...Energising YOUR Cybersecurity with "*Biometrics & Forensics*"

Dr David E. Probert
VAZA International

Dedicated to Grand-Sons: Ethan, Matthew & Roscoe – *Energising their Security!*

…Модернизация ВАШЕЙ Кибербезопасности с помощью “Биометрии & Криминалистики”

Dr David E. Probert

VAZA International

Dedicated to Grand-Daughters – Abigail and Alice - *To Their Secure Future!*

Crucial Cybersecurity – *Dual Themes*

Theme (1) – ...The Crucial Role of Cybersecurity in the "War on Terror"

“

The Crucial Role of Cybersecurity in the - "War on Terror" -

Dr David E. Probert
VAZA International

Dedicated to Grand-Daughters – Abigail and Alice – Securing their Future Life!

33rd International East/West Security Conference

The Crucial Role of Cybersecurity in the "War on Terrorism"
- Prague, Czech Republic: 6th-7th June 2016 -
© *Dr David E. Probert* : www.VAZA.com ©

1

The Prevention of Terrorism requires Business & Government Security Teams to Integrate their Cybersecurity Operations with Real-Time Surveillance, GPS Tracking & Personal Profiling Tools.

"Integration" : "SMART Real-Time Security & Surveillance **11:45 - *6th June 2016***

Theme (2) – ...Energising YOUR Cybersecurity with "Biometrics and Forensics"

...Energising YOUR Cybersecurity with "Biometrics & Forensics"

Dr David E. Probert
VAZA International

Dedicated to Grand-Sons: Ethan, Matthew & Roscoe – Energising their Security!

33rd International East/West Security Conference

Energising YOUR Cybersecurity with "Biometrics & Digital Forensics"
- Prague, Czech Republic: 6th-7th June 2016 -
© *Dr David E. Probert* : www.VAZA.com ©

1

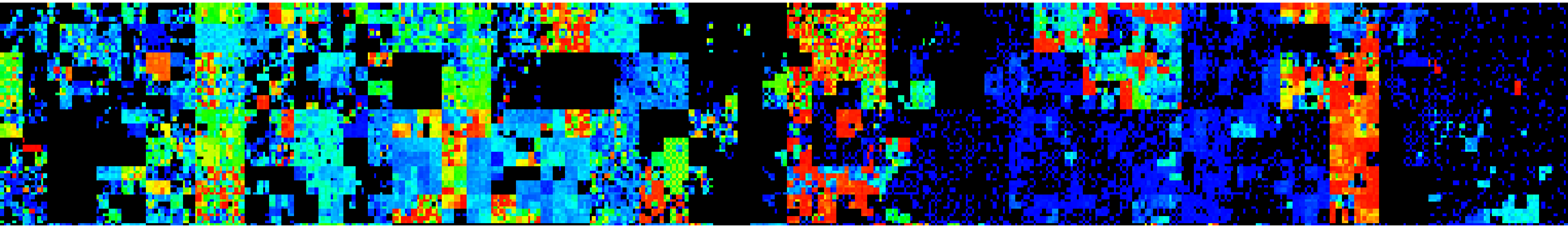
Secure End-User Authentication for the "Internet of Things (IoT)" will require CSOs & Security Teams to Integrate Biometric & Forensic Tools with their Physical & Cybersecurity Operations.

"Intelligence": "ADAPTIVE Cyber-Biometric Security for the IoT" **14:30 - *6thJune 2016***

Download Slides: [*www.valentina.net/Prague2016/*](http://www.valentina.net/Prague2016/)

Energising *Cybersecurity* with "Biometrics & Forensics"

1 – Background: *"CyberCrime & Terrorism"*	2 – 21stC Profiling & Tracking: "Bad Guys"	3 –Real-Time Security & Surveillance
4 – Integrated Cyber Biometrics: Pre-Attack	5 – Cyber Digital Forensics : Post-Attack	6 – Cyber-Bio: Security Sector Scenarios
7 – Biometric User Authentication for "IoT"	8 – Cyber-Bio Vision: Practical Solutions	9 –YOUR TOP 10 Actions & RoadMap



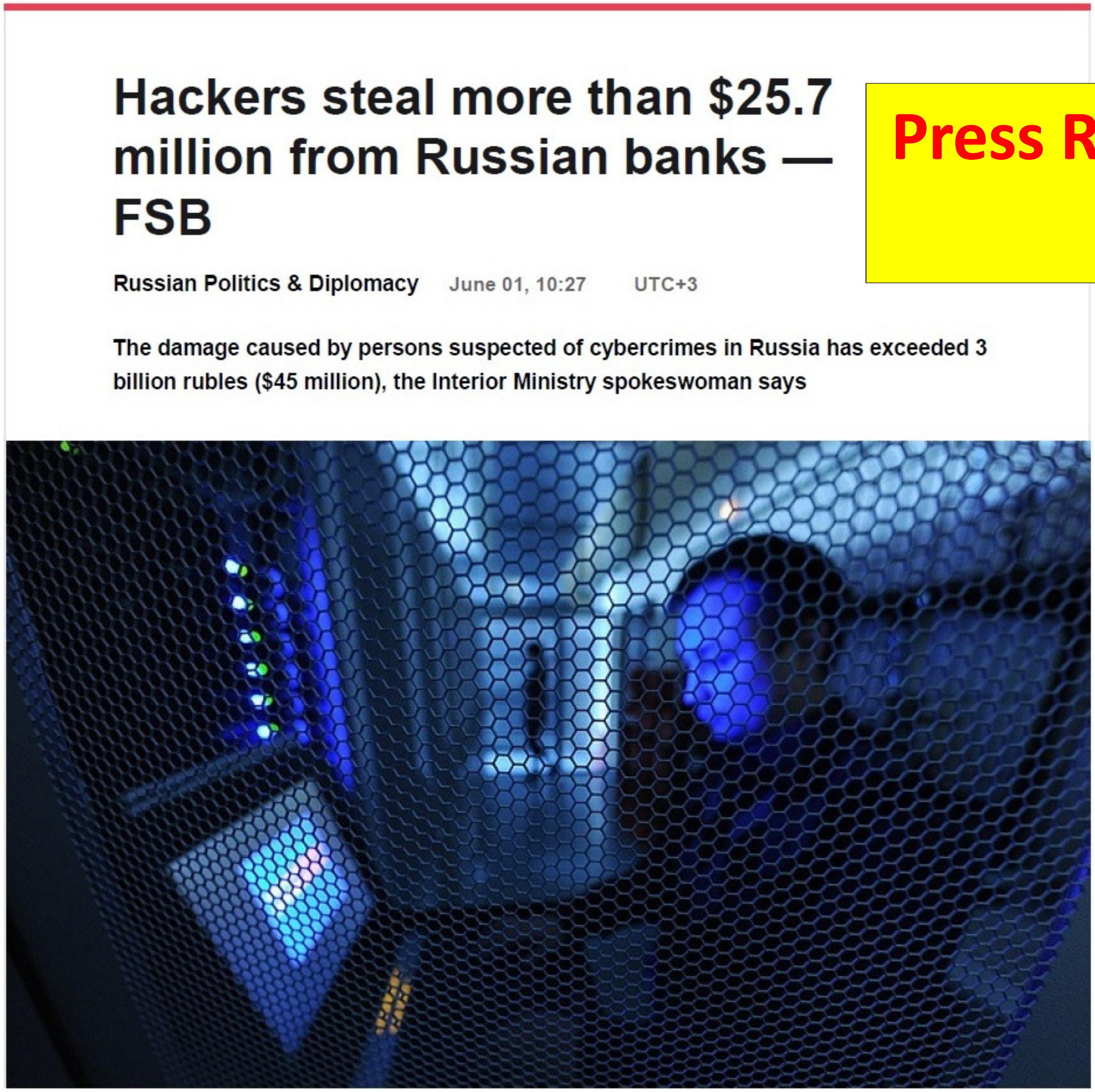
(1) CyberCrime & CyberTerrorism

- Defence against CyberCrime & CyberTerrorism requires us to "Energise" OUR Cybersecurity with *"Cyber Biometrics and Digital Forensics"!...*

  – Migration from 20thC Physical to 21stC Smart Security
  – Bio-Authentication for Critical Systems, Sites & Assets
  – Digital Forensics for Post-Attack Cyber Investigations
  – Real-Time Auto Tracking of "Bad Guy" Bio-Profiles

... In this presentation we review the practical security benefits of current Biometric & Forensic Tools...

CyberCrime: Russian Financial Services



Hackers steal more than $25.7 million from Russian banks — FSB

Russian Politics & Diplomacy June 01, 10:27 UTC+3

The damage caused by persons suspected of cybercrimes in Russia has exceeded 3 billion rubles ($45 million), the Interior Ministry spokeswoman says

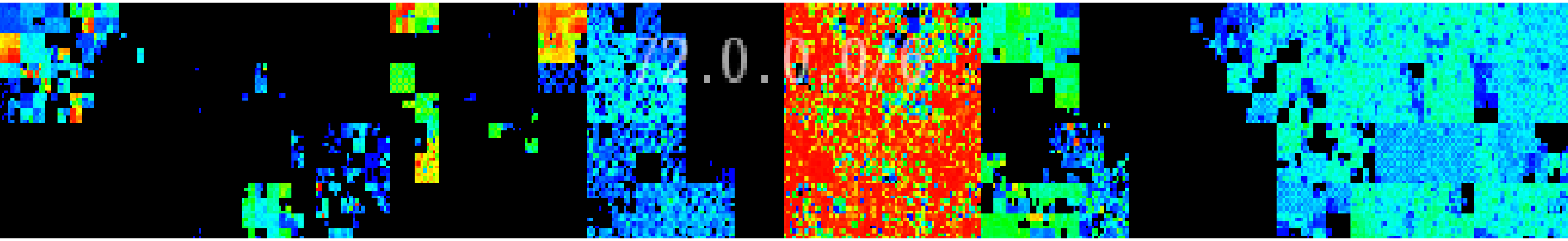
Press Report: TASS News Agency
- 1st June 2016 -

- **6+ Russian Banks “Hacked” as well as other target CIS Banks**
- **Trojan “Lurk” Malware Toolkit**
- **At least 1.7Bn Roubles Stolen**
- **50 “Cyber Hackers” Arrested**
- **Digital Forensics executed by Kaspersky Labs, FSB and Sberbank**

Energising *Cybersecurity* with “Biometrics & Forensics”

