* 21stC Cybersecurity Trends (2) *

"Advanced Cybersecurity"

- *Artificial Intelligence & Machine Learning* -

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

Dedicated to Grand-Sons: Ethan, Matthew & Roscoe – ***To their Secure Future!***

32nd International East/West Security Conference

"Advanced Enterprise Cybersecurity – Artificial Intelligence & Machine Learning"
- Madrid, Spain: 26th – 27th Oct 2915 -

21stC кибербезопасности Тенденции (2)

Расширенный кибербезопасности

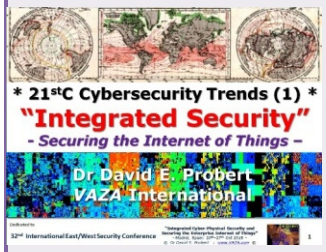
-*Искусственный интеллект и машинного обучения*-

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

Dedicated to Grand-Sons: Ethan, Matthew & Roscoe – ***To their Secure Future!***

Cybersecurity Trends – *"Dual Themes"*

Theme (1) – "Integrated Cyber-Physical Security: *Securing the Internet of Things"*



- *TOTAL Security now requires Integration of Cyber-Physical Operations*
- *Recommendation for Board Level CSO to manage TOTAL Security Ops*
- *Emergence of the "INTERNET of THINGS" as Future Cyber-Conflict Zone*

" Integration": "TOTAL Extended Enterprise Security" ***09:00 - 27th Oct 2015***

Theme (2) – "Advanced Cybersecurity: *Artificial Intelligence & Machine Learning"*

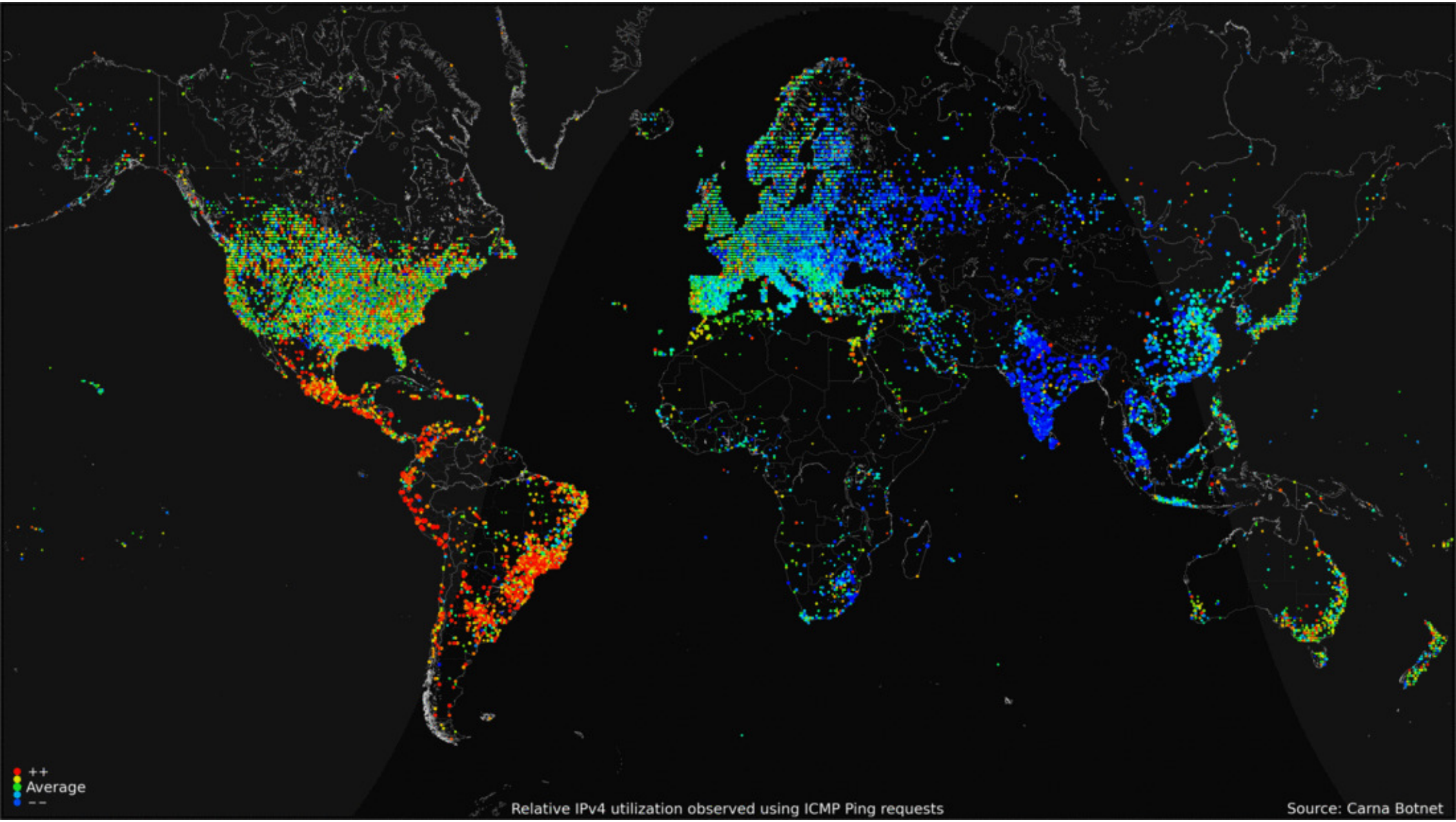
- *Transition from 20thC Security to Hybrid AI-Based 21stC Cyber Models*
- *Using AI & Machine Learning to protect your Enterprise Operations*
- *Developing YOUR Action Plans for Advanced Cybersecurity Solutions!*

"Intelligence": "Real-Time Self-Adaptive Cybersecurity" ***11:15 - 27th Oct 2015***

Download Slides: *www.valentina.net/Madrid2015/*

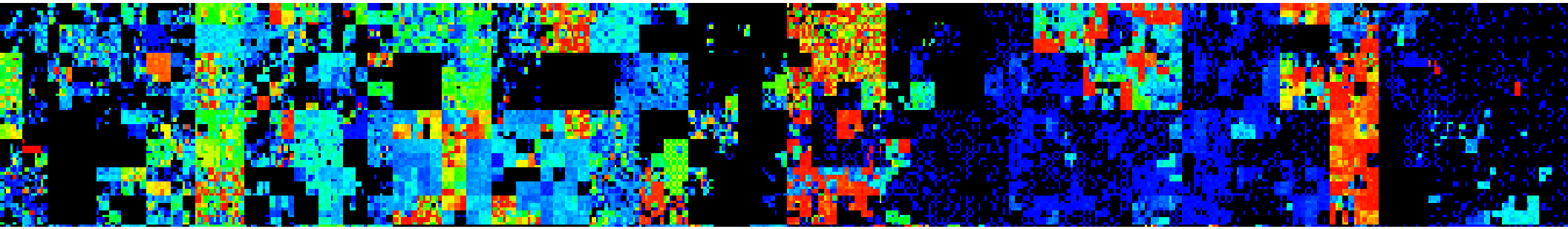
GeoVision 24/7 Internet Connectivity

- "Carna Botnet Internet Census 2012" -



21stC Cybersecurity (2) – *"AI & Machine Learning"*

1 – Background: *20th to 21stC Cybersecurity*	**2 – AI & Machine Learning as Cyber Tools**	**3 – Recent 21stC Cybersecurity Ventures**
4 – Advanced Cyber Scenarios & Analysis	**5 – Hybrid 20thC & 21stC Cyber Solutions**	**6 – Scenario 2020: Integrated Security - IoT**
7 – Scenario 2025: Self-Adaptive Security	**8 – Scenario 2040: Neural Security**	**9 – YOUR Action Plan for Advanced Cyber!**



Background: *20th to 21stC Cybersecurity*

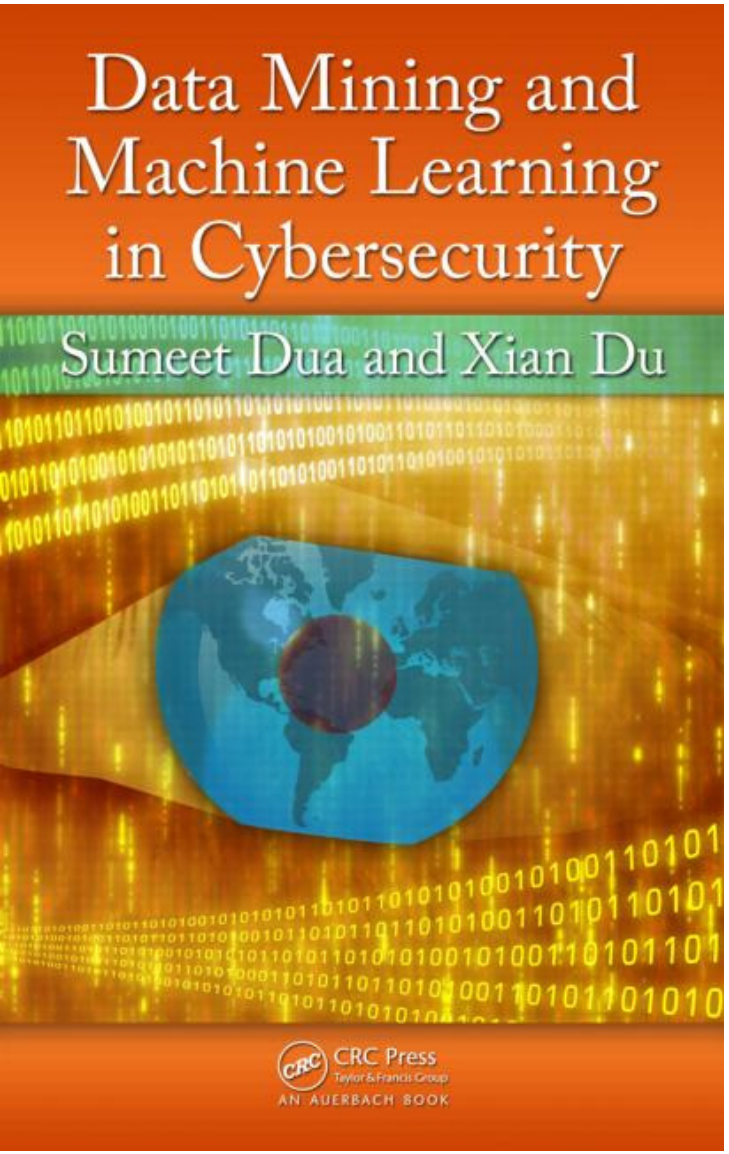
- **20thC – 1995-2010 :** Focus on Firewalls & Antivirus – based upon Physical "Spatial" Security Models (Castles & Moats)

.....Protection @ ***"Speed of Sound"*** *(Space)*

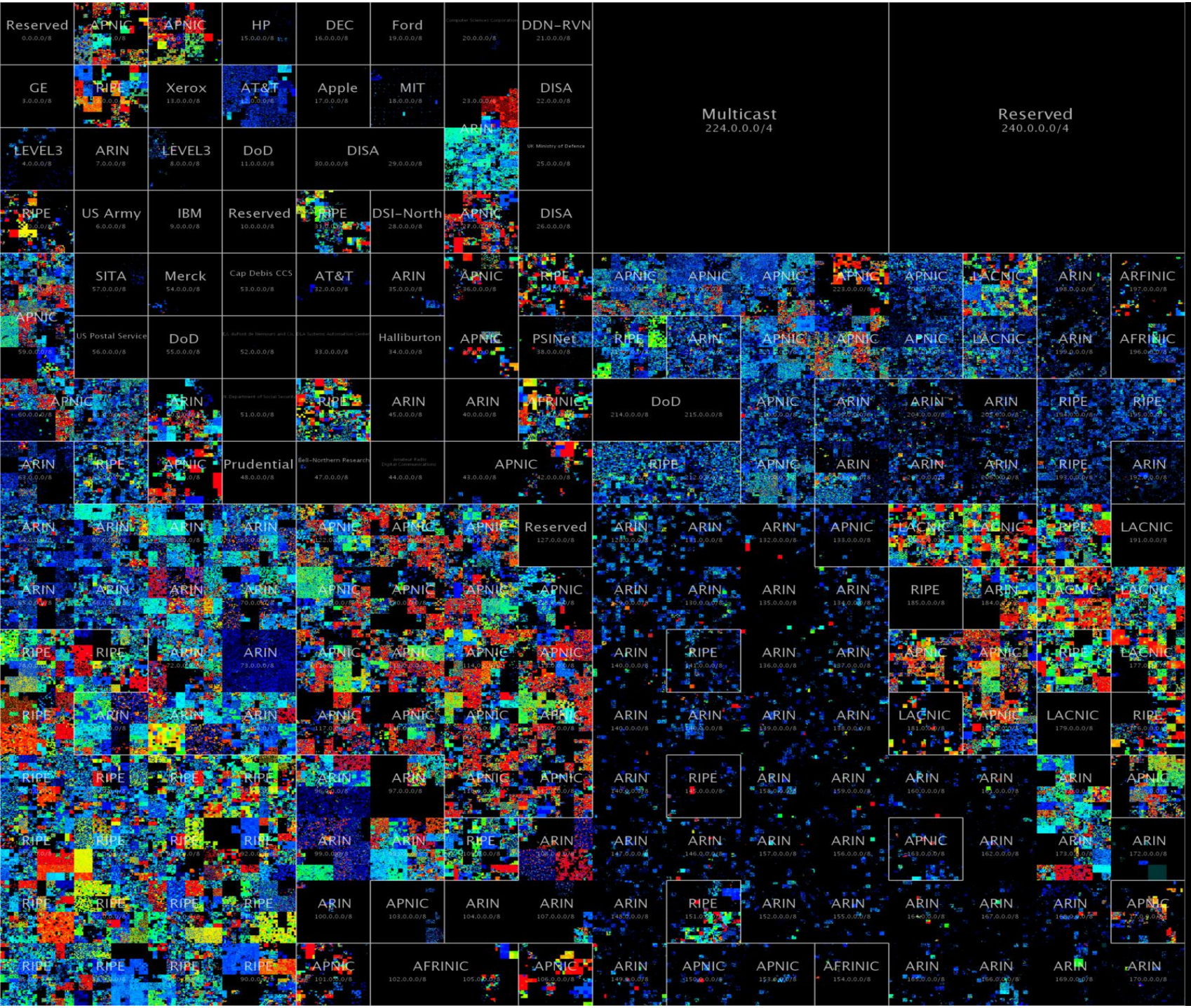
- **21stC – 2010 – 2025 :** Focus on Adaptive, and Self-Organising "Cyber" Tools – based upon Temporal Models (AI & Machine Learning)

.....Defending @ ***"Speed of Light"*** *(Time)*

"Machine Learning Methods" for Cybersecurity developed from 2010



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



IPv4 Census Map

June – October 2012

Utilization

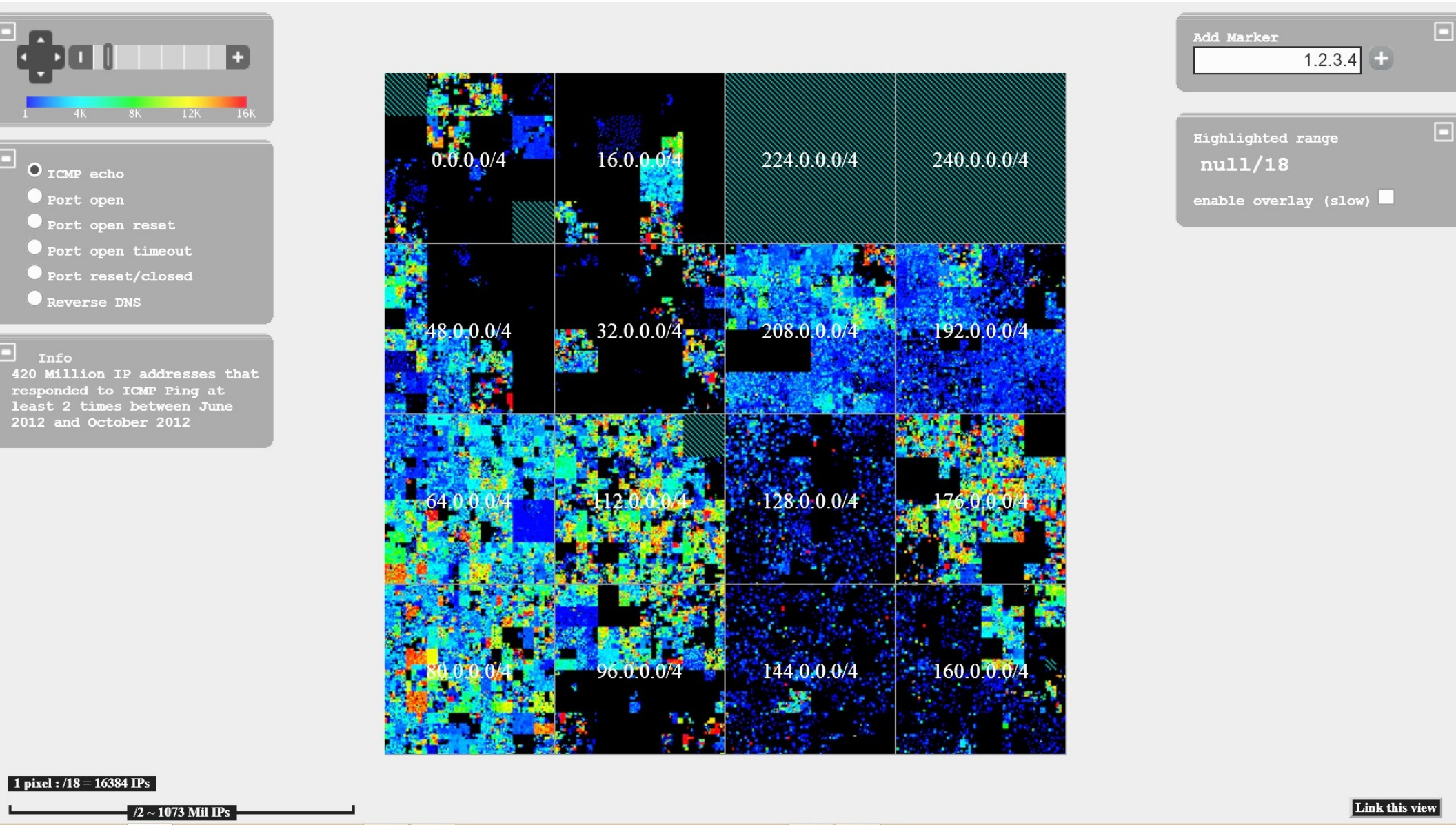
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

Prefix Sizes

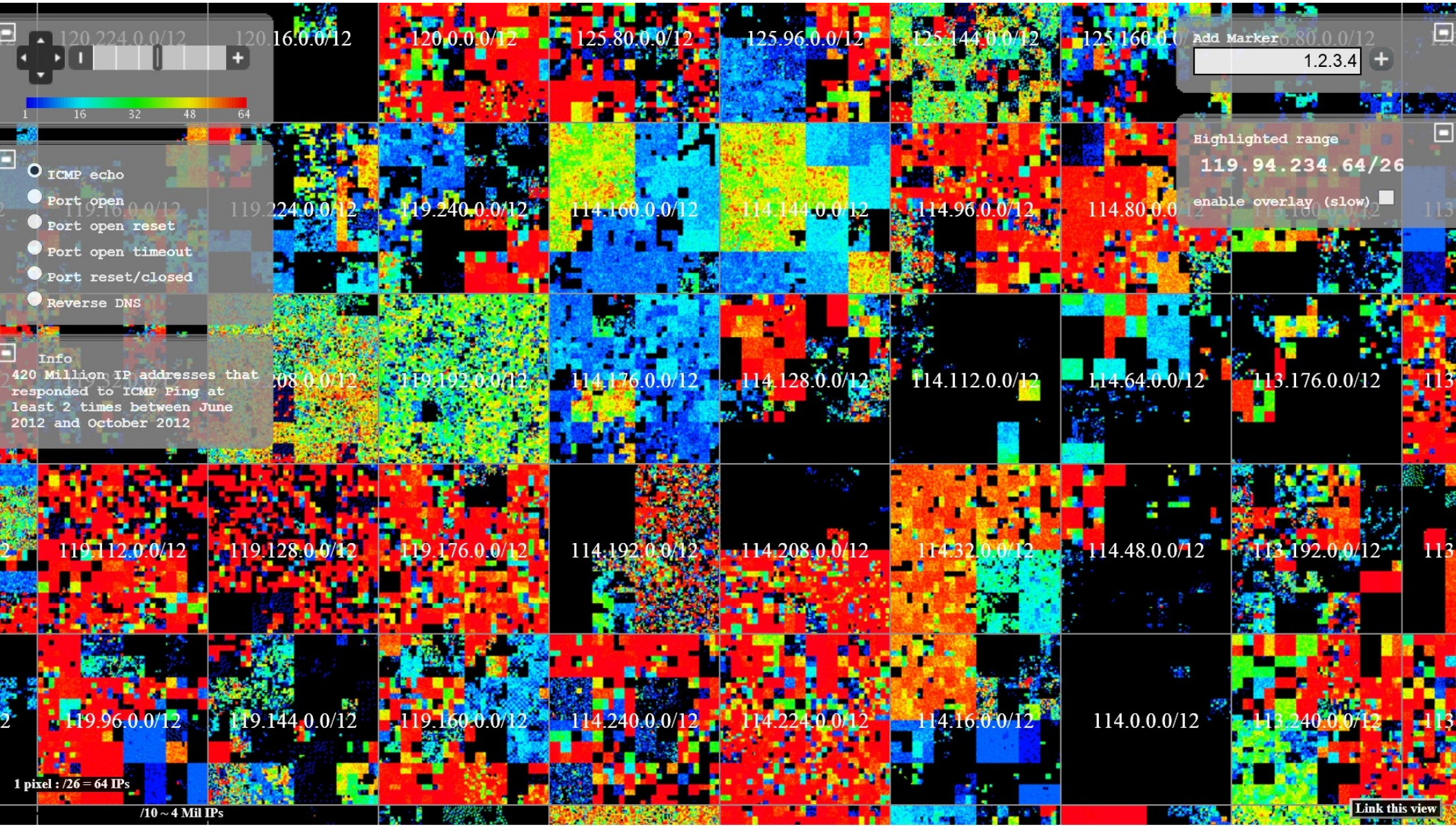
= /8
= /12
= /16
= /20
= /24

420 Million hosts that responded to ICMP Ping at least 2 times between June and October 2012
Source: Carna Botnet

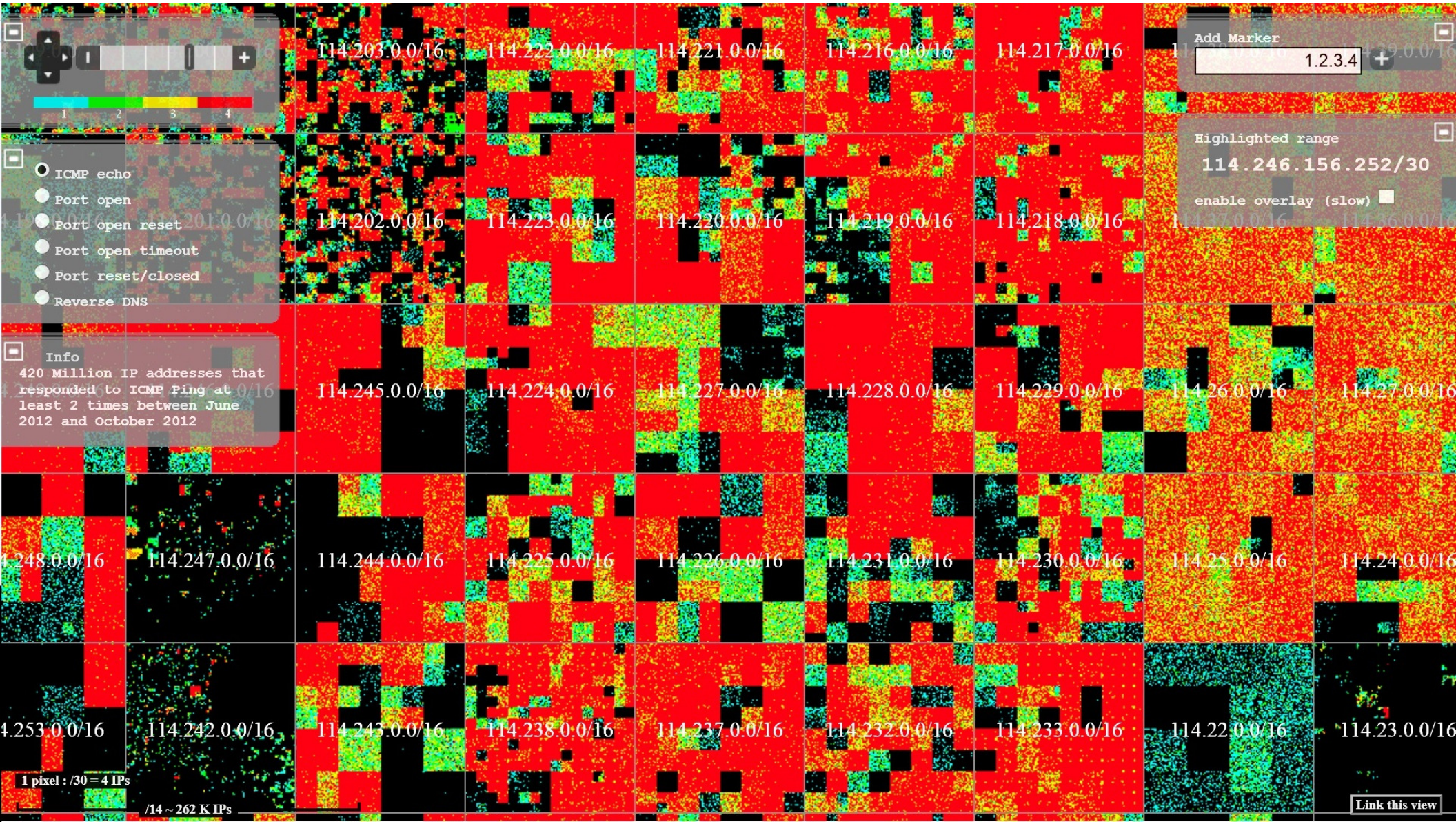
Cyberspace Browser: *Internet Census 2012*



