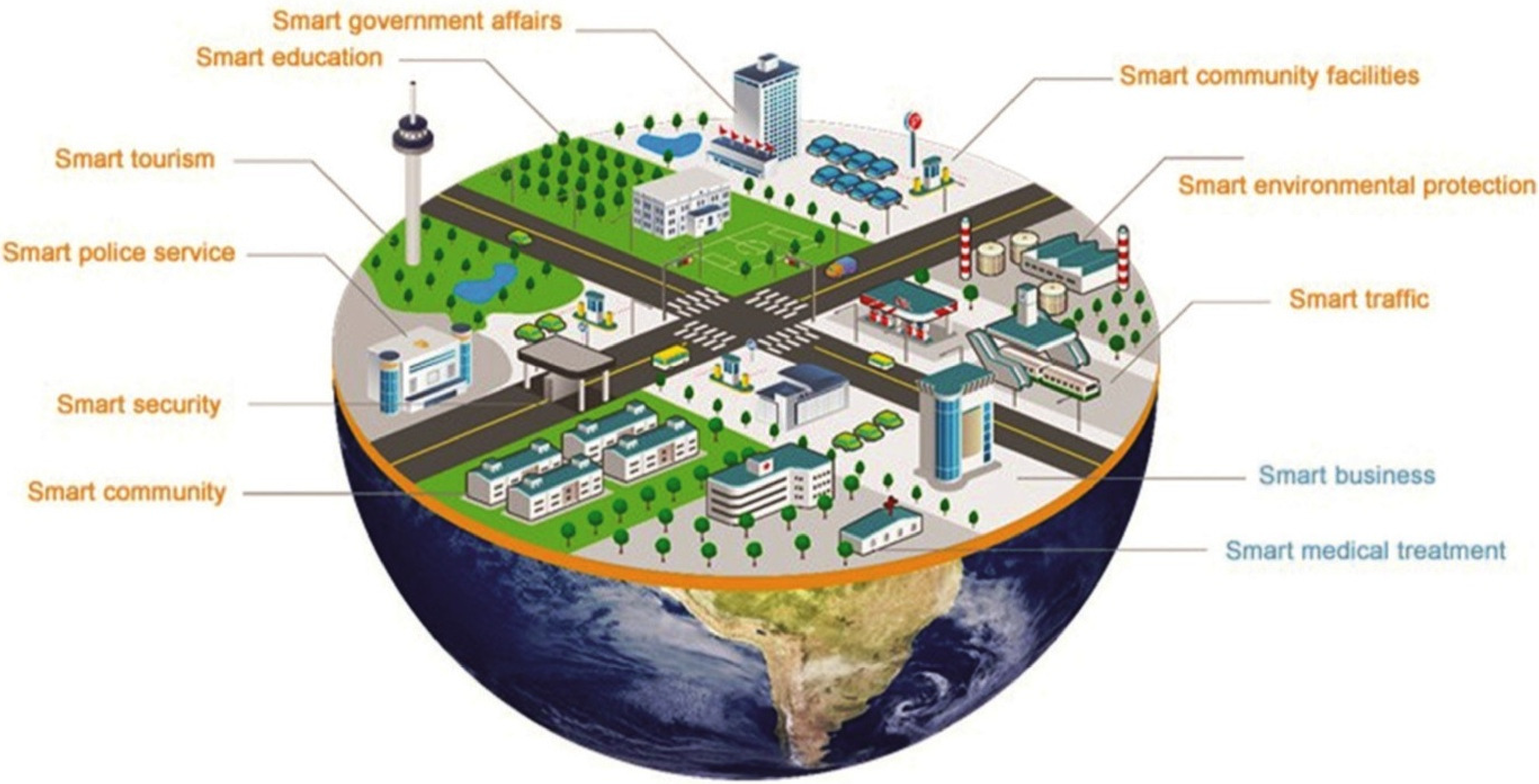
- Adaptive & Intelligent Security Solutions are Crucial to the Defence of ***Critical*** National Infrastructure & ***OUR*** Cities:

  a) **Power Stations:** Particularly Nuclear Energy Sites
  b) **Government Offices:** Parliaments & Govt Ministries
  c) **Oil/Gas/Chemical Facilities:** Risk of Fires/Explosions
  d) **Airports/Metro/Trains:** ALL Transport Transit Hubs
  e) **Cultural/Sports :** Theatres, Olympics, World Cup
  f) **Tourist Resorts & Sights:** High Economic Impact

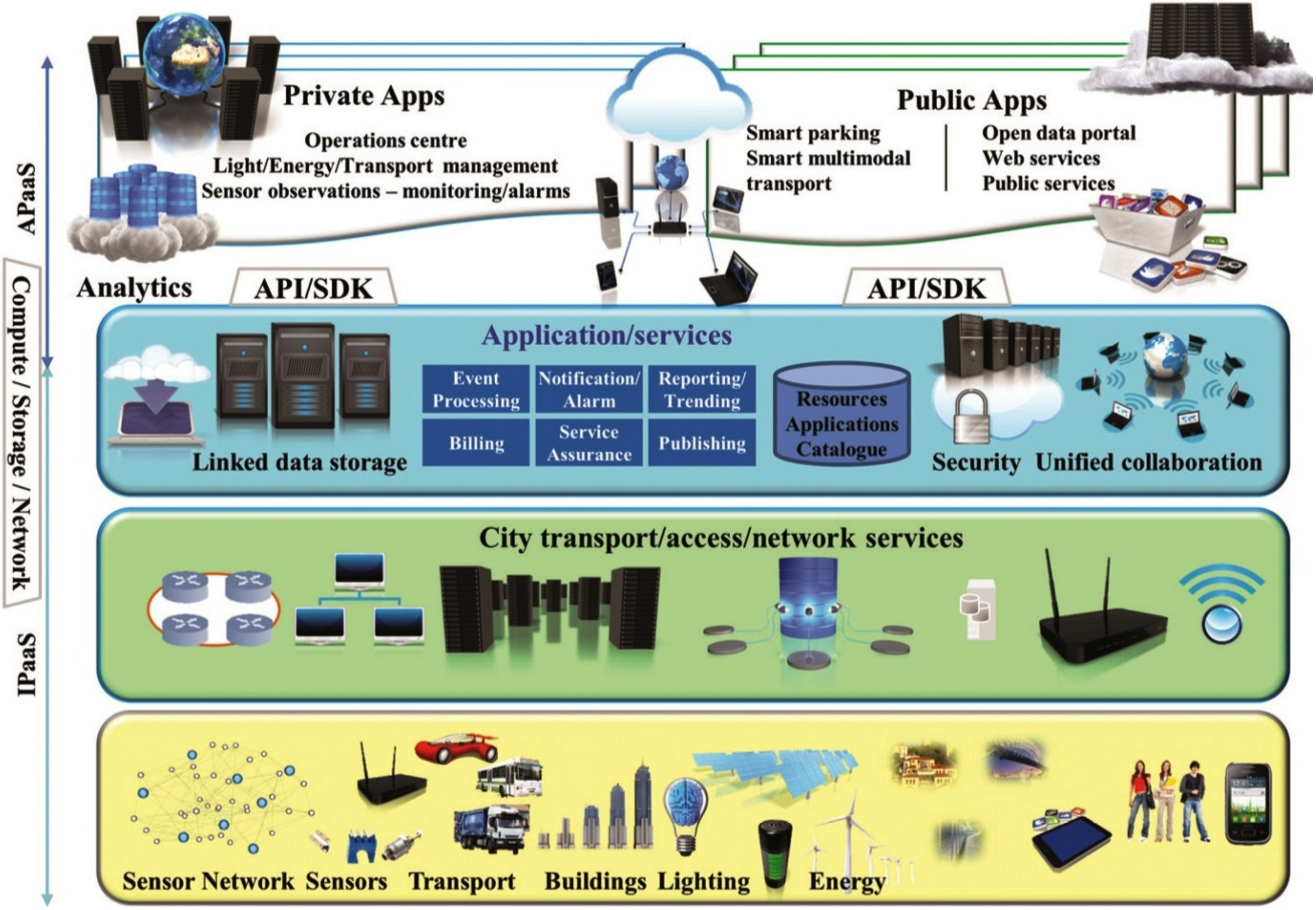
...Physical Security is no longer an effective defence!...

Now ***Crucial*** *to Deploy & Integrate* ***Cyber Solutions*** *that protect User Access, Data Bases & Track* ***"Bad Guys"!***

Smart City: *Scaled "IoT" Architectures*



Smart City: *Multi-Layered Architecture*



APaaS

Compute / Storage / Network

IPaaS

Private Apps

Operations centre
Light/Energy/Transport management
Sensor observations – monitoring/alarms

Analytics

API/SDK

Public Apps

Smart parking
Smart multimodal transport

Open data portal
Web services
Public services

API/SDK

Application/services

Linked data storage

Event Processing	Notification/ Alarm	Reporting/ Trending
Billing	Service Assurance	Publishing