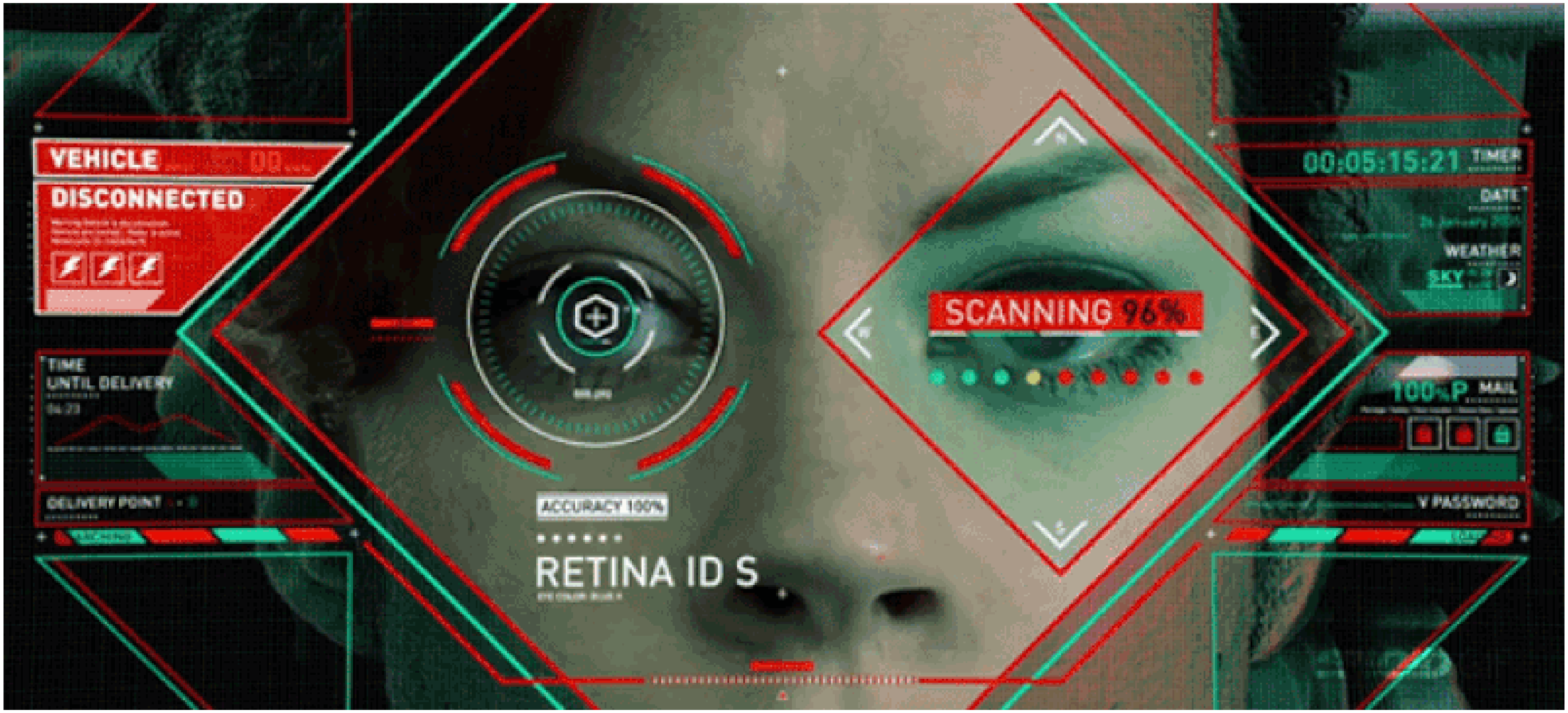
Pilsner Urquell
PLZEN CZECH
CZECH MENU
BEEF GOULASCH with DUMPLINGS
PATATO DUMPLINGS STUFFED with BACON & CABBAGE
CREPES SPINACH with HAM & CHESSE
ROASTED SAUSAGE with DALIBOR'S LOA
Tipicos platos checos
Gulas ternera pan hervido
Pan hervido de patatas con carne ahumada y col
Creps rellenos de espinacas con jamón y queso
Salchichas asadas con rabano picante mostasa y pan checo
APPLE STRUDEL
BRANDY

1 – Background: CyberCrime & Terrorism	2 – 21stC Tracking & Profiling: “Bad Guys”	3 – Real-Time Security & Surveillance
4 –Integrated Cyber Biometrics: Pre-Attack	5 – Cyber Digital Forensics : Post-Attack	6 – Cyber-Bio: Security Sector Scenarios
7 – Biometric User Authentication for “IoT”	8 – Cyber-Bio Vision: Practical Solutions	9 – YOUR TOP 10 Actions & RoadMap



(2) Tracking & Profiling : *"Bad Guys"*

- Mitigating Global Crime & Terrorism requires us to **Profile & Track** the "Bad Guys" in "Real-Time" with Intelligent Networked Computing Systems:



...***Cyber Computing Smart Apps*** can now Track Massive Databases of Target "Bad Guy" Profiles ***@ Light Speed!...***

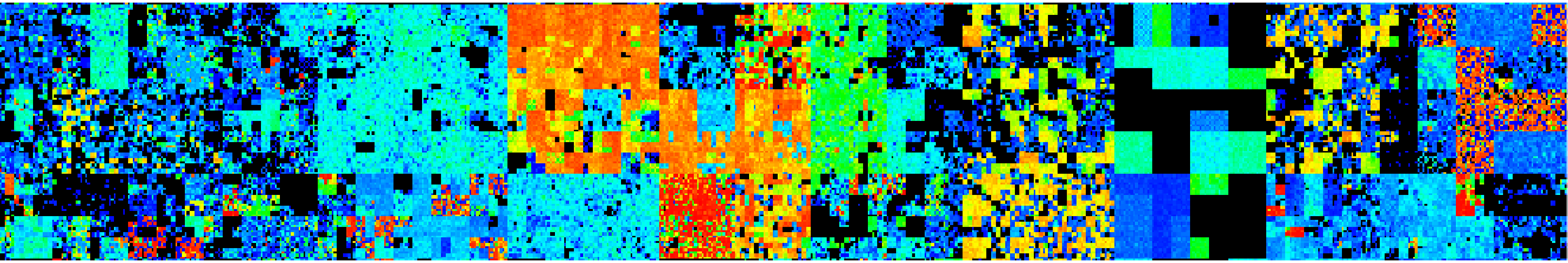
(2) Tracking & Profiling : *"Bad Guys"*

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

...***Cyber Computing Smart Apps*** can now Track Massive Databases of Target "Bad Guy" Profiles ***@ Light Speed!...***

Energising *Cybersecurity* with "Biometrics & Forensics"

1 – Background: CyberCrime & Terrorism	2 – 21stC Profiling & Tracking: "Bad Guys"	3 – Cyber-Physical Threat Scenarios
4 –Integrated Cyber Biometrics: Pre-Attack	5 – Cyber Digital Forensics : Post-Attack	6 – Cyber-Bio: Security Sector Scenarios
7 – Biometric User Authentication for "IoT"	8 – Cyber-Bio Vision: Practical Solutions	9 – YOUR TOP 10 Actions & RoadMap



(3) Cyber-Physical Threat Scenarios

- **CyberCrime:**
  - – Financial Fraud using Cyber Hacking for Client Bank Accounts coupled with Timed ATM Payouts
  - – Secure Access to Lawyer/Real Estate eMail Account in order to steal full payments for Homes/Offices
- **CyberTerror:**
  - – Access/Hack On-Line Plans of Target (Airport, Mall, Resort, Theatre) & secure resources on "DarkNet"
  - – Secure Access to Nuclear Power Facilities with "Fake ID" to disrupt SCADA Control Systems

...ALL Business Sectors are now at risk from ***CyberCrime & CyberTerrorism*** *– Worldwide!...*

Hybrid “4D” *Physical-Cyber* Terrorism

- ***Cyber Terror Attacks*** will typically be integrated within an overall Physical-Cyber Game Plan (4D)
  - Physical Terror focuses on the Target Physical & Social Infrastructure, Buildings & Territory
  - Cyber Terror focuses upon the Target IT Computing & Critical Information Infrastructure

- The Emergence of ***“Hybrid” Terror Attacks*** will demand that we re-design & engineer Security for Government, Business & Society in 21st C!

Hybrid Cyber-Physical Hacktivism

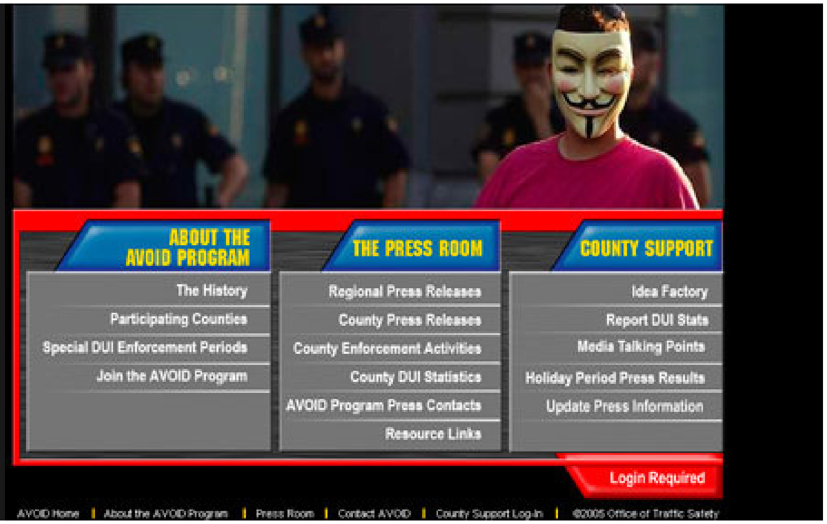
"Anonymous" Attacks on BART - Aug 2011

❖ *Physical Protests* by International *Hacktivist* Group – *"Anonymous"* - coupled with multiple Web-Site *Cyber Attacks* following incident on *Bay Area Transit Network - BART – San Francisco*

We Will **NOT** Tolerate Censorship

San Francisco: Join Us Monday, **August 15th** at 5pm for a **peaceful** protest at Civic Center station.

United as One, divided by Zero. We are Anonymous, We are legion, We never forgive, We never forget, Expect us.



“Cyber to Physical Attacks”

- The illegal penetration of ICT systems may allow criminals to secure information or “make deals” that facilities their real-world activities:
  - *“Sleeping Cyber Bots”* – These can be secretly implanted by skilled hackers to secure on-line systems, and programmed to explore the directories & databases, and & then to transmit certain information – Account & Credit Card Details, Plans, Projects, Deals
  - *Destructive “Cyber Bots”* – If cyber-bots are implanted by terrorist agents within the operational controls of power plants, airports, ports or telecomms facilities then considerable physical damage may result. A simple *“delete *.*”* command for the root directories would instantly wipe out all files unless the facility has real-time fail-over!
  - *Distributed Denial of Service Attacks* – These not only block access to system, but in the case of a Banking ATM Network, means that the national ATM network has to be closed. Alternatively in the case of an airline check-in and dispatch system, flights are delayed.
  - *National CyberAttacks* – Many international organisations such as NATO & US DOD forecast that future regional conflicts will begin with massive cyberattacks to disable their targets’ physical critical communications and information infrastructure (CNI)

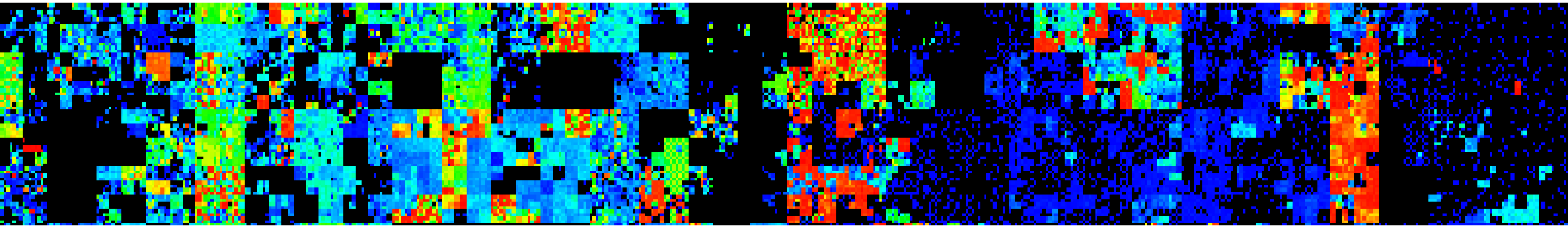
Nations need to upgrade their national cybersecurity to minimise the risks of *Hybrid Cyber-Physical Attacks* from terrorists, criminals, hacktivists and political adversaries

“Physical to Cyber Attacks”

- Most “physical to cyber attacks” involve staff, contractors or visitors performing criminal activities in the “misuse of computer assets”:
  - *Theft & Modification of ICT Assets:* It is now almost a daily occurrence for critical information & databases to be either deliberately stolen or simply lost on PCs or Chips
  - *Fake Maintenance Staff or Contractors:* A relatively easy way for criminals to access secure facilities, particularly in remote regions or developing countries is to fake their personnel IDs and CVs as being legitimate ICT maintenance staff or contractors
  - *Compromised Operations Staff:* Sometime operational ICT staff may be tempted by criminal bribes, or possibly blackmailed into providing passwords, IDs & Access Codes.
  - *Facility Guests and Visitors:* It is standard procedure for guests & visitors to be accompanied at all times in secure premises. In the absence of such procedures, criminals, masquerading as guests or visitors, may install keylogger devices or extract information, plans and databases to wireless enabled USB chips, tablets or phones!