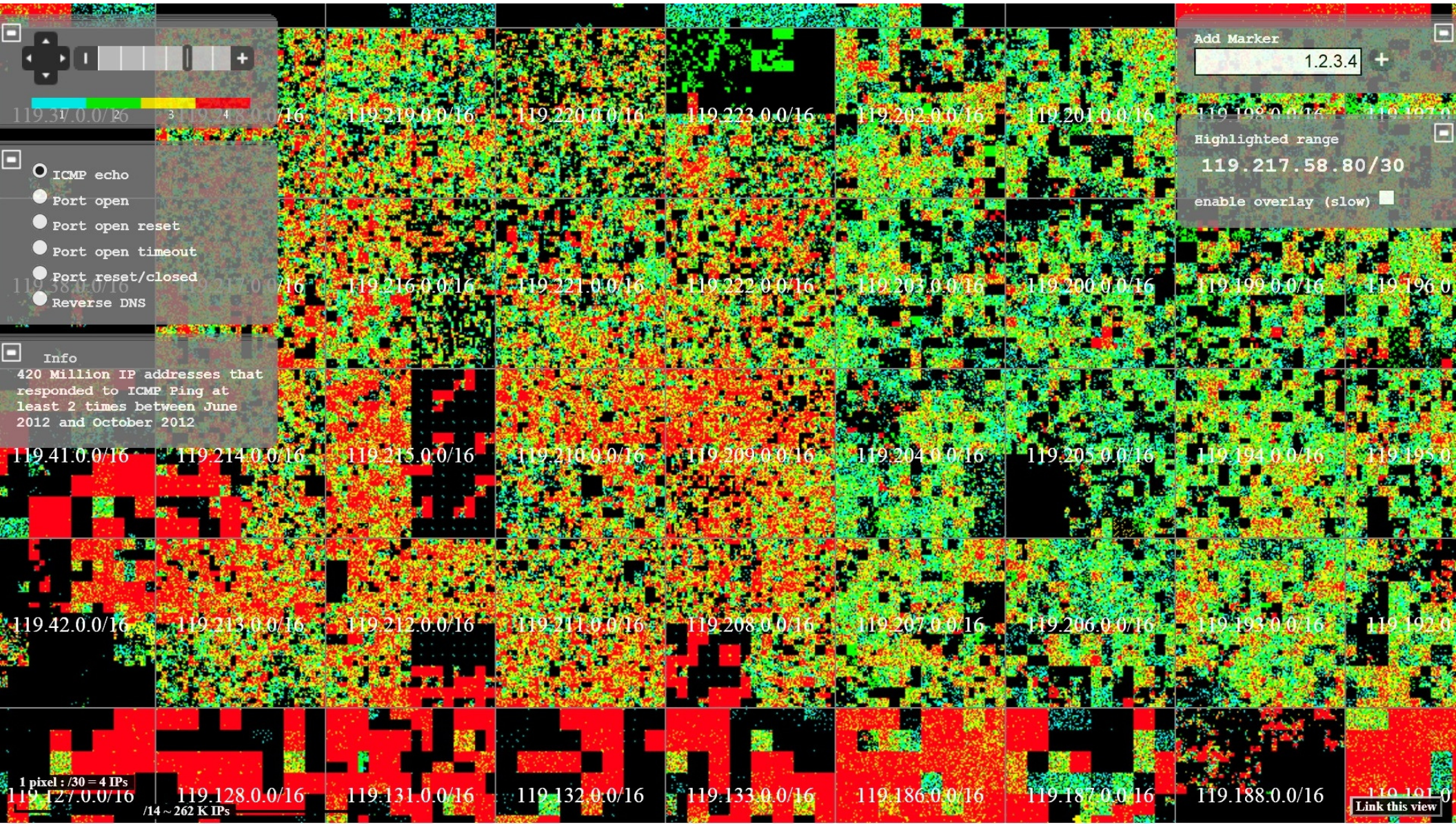
Cyberspace (Hilbert Map): *Browser Zoom(1)*



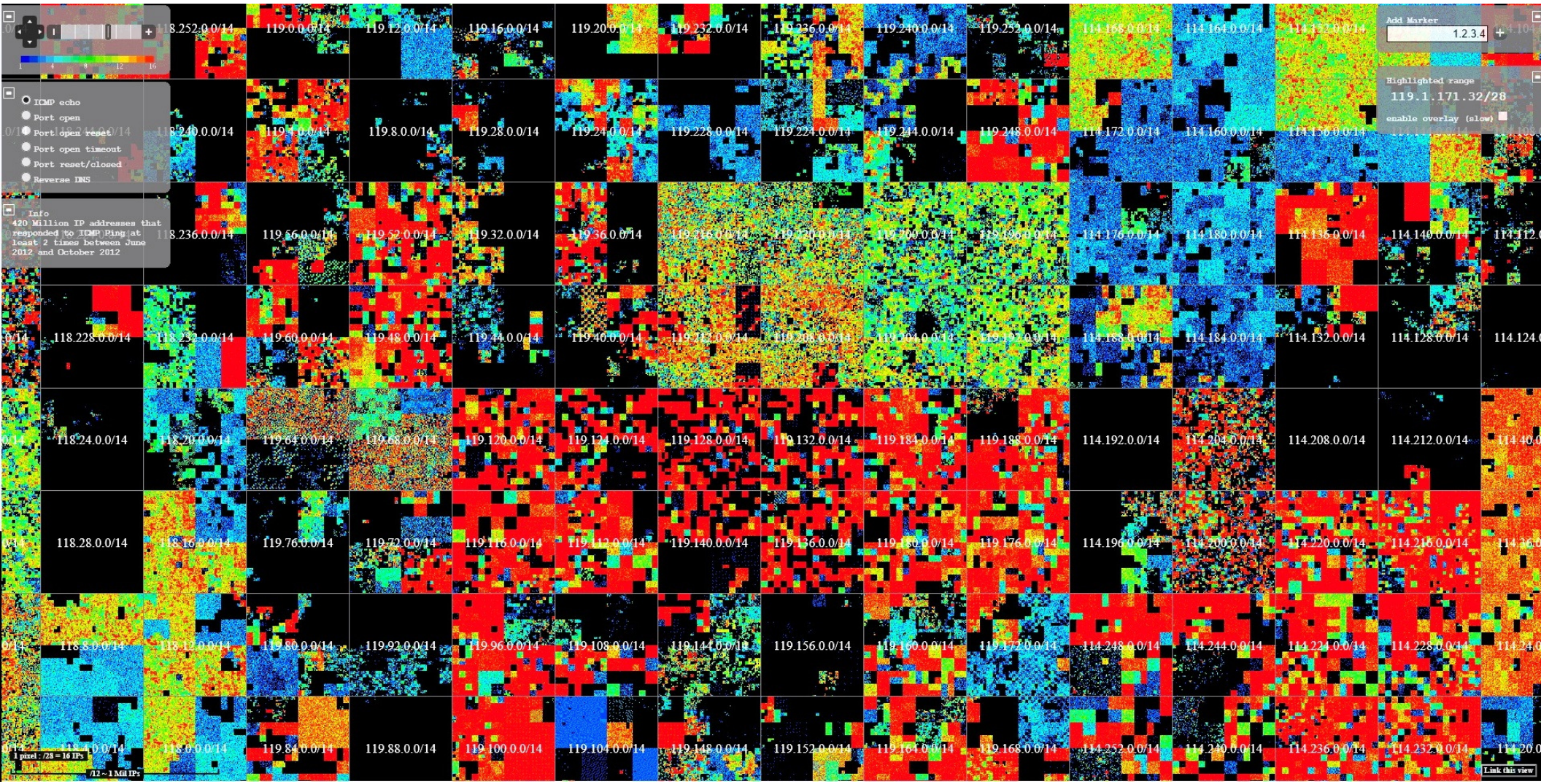
Cyberspace (Hilbert Map): *Browser Zoom(2)*



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



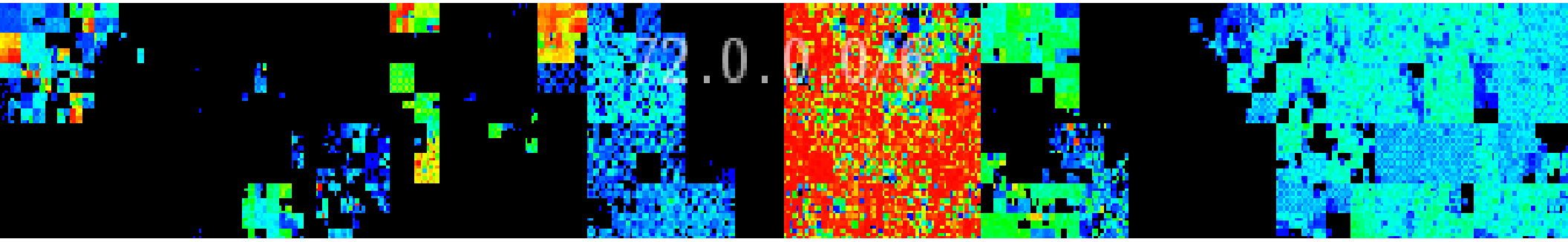
Cyberspace (Hilbert Map): *Browser Zoom(4)*



Link: internetcensus2012.bitbucket.org/hilbert/

21stC Cybersecurity (2) – *"AI & Machine Learning"*

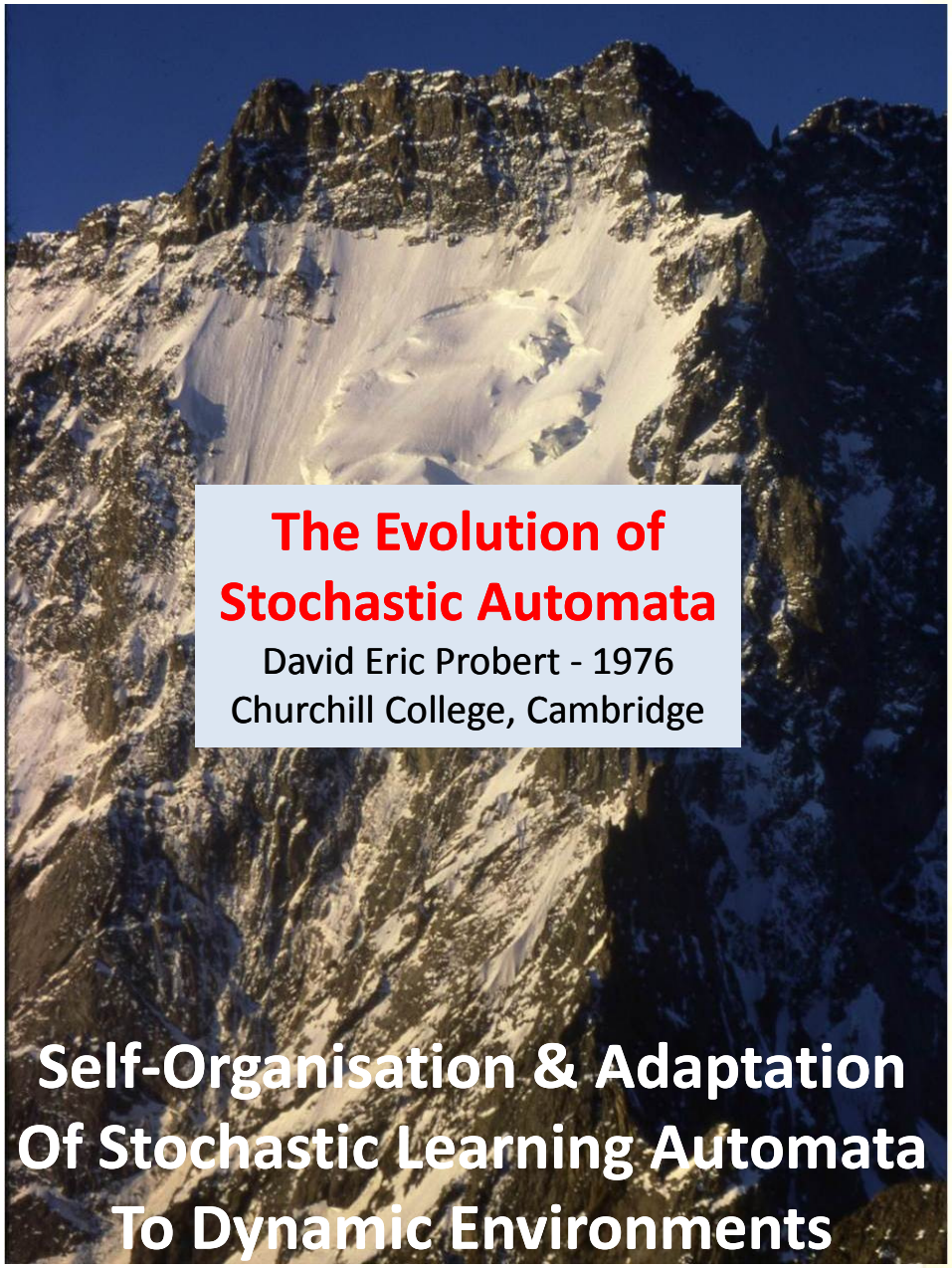
1 – Background: 20th to 21stC Cybersecurity	**2 – AI & Machine Learning as Cyber Tools**	3 – Recent 21stC Cybersecurity Ventures
4 – Advanced Cyber Scenarios & Analysis	5 – Hybrid 20thC & 21stC Cyber Solutions	6 – Scenario 2020: Integrated Security - IoT
7 – Scenario 2025: Self-Adaptive Security	8 – Scenario 2040: Neural Security	9 – YOUR Action Plan for Advanced Cyber!

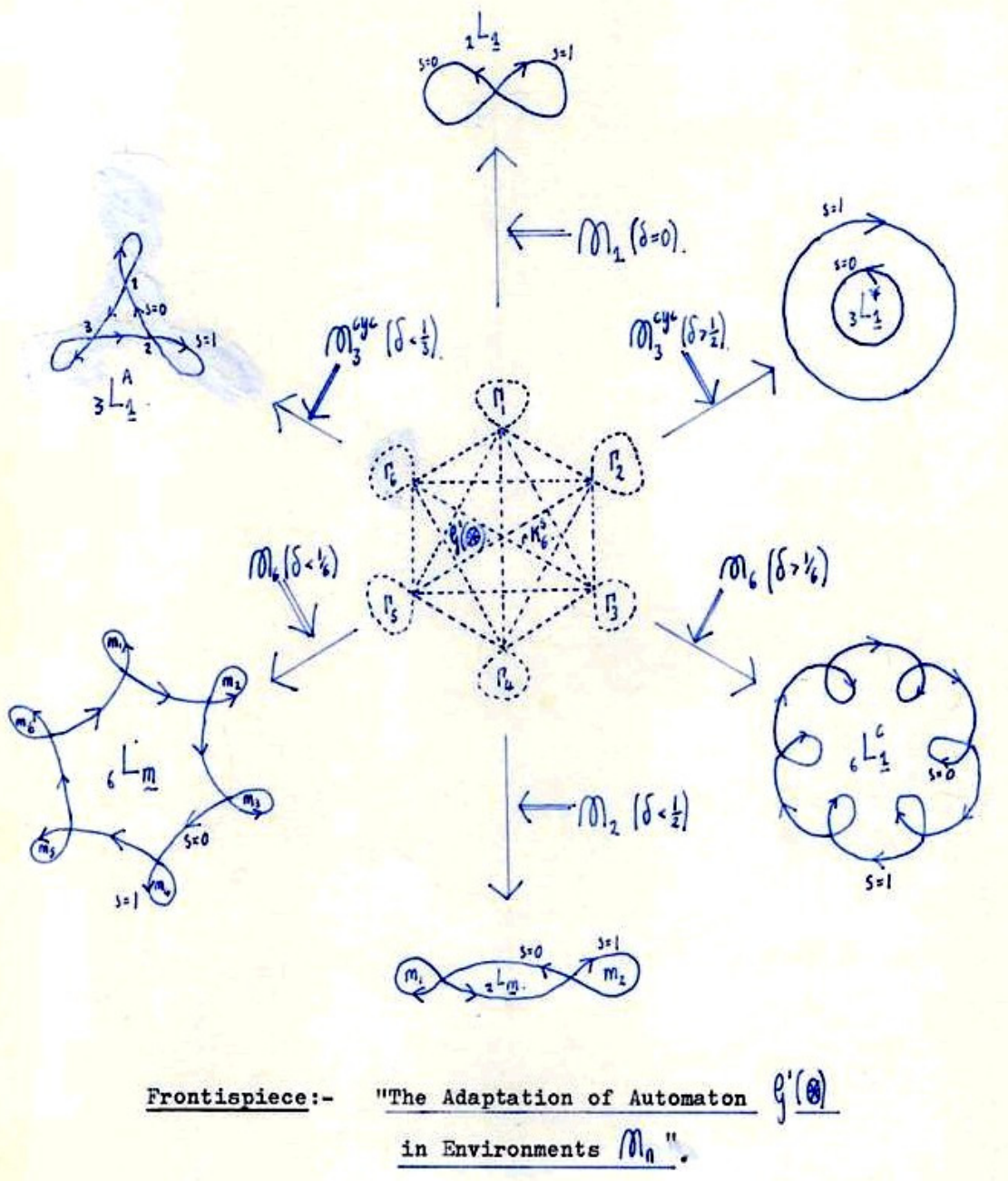


AI & Machine Learning as *Cyber Tools*

- **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...)