Resources Applications Catalogue

Security

Unified collaboration

City transport/access/network services

Sensor Network

Sensors

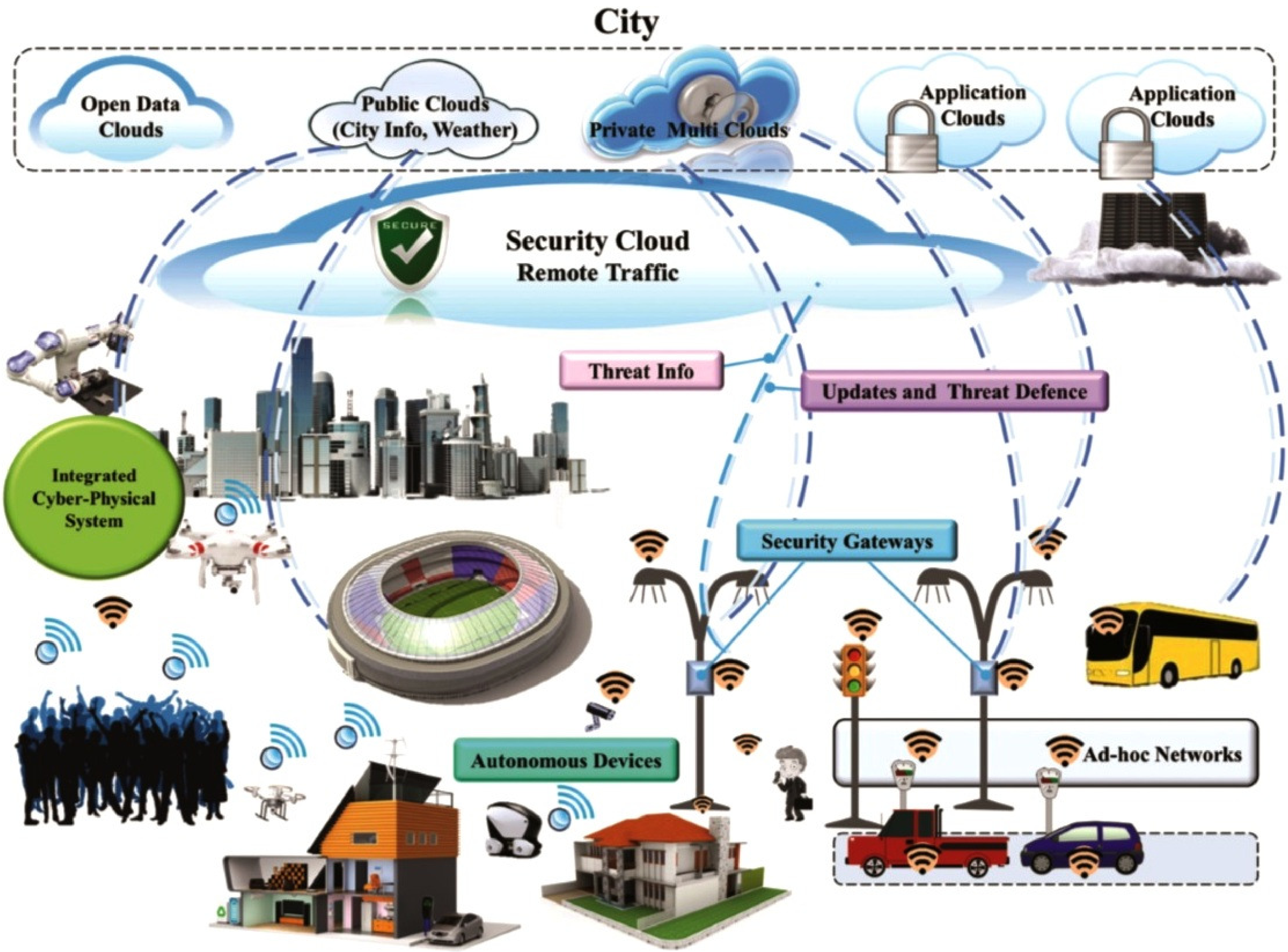
Transport

Buildings

Lighting

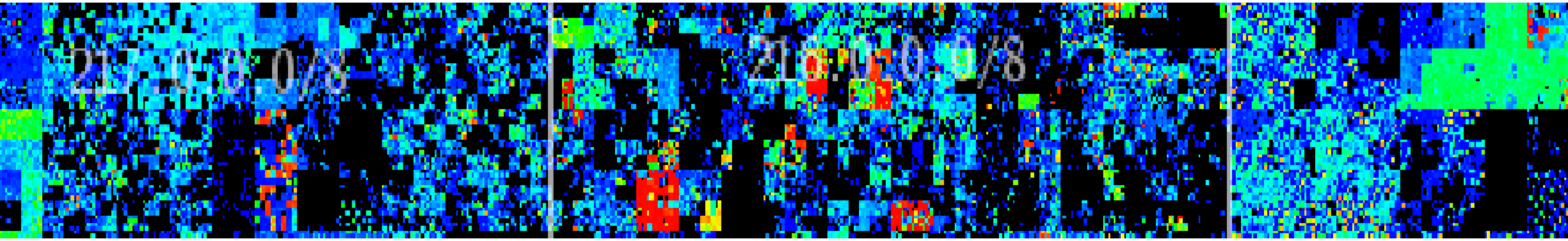
Energy

Smart City: *Multi-Layer Security Framework*



"CyberSecurity Vision": *2017–2027 & Beyond!*

1 – Cyber Crime, Cyber Terror & Cyber War	2 – CyberVision: 21stC Players & Threats	3 – CyberSecurity: 21stC Radical Innovation
4 – Scenario 2018 - CSO: C-Suite Integration **"Integrated"**	5 –Scenario 2020 – Internet of Things(IoT) **"Adaptive"**	6 – Scenario 2025 - AI & Machine Learning **"Intelligent"**
7 – In-Depth: Critical Sector Scenarios"	**8 – From CyberVision to Business Reality!**	**9 – YOUR TOP 10 Actions & RoadMap**



From *CyberVision* to *Business Reality*!

- **20thC - Past Research:** Adaptive AI/ML algorithms have been researched since 1960s/1970s. Computer Network Architectures now support such intelligent solutions!
- **2017 - Present Vision:** Start-Ups such as DarkTrace are now successfully marketing Intelligent Security Solutions
- **2025 - Future Reality:** Most Businesses & Government will deploy AI/ML Security Solutions within 5 to 10 years.

ALL **Corporate & Government CSO's** will eventually need to upgrade to **Intelligent Real-Time Security** to defend against

Cyber Crime, Cyber Terrorism and Cyber War!

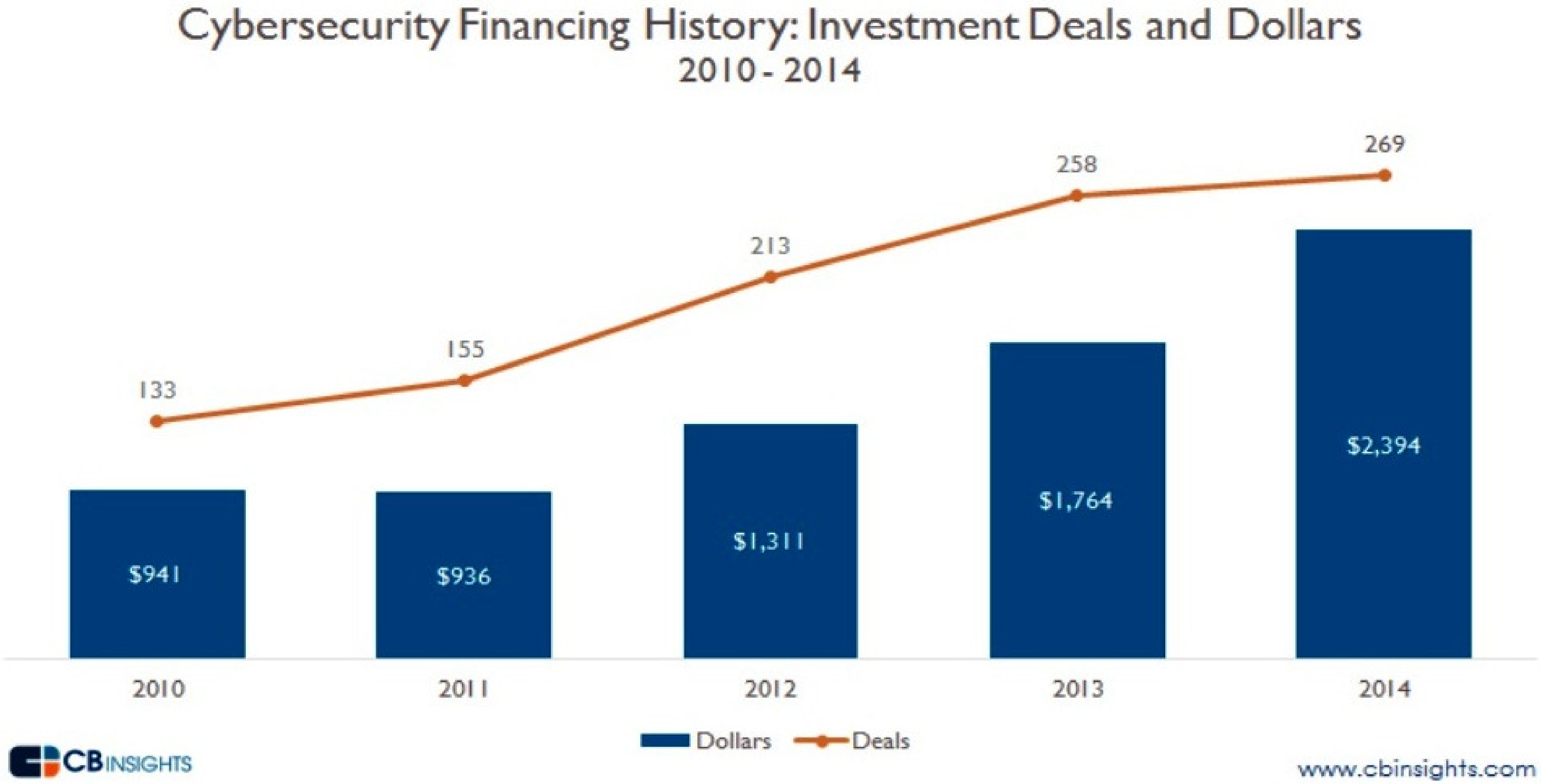
- “*Innovative*” *Cybersecurity* Ventures -

“AI & Machine Learning Solutions”

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

New Cyber Ventures based on AI/ML algorithms are starting-up every Month!