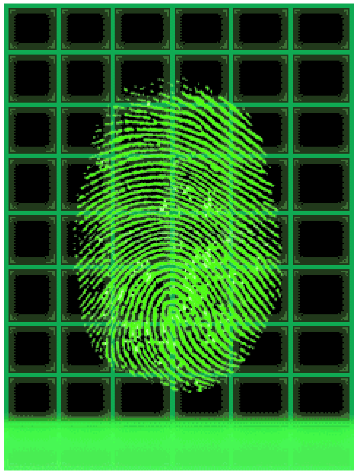
Energising *Cybersecurity* with “Biometrics & Forensics”

1 – Background: CyberCrime & Terrorism	2 – 21stC Profiling & Tracking: “Bad Guys”	3 – Real-Time Security & Surveillance
4 –Integrated Cyber Biometrics: Pre Attack	5 – Cyber Digital Forensics : Post-Attack	6 – Cyber-Bio: Security Sector Scenarios
7 –Biometric User Authentication for “IoT”	8 – Cyber-Bio Vision: Practical Solutions	9 – YOUR TOP 10 Actions & RoadMap

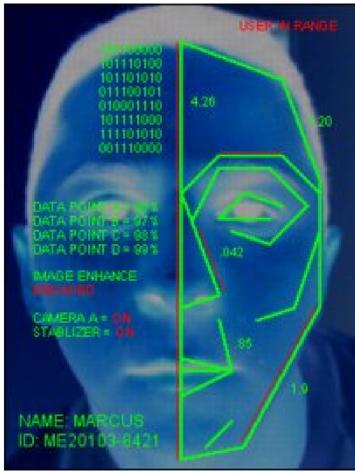


(4) Integrated *Cyber* Biometrics: ***Pre-Attack***

- *Intelligent Biometrics Tools* can significantly reduce ***YOUR*** Risks of Cyber Threats & Attacks...

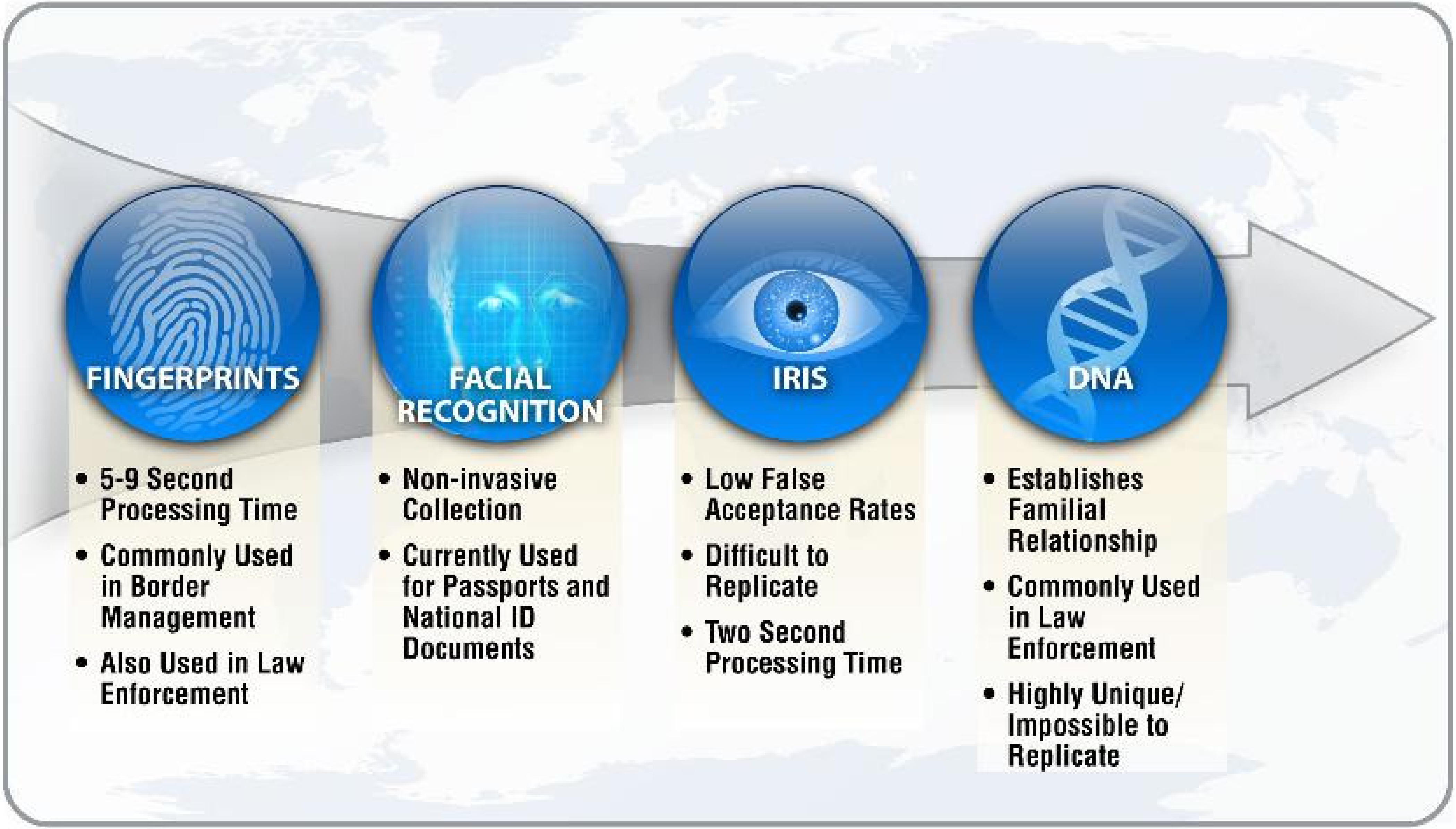


  - Device & Access Authentication by Fingerprints, Retinal/Iris Scan or Palm Vein Scan
  - Facility Access with "Live" 3D Facial Recognition
  - "Behavioural Biometrics" for Secure User Authentication
  - City/Campus Regional Tracking with Intelligent 4K Networked CCTV & Real-Time *Self-Learning* Video Analytics
  - "Live" **CBRN** Scanning for Hazardous materials – (**C**hemical, **B**iological, **R**adiological, **N**uclear)



...It is crucial that *Cyber Biometrics Tools* are Integrated with the CSO-led ***Business Security Operations***

Typical Cyber-Biometric Solutions



FINGERPRINTS

- 5-9 Second Processing Time
- Commonly Used in Border Management
- Also Used in Law Enforcement

FACIAL RECOGNITION

- Non-invasive Collection
- Currently Used for Passports and National ID Documents

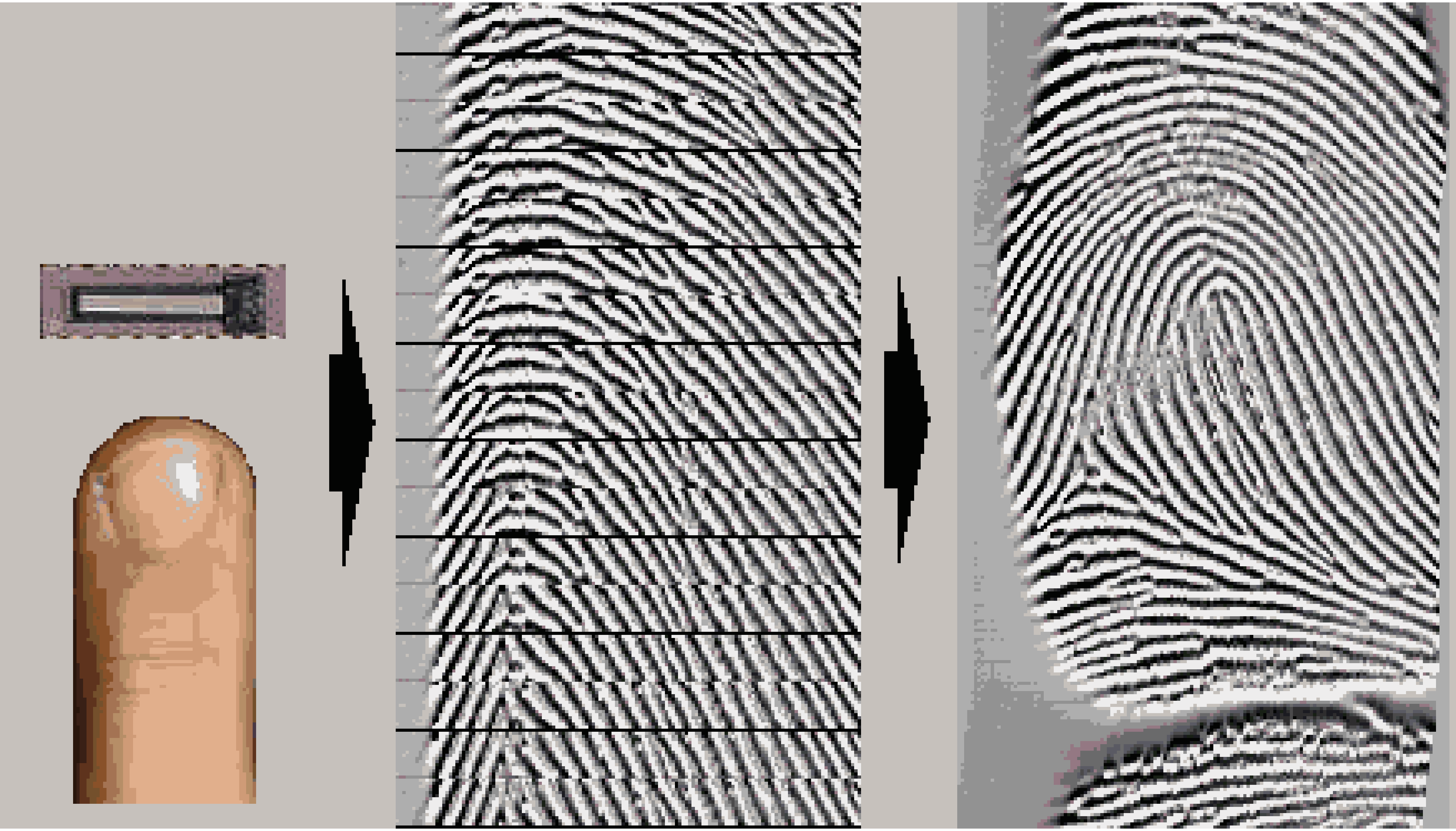
IRIS

- Low False Acceptance Rates
- Difficult to Replicate
- Two Second Processing Time

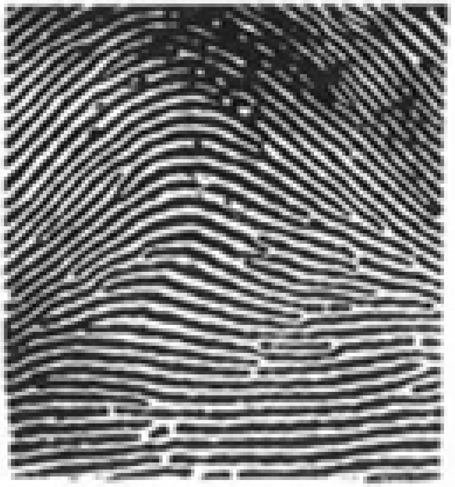
DNA

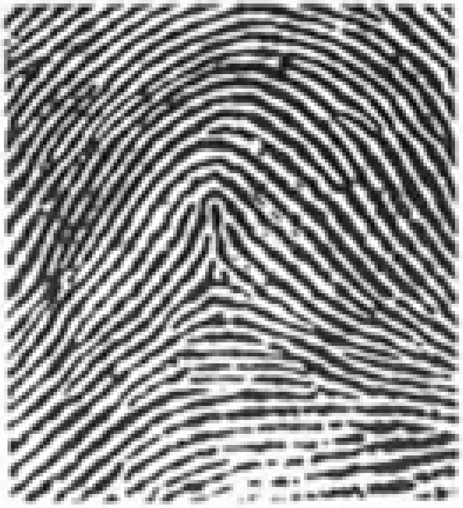
- Establishes Familial Relationship
- Commonly Used in Law Enforcement
- Highly Unique/ Impossible to Replicate