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



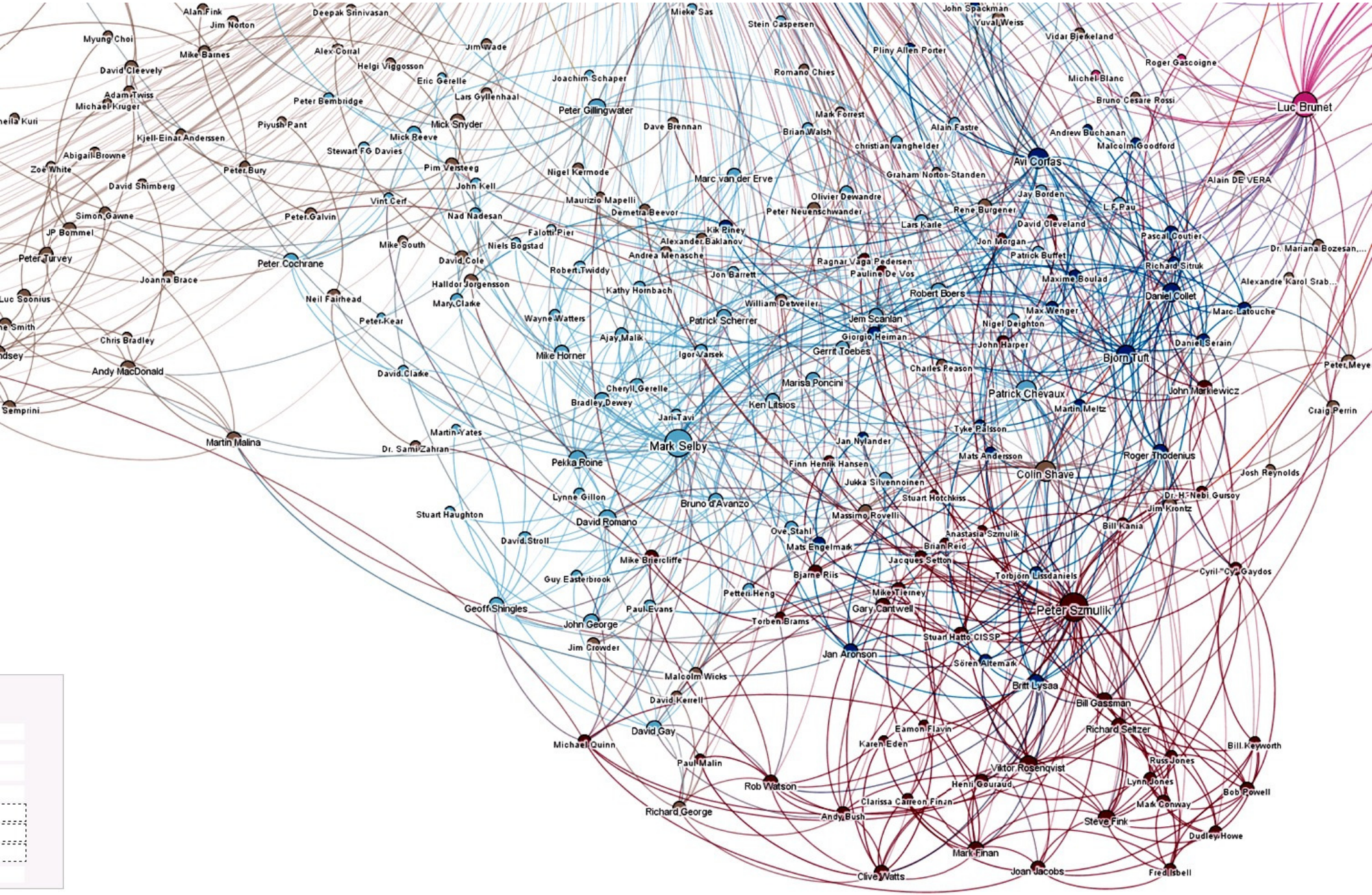


Download : www.valentina.net/Thesis/Thesis.pdf

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

Summer 1974 – **Dr David Eric Probert** *– Cambridge Stats Lab*

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

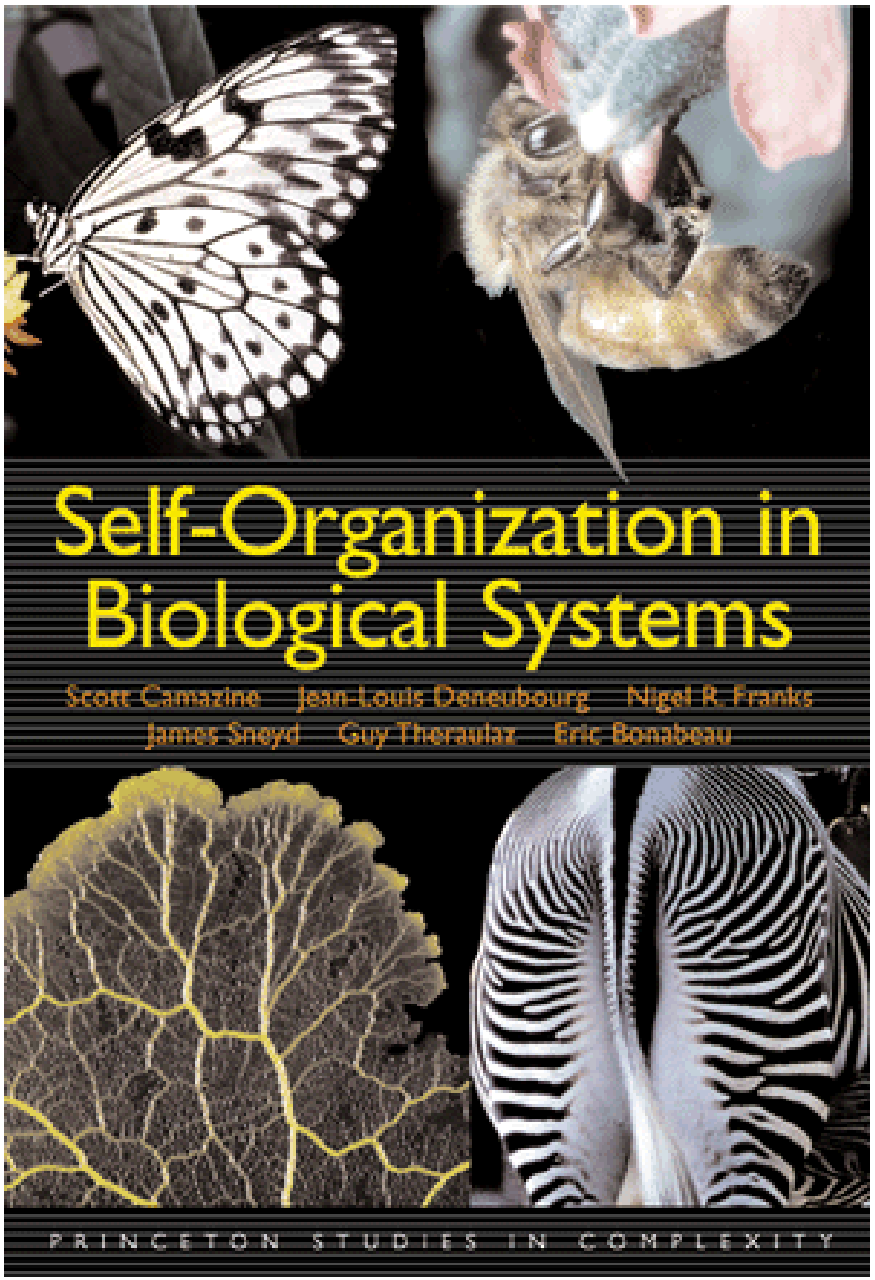


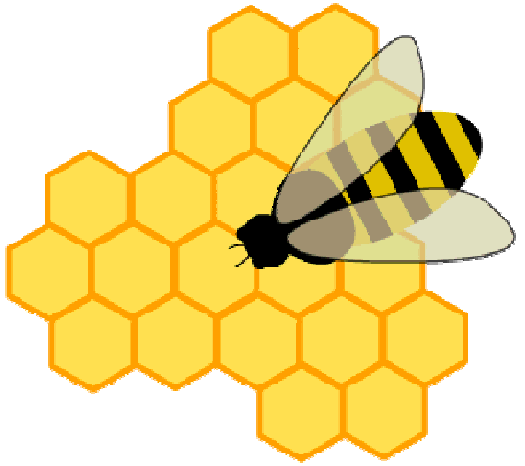
Self-Organisation in *Bio-Sciences*

- 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"*





- Smart Sustainable Security in the Wild! -

The Sociable Weaver Bird

"World's largest Bird Nests"

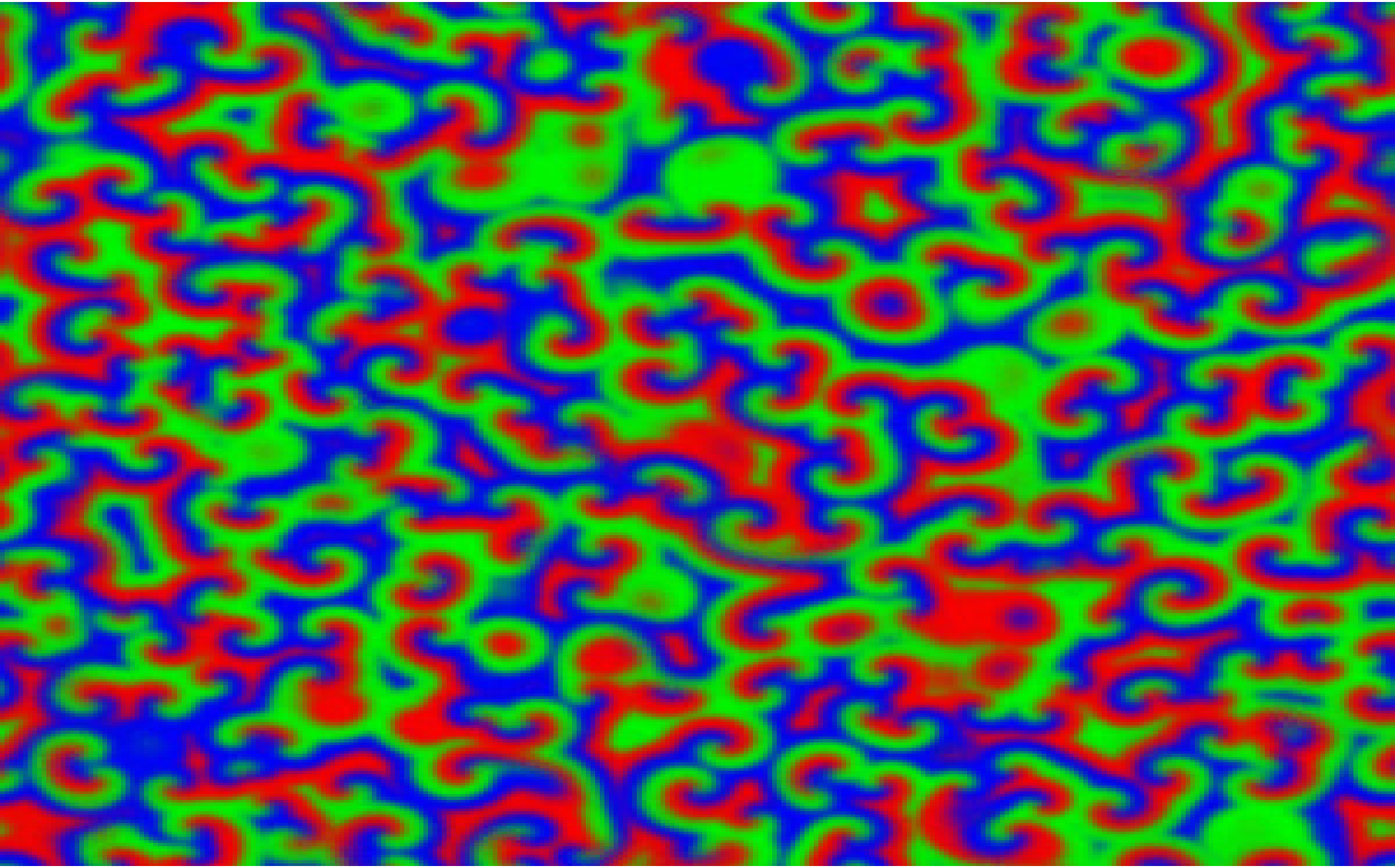
*** Southern Africa ***

- 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 21st C-"Cyber Defence Centre"–including Disaster Recovery & Business Continuity!

"Smart" Autonomous Chemical Oscillator:

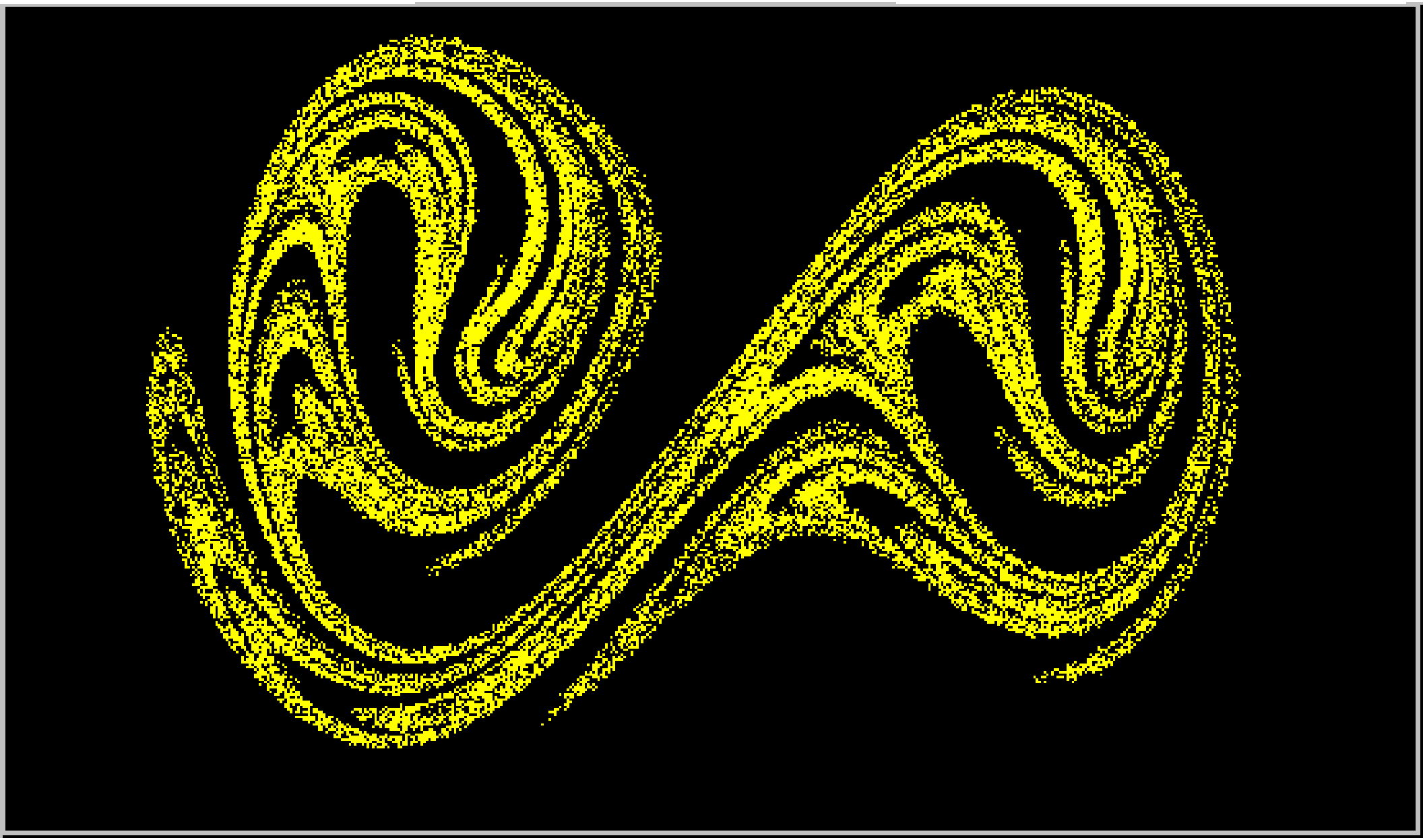
- Belousov–Zhabotinsky Reaction (BZ) -



Chaotic Attractor: *Duffing Oscillator*

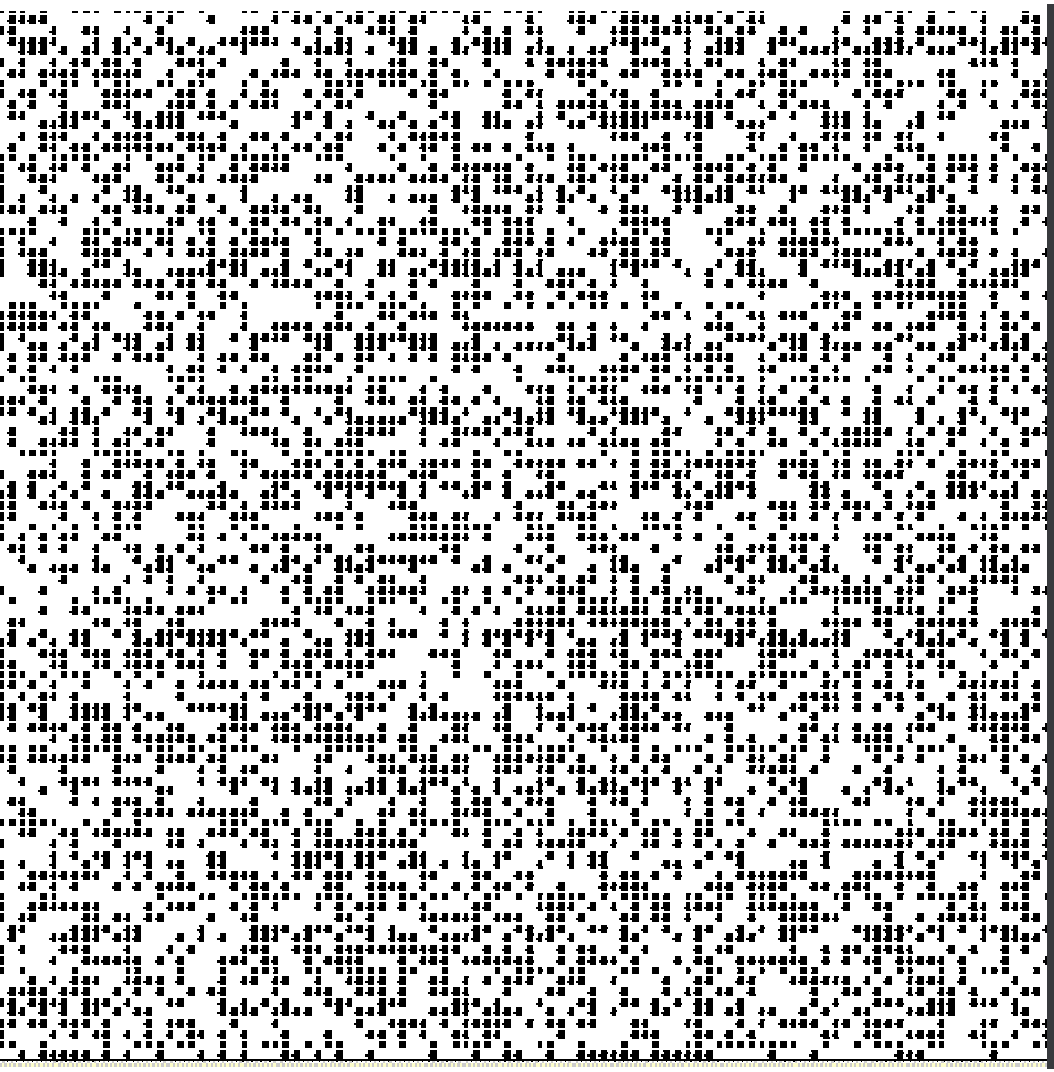
...."Chaos" is common in "Smart Systems" and "Cyber Communities"

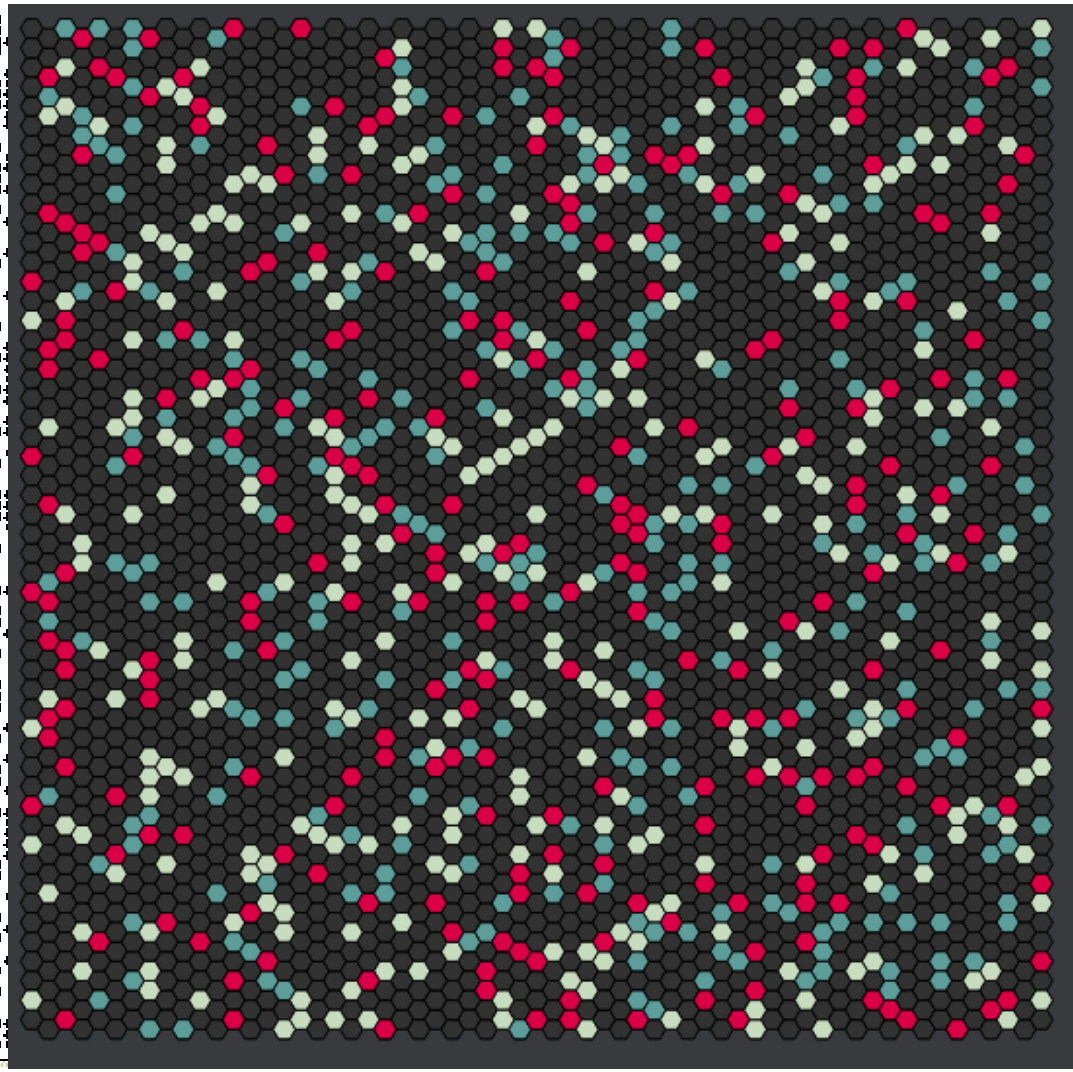
Dynamic Duffing Equation: $\ddot{x} + \delta\dot{x} + \alpha x + \beta x^3 = \gamma\cos(\omega t)$ - Exhibits Chaotic Behaviour