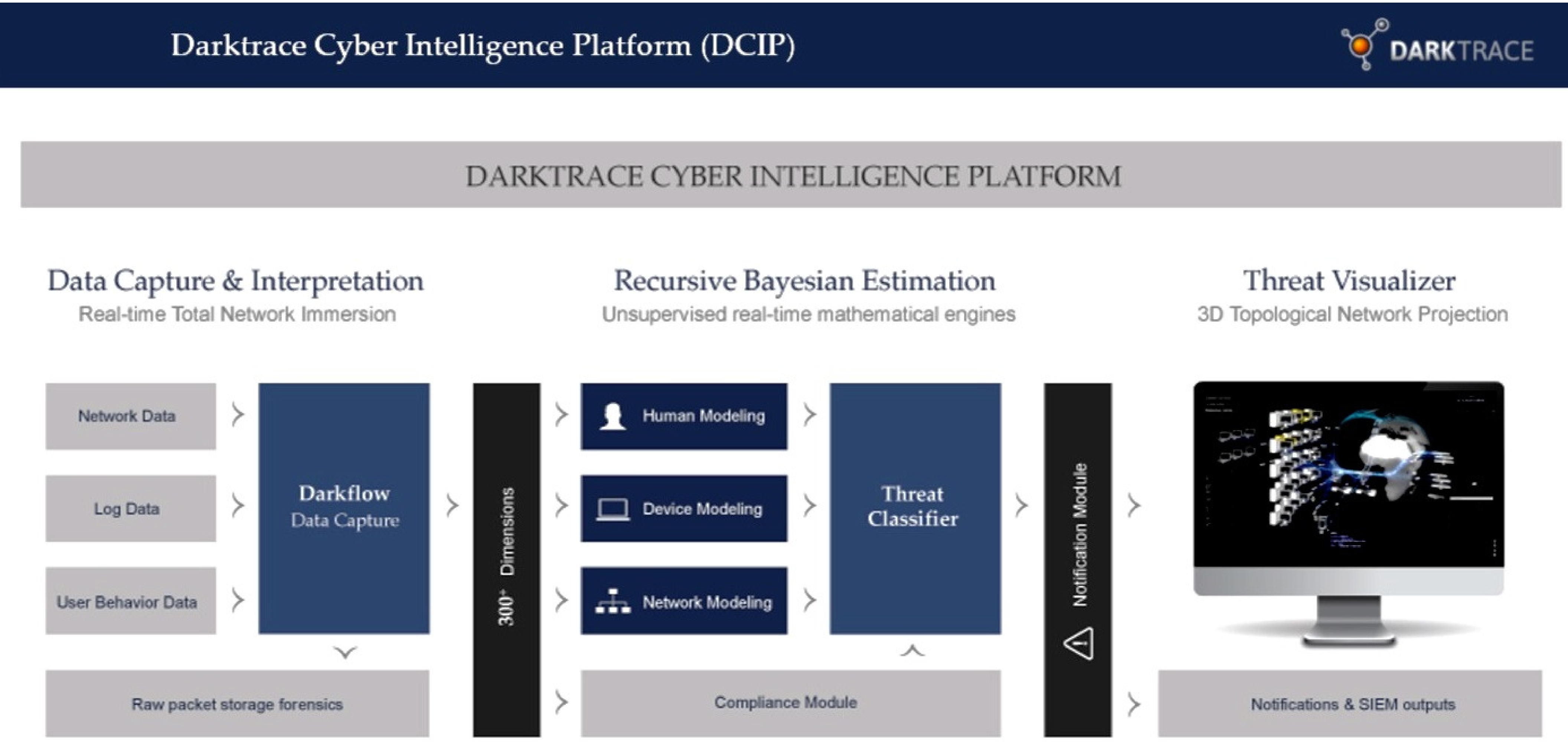
Cybersecurity VC Funding: 2010 - 2014



Summary - 2009/2014 - $7.3Billion VC Investment in 1028+ Ventures

Source: CBInsights - *www.cbinsights.com/blog/cybersecurity-startup-financing/*

Darktrace: *Cyber Intelligence Platform*



Darktrace Cyber Intelligence Platform (DCIP)

DARKTRACE

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

Network Data
Log Data
User Behavior Data

Darkflow
Data Capture

Raw packet storage forensics

300+ Dimensions

Human Modeling
Device Modeling
Network Modeling

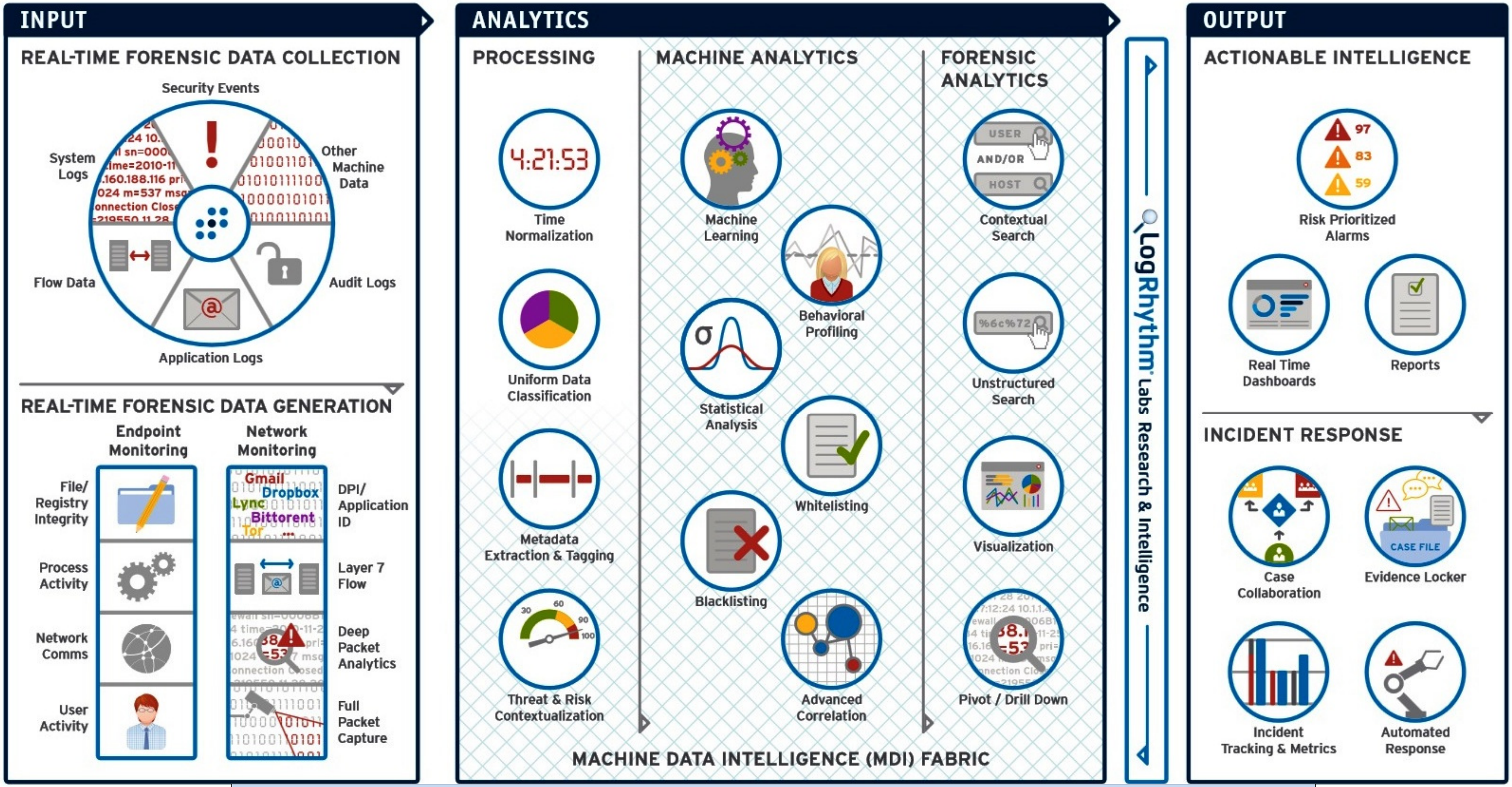
Threat Classifier

Compliance Module

Notification Module

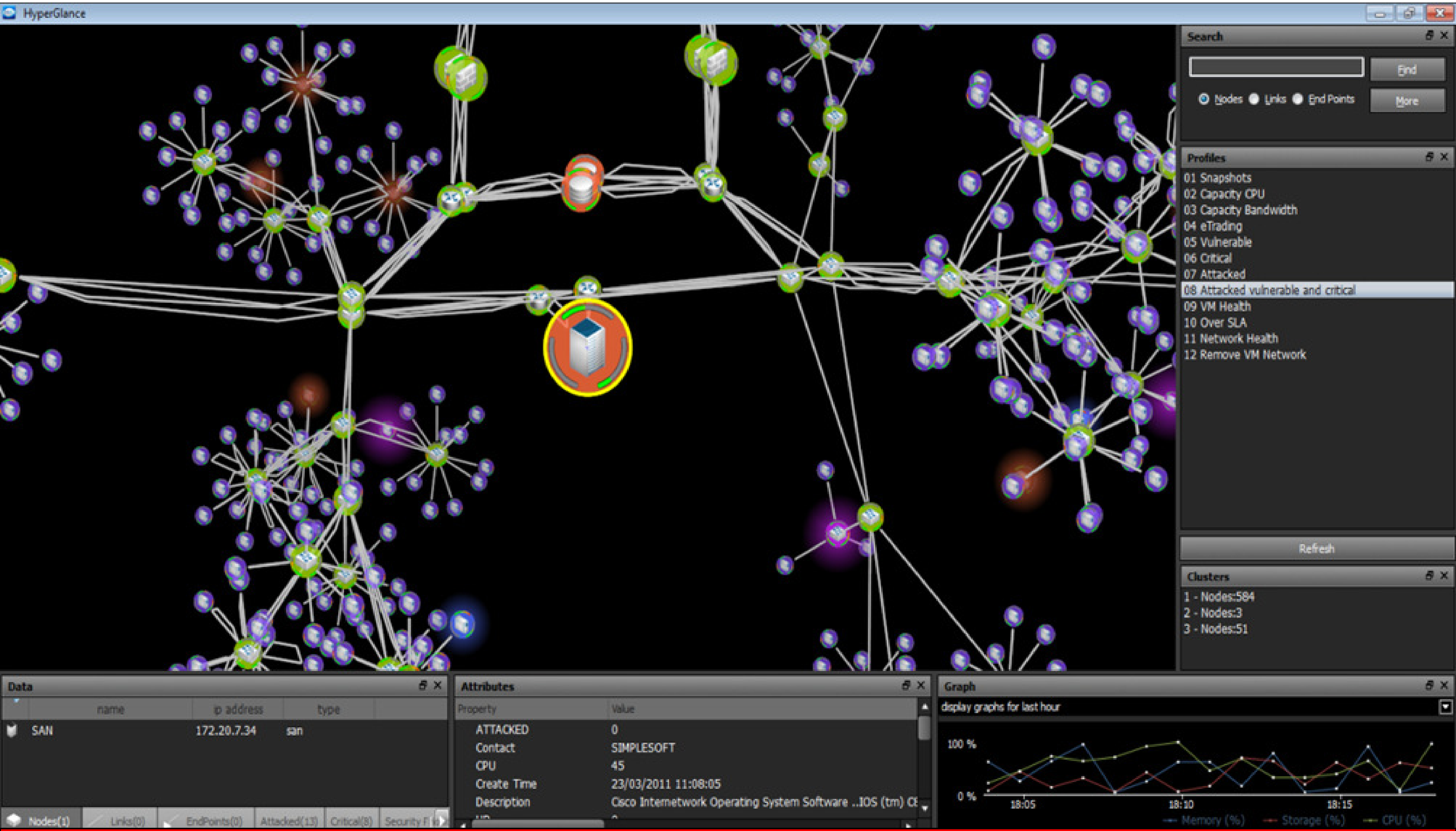
Notifications & SIEM outputs

LogRhythm: *Machine Learning Forensics*



LogRhythm's *Security Intelligence Platform*

Hyperglance:*Smart 3D Network Modelling*



Profiles

01 Snapshots
02 Capacity CPU
03 Capacity Bandwidth
04 eTrading
05 Vulnerable
06 Critical
07 Attacked
08 Attacked vulnerable and critical
09 VM Health
10 Over SLA
11 Network Health
12 Remove VM Network

Clusters

1 - Nodes:584
2 - Nodes:3
3 - Nodes:51

Data

name	ip address	type
SAN	172.20.7.34	san

Nodes(1) | Links(0) | EndPoints(0) | Attacked(13) | Critical(8) | Security F

Attributes

Property	Value
ATTACKED	0
Contact	SIMPLESOFT
CPU	45
Create Time	23/03/2011 11:08:05
Description	Cisco Internetwork Operating System Software ..IOS (tm) C