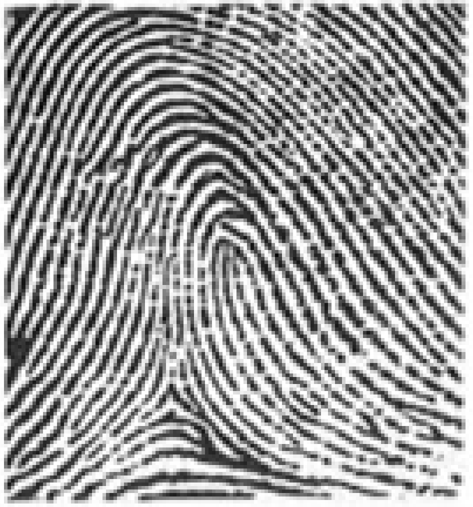
Linear Biometric *Finger Print Scanner*

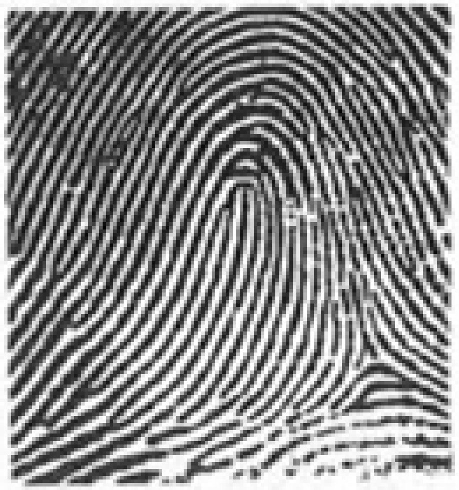


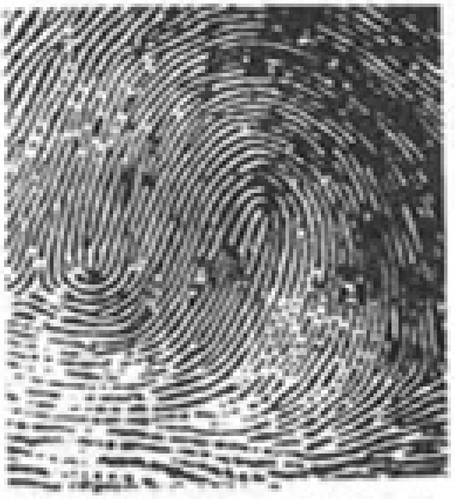
Characteristic *Fingerprint* Patterns

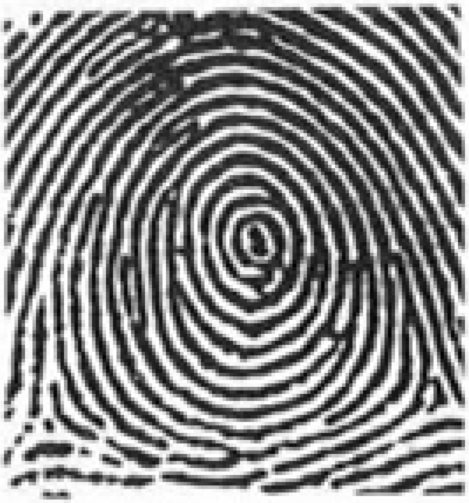

Plain Arch

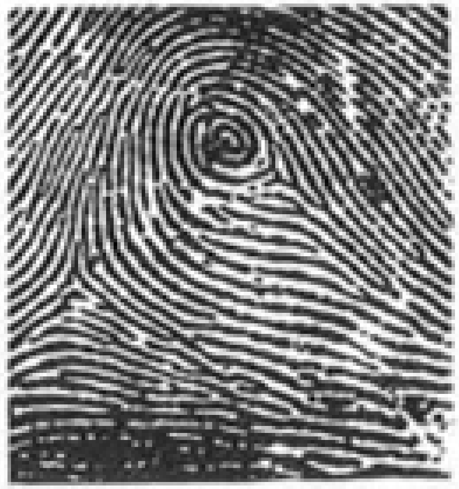

Tented Arch

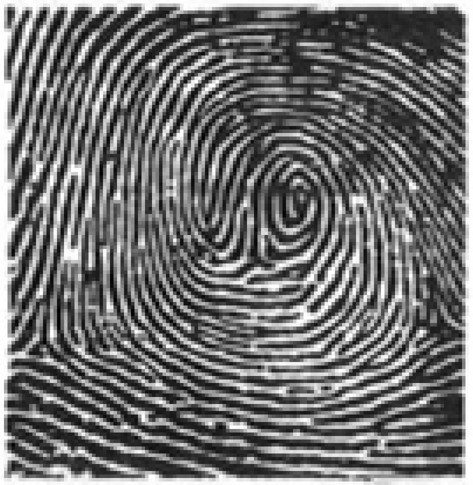

Ulnar Loop


Radial Loop


Double Loop Whorl

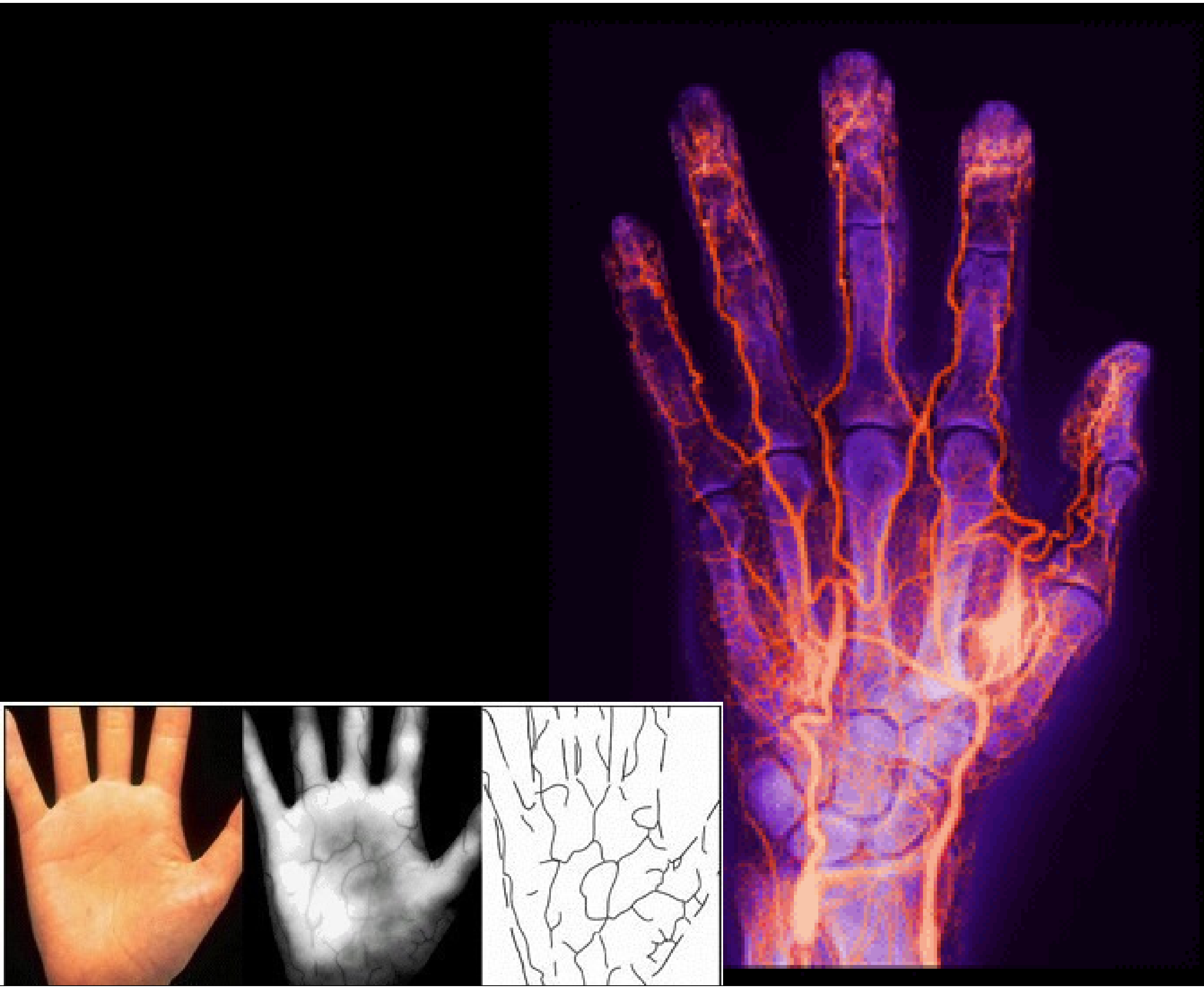

Plain Whorl


Central Pocket Loop Whorl

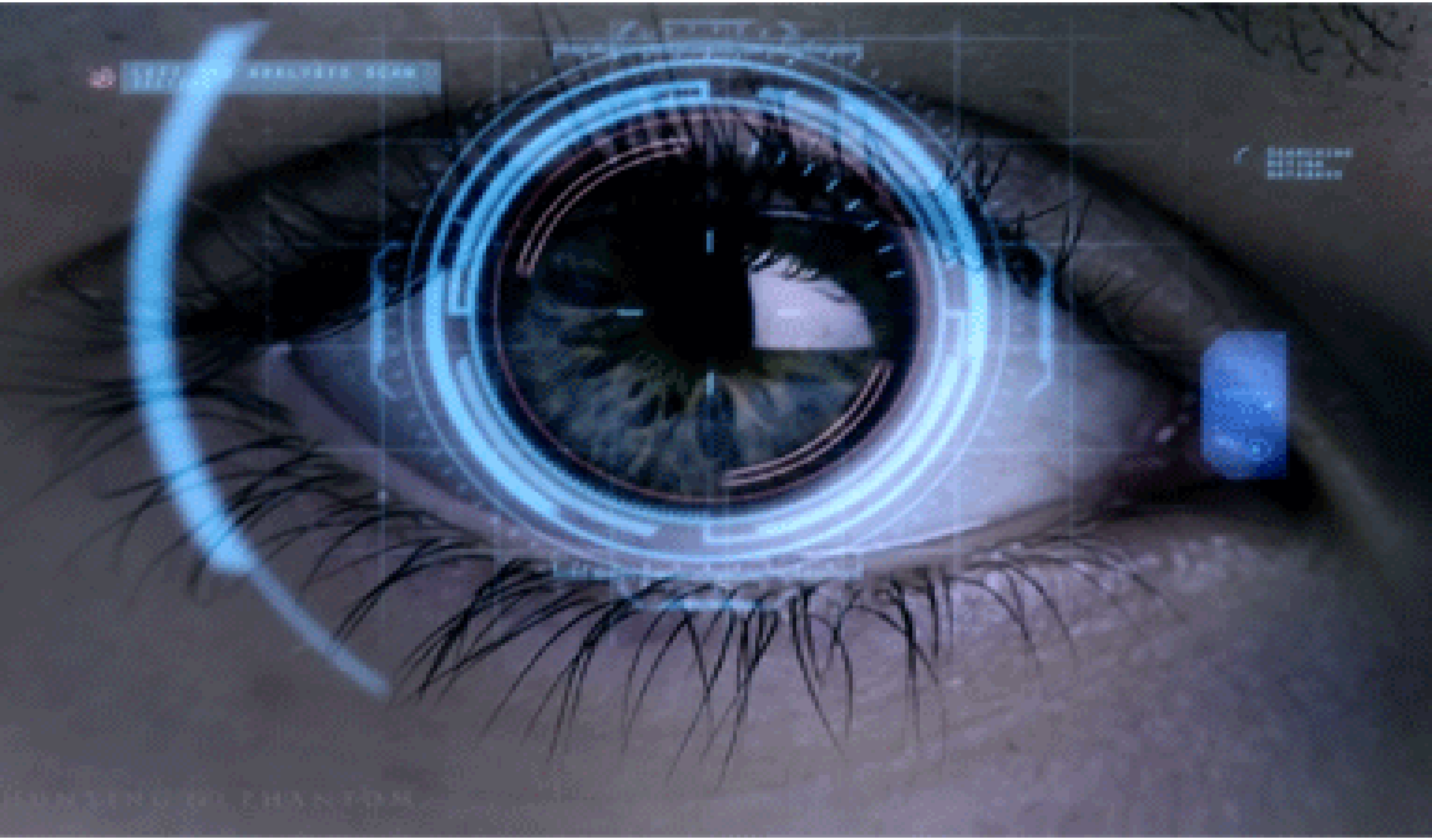

Accidental Whorl

Cyber-Biometrics: *Fingerprint Solutions*

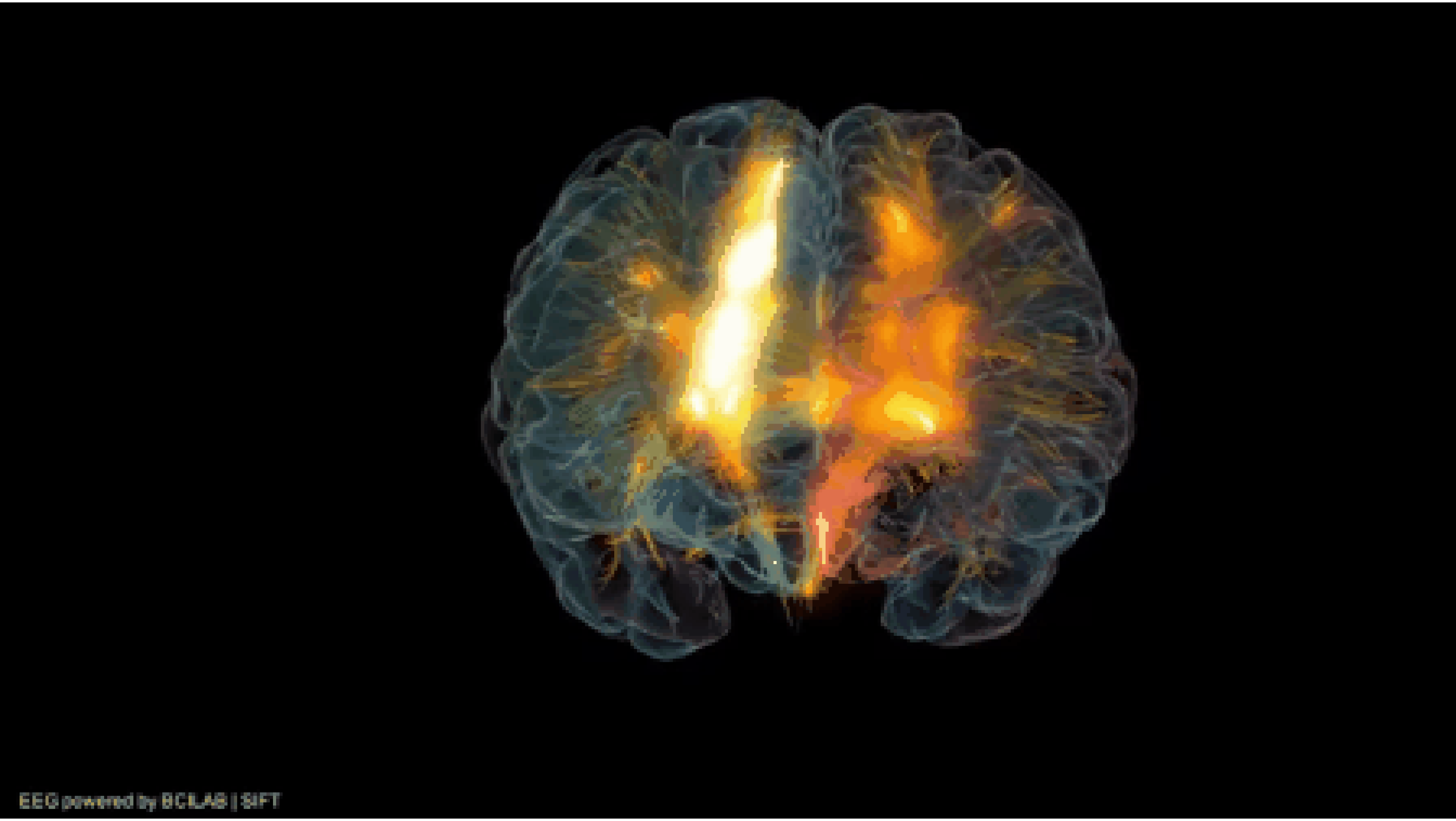
Cyber-Biometrics: *"Live" Vein Analytics*



Cyber-Biometrics: *Retinal & Iris Scans*



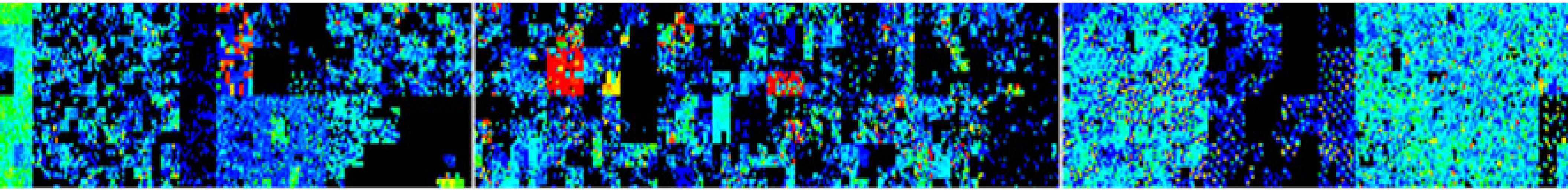
Real-Time Brain Scan: *Neural Networks*



EEG powered by BCILAB | SIFT

Energising *Cybersecurity* with "Biometrics & Forensics"