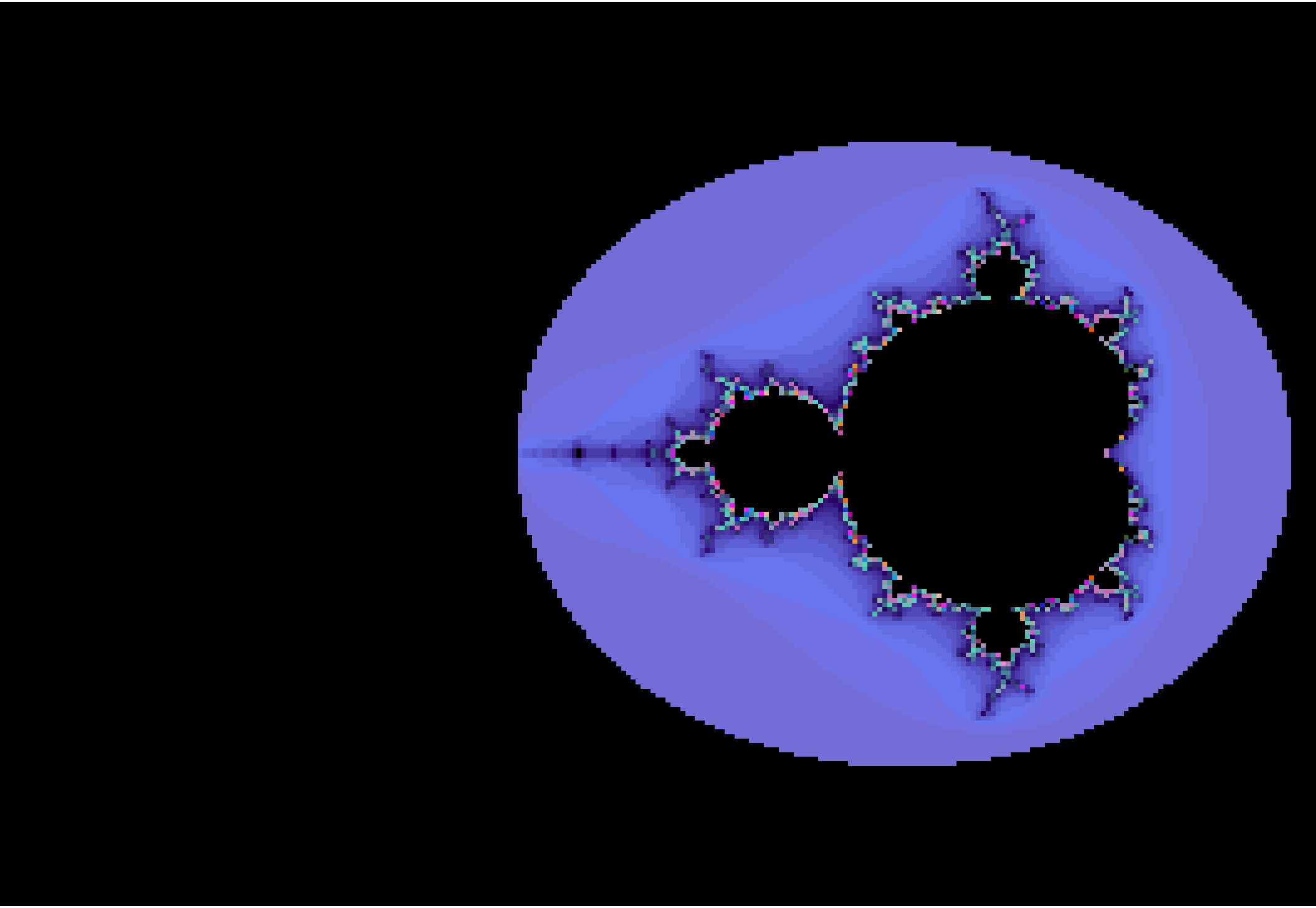
Cellular Automata: *"Games of Life"*

- Professor John Horton Conway FRS -

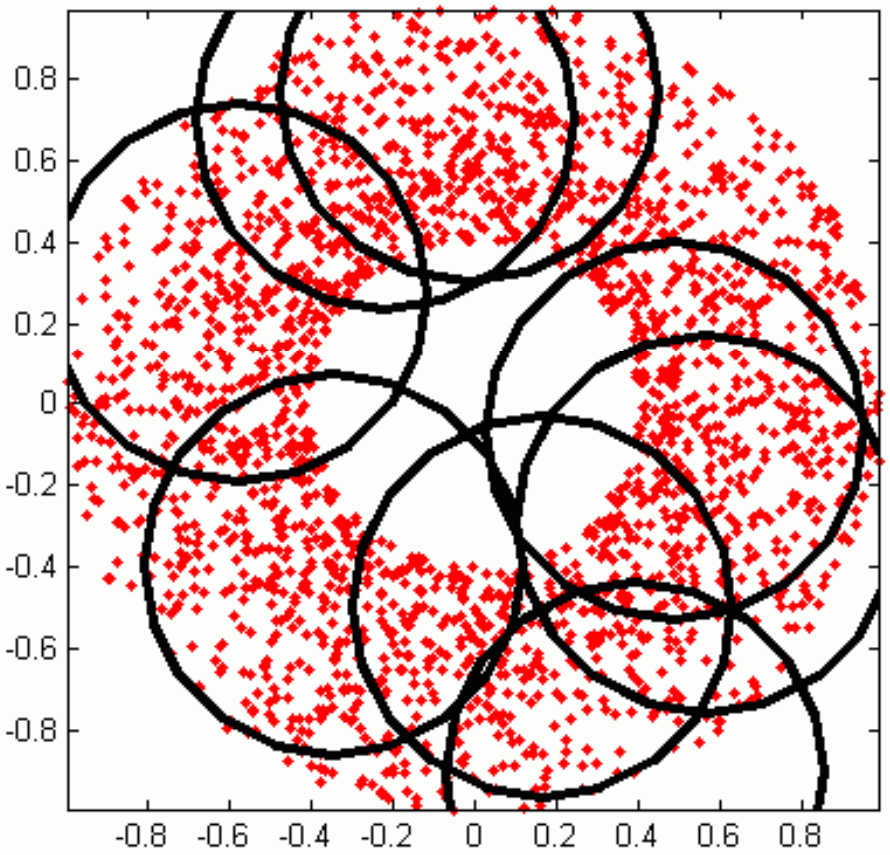


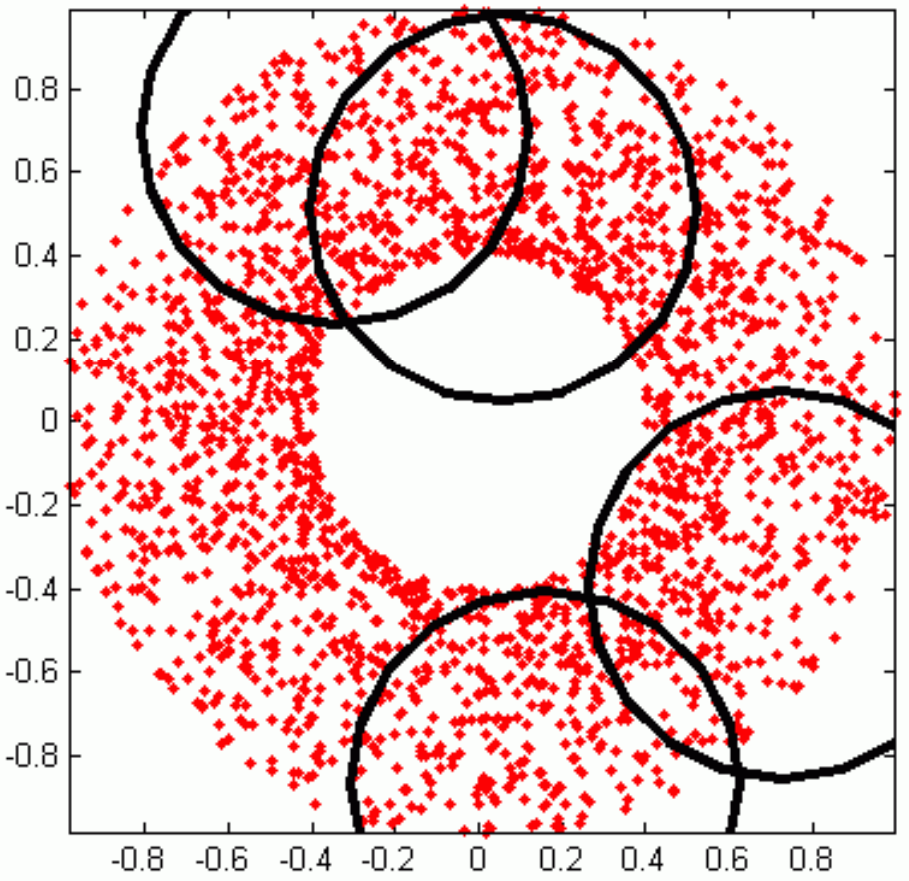


“Smart Scaling”: Fractal Mandelbrot Set



"Machine Learning Algorithms"





Basic Principles of *"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 Social Networks, Search & On-Line Commerce
7) ***Systems Integration:*** Cyber and Physical Solutions & Operations

……..Now we'll consider how such Smart AI-based Features can be designed & engineered into future 21stC Cybersecurity Toolkits…

Building our 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 (such as Denial of Service) occur in real-time @Optical Speeds via worldwide proxy servers, so ultra fast analysis, decisions and action is a must!

Building our 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 both plants & animal life, and Mandelbrot's theory of Fractal Curves provides vivid examples.
- ***Current Trends:*** Research into Learning, Self-Organisation & Adaptation remains extremely active in both ICT R&D Labs & Academic Institutions

"How to Build Smart Security Solutions?"

- Conceptually - Smart Solutions all use combinations of these basic ICT "genes" shared with Intelligent Living Systems:

1) ***Hybrid Organisation:*** Hierarchical (Pyramid) & Organic (Networked)

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

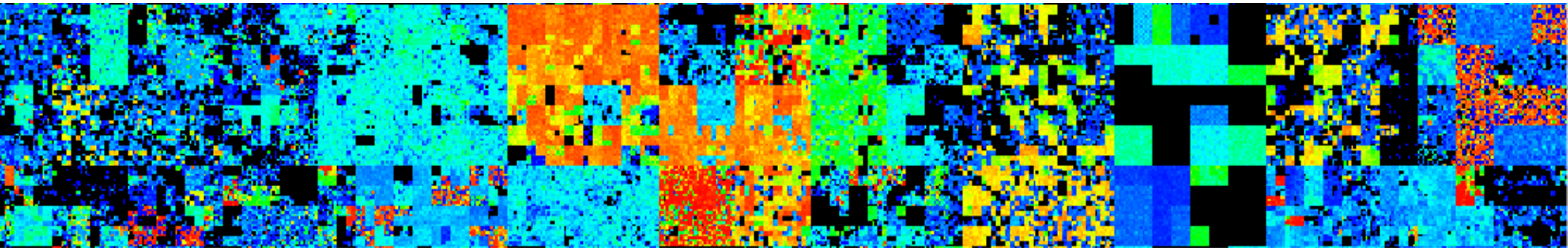
3) ***Smart Learning Principles (L-Genes):*** Memory, Scaling & Adaptation

4) ***Smart Solutions & Business Architecture:*** Integration of the Decision + Learning "Genes", within a Secure & Resilient Systems Environment

.....Using AI & Machine Learning we can now design "Smart" Self-Learning Cybersecurity Tools to secure YOUR Enterprise!

21stC Cybersecurity (2) – *"AI & Machine Learning"*

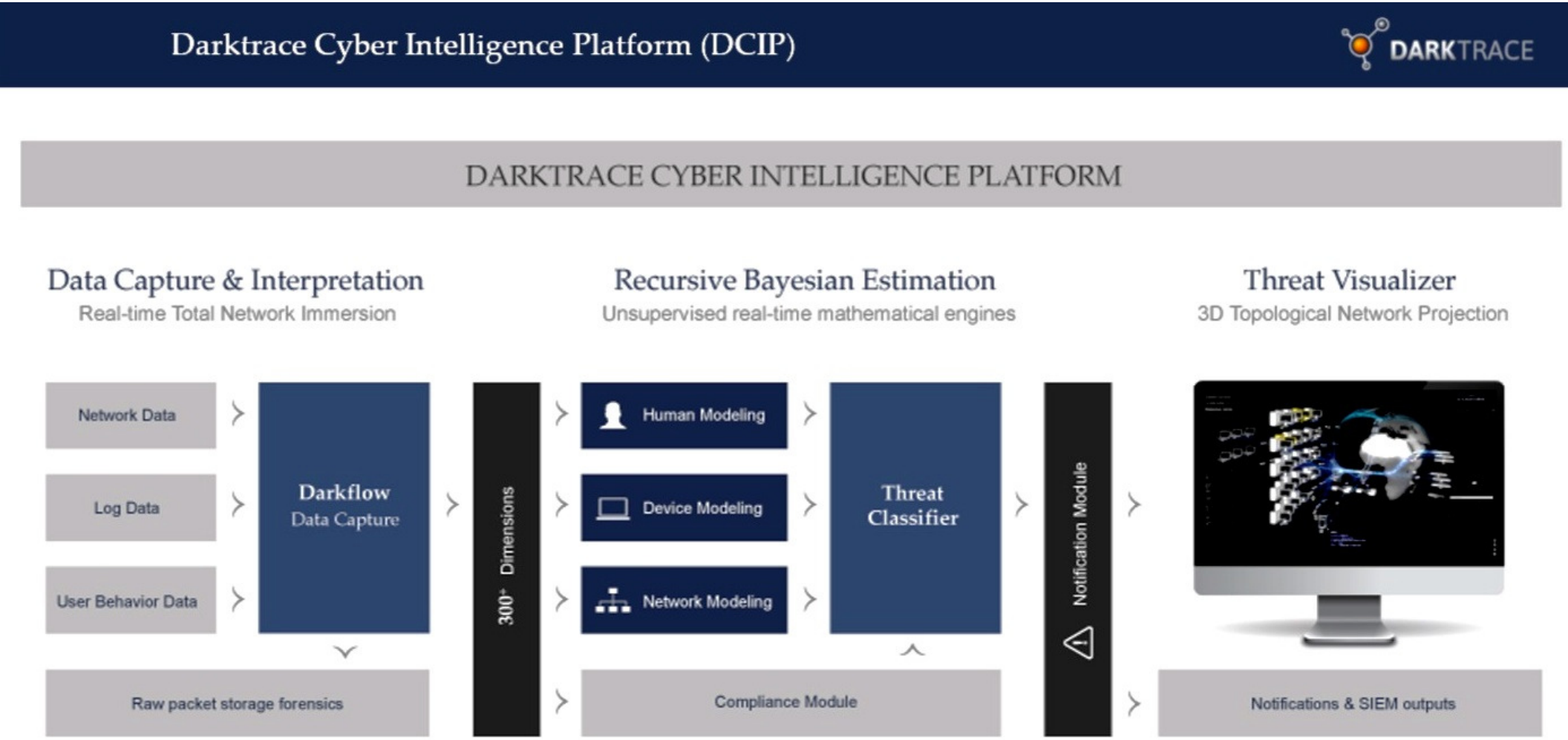
1 – Background: 20th to 21stC Cybersecurity	2 – AI & Machine Learning as Cyber Tools	**3 – Recent 21stC Cybersecurity Ventures**
4 – Advanced Cyber Scenarios & Analysis	5 – Hybrid 20thC & 21stC Cyber Solutions	6 – Scenario 2020: Integrated Security - IoT
7 – Scenario 2025: Self-Adaptive Security	8 – Scenario 2040: Neural Security	9 – YOUR Action Plan for Advanced Cyber!



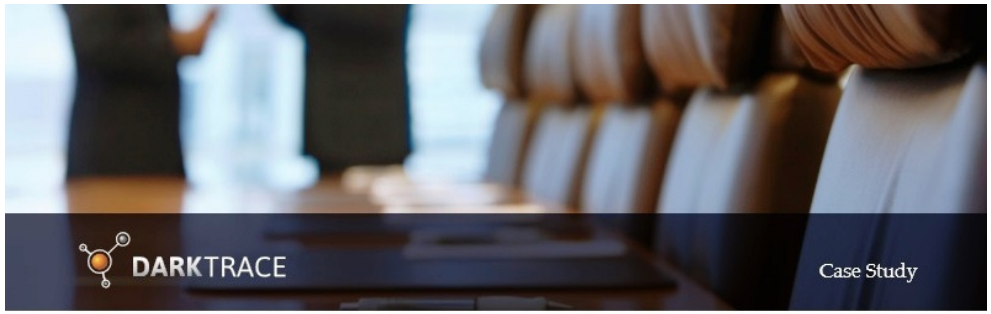
Recent 21stC *Cybersecurity Ventures*

- **Darktrace:** Enterprise Immune System
  - Cambridge Venture (UK) that focuses on Adaptive Behavioural Learning (Recursive Bayesian Rules)
- **LogRhythm:** Security Intelligence Platform
  - Real-Time Machine Analytics & Data Intelligence based upon Forensic Data Files (System & Event Logs)
- **CyLon:** London-based Cybersecurity Incubator
  - Start-Up Ventures: Ripjar, Cyberlytic, Digital Shadows, Intruder, AimBrain, Mentat Innovations, and Surevine
- **Norse Corporation:** San Francisco Venture focused upon global real-time cyber threat monitoring & Analytics.

Darktrace *Cyber Intelligence Platform*



Virgin Trains - Leading UK Rail Operator



EUROPEAN FINANCIAL SERVICES LEADER

GLOBAL ASSET MANAGEMENT FIRM

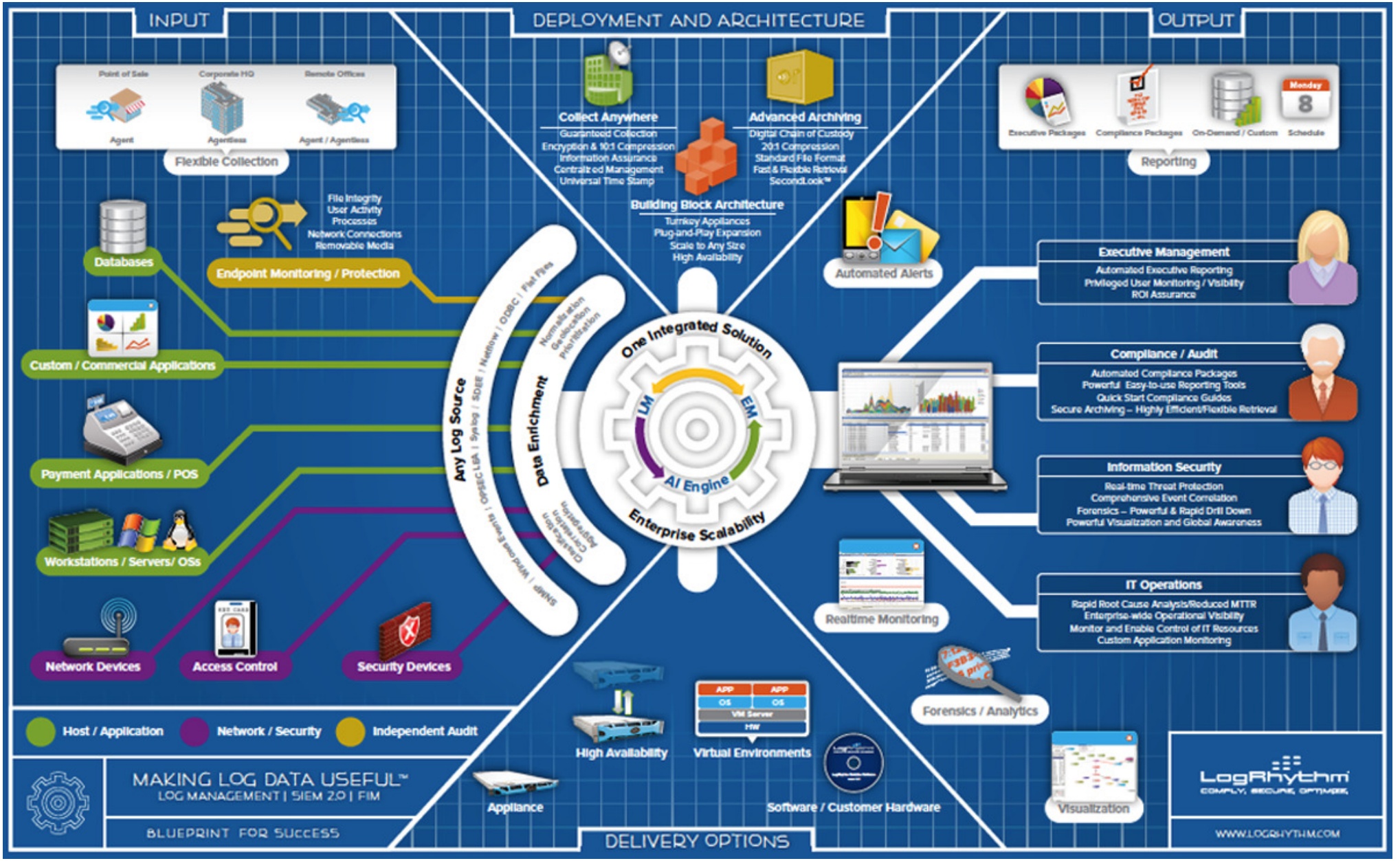
Sisley - Global cosmetics company

Drax - Major European Power Infrastructure Company

DNK, Leading Norwegian Insurance Company

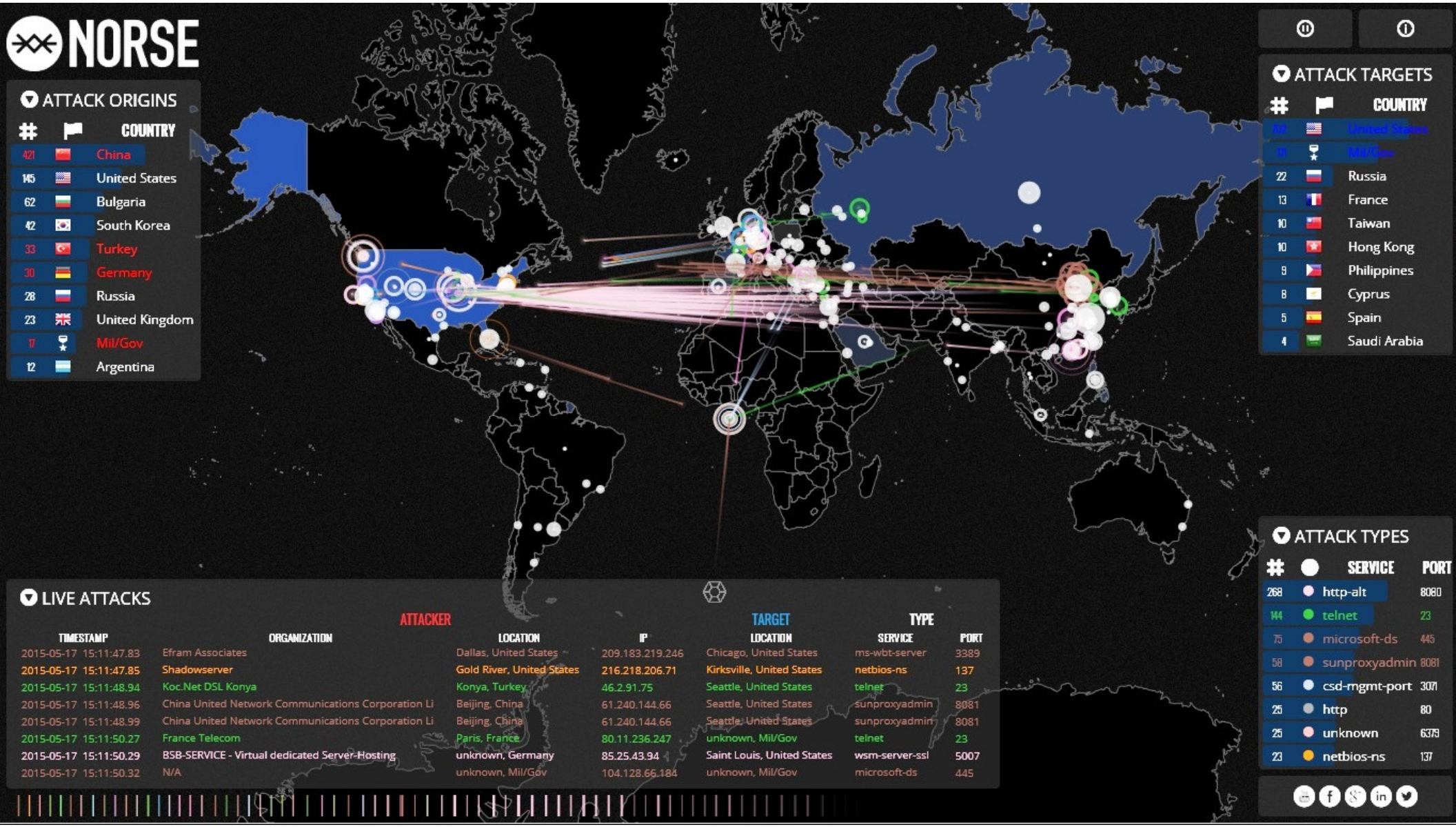
Web: *www.darktrace.com/industries*

LogRhythm: *Security Intelligence*



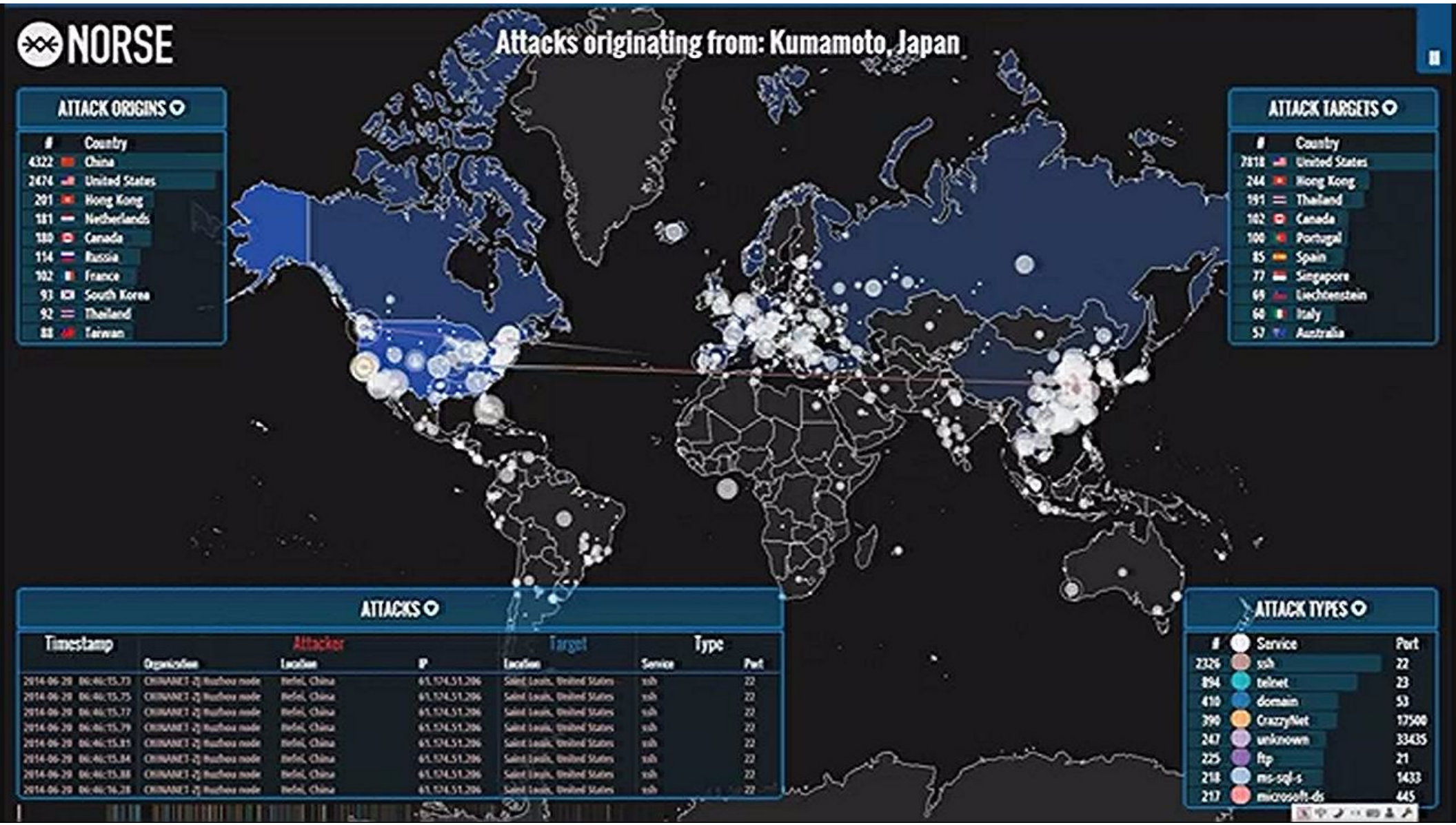
Corporate Web: www.LogRhythm.com

Norse Corporation: *Intelligence Service*



Link: **map.ipviking.com** - Norse Corporation

Global "Real-Time" DarkNet CyberAttacks



Link: map.ipviking.com - Norse Corporation

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

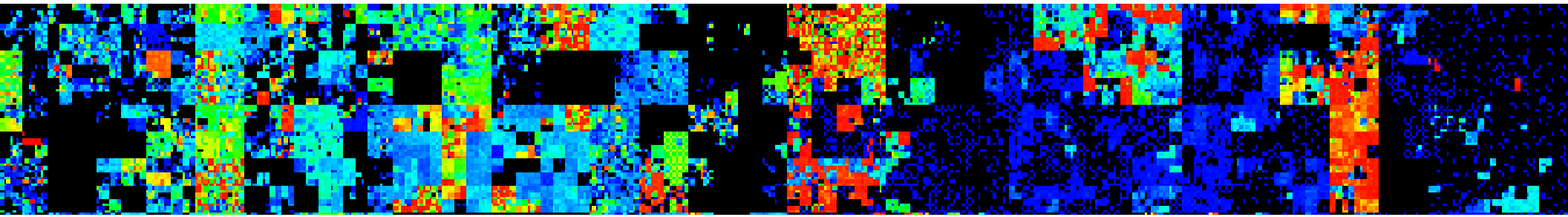
32nd International East/West Security Conference