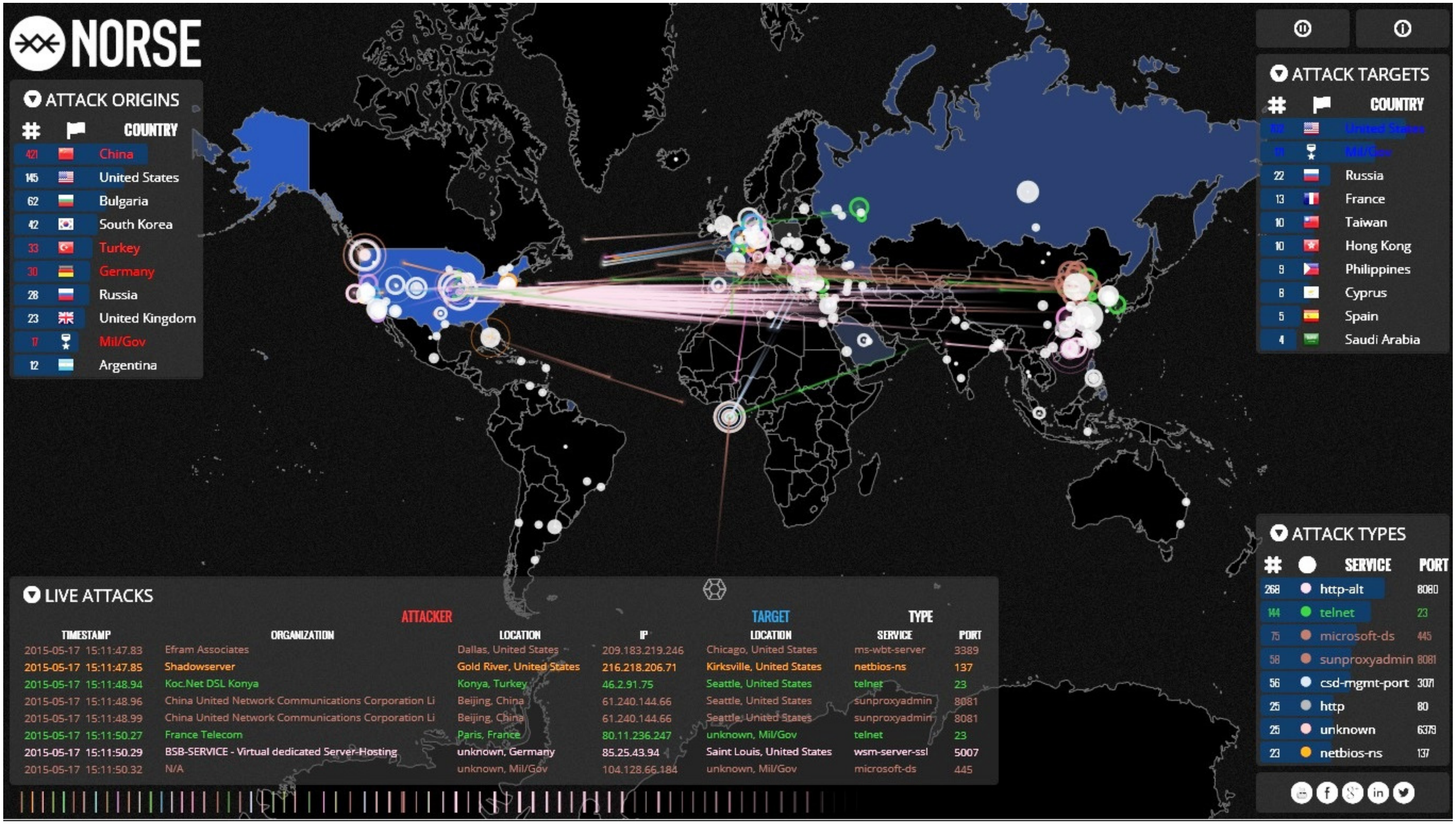
Graph

display graphs for last hour

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

The Cybersecurity Industry 10 Year Challenge:

- Apply AI Apps for Real-Time Cyber Defence -



ATTACK ORIGINS

#	COUNTRY
421	China
145	United States
62	Bulgaria
42	South Korea
33	Turkey
30	Germany
28	Russia
23	United Kingdom
17	Mil/Gov
12	Argentina

ATTACK TARGETS

#	COUNTRY
[illegible]	United States
[illegible]	Mil/Gov
22	Russia
13	France
10	Taiwan
10	Hong Kong
9	Philippines
8	Cyprus
5	Spain
4	Saudi Arabia

ATTACK TYPES

#	●	SERVICE	PORT
268	●	http-alt	8080
144	●	telnet	23
75	●	microsoft-ds	445
58	●	sunproxyadmin	8081
56	●	csd-mgmt-port	3071
25	●	http	80
25	●	unknown	6379
23	●	netbios-ns	137

LIVE ATTACKS

	ATTACKER			TARGET	TYPE	
TIMESTAMP	ORGANIZATION	LOCATION	IP	LOCATION	SERVICE	PORT
2015-05-17 15:11:47.83	Efram Associates	Dallas, United States	209.183.219.246	Chicago, United States	ms-wbt-server	3389
2015-05-17 15:11:47.85	Shadowserver	Gold River, United States	216.218.206.71	Kirksville, United States	netbios-ns	137
2015-05-17 15:11:48.94	Koc.Net DSL Konya	Konya, Turkey	46.2.91.75	Seattle, United States	telnet	23
2015-05-17 15:11:48.96	China United Network Communications Corporation Li	Beijing, China	61.240.144.66	Seattle, United States	sunproxyadmin	8081
2015-05-17 15:11:48.99	China United Network Communications Corporation Li	Beijing, China	61.240.144.66	Seattle, United States	sunproxyadmin	8081
2015-05-17 15:11:50.27	France Telecom	Paris, France	80.11.236.247	unknown, Mil/Gov	telnet	23
2015-05-17 15:11:50.29	BSB-SERVICE - Virtual dedicated Server-Hosting	unknown, Germany	85.25.43.94	Saint Louis, United States	wsm-server-ssl	5007
2015-05-17 15:11:50.32	N/A	unknown, Mil/Gov	104.128.66.184	unknown, Mil/Gov	microsoft-ds	445

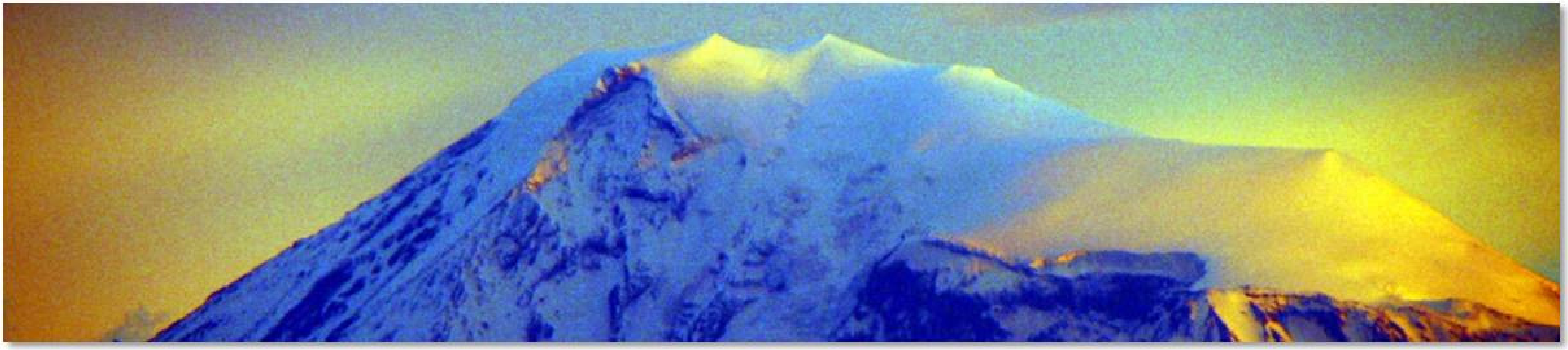
Deploy *Light-Speed "AI-Neural Security"* against 24/7 Attacks from *"Bad Guys"*

The Cybersecurity Industry 10 Year Challenge:

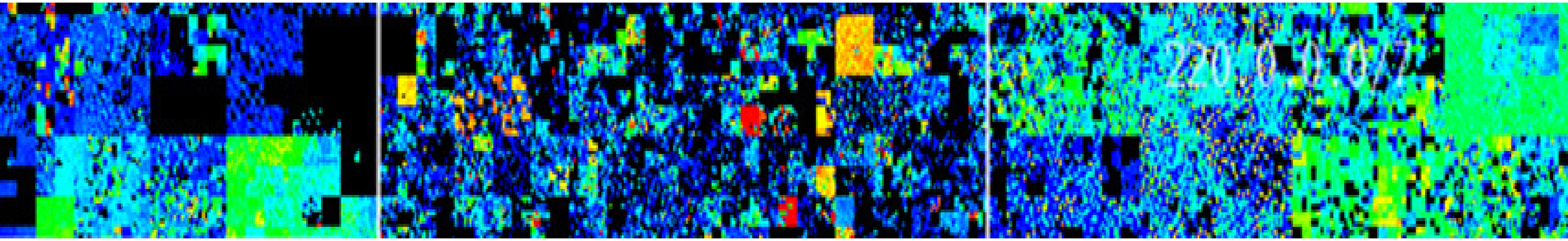
- Apply AI Apps for Real-Time Cyber Defence -

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

"CyberSecurity Vision": *2017–2027 & Beyond!*



1 – Cyber Crime, Cyber Terror & Cyber War	2 – CyberVision: 21stC Players & Threats	3 – CyberSecurity: 21stC Radical Innovation
4 – Scenario 2018 - CSO: C-Suite Integration **"Integrated"**	5 –Scenario 2020 – Internet of Things(IoT) **"Adaptive"**	6 – Scenario 2025 - AI & Machine Learning **"Intelligent"**
7 – In-Depth: Critical Sector Scenarios"	8 – From CyberVision to Business Reality!	**9 – *YOUR* TOP 10 Actions & RoadMap**