1 – Background: CyberCrime & Terrorism	2 – 21stC Profiling & Tracking: "Bad Guys"	3 – Real-Time Security & Surveillance
4 –Integrated Cyber Biometrics: Pre-Attack	**5 – Cyber Digital Forensics: Post Attack**	6 – The Enterprise Internet of Things (IoT)
7 –Biometric User Authentication for "IoT"	8 – Cyber-Bio Vision: Practical Solutions	9 – YOUR TOP 10 Actions & RoadMap

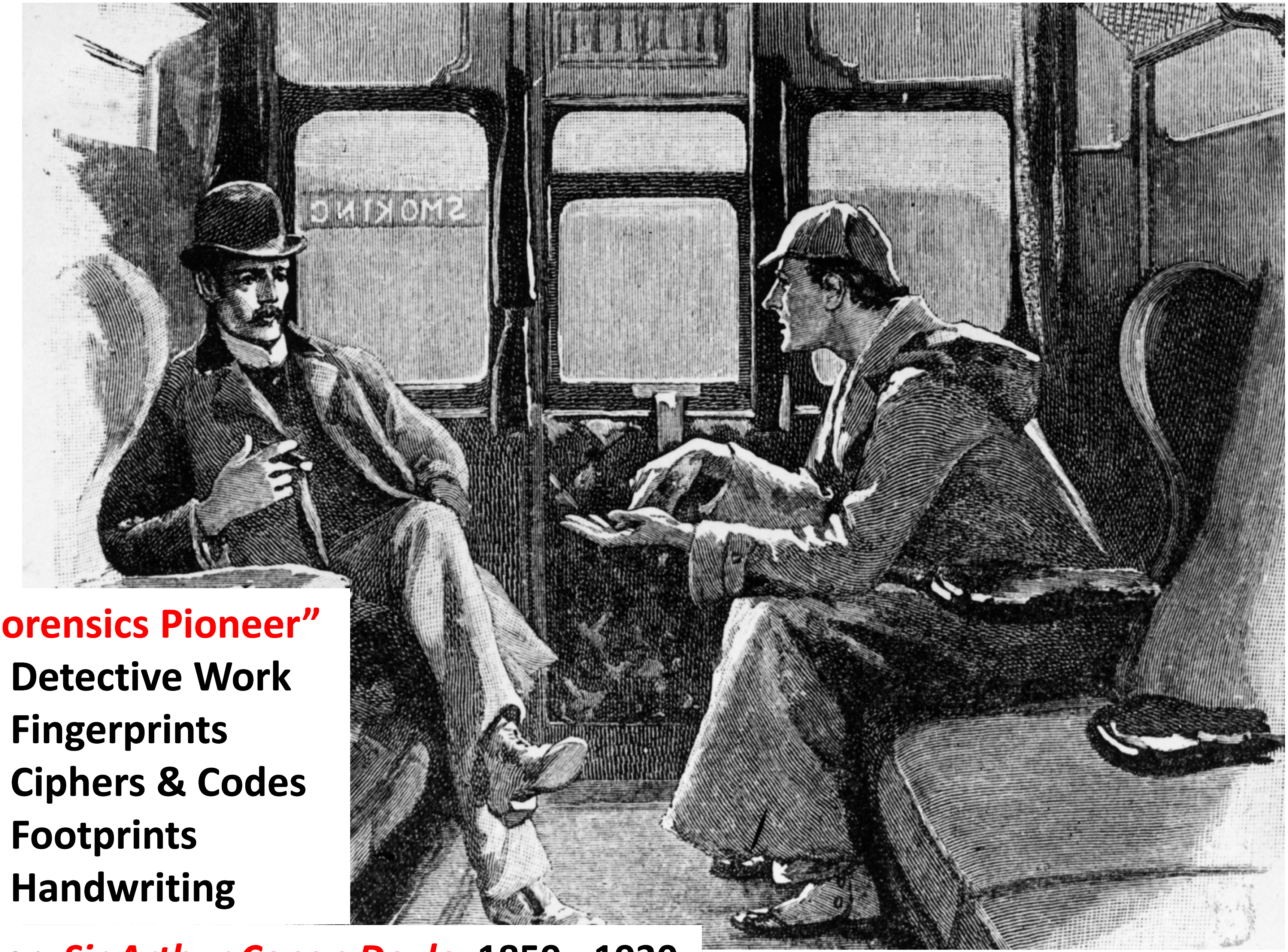


(5) *Cyber* **Digital Forensics:** ***Post-Attack***

- Evidence from Cyber Digital Forensics can help to identify the Criminals, Terrorists and Cyber Attackers:
- **Physical Forensics:**
  - Blood & Tissue Samples
  - DNA & Genetic Analysis
  - Chemical Agents, GSR, Fibres
- **Cyber Forensics:**
  - Cyber Attack IP Address/DNS/Proxies
  - Malware/Trojan/Virus Analysis
  - Botnet/DDOS , Targets & Payload
  - RansomWare/Encryption & Attack "Signatures"

...Evidence from BOTH ***Cyber & Physical Forensics*** will be relevant to 21stC Terror Threats & Attacks!...