"Advanced Enterprise Cybersecurity – Artificial Intelligence & Machine Learning"
- Madrid, Spain: 26th – 27th Oct 2915 -

"Smart Analysis Tools": *4D Simulation Modelling for Hybrid Terror Alert & Disaster Management*

21stC Cybersecurity (2) – *"AI & Machine Learning"*

1 – Background: 20th to 21stC Cybersecurity	2 – AI & Machine Learning as Cyber Tools	3 – Recent 21stC Cybersecurity Ventures
4 – Advanced Cyber Scenarios and Analysis	5 – Hybrid 20thC & 21stC Cyber Solutions	6 – Scenario 2020: Integrated Security - IoT
7 – Scenario 2025: Self-Adaptive Security	8 – Scenario 2040: Neural Security	9 – YOUR Action Plan for Advanced Cyber!

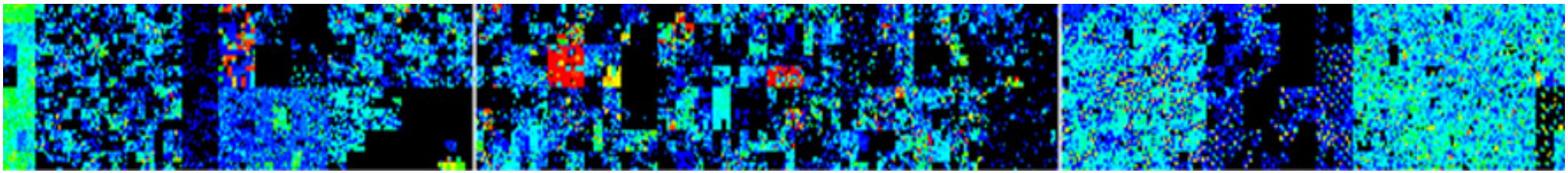


Advanced *Cyber Scenarios* & Analysis

- **Insider Security Threats:** Adaptive Modelling & Learning provides early alert to unusual cyber behavioural such as remote logons, data downloads, finance transfers & malicious access.
- **Zero Day & APTs:** Traditional Cyber Tools are weak with sudden attacks, whilst real-time AI tools can provide instant management alerts.
- **Securing the "Internet of Things":** The IoT can only be effectively secured through distributed AI-based self-organising & adaptive security tools.

21stC Cybersecurity (2) – *"AI & Machine Learning"*

1 – Background: 20th to 21stC Cybersecurity	2 – AI & Machine Learning as Cyber Tools	3 – Recent 21stC Cybersecurity Ventures
4 – Advanced Cyber Scenarios & Analysis	**5 – Hybrid 20thC & 21stC Cyber Solutions**	6 – Scenario 2020: Integrated Security - IoT
7 – Scenario 2025: Self-Adaptive Security	8 – Scenario 2040: Neural Security	9 – YOUR Action Plan for Advanced Cyber!



Hybrid 20thC & 21stC *Cyber Solutions*

- Effective 21stC Enterprise Cybersecurity requires CSOs to deploy **Hybrid Solutions**:
  - *Physical Security* – Perimeter, Access Controls, CCTV, Biometrics, Staff Profiling & Vetting
  - *Traditional Cyber Tools* – Firewalls, Anti-Virus, DDOS Alerts, & Malware & Adware Protection
  - *Advanced Cyber Tools* – AI-based Network & User Behaviour Modelling (Enterprise Immune System)
- **New Generation** Intelligent "Cyber" Tools will evolve during the next 5 to 10 years for *"Smart Security"*
  - We define ***"CyberVisions"*** for ***2020*** (5 years - Integrated), ***2025*** (10 Years - Adaptive) and ***2040*** (25 Years - Neural) .

Hybrid 21stC Organisation: *Hierarchical & Organic*

- ***Transition*** from 19thC/20thC to 21stC Business & Governance requires fundamental re-structuring of operations:
  - ***19thC /20thC Industrial Organisations:*** Hierarchical Bureaucracies (Pyramids) to 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 environmental adaptation
- ***Smart Security Solutions*** will also require **hybrid** organisation to optimise real-time response to cyber & physical attacks.

Smart Security based upon AI & Machine Learning will span ALL *Economic Sectors*

(1) Banking and Financial Services
(2) Healthcare and Social Welfare
(3) ICT, Mobile and Telecommunications
(4) Education and Research
(5) Manufacturing & Logistics
(6) Retail and Distribution
(7) Central & Regional Government

*.....ALL **Economic Sectors** will eventually require embedded **"smart security"** in order to provide real-time resilience to simultaneous physical & cyber attacks, crime or terrorism.*

"Smart Security" - *Banking and Finance*

- For each economic sector we'll begin by analysing each of the critical sectors in the context of the Smart Genetic Design Principles of "Decisions" and "Learning", and then discuss the implications for upgraded Smart Security and Governance:
  - ***Smart Decisions:***
    - *Geo-Location:* Smart Mobile Banking, with GPS Location to provide suggestions for shopping (based on profile), cafes, restaurants, nearby on-line friends…
    - *Real-Time:* Financial & Commodity Trading, on-line share dealing, maximise interest rates, foreign exchange dealing. Banking has really pioneered "real-time" financial trading & networking during last 30 years!
    - *Knowledge Lens:* Deep Data Mining, Business Intelligence2.0 and CRM (Customer Relationship Management for Banking & Investment Clients
  - ***Smart Learning:***
    - *Adaptation & Self-Organisation:* Investment Banks have pioneered applications of Smart Neural Network Apps, Adaptive Trading and Real-Time Risk Management.
    - *Massive Memory & Storage:* Secure Resilient Databases are Fundamental to Banking
    - *Scalable Architecture:* Banks are moving from "bricks & mortar" to global scalable networks, and most now provide mobile & home banking "apps" and highly secure on-line account services
  - ***Smart Sustainable Security*** Encryption, Portable Pin Pads, Biometrics, Cyber Risk Management
  - ***Smart Governance, Management and Operations :*** Data Integrity, Compliance & Audit, New Financial Regulations

"Smart Security" – *Healthcare & Social Welfare*

- ***Smart Decisions:***
  - *Geo-Location:* GPS Location for Medical Emergencies, Patient Images, Crisis Management, Ambulance Routing, Regional Social Support
  - *Real-Time:* On-Line Telemedicine Consultation & Preliminary Diagnosis. Also Smart Support during Intensive Hospital Surgery
  - *Knowledge Lens:* Filtering & Analysing Complex 3D Medical Scan Images, as well as future Data Mining for On-Line Patient Records
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Challenging Medical Research in New Treatments for Cancer & Neural Diseases through Global Partnerships
  - *Massive Memory & Storage:* Design, Analysis and extensive Patient Trials of New Pharmaceutical Drugs, including new "Smart Drugs"
  - *Scalable Architecture:* National professional support network for both social welfare as well as citizen health, diagnosis and treatments
- ***Smart Security:*** Cybersecurity & Personal Privacy for Patient Records, as well as integrated security for hospitals, medical assets, drugs & social welfare facilities
- ***Smart Governance:*** Professional Government Support, Management & Funding for National Medical & Social Welfare Services

"Smart Security" - *ICT, Mobile & Telecommunications*

- ***Smart Decisions:***
  - *Geo-Location:* Local Mobile Information – Maps, Satellite Imagery, Climate, Geology, History, On-Line Persons on Smart Devices.
  - *Real-Time:* Financial Transactions, ePayments, eGovernment Services, IM, Social Media, MMORG and Immersive Virtual Worlds
  - *Knowledge Lens:* Global Data & Information can be filtered and focused for Local Decisions with ICT enabled "Knowledge Lens"
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Mobile, Wireless & Cellular Ad-Hoc Networks use adaptive routing & roaming protocols
  - *Massive Memory & Storage:* ICT provides the essential Smart Storage & Processing Tools including System Virtualisation & Cloud Computing
  - *Scalable Architecture:* Fundamental for smart ICT systems that already scale from nano machines to global search & social media "apps"
- ***Smart Security:*** Cybersecurity needs to be embedded EVERYWHERE!
- ***Smart Governance:*** ICT requires new laws, regulations & governance

"Smart Security" - *Education & Research*

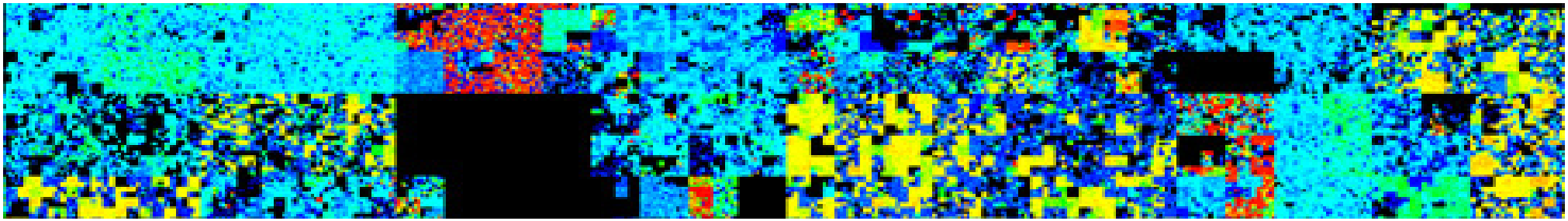
- ***Smart Decisions:***
  - *Geo-Location:* Mobile Education, Navigation & Mapping, Augmented & Immersive Reality based on Geo-Location with Mobile Devices & Headsets
  - *Real-Time:* Networked Laboratories for Synchronised Parallel Research in Genetics, High-Energy Physics, Optical & Radio-Astronomy
  - *Knowledge Lens:* Smart Grid Computing with In-Depth Data Mining in search for New Particles in CERN LHC Collider.
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Virtual On-Line Colleges for remote students. Collaborative academic & commercial Techno Parks & Labs
  - *Massive Memory & Storage:* Crowd Sourced Volunteer PC Research as in the SETI Project (BOINC – Berkeley Open Net Computing)
  - *Scalable Architecture:* Business Opportunities for Global Niche College for minority study & research themes. Study courses on mobile "apps"!
- ***Smart Security:*** College Campus & Laboratory Cyber & Physical Security
- ***Smart Governance:*** Rigorous Educational Data Audit & Compliance Regime

"Smart Security" - *Government*

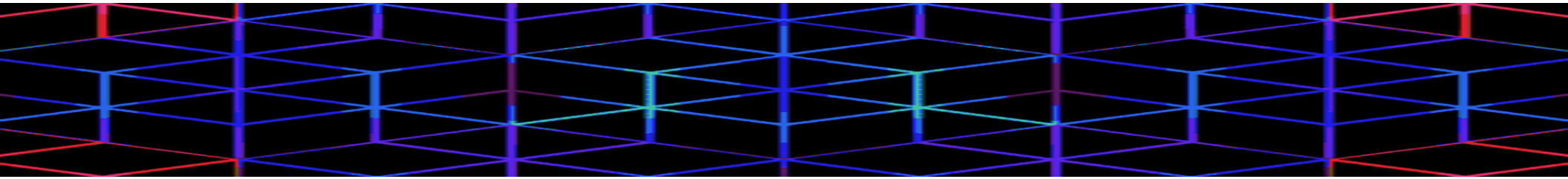
- ***Smart Decisions:***
  - *Geo-Location:* Tracking all government assets, physical & electronic documents and devices to reduce loss or corruption of information
  - *Real-Time:* Ensure that the government ALWAYS has complete real-time info on its resources, staff and financial & political affairs
  - *Knowledge Lens:* "In-Depth" Smart Data Mining to link Government Databases relating to ALL Government Ministries & Agencies
- ***Smart Learning:***
  - *Adaptation & Self-Organisation:* Flexible Networked Government Organisations and Operations to respond to evolving national & international events, policies & overall business & political environment
  - *Massive Memory & Storage:* Ability to store and analyse PetaBytes of Government Data relating to Programmes, Policies & Governance
  - *Scalable Architecture*: Efficient networked operational framework for the transparent management of national, region and local citizen programmes
- ***Smart Security:*** Implementation of integrated Physical and Cyber Security Operations according to International Standards – ISO/ITU
- ***Smart Governance:*** Provision of Open eGovernment Portal supporting ALL major Ministries, Agencies and Partners for On-Line Transaction Processing & Analysis

21stC Cybersecurity (2) – *"AI & Machine Learning"*

1 – Background: 20th to 21stC Cybersecurity	2 – Cyber Players & Targets	3 – Recent 21stC Cybersecurity Ventures
4 – Advanced Cyber Scenarios & Analysis	5 – Hybrid 20thC & 21stC Cyber Solutions	6 – Scenario 2020: Integrated Security - IoT
7 – Scenario 2025: Self-Adaptive Security	8 – Scenario 2040: Neural Security	9 – YOUR Action Plan for Advanced Cyber!



Our CyberVisions: *2015 to 2040*



- **Scenario 2020 – *Integrated Security-IoT*:** Managed Integration of IoT, *Cyber* & Physical Ops under CSO
- **Scenario 2025 – *Adaptive Security:*** Transition to Global Real-Time AI & ML Based Cyber Applications
- **Scenario 2040 – *Neural Security:*** Enterprise-Wide Deployment of Real-Time AI-Based Cyber Defences

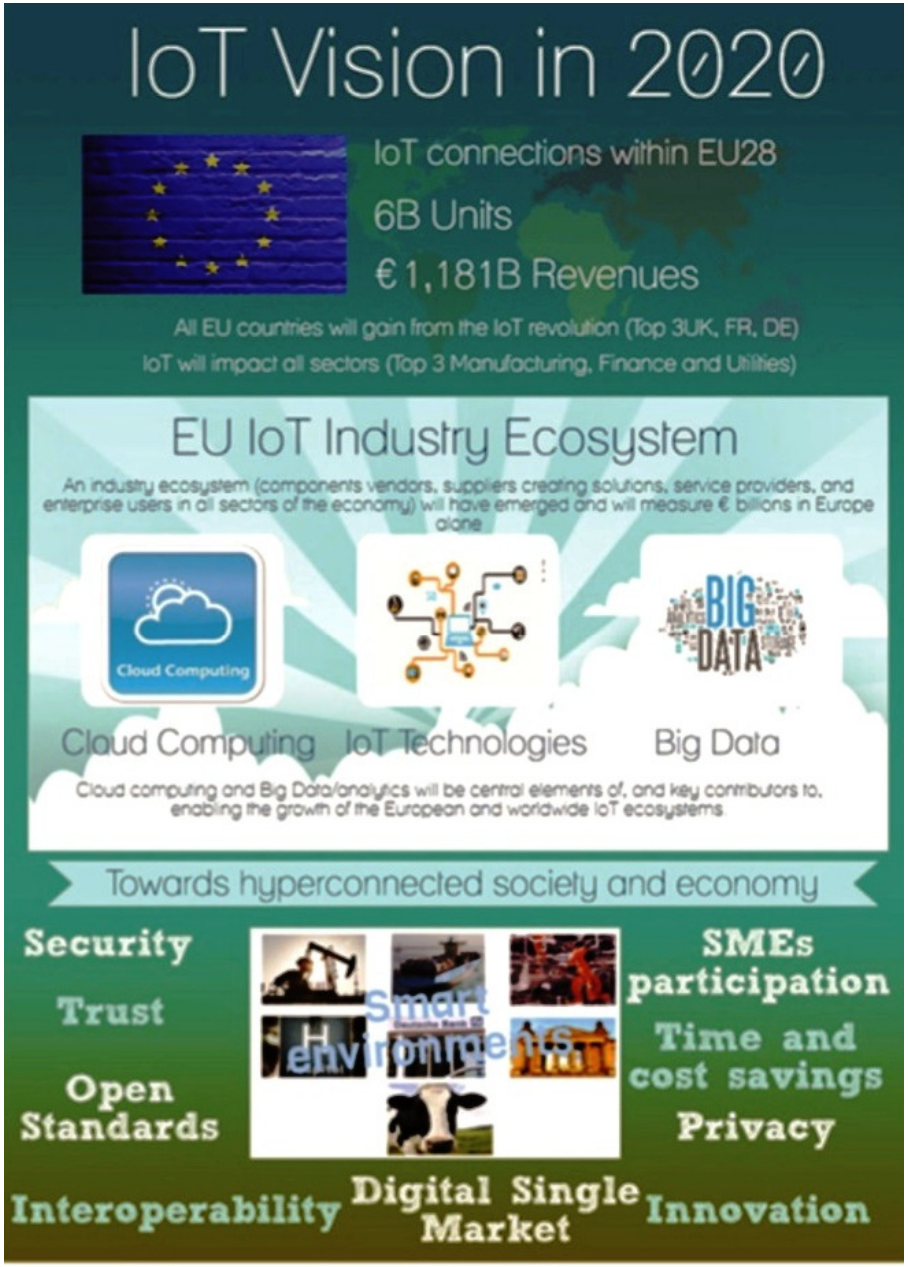
Scenario 2020: Integrated Security - IoT

- ....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

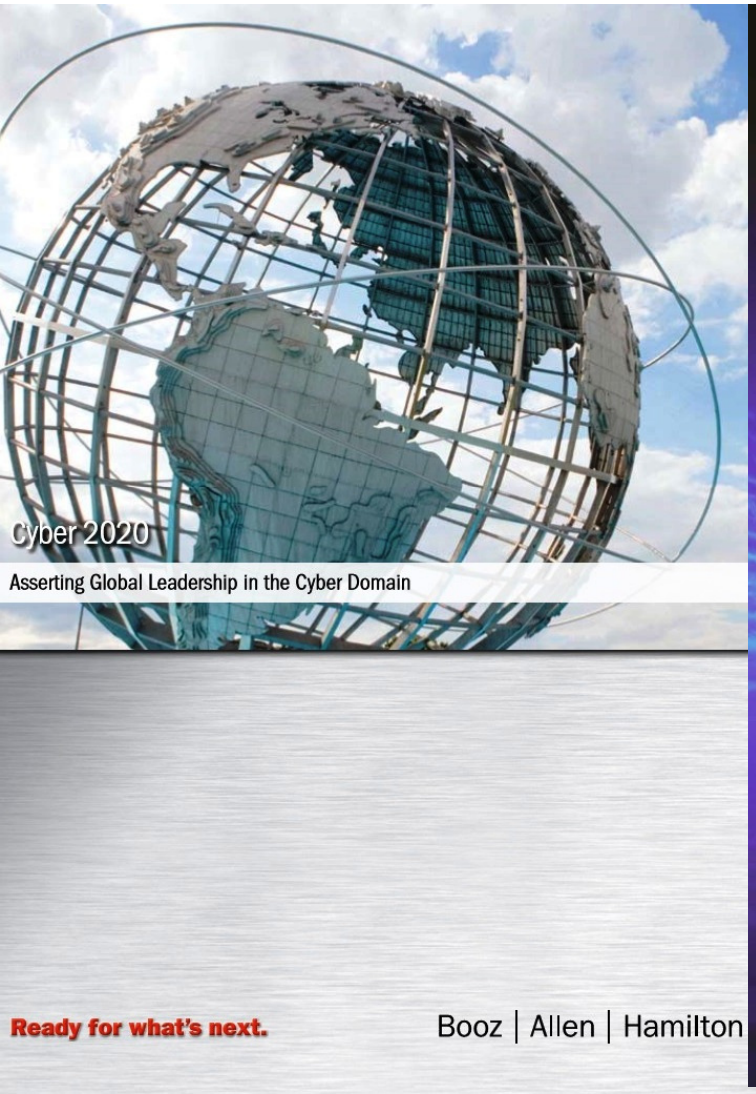
Transition from 20thC to 21stC *Smart Security*