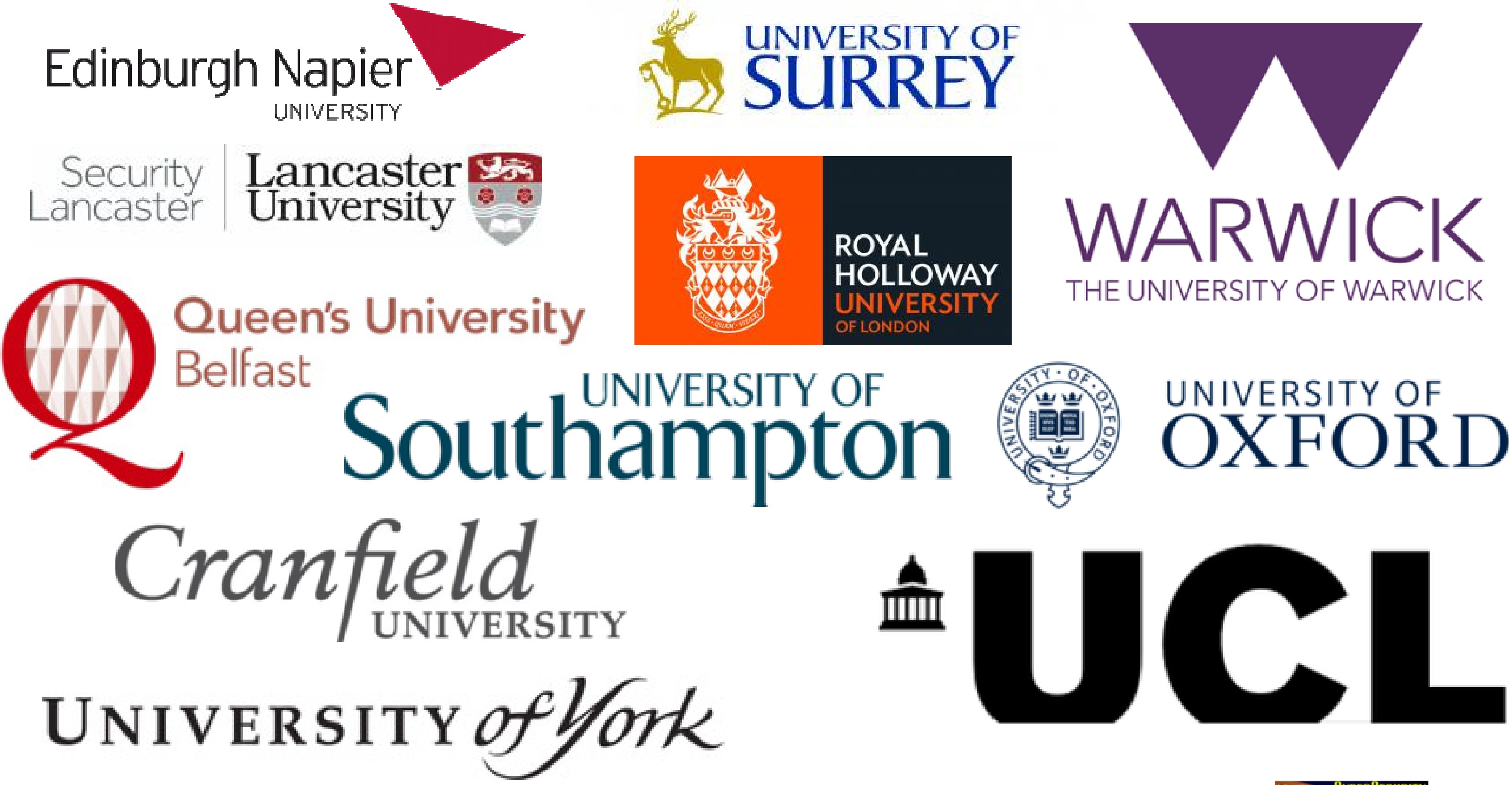
YOUR TOP 10 Actions & RoadMap

1) Assign CSO – Chief Security Officer with Strategic Security Action Plan
2) Professional CyberSecurity Training to International Certification - CISSP
3) Implement International Security Standards (ISO/IEC- Biometrics)
4) Open Discussions with “Cyber” Vendors and Trial AI/ML Tools
5) Profile YOUR Security Staff and Contractors for Possible Risks

6) ICT: Hire Qualified Cybersecurity Systems Technology, Software & Operations Team
7) Review Security Risks & Connectivity of ALL Enterprise IP Legacy Assets & Devices (IoT)
8) Design Practical Multi-Year Roadmap for Strategic Operational Security Integration
9) Professional Association Membership for Team Networking & Skill Building - IPSA
10) Cyber Legal Protection – Check *Your* Legacy Contracts for “Cyber Theft” Trading Risks

Now ***YOUR*** Business will be Fully Fit to Defend against ***“Smart” Cyber-Physical*** Attacks!

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


Edinburgh Napier UNIVERSITY
UNIVERSITY OF SURREY
Security Lancaster
Lancaster University
ROYAL HOLLOWAY UNIVERSITY OF LONDON
WARWICK THE UNIVERSITY OF WARWICK
Queen's University Belfast
UNIVERSITY OF Southampton
UNIVERSITY OF OXFORD
Cranfield UNIVERSITY
UCL
UNIVERSITY of York

“Real-Time Security” @ “Light Speed”!

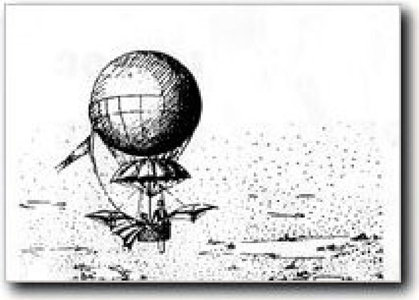
Machine Learning Cybersecurity Tools Provide Real-Time

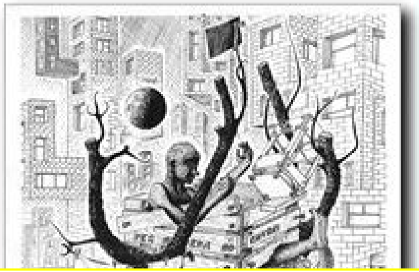
“Light Speed”

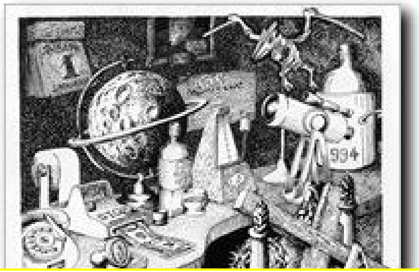
Defence against Threats & Attacks!

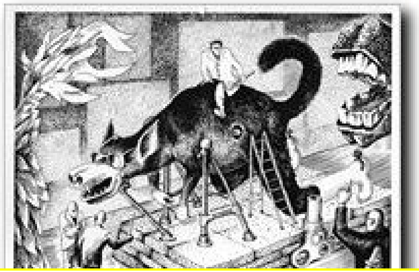
“Frog Spirit shows the Ring of Dark Matter around the Sun” - 2002

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

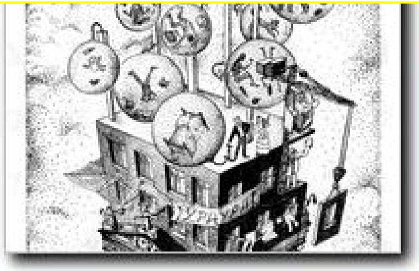


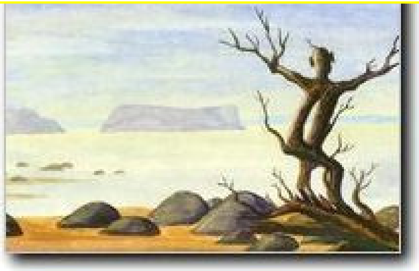


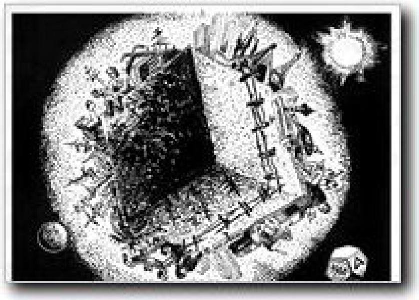




The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov







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

"CyberVision": *21stC Business Architectures*

International East-West Security Conference: Rome

Download Presentation Slides:

www.Valentina.net/Rome2016/

“CyberVision”: *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 November2016 -
© *Dr David E. Probert : www.VAZA.com* ©

1

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 (1) –"21stC Smart Security"

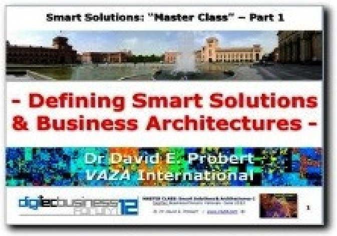
Theme (2) –"CyberVision: 2017-2027"

Download Link: www.valentina.net/Rome2016/

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

Thank you for your time!

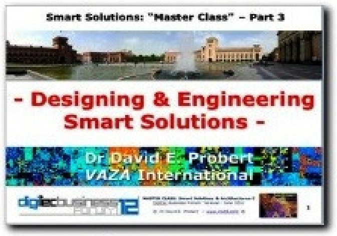
Additional *Cybersecurity* Resources


Smart Solutions: "Master Class" – Part 1

- Defining Smart Solutions & Business Architectures -

Dr David E. Probert
VAZA International

"Master Class - Smart Theory & Practice


Smart Solutions: "Master Class" – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

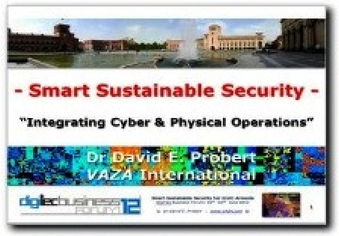
"Master Class 2012 - Smart Design"

- Armenia: Smart Economy -

"Smart Business Architectures for Intelligent Economic Development"

Dr David E. Probert
VAZA International

"21stC Armenia- 2012: Smart Economy"


- Smart Sustainable Security -

"Integrating Cyber & Physical Operations"

Dr David E. Probert
VAZA International

"21stC Armenia - 2012: Smart Security"

- Smart Governance -

"Stimulating Innovation & Economic Growth"

Dr David E. Probert
VAZA International

"21stC Armenia: Smart Governance"

"Real-Time Armenia"

Securing Government & Financial Enterprise Operations

"Real-Time Armenia" - White Paper

"Real-Time" ARMENIA!...

...Securing Government & Financial Enterprise Operations

Dr David E Probert
VAZA International

"Real-Time Armenia" - Slides

"Awesome Armenia!"
Photos and Panoramas

Armenia Spring - 2009

Armenia Summer 2009

Armenian Panoramas Summer - 2009

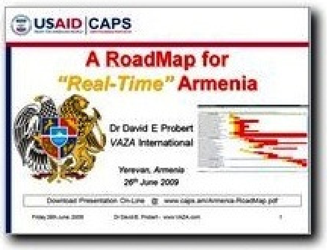
Awesome Armenia: In Photos

"Roadmap for Real-Time Armenia"

E-Government, E-Commerce and E-Security

USAID | CAPS

Roadmap for Real-Time Armenia- Report


USAID | CAPS

A RoadMap for "Real-Time" Armenia

Dr David E Probert
VAZA International

Yerevan, Armenia
26th June 2009

RoadMap for Real-Time Armenia- Slides

"Real-Time" Georgia!.....

.....Securing Government & Enterprise Operations

Dr David E Probert
VAZA International

"Real-Time Georgia" - GITI 2008 Slides

"Real-Time Georgia"

Securing Government & Enterprise Operations

"Real-Time Georgia" - GITI 2008 Paper

"Republic of Georgia"
Photos and Panoramas

Georgian Panoramas Autumn 2007

Caucasus Aerial Panoramas

Georgian Panoramas Autumn 2008

Georgia 2008

Gorgeous Georgia: In Photos

..."21stC Georgia"...