Private Detective: *"Sherlock Holmes"!*

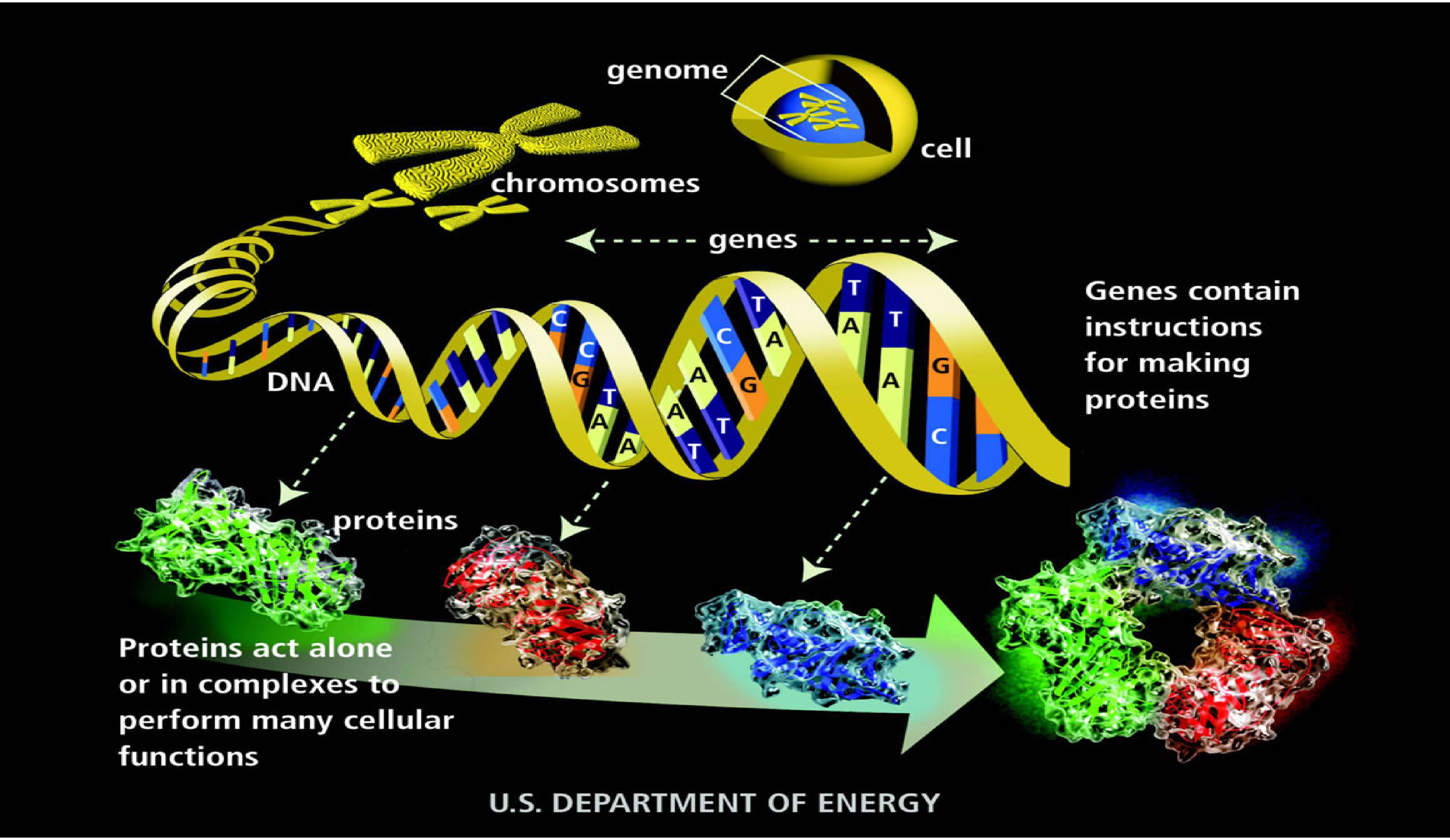


"Forensics Pioneer"

a) **Detective Work**
b) **Fingerprints**
c) **Ciphers & Codes**
d) **Footprints**
e) **Handwriting**

Author: *Sir Arthur Conan Doyle:* 1859 - 1930

Forensics: *Fast DNA Finger Printing*

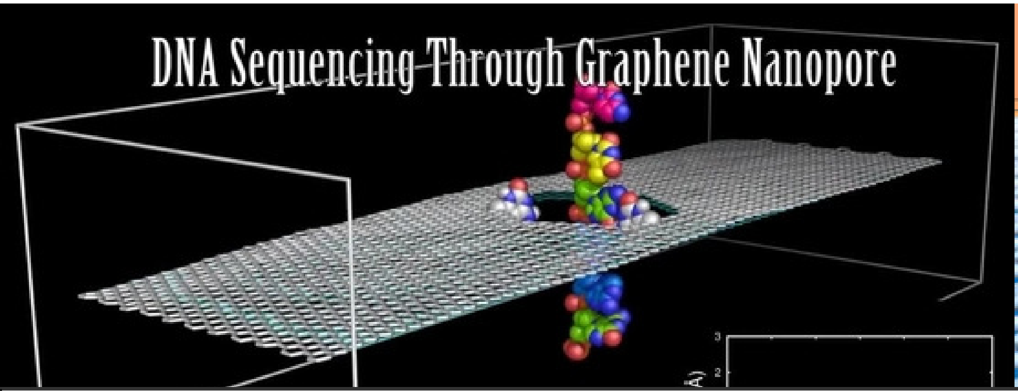


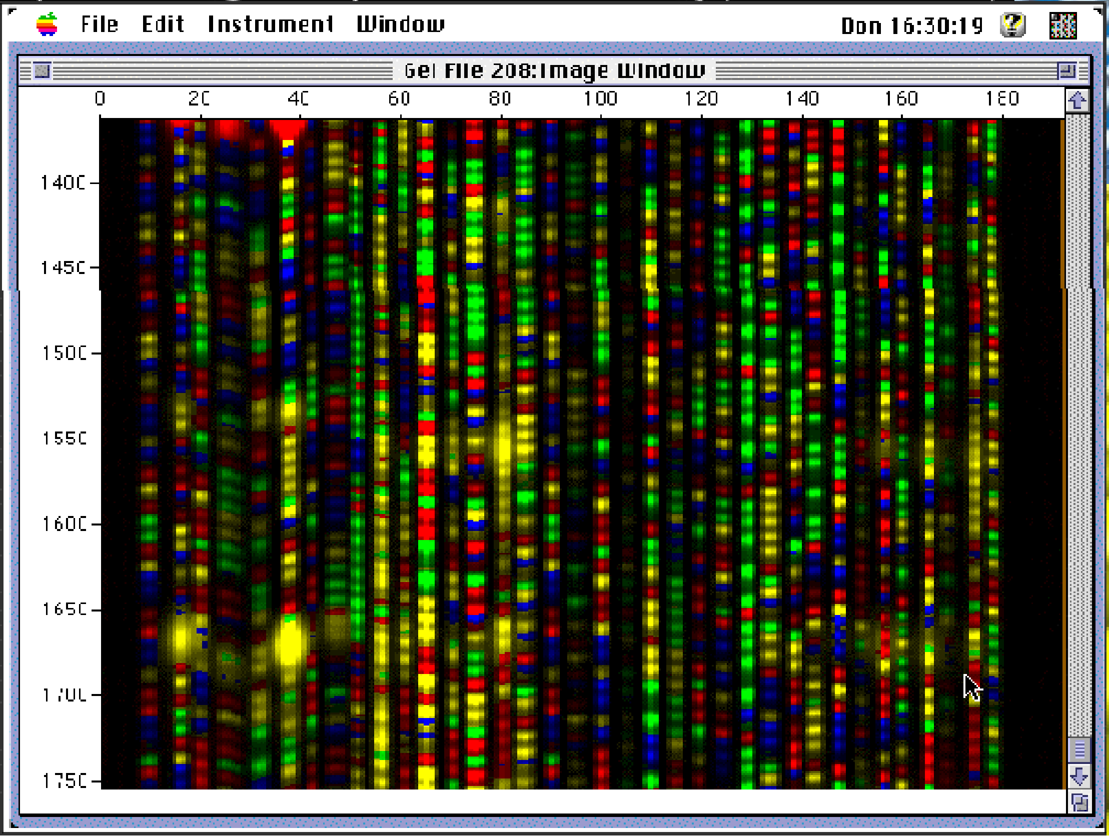
Genes contain instructions for making proteins

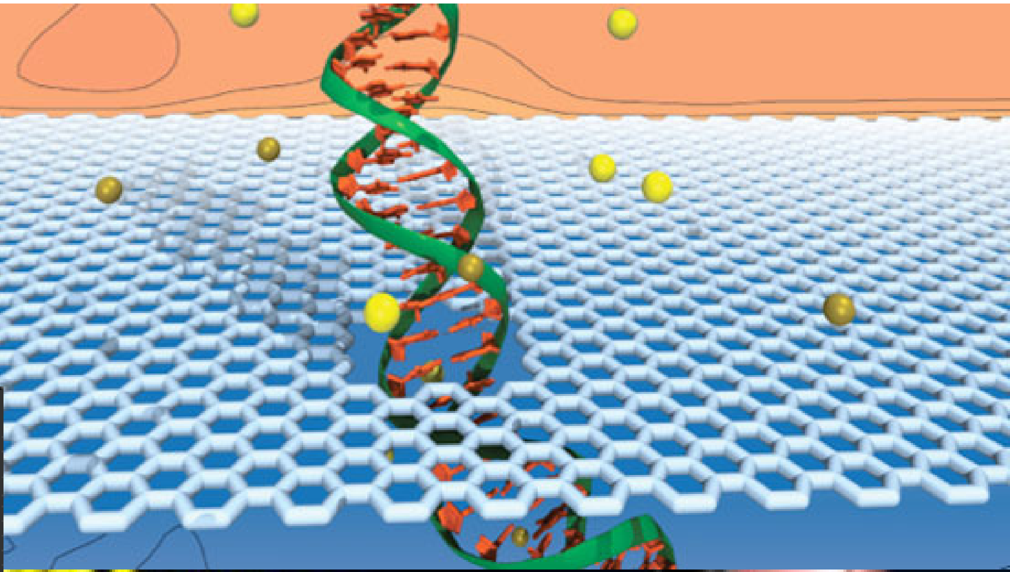
Proteins act alone or in complexes to perform many cellular functions