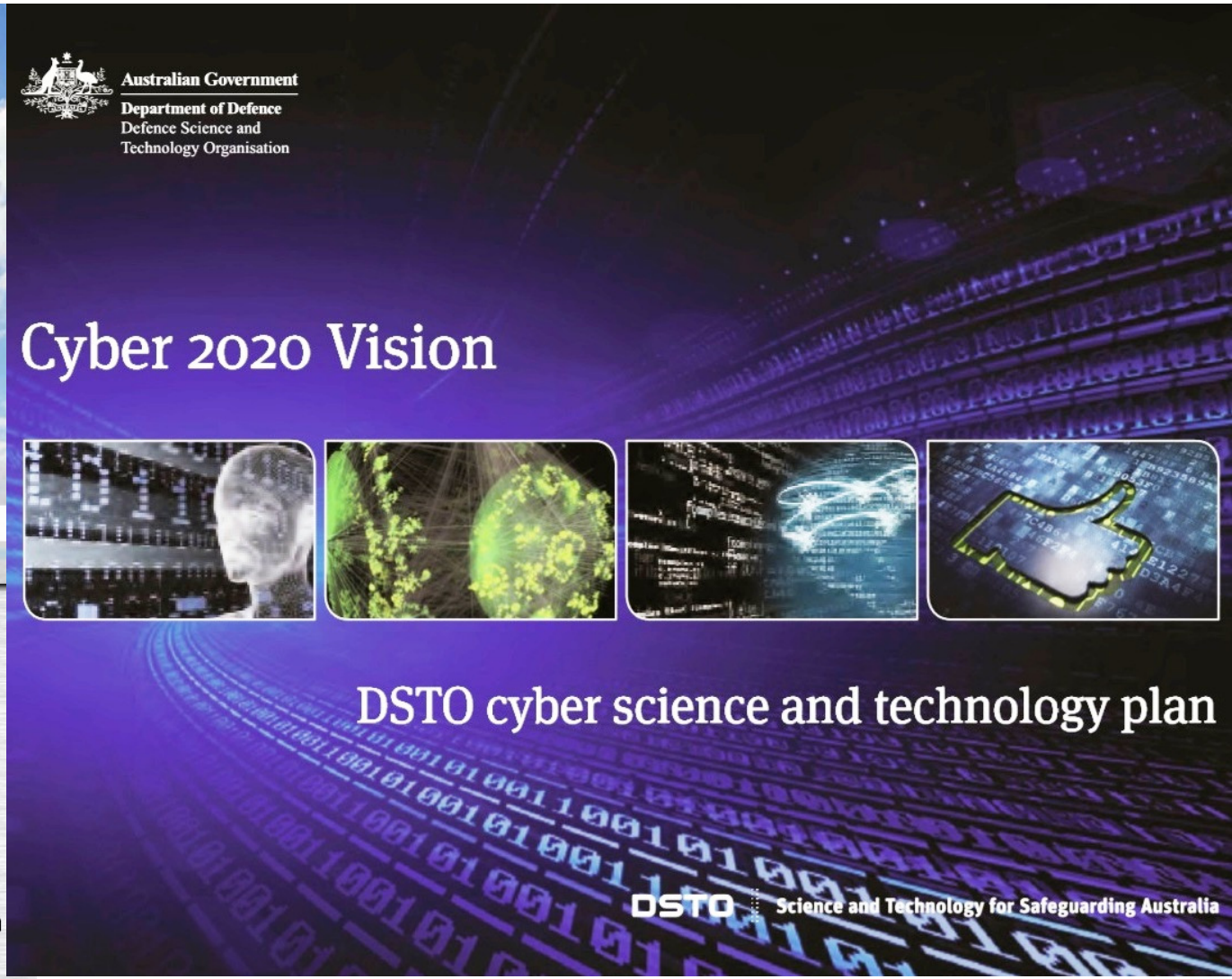
- **Cybersecurity 2015-2020:**
  - Every country in the world will need to transition from the traditional 20thC culture & policy of massive physical defence to the connected "neural" 21stC world of in-depth intelligent & integrated cyber defence solutions
- **National Boundaries:**
  - Traditional physical defence and geographical boundaries are still strategic national assets , but they need to be augmented through integrated cyber defence organisations & assets.
- **Critical National Information Infrastructure:**
  - 21stC national economies function electronically, & yet they are poorly defended in cyberspace, and very often open to criminal & political attacks
- **Multi-Dimensional Cyber Defence:**
  - Nations need to audit their critical infrastructure – government, banks, telecommunications, energy, & transport – and to upgrade to international cybersecurity standards based upon accepted "best practice" (ISO/IEC)

EU "IoT" Programme Visions for 2015 and 2020



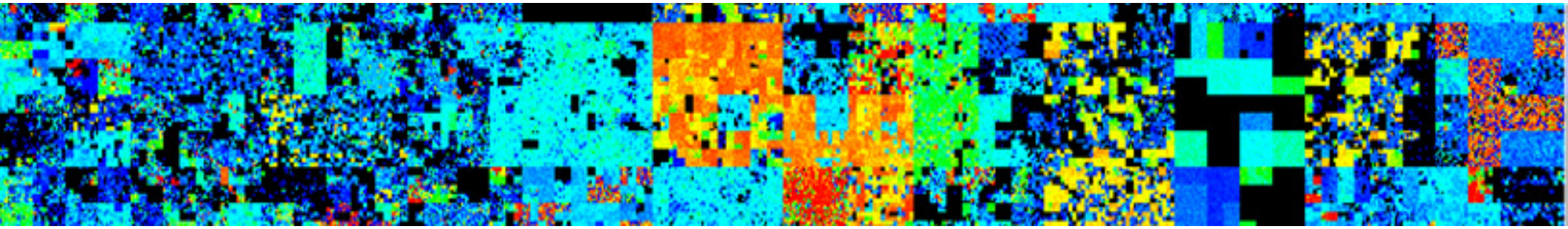
Cyber 2020 Visions: Booz, Allen & Hamilton and The Australian Government (Defence)





21stC Cybersecurity (2) – *"AI & Machine Learning"*

1 – Background: 20th to 21stC Cybersecurity	2 – AI & Machine Learning as Cyber Tools	3 – Recent 21stC Cybersecurity Ventures
4 – Advanced Cyber Scenarios & Analysis	5 – Hybrid 20thC & 21stC Cyber Solutions	6 – Scenario 2020: Integrated Security - IoT
7 – Scenario 2025: Self-Adaptive Security	8 – Scenario 2040: Neural Security	9 – YOUR Action Plan for Advanced Cyber!

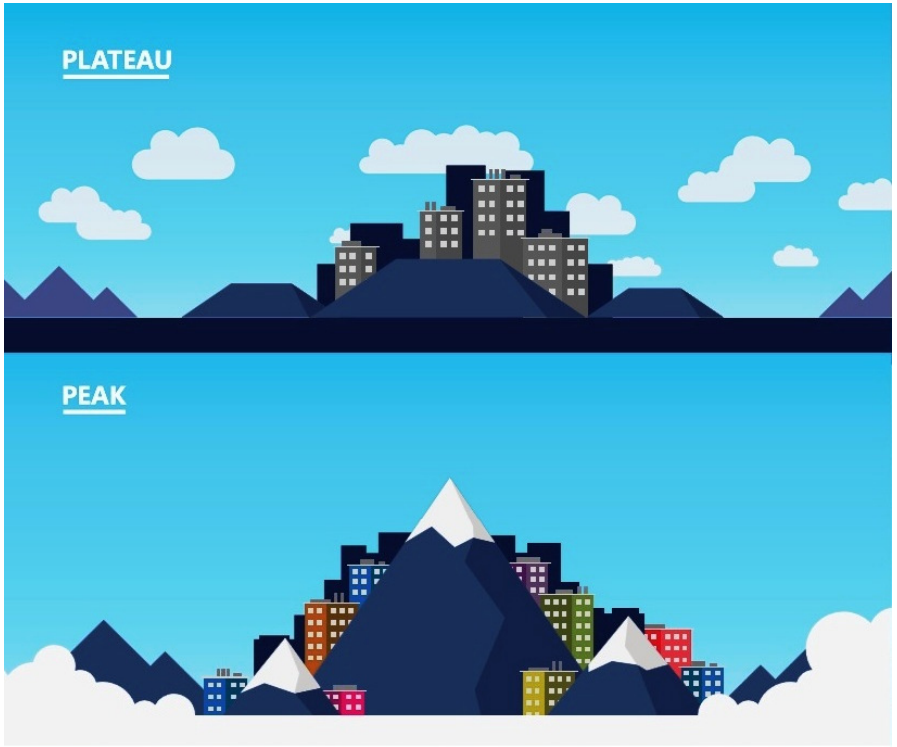


Scenario 2025: Self-Adaptive Security

- ..10 Year Time Window - **2005 <– 2015 -> 2025**
- Transition & Full Deployment of Enterprise-Wide AI-based **Self-Adaptive** "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 ***

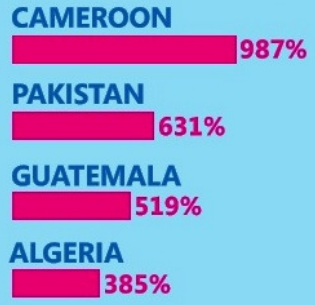


QUANTIFYING THE WORLD IN 2025

HOW MANY INTERNET USERS WILL THERE BE IN 2025?

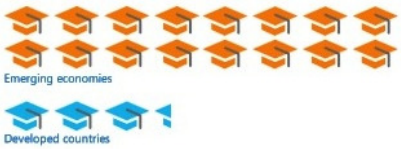
Percentage from emerging economies

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.

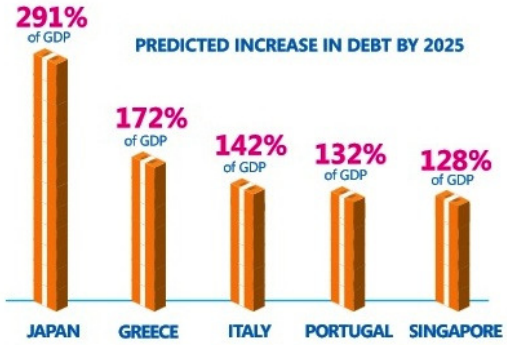
COUNTRIES WITH THE STRONGEST GROWTH IN STEM GRADUATES FROM 2013

(PERCENTAGE OF GROWTH)

4

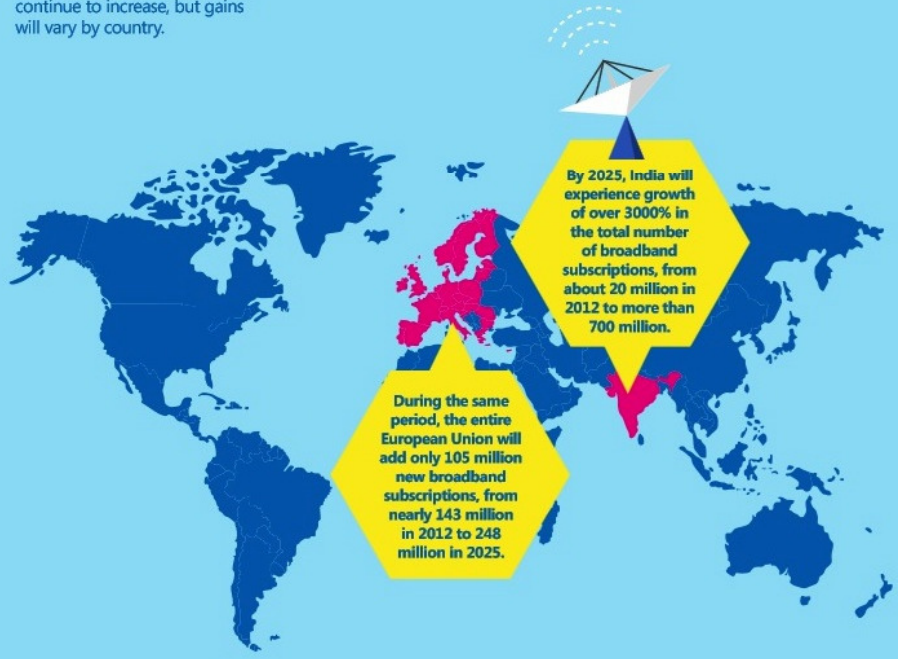
HOW WILL THE WORLD MANAGE GROWING PUBLIC DEBT?

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?

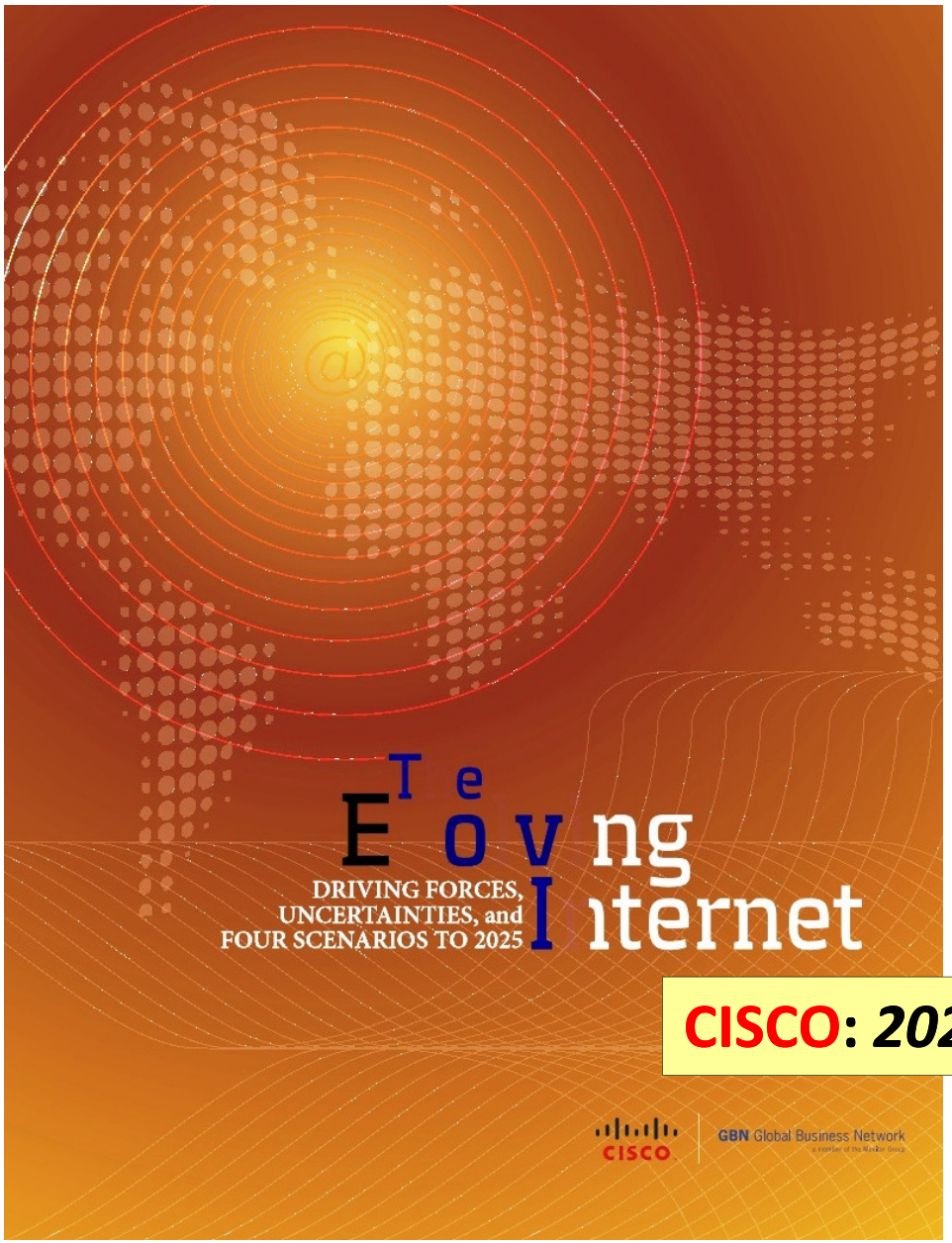
Broadband penetration will continue to increase, but gains will vary by country.



5

Microsoft 2025: *Cyberspace Scenarios*

Technology Visions: Scenario *2025*



The Future Internet in 2025

Open paradigms for personal data and platforms?

M14117MRA – November 2014

CISCO: *2025* Scenarios: IDATE

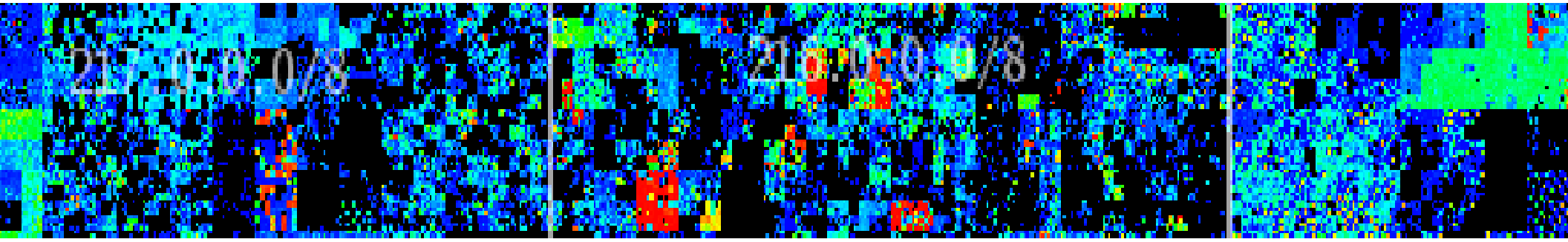
This document is a part of our "Telecom & Over-The-Top" category which includes in 2014:
- a dataset in Excel,
- a state-of-the-art report in PowerPoint,
- six market reports in Word, each with its synopsis in PowerPoint
- Privileged access to our lead OTT analysts

www.idate.org

DIGIWORLD by IDATE

21stC Cybersecurity (2) – *"AI & Machine Learning"*

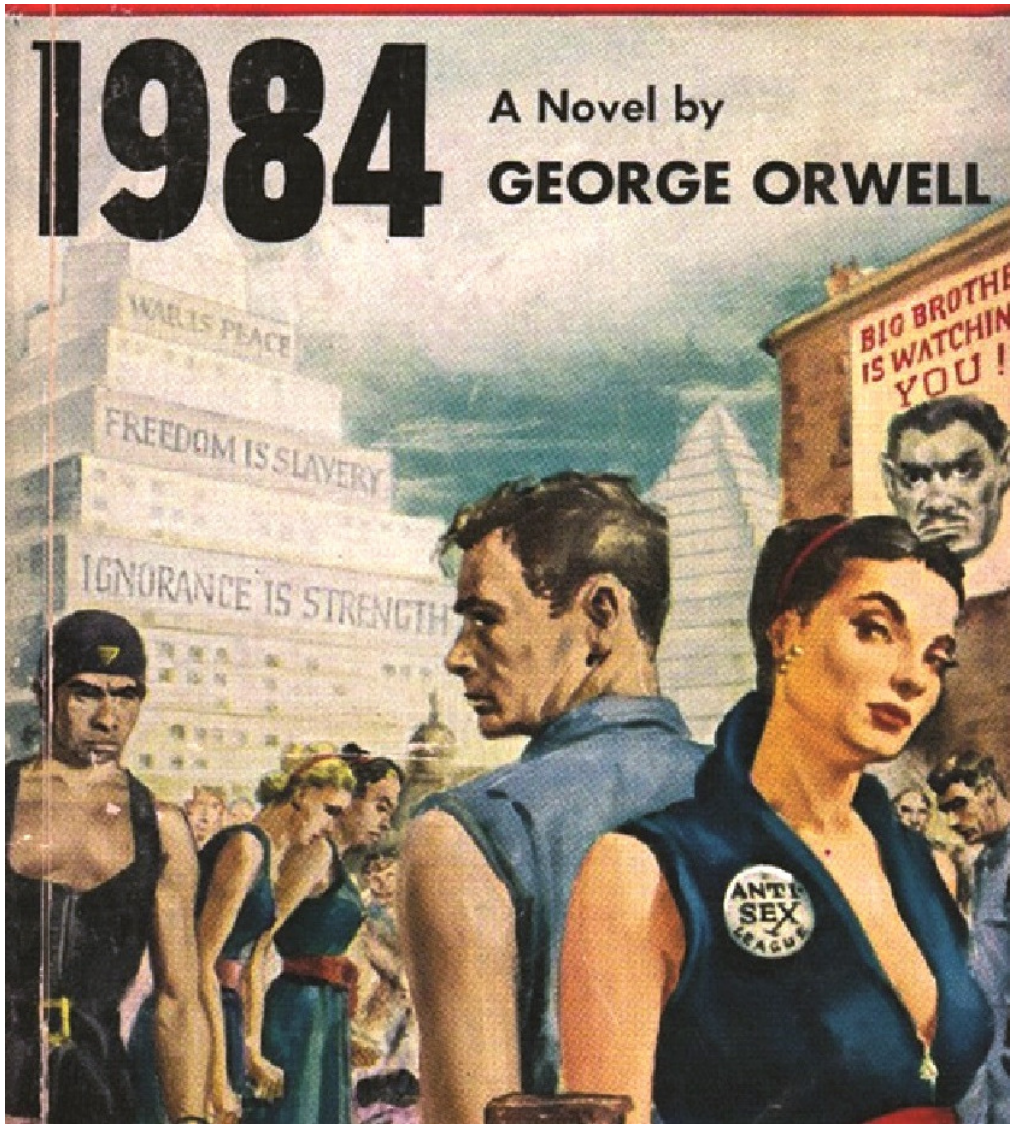
1 – Background: 20th to 21stC Cybersecurity	2 – AI & Machine Learning as Cyber Tools	3 – Recent 21stC Cybersecurity Ventures
4 – Advanced Cyber Scenarios & Analysis	5 – Hybrid 20thC & 21stC Cyber Solutions	6 – Scenario 2020: Integrated Security - IoT
7 – Scenario 2025: Self-Adaptive Security	**8 – Scenario 2040: Neural Security**	9 – YOUR Action Plan for Advanced Cyber!



Scenario 2040: Neural Security

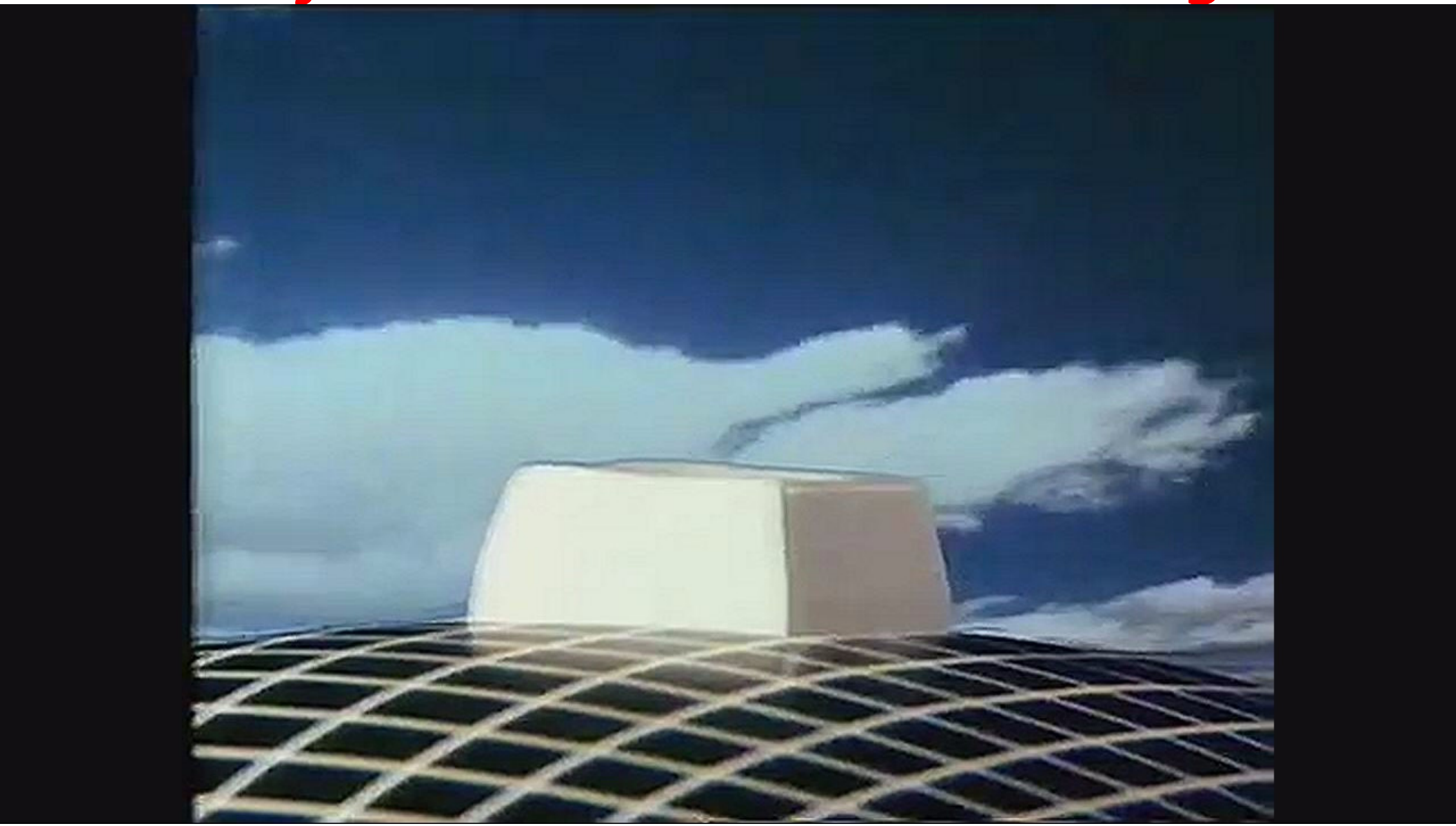
- ..25 Year Time Window - **1990 <– 2015 -> 2040**
- Full Implementation of Intelligent & Adaptive Cybersecurity across the Extended Enterprise
- Autonomous "Alerts" and Real-Time AI-based Cyber Event, Traffic & User Modelling
- New Scaled Architectures and Operational Standards for "Smart Systems" – Smart Devices, Business, Cities, Government, Economy & Society
- Cybersecurity Operations transition to become ultra-intelligent – "Neural Security" .