..."Cyber-Vardzia"...

21stC Georgia: "CyberVardzia" - Paper

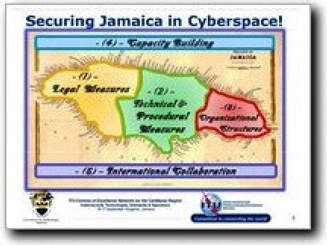
21stC Georgia – "Cyber Vardzia"

"Integrated Cyber & Physical Security"

for e-Government & e-Georgia

Dr David E. Probert
VAZA International

21stC Georgia - "CyberVardzia" - Slides


Securing Jamaica in Cyberspace!

- (4) - Capacity Building

- (1) - Legal Measures

- (2) - Technical & Procedural Measures

- (3) - Organisational Structures

- (5) - International Collaboration

Jamaica: Cybersecurity Technology- Slides

* ITU Cybersecurity Strategy *

"3-Day Workshop Overview"

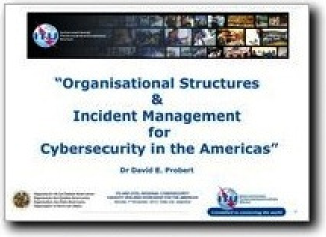
Workshop Presentations

Group Tasks & Discussions

Jamaica: Cybersecurity Strategy- Slides

Dr. David E PROBERT (Executive Director, VAZA International)

"Short Professional Bio"


"Organisational Structures & Incident Management for Cybersecurity in the Americas"

Dr David E. Probert

ITU/CITEL: Cybersecurity in the Americas

"Cybersecurity Capacity Building & International Collaboration "

Dr David E. Probert

ITU/CITEL: Cybersecurity Skills Building

Link: www.valentina.net/vaza/CyberDocs

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, and then by UN/ITU to review Cybersecurity for the Government Ministries.

- ***UN/ITU*** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

Dr David E. Probert is a Fellow of the Royal Statistical Society, IEEE Life Member and 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 -

Smart Solutions: "Master Class" – Part 1

- Defining Smart Solutions & Business Architectures -

Dr David E. Probert
VAZA International

MASTER CLASS: Smart Solutions & Architectures-1
DigiTec Business Forum: Yerevan - June 2012
© Dr David E. Probert : www.VAZA.com ©

1

"Master Class - Smart Theory"

Smart Solutions: "Master Class" – Part 2

- Smart Solutions in Practice for 21stC Armenia -

Dr David E. Probert
VAZA International

MASTER CLASS: Smart Solutions & Architectures-2
DigiTec Business Forum: Yerevan - June 2012
© Dr David E. Probert : www.VAZA.com ©

1

"Master Class - Smart Practice"

Smart Solutions: "Master Class" – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

MASTER CLASS: Smart Solutions & Architectures-3
DigiTec Business Forum: Yerevan - June 2012
© Dr David E. Probert : www.VAZA.com ©

1

"Master Class - Smart Design"

- Armenia: Smart Economy -

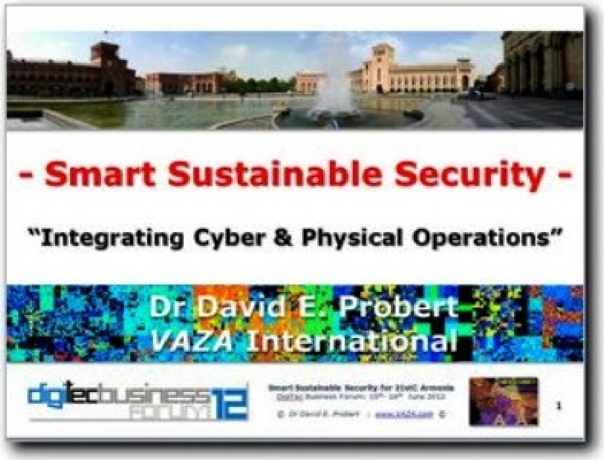
"Smart Business Architectures for Intelligent Economic Development"

Dr David E. Probert
VAZA International

Smart Business Architectures for 21stC Armenia
DigiTec Business Forum: 15th - 16th June 2012
© Dr David E. Probert : www.VAZA.com ©

1

"Armenia: Smart Economy"



- Smart Sustainable Security -

"Integrating Cyber & Physical Operations"

Dr David E. Probert
VAZA International

Smart Sustainable Security for 21stC Armenia
DigiTec Business Forum: 15th - 16th June 2012
© Dr David E. Probert : www.VAZA.com ©

1

"Armenia: Smart Sustainable Security"

- Smart Governance -

"Stimulating Innovation & Economic Growth"

Dr David E. Probert
VAZA International

Smart Governance for 21stC Armenia
DigiTec Business Forum: 15th - 16th June 2012
© Dr David E. Probert : www.VAZA.com ©

1

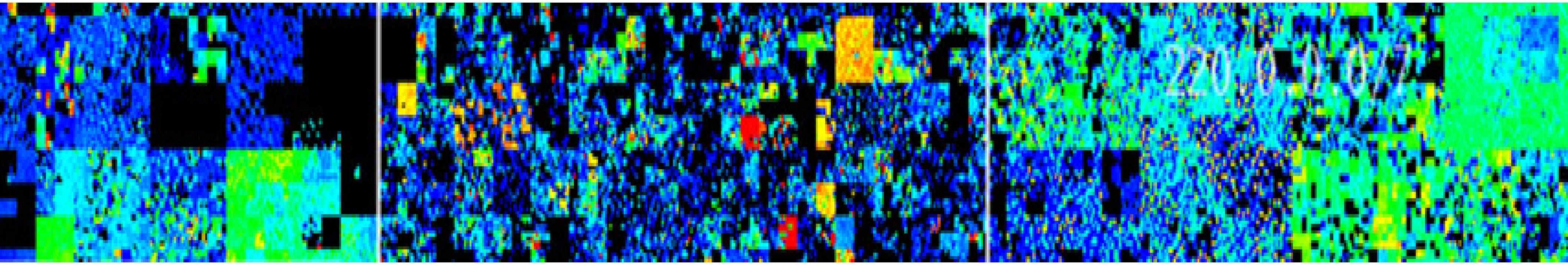
"Armenia: Smart Governance"

Download: www.valentina.net/DigiTec2012/

“CyberSecurity Vision”: *2017–2027 & Beyond!*

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

BACK-UP SLIDES



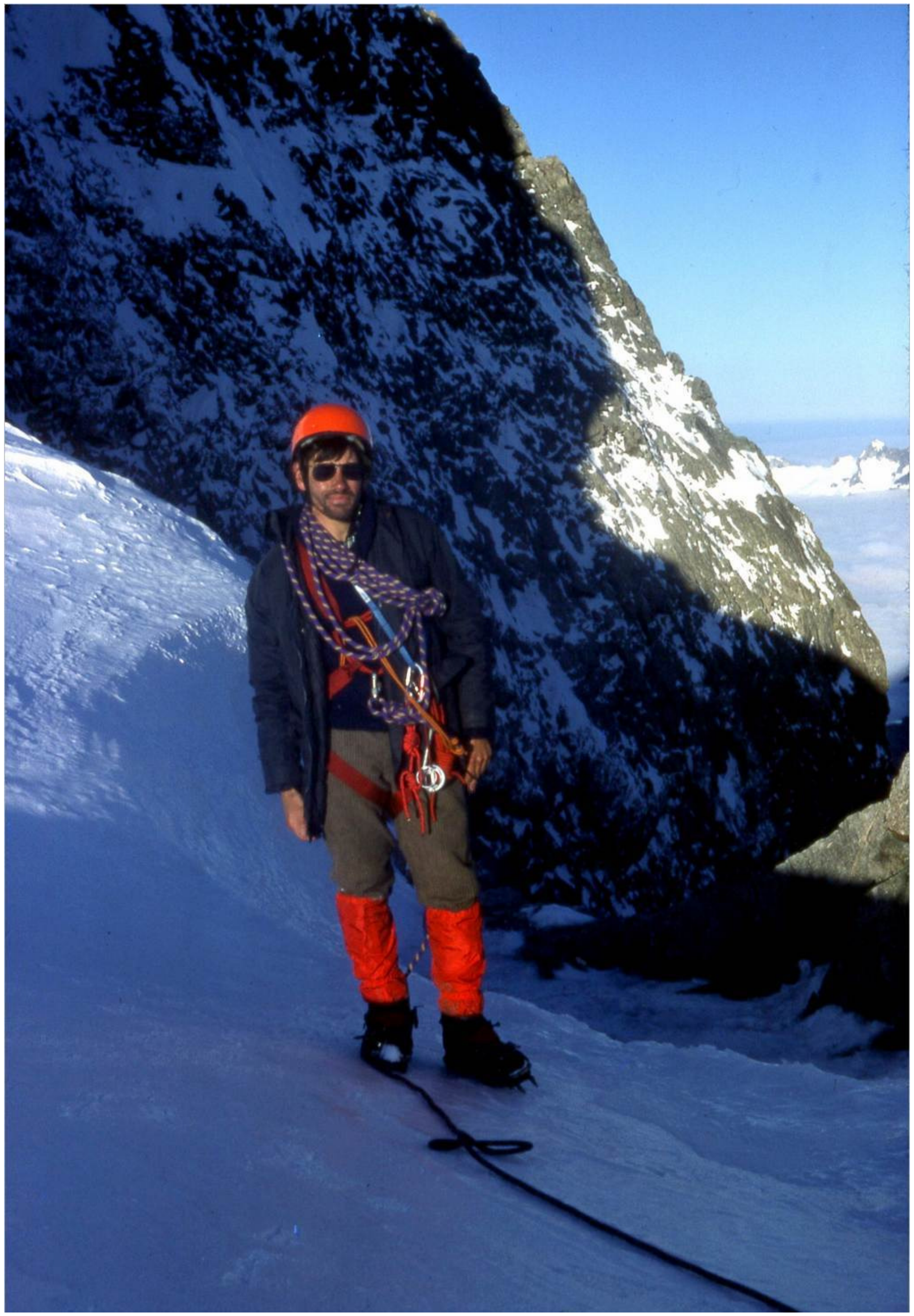
*** Security Equipment for Alpine Climbing ***