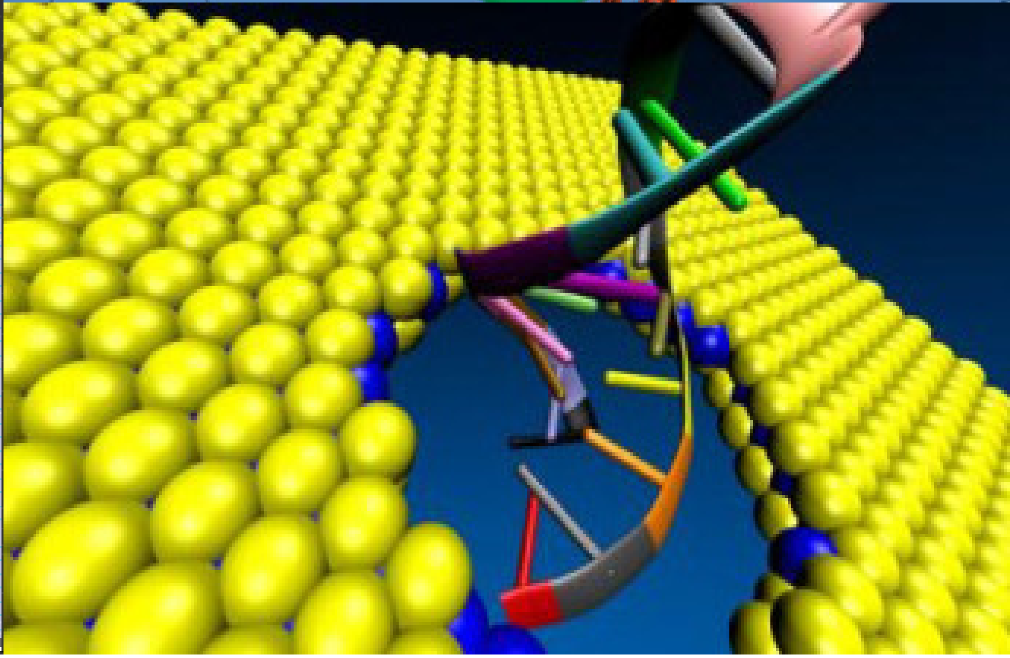
U.S. DEPARTMENT OF ENERGY

Fast DNA Sequencing:*Graphene Nanopore*

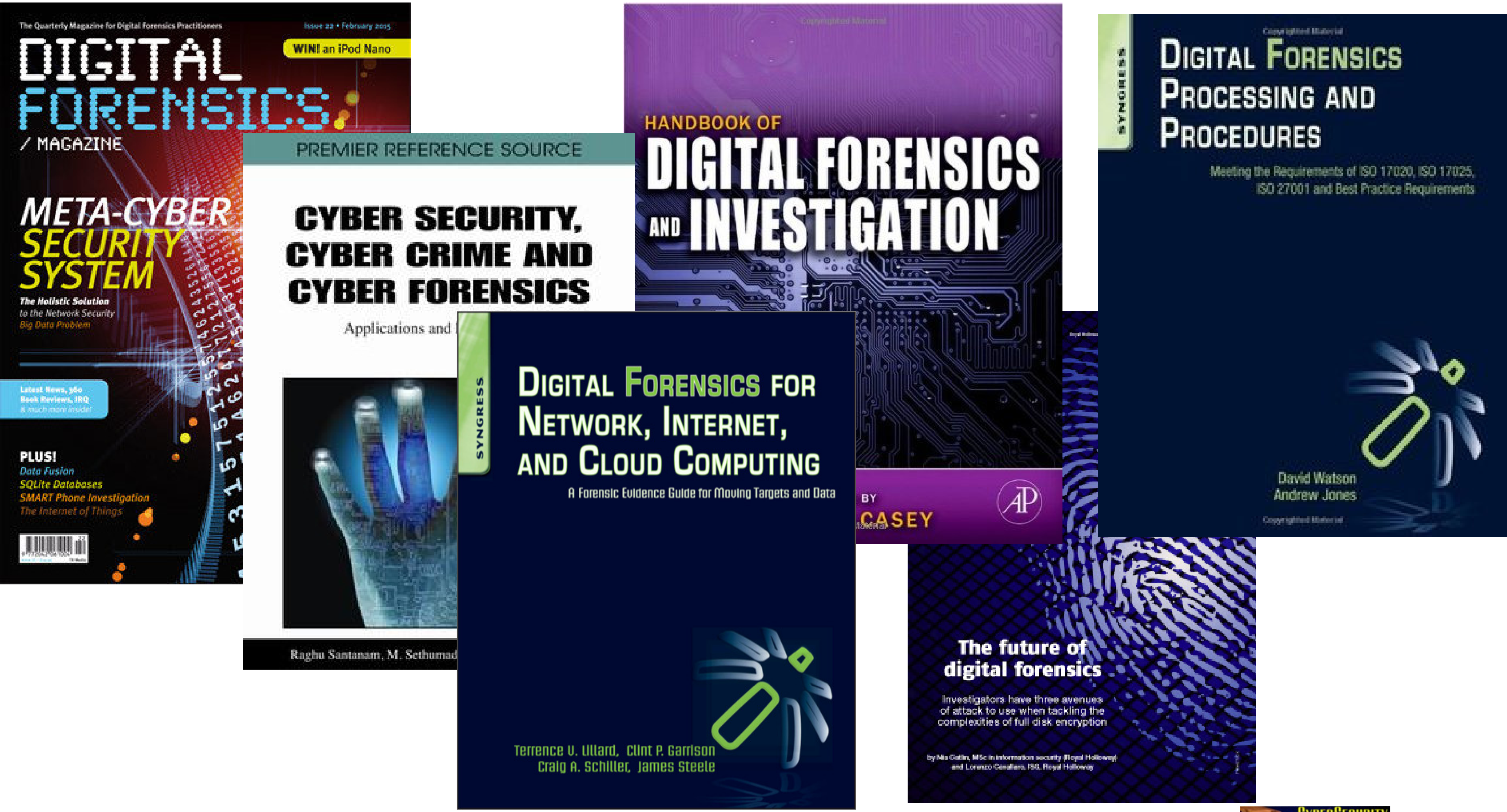




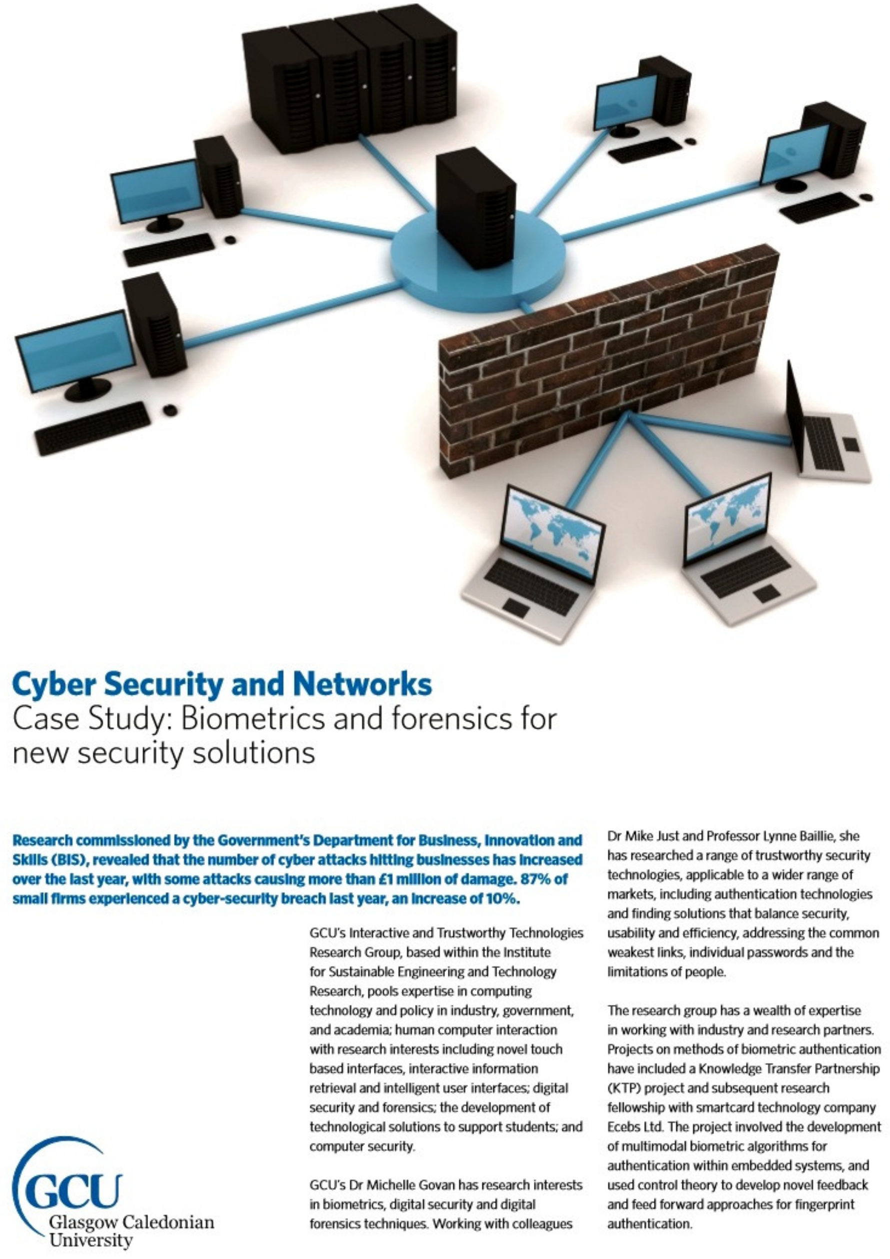




Digital Forensics: *Books & Journals*


The Quarterly Magazine for Digital Forensics Practitioners
Issue 22 • February 2015
WIN! an iPod Nano
DIGITAL FORENSICS / MAGAZINE
META-CYBER SECURITY SYSTEM
The Holistic Solution to the Network Security Big Data Problem
Latest News, 360 Book Reviews, IRQ & much more inside!
PLUS!
Data Fusion
SQLite Databases
SMART Phone Investigation
The Internet of Things
PREMIER REFERENCE SOURCE
CYBER SECURITY, CYBER CRIME AND CYBER FORENSICS
Applications and
Raghu Santanam, M. Sethumad
HANDBOOK OF DIGITAL FORENSICS AND INVESTIGATION
BY
CASEY
AP
SYNGRESS
DIGITAL FORENSICS PROCESSING AND PROCEDURES
Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements
David Watson
Andrew Jones
SYNGRESS
DIGITAL FORENSICS FOR NETWORK, INTERNET, AND CLOUD COMPUTING
A Forensic Evidence Guide for Moving Targets and Data
Terrence V. Lillard, Clint P. Garrison
Craig A. Schiller, James Steele
The future of digital forensics
Investigators have three avenues of attack to use when tackling the complexities of full disk encryption

Biometrics & Forensics: Glasgow University



Cyber Security and Networks

Case Study: Biometrics and forensics for new security solutions

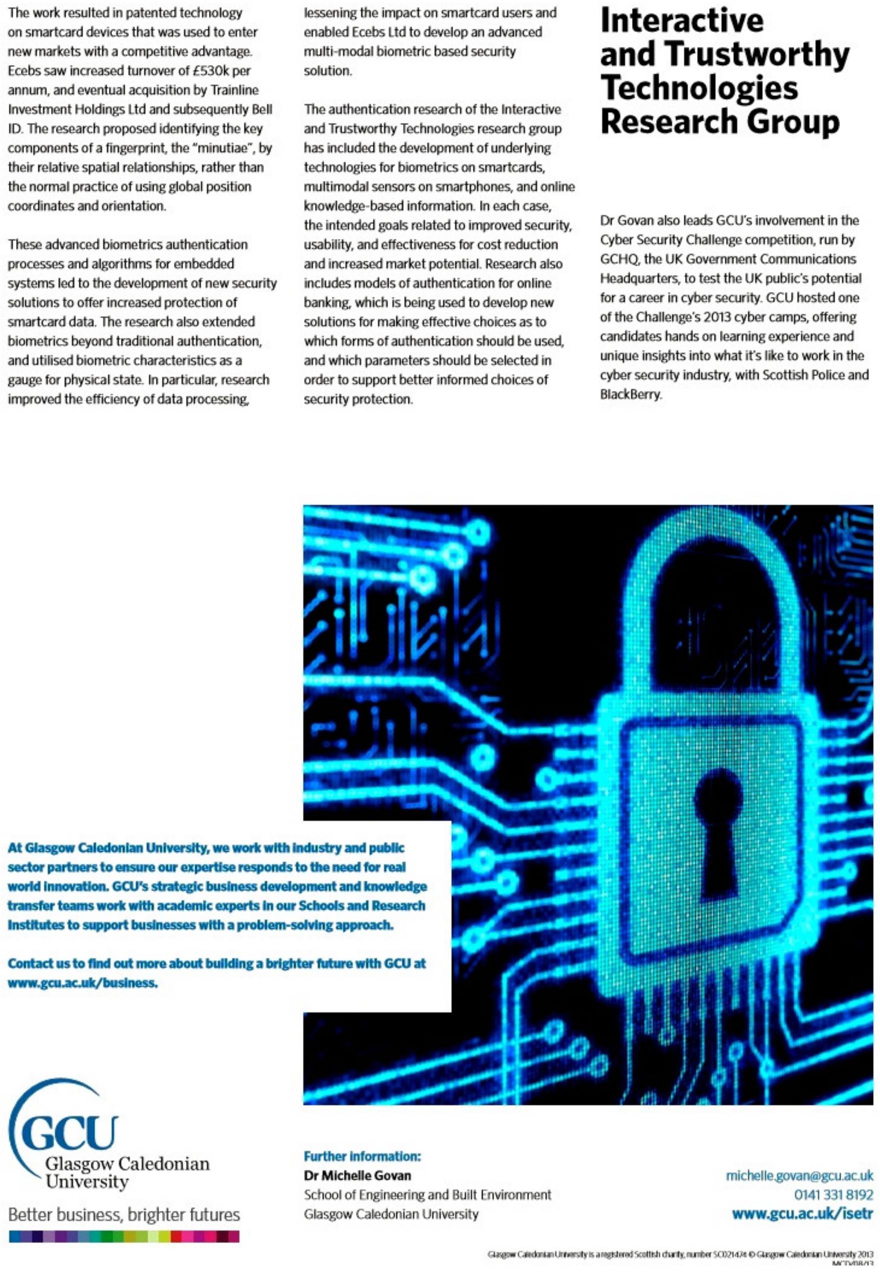
Research commissioned by the Government's Department for Business, Innovation and Skills (BIS), revealed that the number of cyber attacks hitting businesses has increased over the last year, with some attacks causing more than £1 million of damage. 87% of small firms experienced a cyber-security breach last year, an increase of 10%.