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

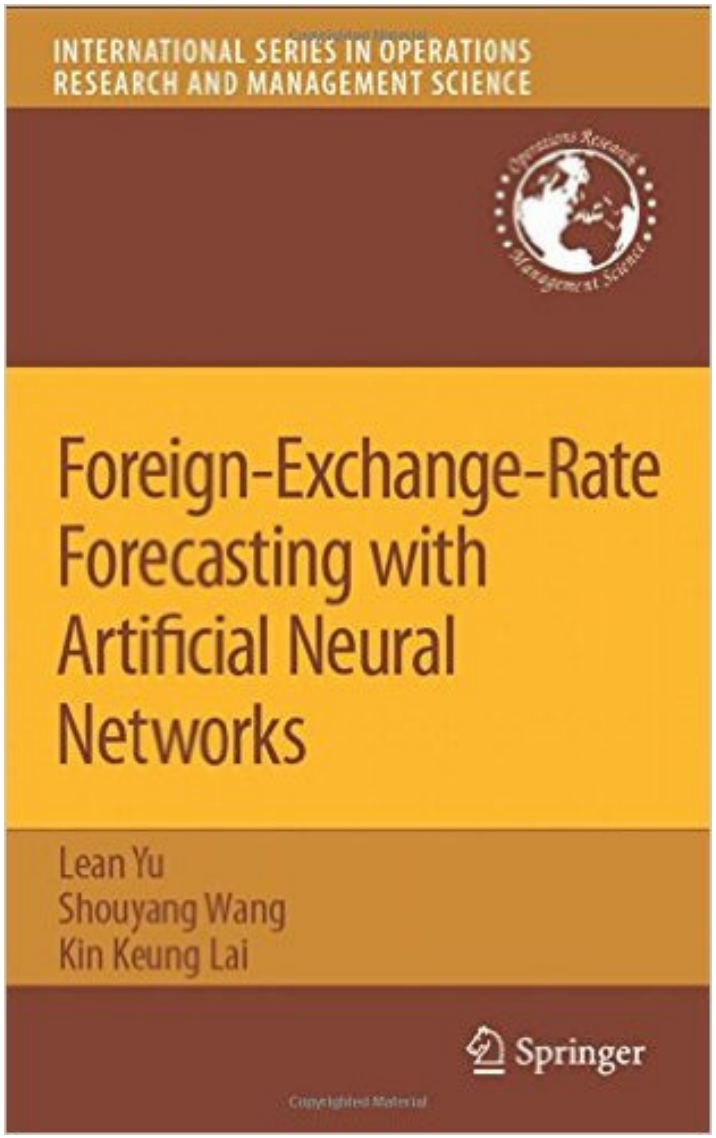


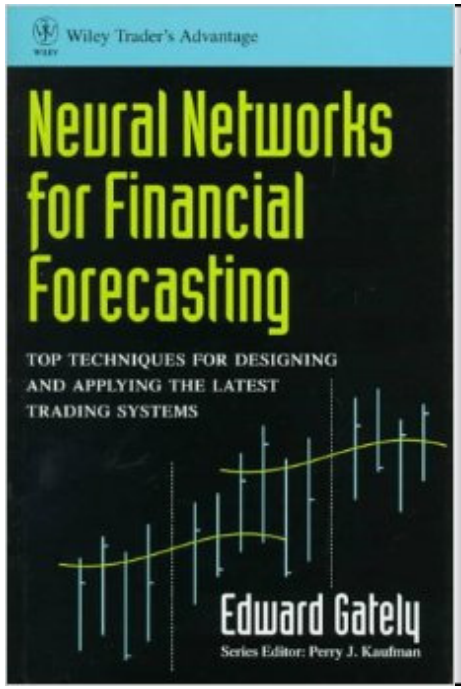
- City Business Systems – British Telecom –

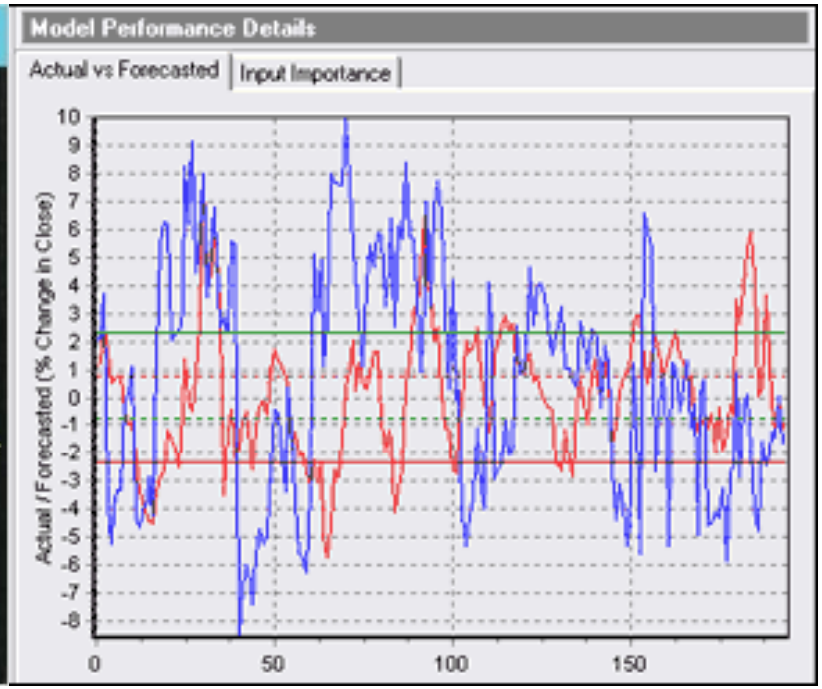
Launch of Real-Time Financial Trading: 1984



Artificial Neural Networks applied to Real-Time Foreign Exchange Dealing





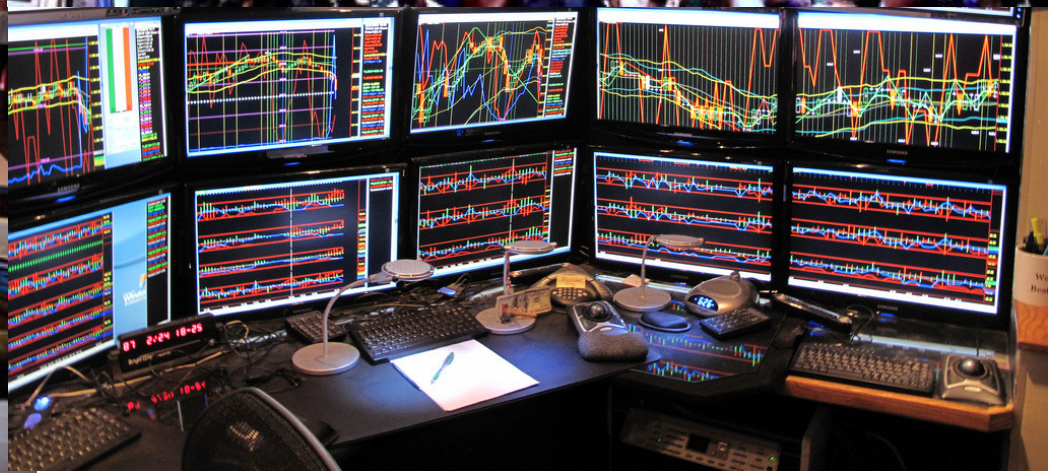


Algorithmic Computer Trading using Real-Time Neural Nets & Statistical Maths Tools have been used for 20+ Years!

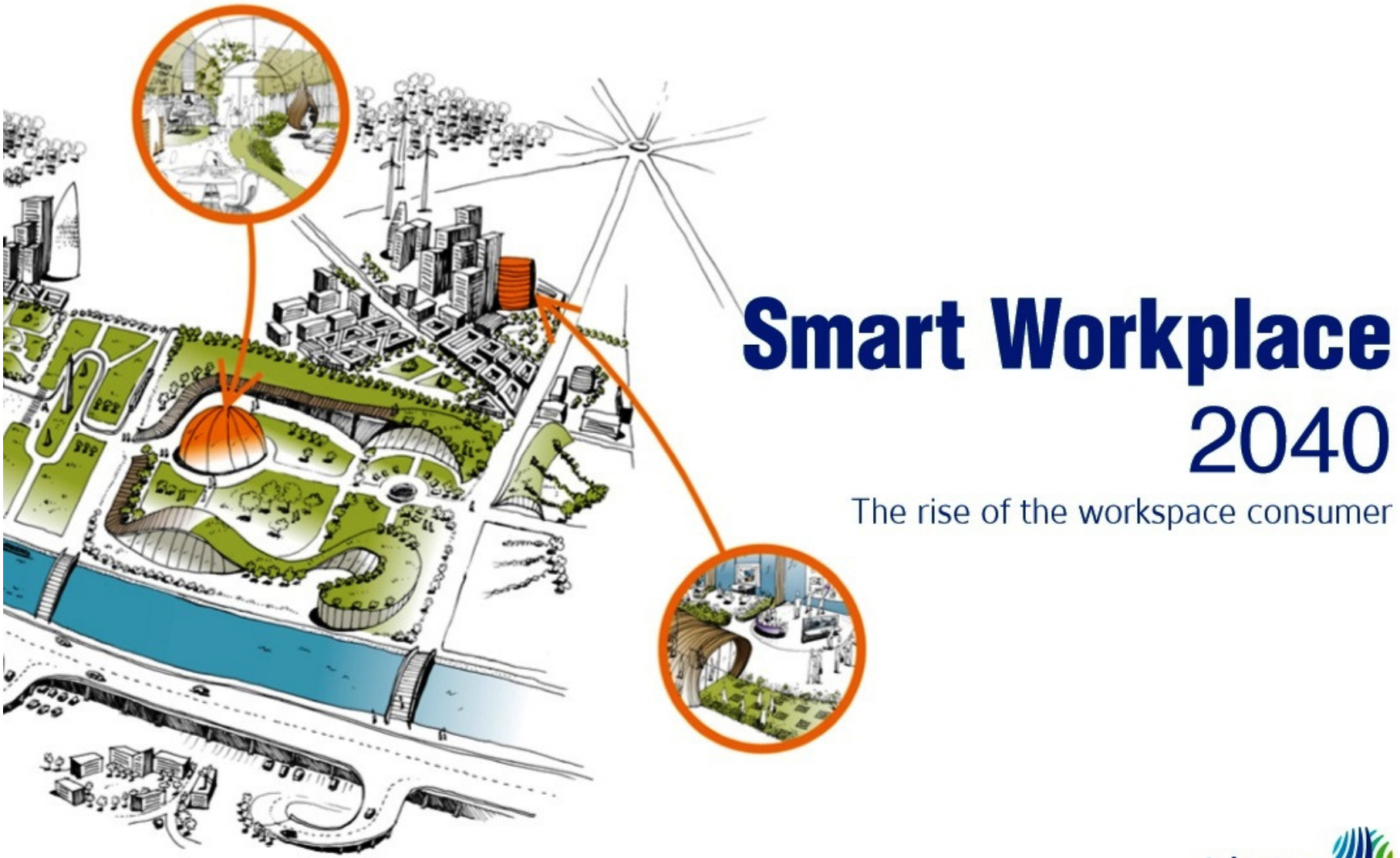
.....Now they are being applied to provide intelligent real-time forecasts for enterprise cybersecurity threats!

Worldwide Real-Time Financial Trading

@Light Speed – 24/7 – Global Networks



Smart Workplace: 2040 – Johnson Controls



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

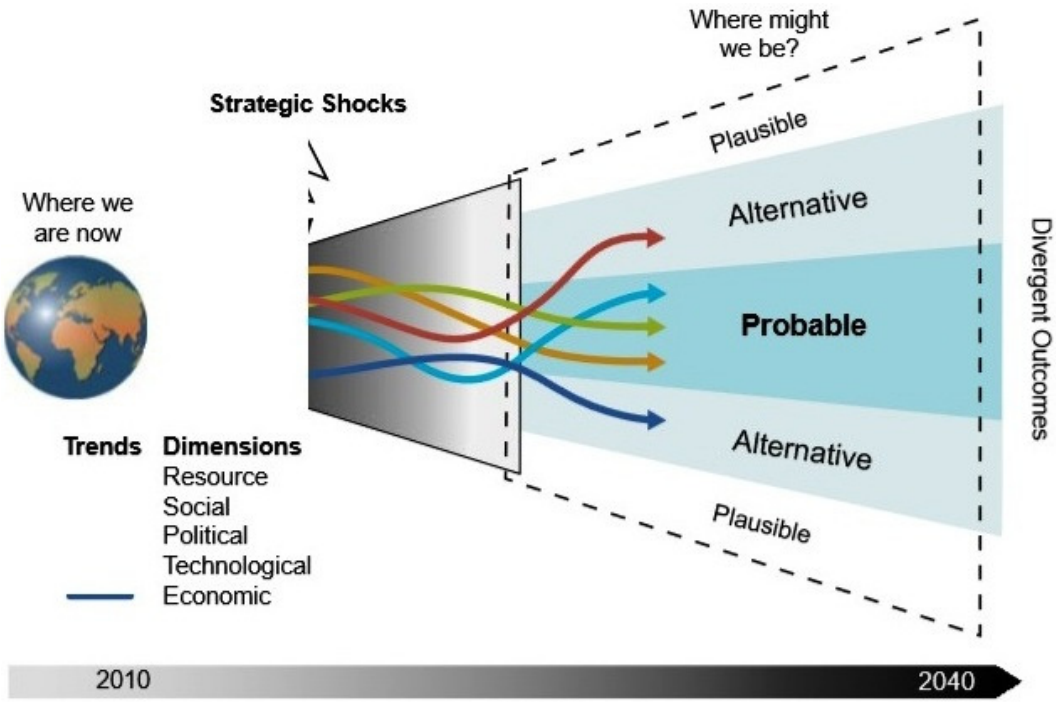
Artificial Intelligence in Cyber Defense

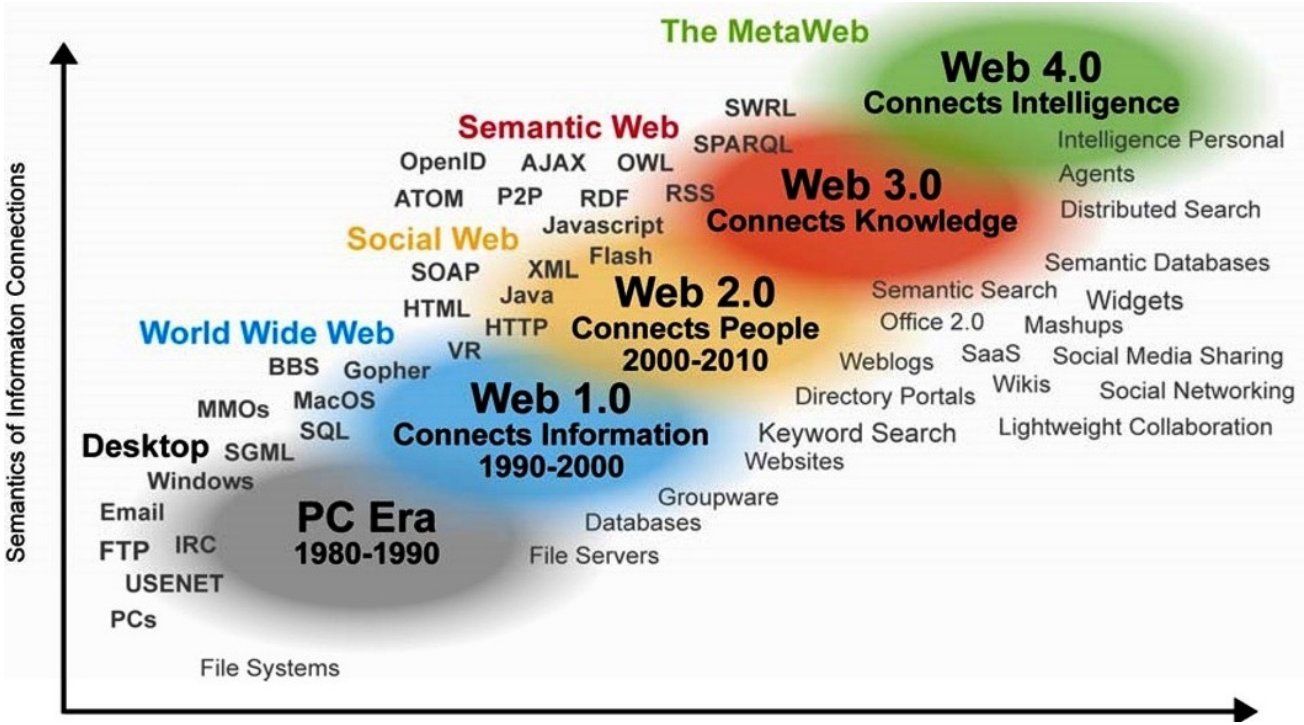
Enn Tyugu
R&D Branch
Cooperative Cyber Defense Center of Excellence (CCD COE)
and Estonian Academy of Sciences
Tallinn, Estonia
tyugu@ieee.org

***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.


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


Where might we be?
Strategic Shocks
Plausible
Alternative
Probable
Alternative
Plausible
Where we are now
Trends
Dimensions
Resource
Social
Political
Technological
Economic
Divergent Outcomes
2010
2040


The MetaWeb
Web 4.0
Connects Intelligence
Intelligence Personal Agents
Distributed Search
Semantic Databases
Widgets
Mashups
Social Media Sharing
Social Networking
Lightweight Collaboration
Web 3.0
Connects Knowledge
Semantic Search
Office 2.0
SaaS
Wikis
Web 2.0
Connects People
2000-2010
Weblogs
Directory Portals
Web 1.0
Connects Information
1990-2000
Keyword Search
Websites
PC Era
1980-1990
Groupware
Databases
File Servers
Semantic Web
SWRL
SPARQL
OpenID
AJAX
OWL
ATOM
P2P
RDF
RSS
Javascript
Social Web
SOAP
XML
Flash
HTML
Java
HTTP
World Wide Web
VR
BBS
Gopher
MMOs
MacOS
SQL
Desktop
SGML
Windows
Email
FTP
IRC
USENET
PCs
File Systems
Semantics of Information Connections

BBC Worldwide Internet Scenario: *2040*

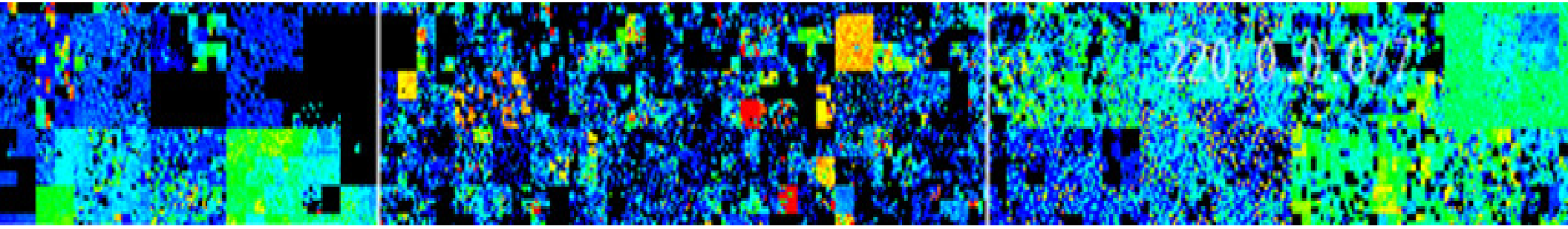
Our Cybersecurity Industry 25 Year Challenge:

- Apply AI Apps for Real-Time Cyber Defence -

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

21stC Cybersecurity (2) – *"AI & Machine Learning"*

1 – Background: 20th to 21stC Cybersecurity	2 – AI & Machine Learning as Cyber Tools	3 – Recent 21stC Cybersecurity Ventures
4 – Advanced Cyber Scenarios & Analysis	5 – Hybrid 20thC & 21stC Cyber Solutions	6 – Scenario 2020: Integrated Security - IoT
7 – Scenario 2025: Self-Adaptive Security	8 – Scenario 2040: Neural Security	**9 – YOUR Action Plan for Advanced Cyber!**



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"*

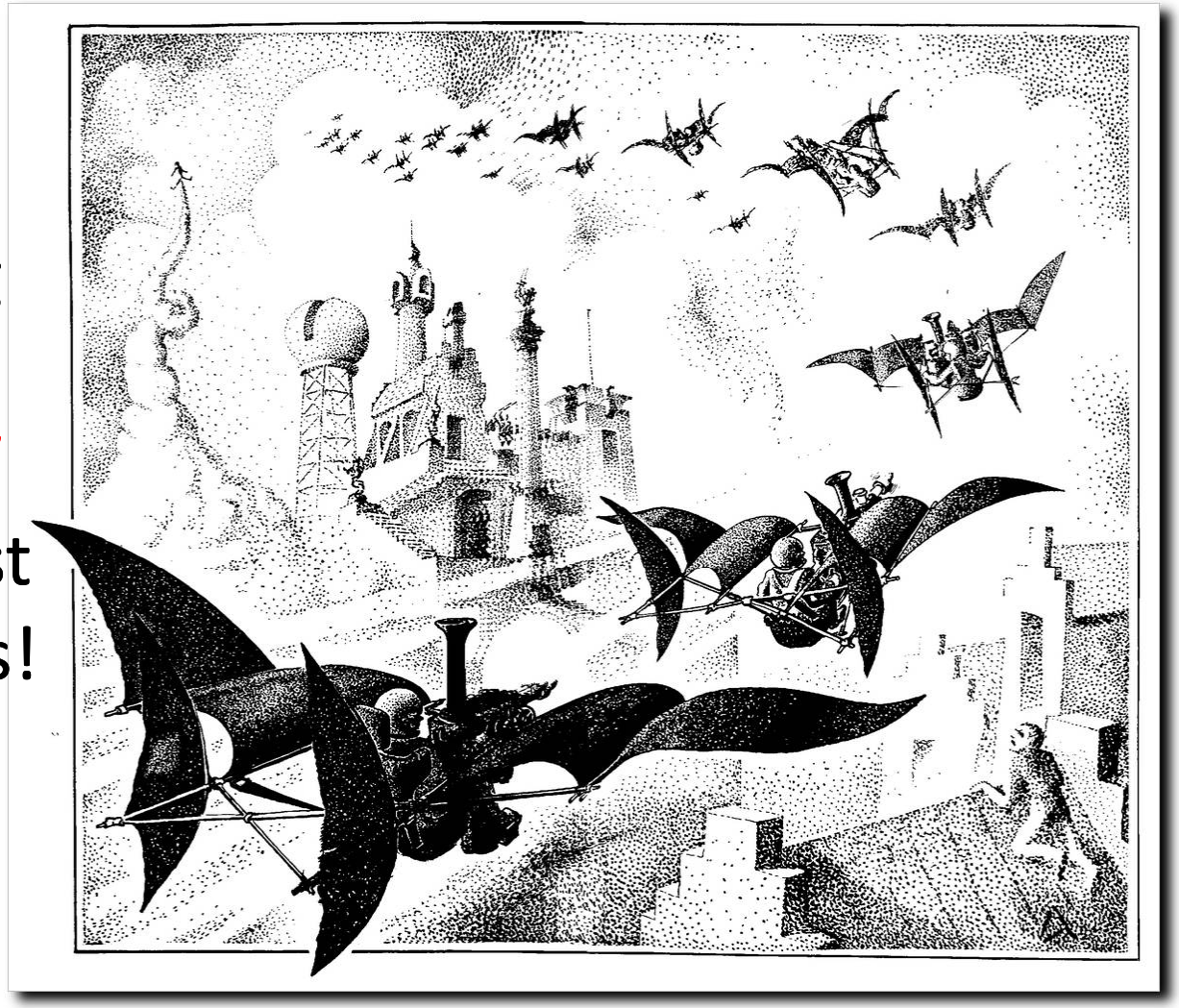
.....Meet the Long Term Challenge of Deploying AI & Machine Learning Based Cybersecurity Tools across YOUR Enterprise!