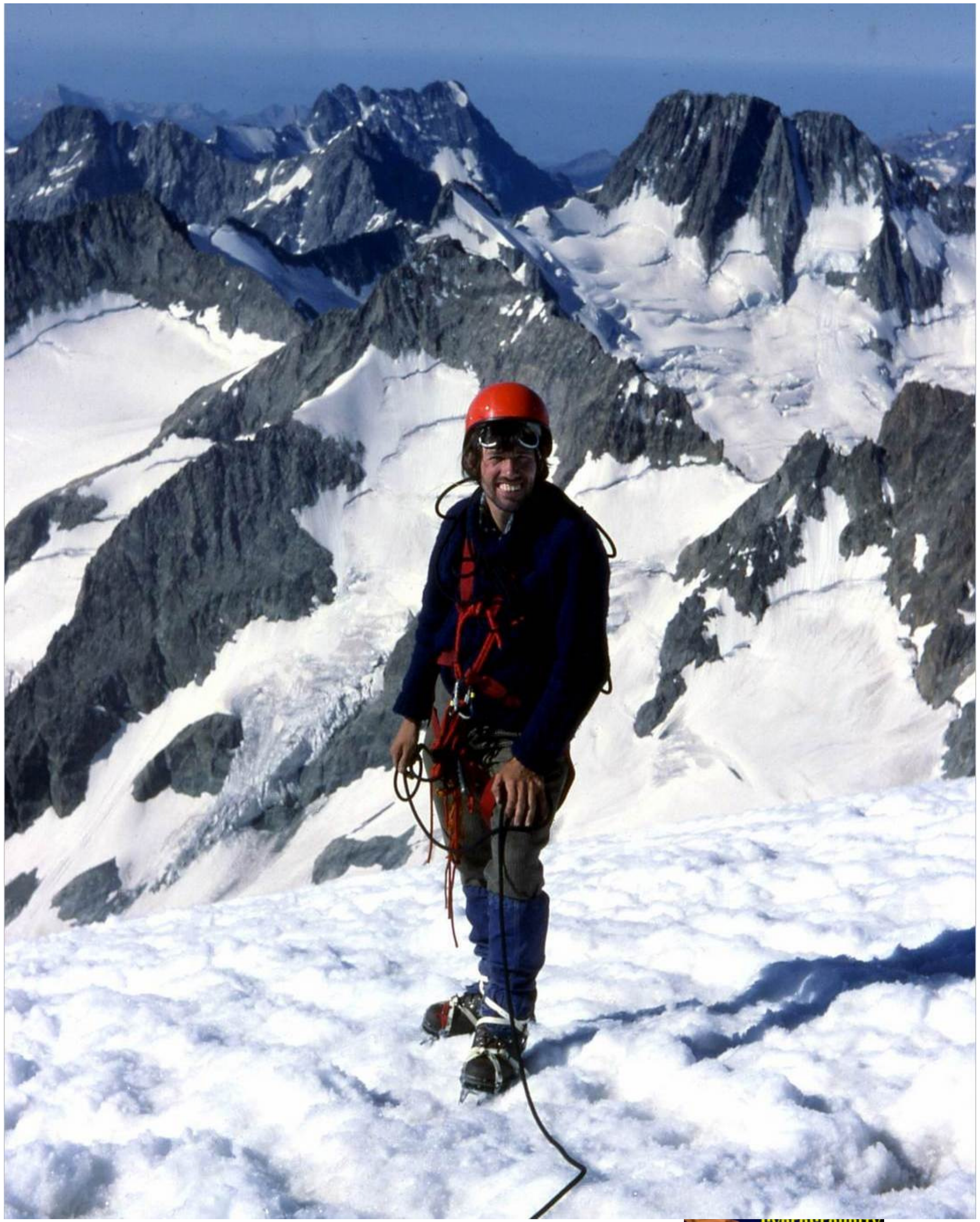
Sunrise on « Barre des Écrins » – 4102metres

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

15th Sept 2015: « 7 Alpinistes died in Avalanche »

Security Equipment for *Alpine Ascents*





- Secure Navigation in the *"Southern Seas"* -

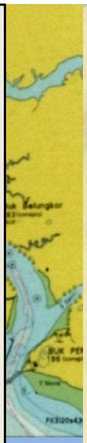
"Captain James Horsburgh" (1762 – 1836)

Charting the *"Southern Seas"*

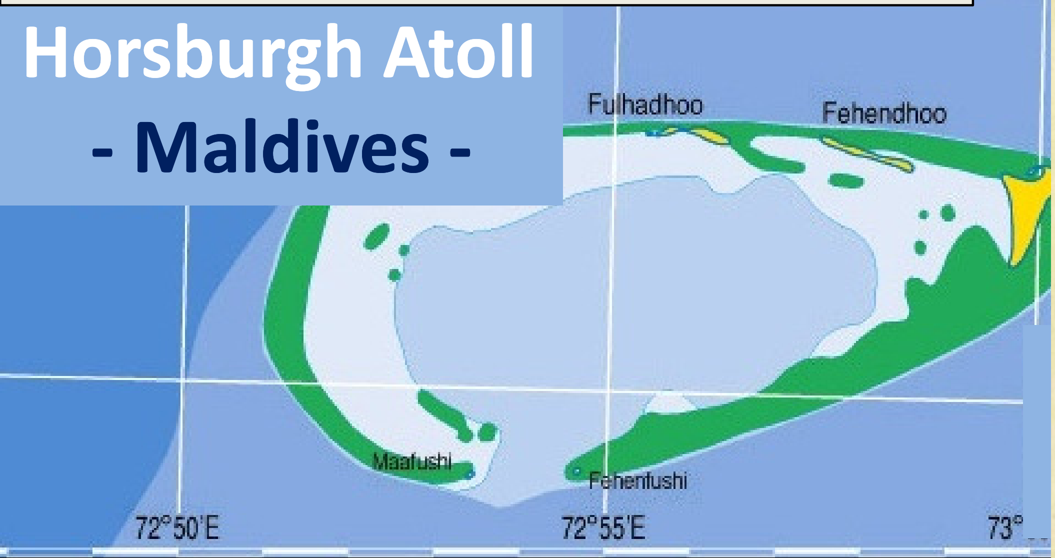
-"The India Directory"(1809) -

for "The East India Company"

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

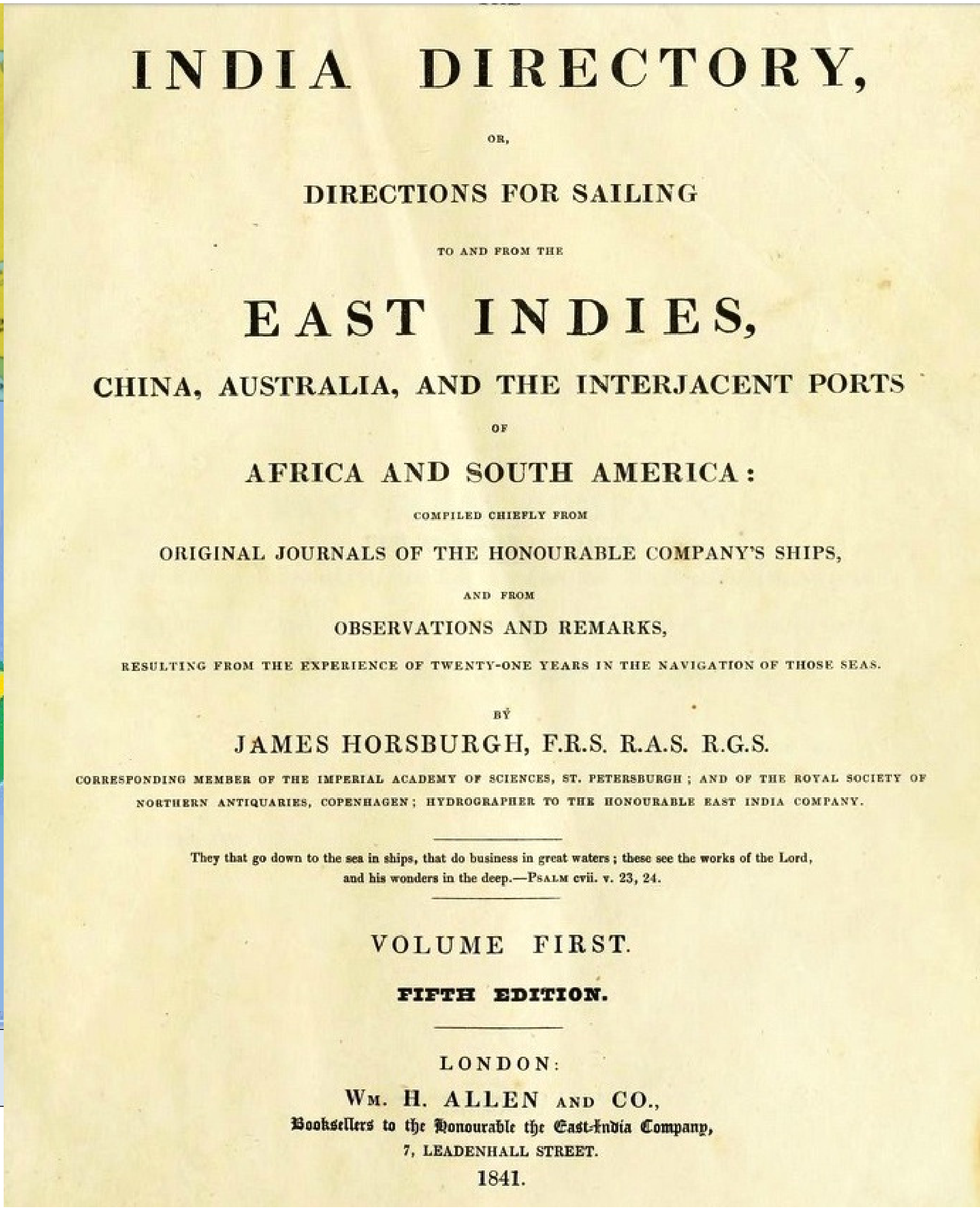


H



Horsburgh Atoll

- Maldives -



INDIA DIRECTORY,

OR,

DIRECTIONS FOR SAILING

TO AND FROM THE

EAST INDIES,

CHINA, AUSTRALIA, AND THE INTERJACENT PORTS

OF

AFRICA AND SOUTH AMERICA:

COMPILED CHIEFLY FROM

ORIGINAL JOURNALS OF THE HONOURABLE COMPANY'S SHIPS,

AND FROM

OBSERVATIONS AND REMARKS,

RESULTING FROM THE EXPERIENCE OF TWENTY-ONE YEARS IN THE NAVIGATION OF THOSE SEAS.

BY

JAMES HORSBURGH, F.R.S. R.A.S. R.G.S.

CORRESPONDING MEMBER OF THE IMPERIAL ACADEMY OF SCIENCES, ST. PETERSBURGH; AND OF THE ROYAL SOCIETY OF NORTHERN ANTIQUARIES, COPENHAGEN; HYDROGRAPHER TO THE HONOURABLE EAST INDIA COMPANY.

They that go down to the sea in ships, that do business in great waters; these see the works of the Lord, and his wonders in the deep.—PSALM cvii. v. 23, 24.

VOLUME FIRST.

FIFTH EDITION.

LONDON:
WM. H. ALLEN AND CO.,
Booksellers to the Honourable the East-India Company,
7, LEADENHALL STREET.
1841.

From "Smart Navigation" to "Smart Security"!