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.

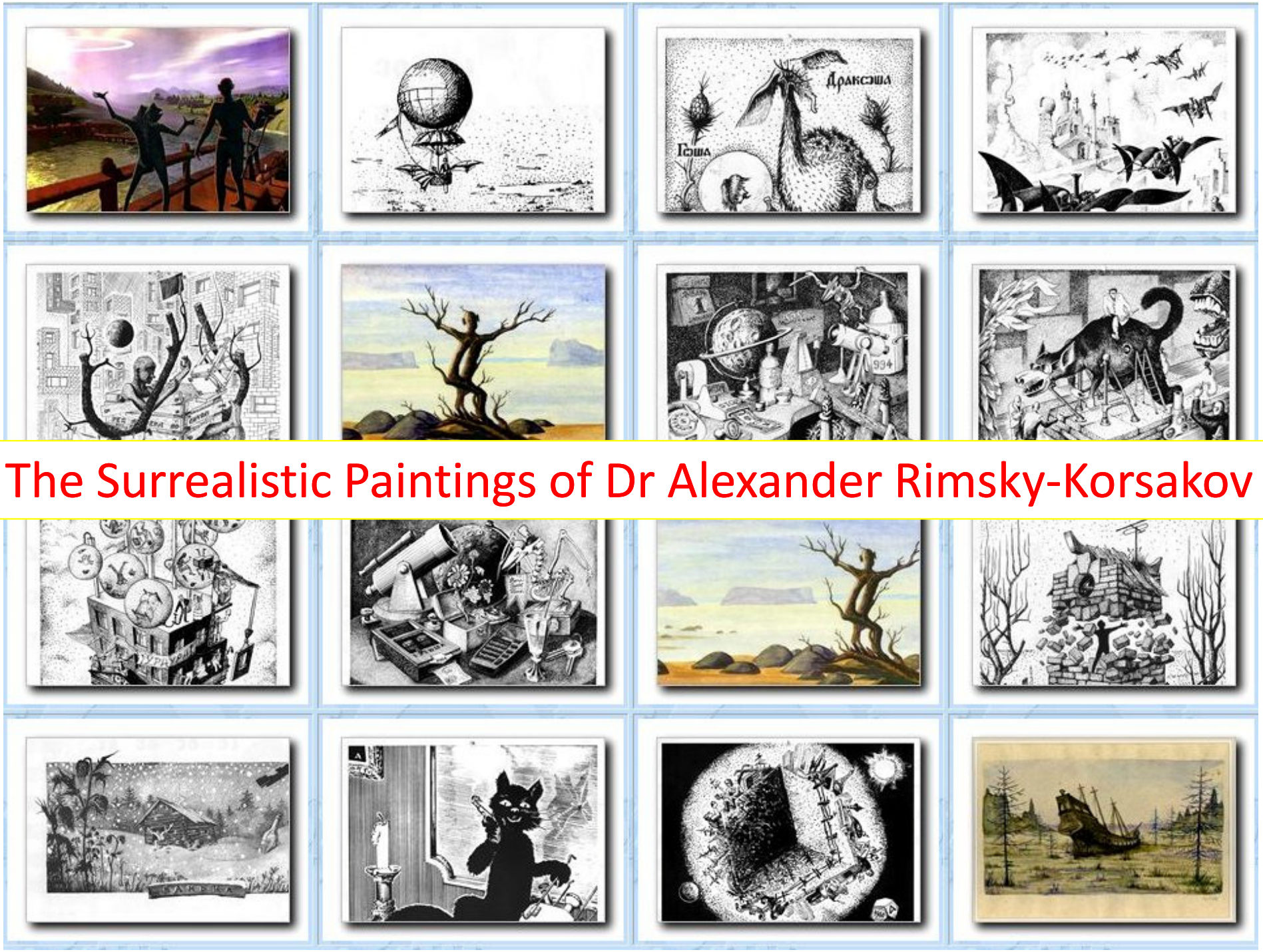
"Real-Time Defence" for Alien Invaders"

A.I. & Machine Learning Cybersecurity Tools will Provide *"Speed of Light"* Real-Time Defence against ***"DARK"*** Threats & Attacks!



"Steam Powered Birds arrive over our Cities! - 1981

Pen & Ink Drawing by Alexander Rimski-Korsakov



The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov

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

East-West Security Conference – Spain2015

- 21stC *CyberTrends Presentation Slides (PDF)* -

Theme (1) – "Integrated Security" **Theme (2) – "Advanced Cybersecurity"**

Download Link: *www.valentina.net/Madrid2015/*

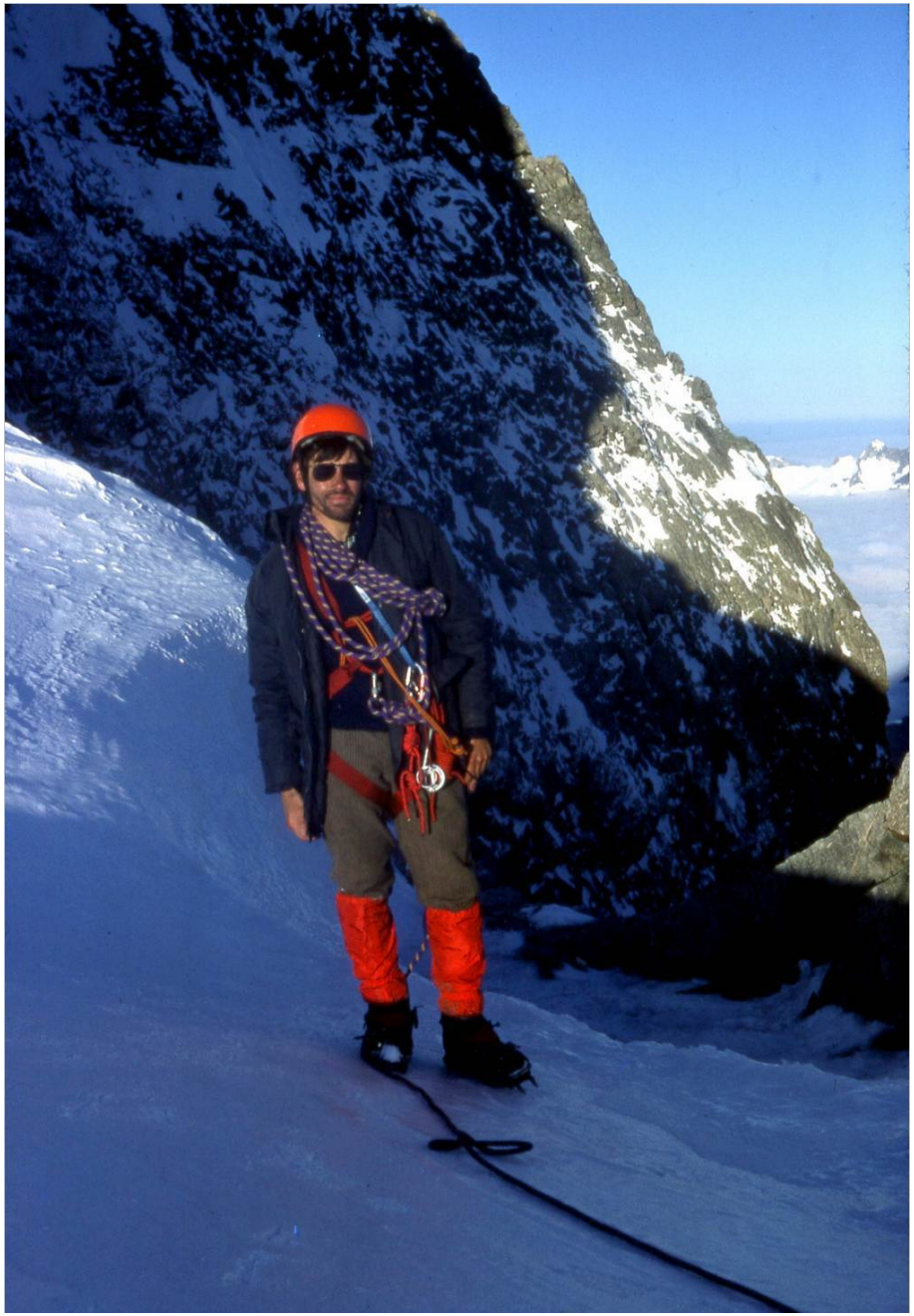
*** Security Equipment for Alpine Climbing ***

Sunrise on « Barre des Écrins » – 4102metres

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

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

Security Equipment for *Alpine Ascents*



Cybersecurity Trends (2): AI & Machine Learning

International East-West Security Conference: Spain, Italy

Thank-You!...

Download Presentation Slides:

www.Valentina.net/Madrid2015/

Download Presentation Slides:
www.Valentina.net/Madrid2015/

Thank you for your time!

Additional *Cybersecurity* Resources

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.

- ***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 Editions.

"Master Class": Armenia - *DigiTec2012*

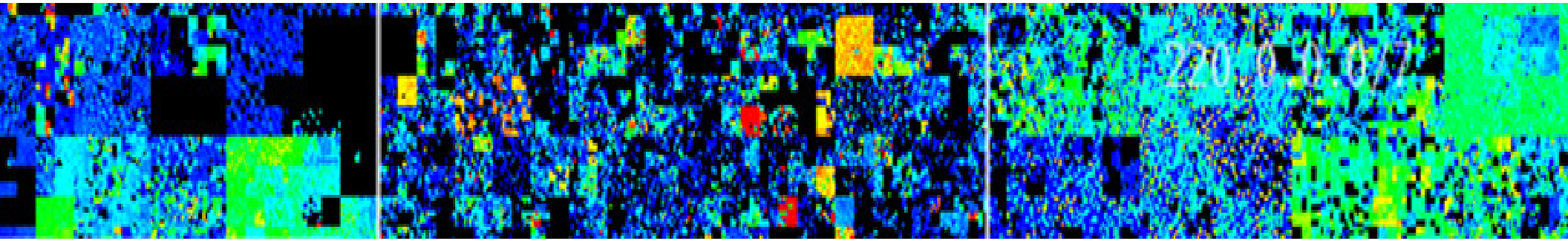
- Smart Security, Economy & Governance -

Download: www.valentina.net/DigiTec2012/

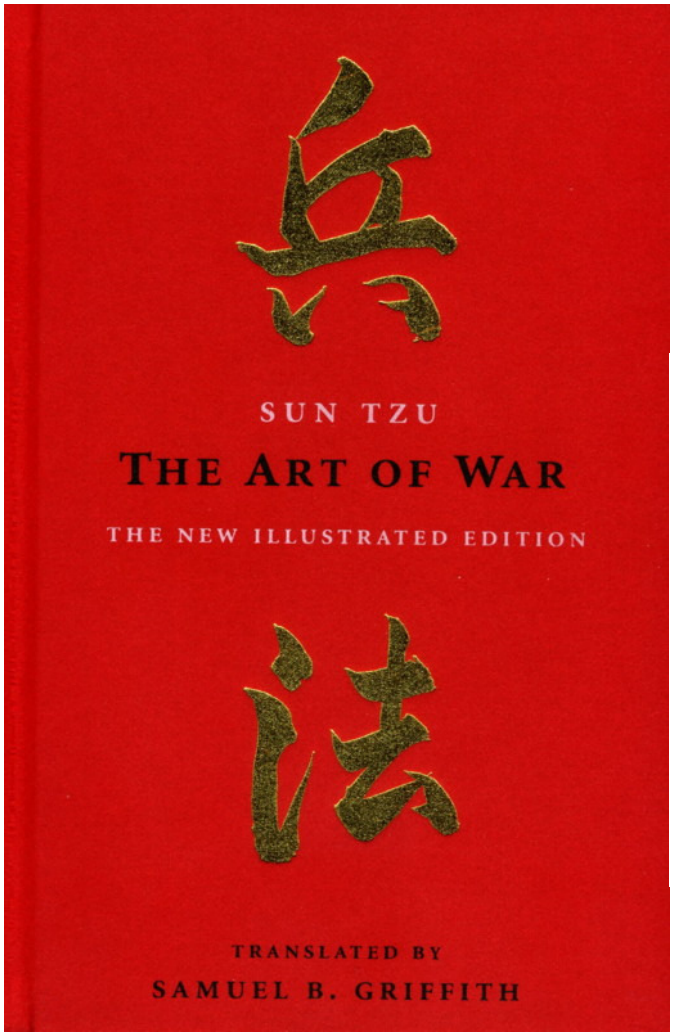
Cybersecurity Trends (1) : "Integrated Security"

International East-West Security Conference: Madrid, Spain

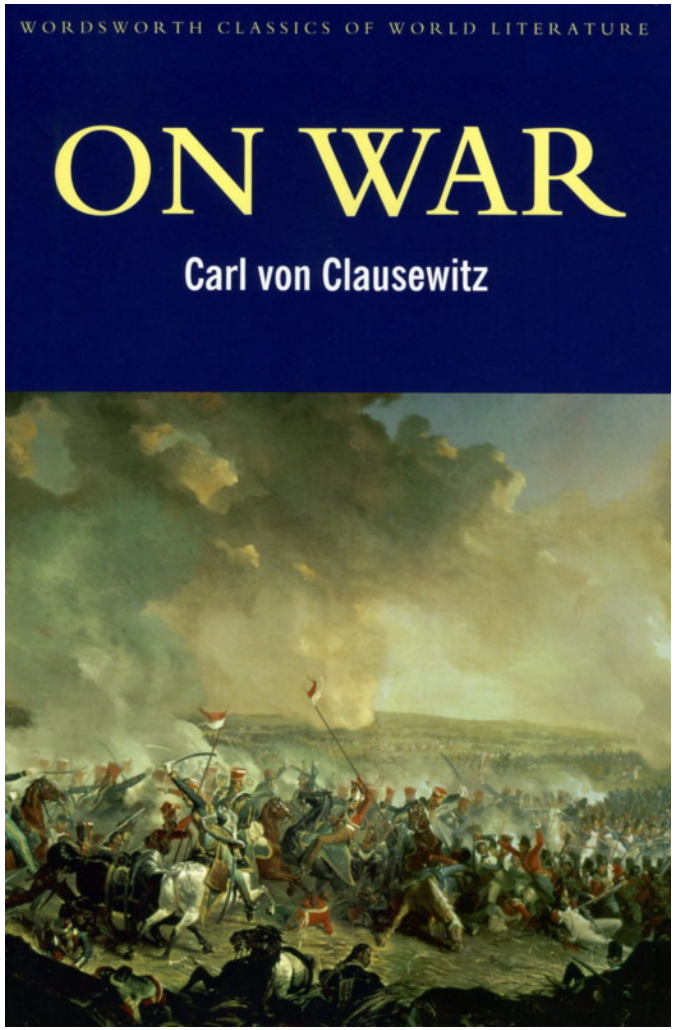
BACK-UP SLIDES



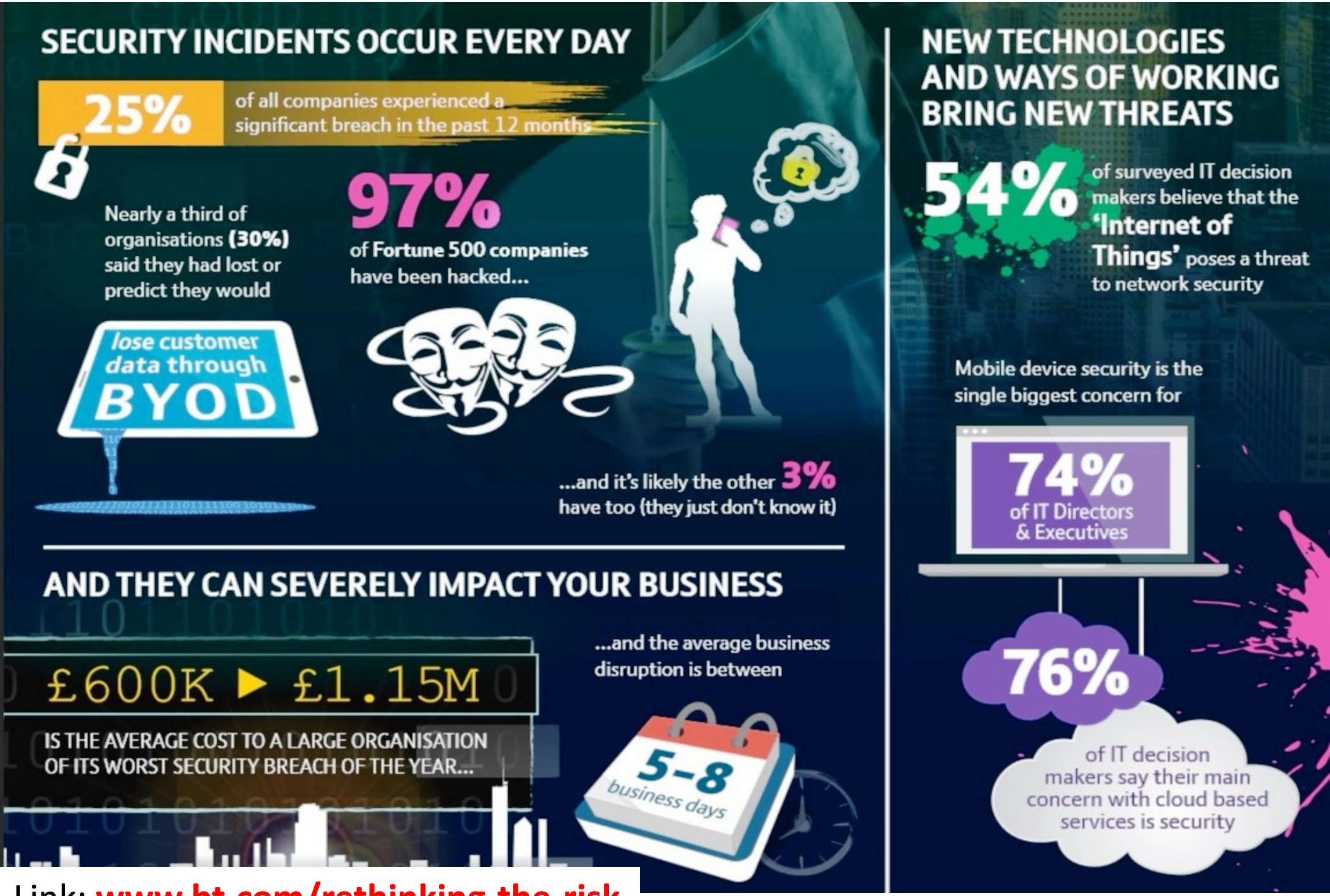
"CyberWar" Strategies & *Models from* Classic Works!



Recommended "Bedtime Reading" *for* Cybersecurity Specialists!



Classic Works on "War" are as relevant today for Cybersecurity as pre-21st C!



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

21stC Architectures for Smart Business Sectors

- We can also design new economic architectures using our Smart Design Principles & then customise sector by sector. We focus upon adaptation, scaling, massive data, & network transparency:

  - ***Education & Research:*** Transition from Monolithic to Niche Networks
  - ***HealthCare & Social Welfare:*** Telemedicine for towns & villages
  - ***Banking & Finance:*** "Real-Time" financial & commodity trading
  - ***Transportation:*** Smart Airports, Roads and Transportation Services
  - ***ICT Infrastructure:*** Launch 3G/4G Mobile Networks, and maximise Internet Services, Local Wireless Hubs & eGovernance across all supported Regions
  - ***National Security & Defence:*** Both for Physical Borders & CyberSpace
  - ***Travel & Tourism:*** Major opportunities for on-line bookings & marketing
  - ***Energy & Utilities:*** Secure Management of National Energy & Utility Grids

- *Tomorrow morning we'll explore the practical design requirements of Smart Security Solutions for Critical National Infrastructure (CNI) .....*

21stC Smart Models for Business

- From 1980s onwards, many Enterprises started to deploy ICT networks, and then to "flatten" their organisations from Hierarchical to Hybrid.
- In the 21stC, Business is now starting to fully deploy more advanced ICT Solutions using the *"Smart Design Principles"* that we summarise below:

  - ***Space-Time Awareness:*** Utilise GPS Location and RFID Technologies to Track and Trace both Products, Staff and all moveable Business Assets to provide Real-Time Corporation
  - ***Adaptation*** to Markets, New Product Features, Delivery Logistics, Minimise Stock Levels
  - ***Massive Memory & Storage:*** Low Cloud Storage Costs permit massive data mining on customer orders, profiles, search and buying behaviours. Already used by major international supermarket chains & global on-line players such as Amazon, eBay, Google.
  - ***Sustainable Security :*** Integrated adaptive management of cyber and physical security
  - ***Self-Organisation:*** Empower staff for Local Decisions with almost "Flat Organisation"
  - ***Scalable Architecture:*** Building Business as Cellular Organisation using High-Speed Nets
  - ***Systems Integration:*** Many Businesses need to integrate their on-line cyber & traditional physical operations to provide a integrated & coherent cyber-physical managed operation

...Now for examples of smart systems – "Self-Organisation" & "Scalability" in science

Cyber "Genes" for *Smart Systems*

- Intelligent Systems, either Artificial or Organic – Living Systems - are based on just a few shared common principles that include:

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) ***Sustainable Security :*** Embedded Smart Security – *Everywhere!*
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 Social Networks, Search & On-Line Commerce
7) ***Systems Integration:*** Cyber and Physical Solutions & Operations

……Advanced ICT Solutions now provide ALL these "Genetic" Functions which will enable us to design ***Smart Cyber-Physical Security Solutions***

Smart Security – *"Design Toolkit"*

- The plan is now to apply the Smart Decision and Learning "Genes" as the design tools for critical economic sectors such as Banking, Energy & Defence

  - ***Smart Decision "D-Genes" :*** Spatial Geo-Location, Real-Time Operations, & Transforming Data to Decision through "Knowledge Lens"
  - ***Smart Learning "L-Genes":*** Adaptation, Self-Organisation, Scalable Architecture and Massive Memory & Data Storage
  - ***Smart Sustainability:*** Joint Operations for Cyber & Physical Security
  - ***Smart Governance:*** On-Line eGovernment Services together with new Laws, Legislation & Regulations for Cybercrime, eCommerce & Privacy

*…..Together these Smart Principles form our **"Design Toolkit"!***

10 Steps To Cyber Security

CESG

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.

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.

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.

Establish an effective governance structure and determine your risk appetite.

Information Risk Management Regime

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

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.

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.

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.

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.

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.

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**