34th International East/West Security Conference

- Secure Navigation in the *"Southern Seas"* -

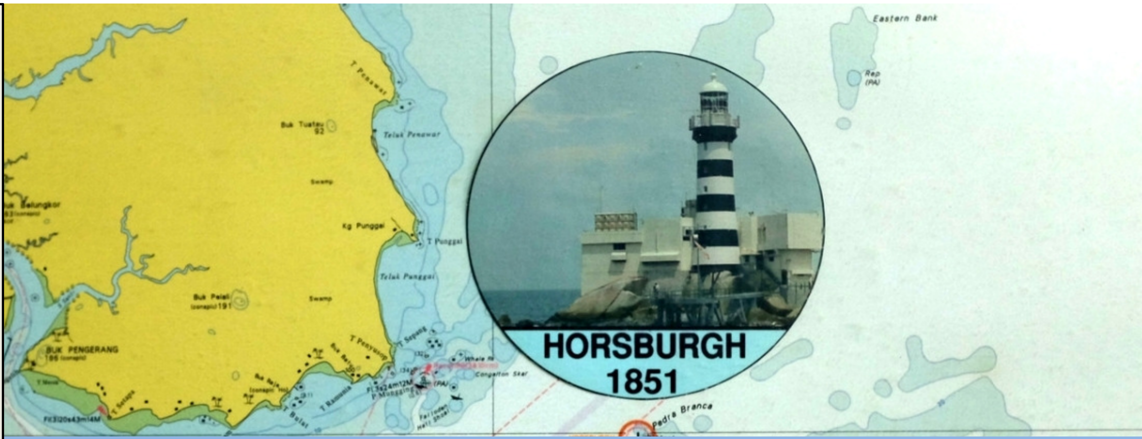
"Captain James Horsburgh" (1762 – 1836)

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

Fulhadhoo
Fehendhoo
Goidhoo
Maafushi
Fehenfushi
72°50'E
72°55'E
73°

Horsburgh Atoll

- Maldives -

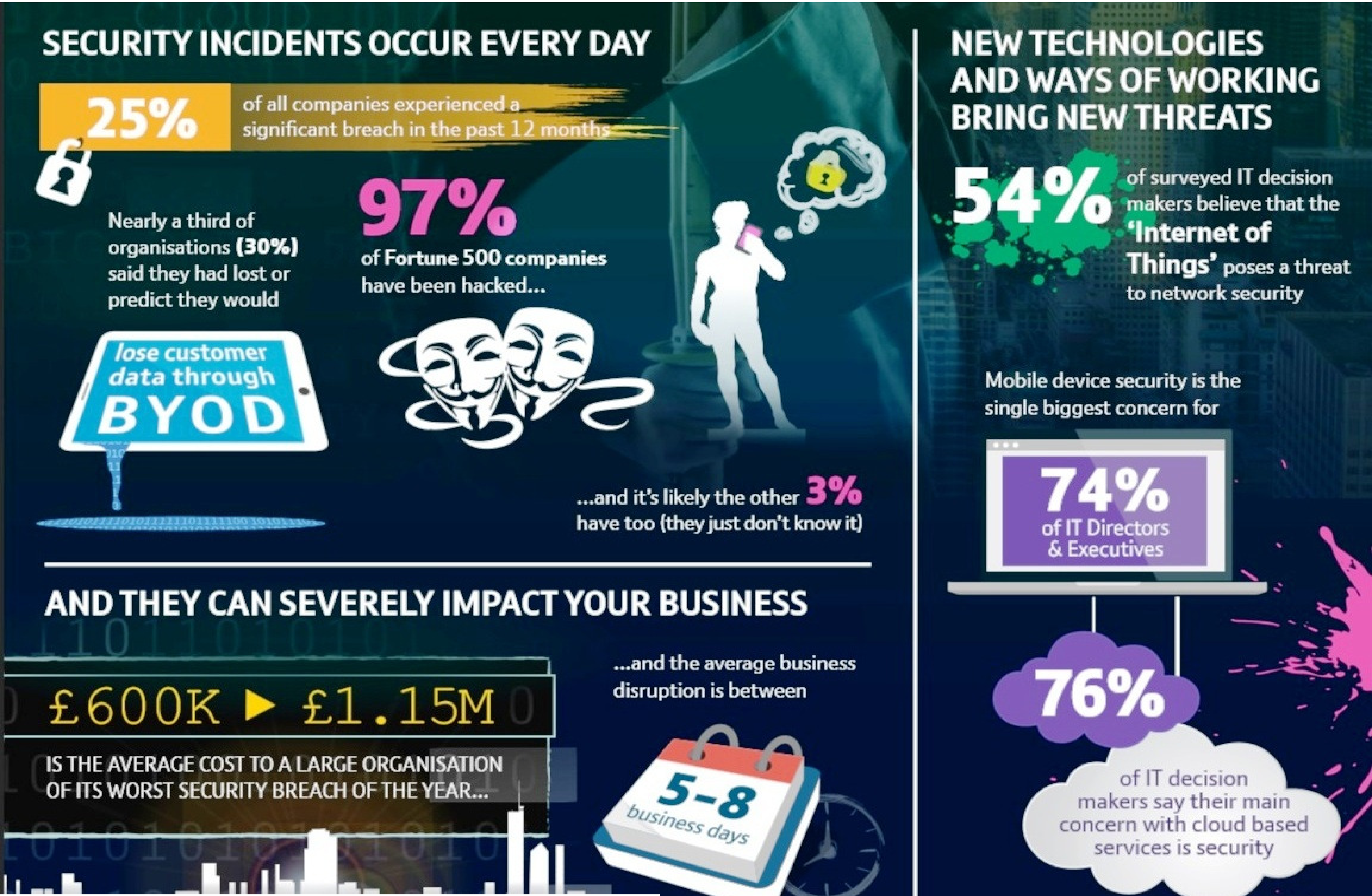
96°50'
Horsburgh Island
Possession Point
Direction Island
Jetty
Port Refuge
Prison Island

Horsburgh Island

-Cocos/Keeling-

From "Smart Navigation" to "Smart Security"!

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



SECURITY INCIDENTS OCCUR EVERY DAY

25% of all companies experienced a significant breach in the past 12 months

Nearly a third of organisations **(30%)** said they had lost or predict they would

lose customer data through **BYOD**

97% of Fortune 500 companies have been hacked...

...and it's likely the other **3%** have too (they just don't know it)

AND THEY CAN SEVERELY IMPACT YOUR BUSINESS

£600K ▶ £1.15M

IS THE AVERAGE COST TO A LARGE ORGANISATION OF ITS WORST SECURITY BREACH OF THE YEAR...

...and the average business disruption is between

5-8 business days

NEW TECHNOLOGIES AND WAYS OF WORKING BRING NEW THREATS

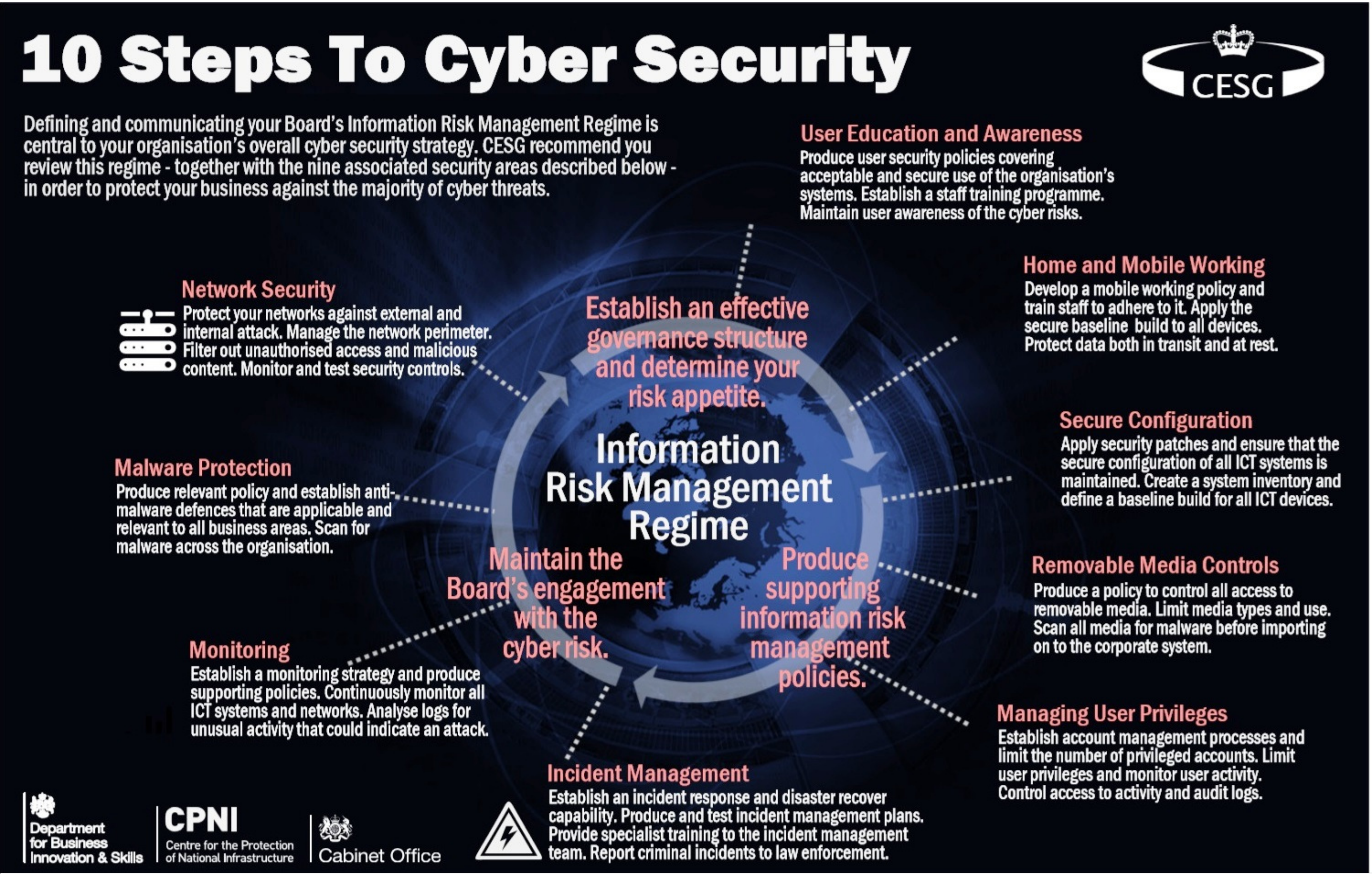
54% of surveyed IT decision makers believe that the **'Internet of Things'** poses a threat to network security

Mobile device security is the single biggest concern for

74% of IT Directors & Executives

76% of IT decision makers say their main concern with cloud based services is security

Link: www.bt.com/rethinking-the-risk



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.

Information Risk Management Regime

Establish an effective governance structure and determine your risk appetite.

Maintain the Board's engagement with the cyber risk.

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.

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.

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.

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.

Department for Business Innovation & Skills
CPNI Centre for the Protection of National Infrastructure
Cabinet Office

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