GCU's Interactive and Trustworthy Technologies Research Group, based within the Institute for Sustainable Engineering and Technology Research, pools expertise in computing technology and policy in industry, government, and academia; human computer interaction with research interests including novel touch based interfaces, interactive information retrieval and intelligent user interfaces; digital security and forensics; the development of technological solutions to support students; and computer security.

GCU's Dr Michelle Govan has research interests in biometrics, digital security and digital forensics techniques. Working with colleagues Dr Mike Just and Professor Lynne Baillie, she has researched a range of trustworthy security technologies, applicable to a wider range of markets, including authentication technologies and finding solutions that balance security, usability and efficiency, addressing the common weakest links, individual passwords and the limitations of people.

The research group has a wealth of expertise in working with industry and research partners. Projects on methods of biometric authentication have included a Knowledge Transfer Partnership (KTP) project and subsequent research fellowship with smartcard technology company Ecebs Ltd. The project involved the development of multimodal biometric algorithms for authentication within embedded systems, and used control theory to develop novel feedback and feed forward approaches for fingerprint authentication.

GCU
Glasgow Caledonian
University



The work resulted in patented technology on smartcard devices that was used to enter new markets with a competitive advantage. Ecebs saw increased turnover of £530k per annum, and eventual acquisition by Trainline Investment Holdings Ltd and subsequently Bell ID. The research proposed identifying the key components of a fingerprint, the "minutiae", by their relative spatial relationships, rather than the normal practice of using global position coordinates and orientation.

These advanced biometrics authentication processes and algorithms for embedded systems led to the development of new security solutions to offer increased protection of smartcard data. The research also extended biometrics beyond traditional authentication, and utilised biometric characteristics as a gauge for physical state. In particular, research improved the efficiency of data processing, lessening the impact on smartcard users and enabled Ecebs Ltd to develop an advanced multi-modal biometric based security solution.

The authentication research of the Interactive and Trustworthy Technologies research group has included the development of underlying technologies for biometrics on smartcards, multimodal sensors on smartphones, and online knowledge-based information. In each case, the intended goals related to improved security, usability, and effectiveness for cost reduction and increased market potential. Research also includes models of authentication for online banking, which is being used to develop new solutions for making effective choices as to which forms of authentication should be used, and which parameters should be selected in order to support better informed choices of security protection.

Interactive and Trustworthy Technologies Research Group

Dr Govan also leads GCU's involvement in the Cyber Security Challenge competition, run by GCHQ, the UK Government Communications Headquarters, to test the UK public's potential for a career in cyber security. GCU hosted one of the Challenge's 2013 cyber camps, offering candidates hands on learning experience and unique insights into what it's like to work in the cyber security industry, with Scottish Police and BlackBerry.

At Glasgow Caledonian University, we work with industry and public sector partners to ensure our expertise responds to the need for real world innovation. GCU's strategic business development and knowledge transfer teams work with academic experts in our Schools and Research Institutes to support businesses with a problem-solving approach.

Contact us to find out more about building a brighter future with GCU at www.gcu.ac.uk/business.

GCU
Glasgow Caledonian
University

Better business, brighter futures

Further information:
Dr Michelle Govan
School of Engineering and Built Environment
Glasgow Caledonian University

michelle.govan@gcu.ac.uk
0141 331 8192
www.gcu.ac.uk/isetr

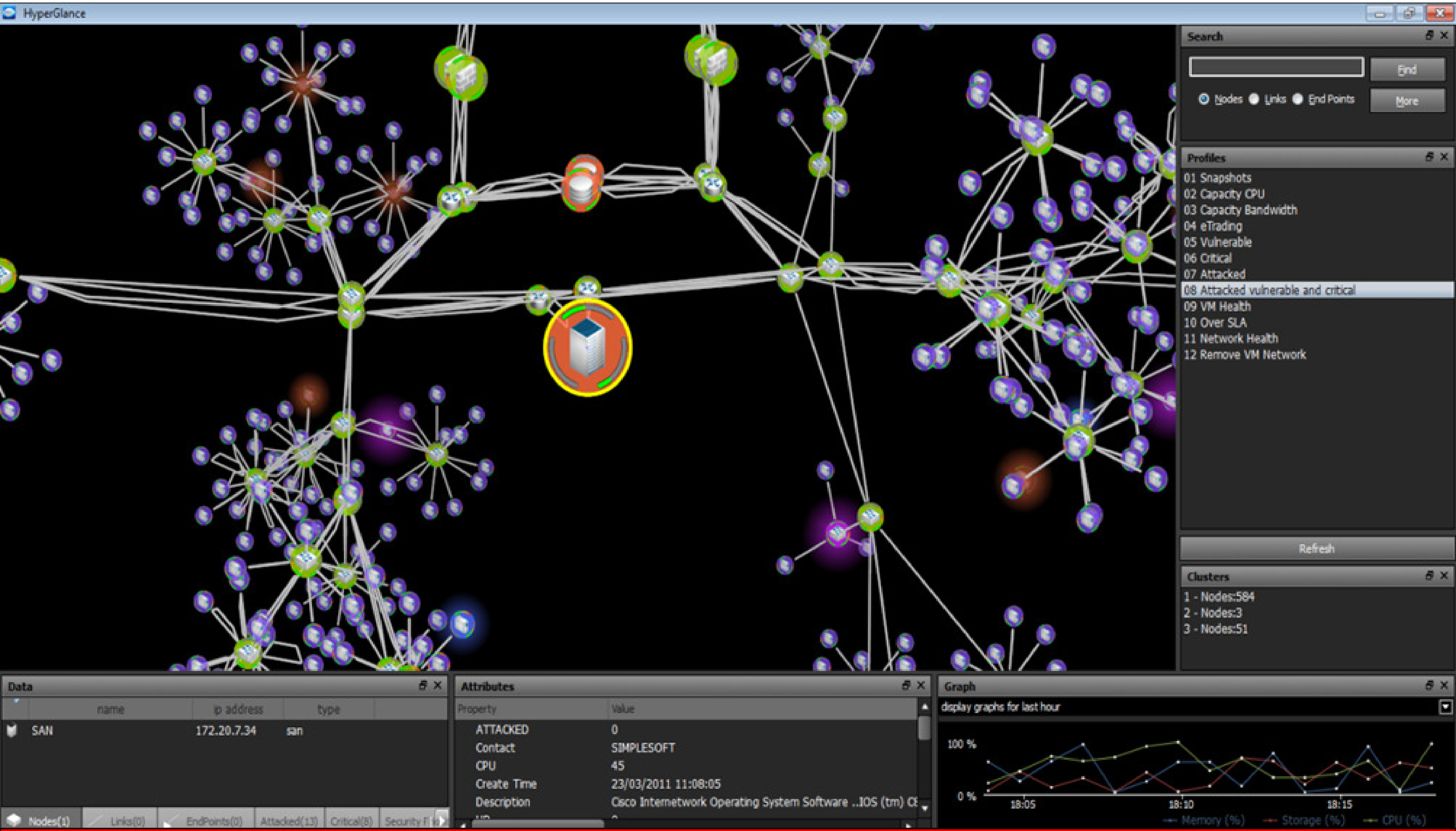
Glasgow Caledonian University is a registered Scottish charity, number SC021474 © Glasgow Caledonian University 2013
MCTV08/13

- UN/ITU *CyberSecurity* Agenda -

Quest for CyberConfidence (Eng/Rus)

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

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

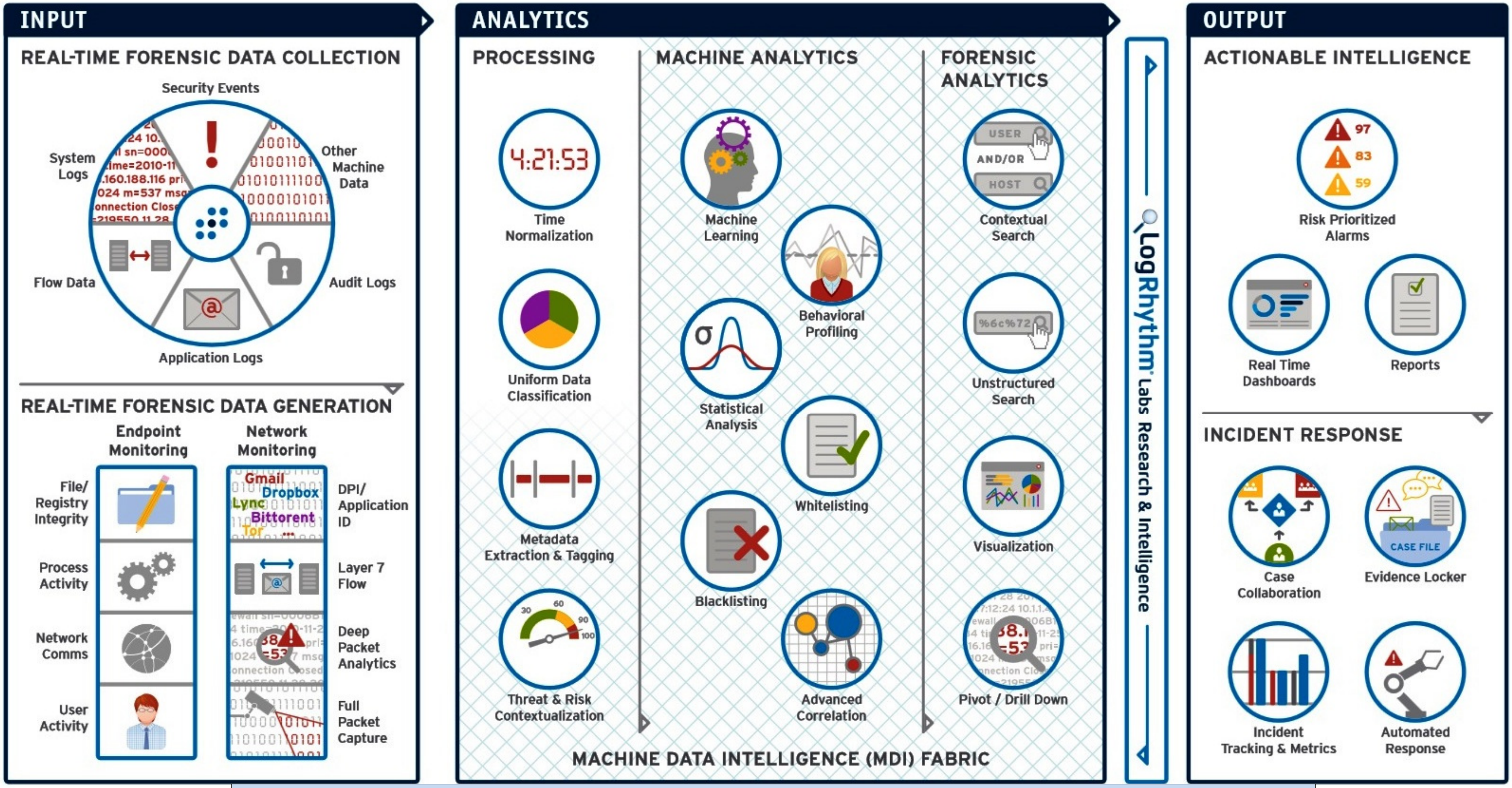
name	ip address	type
SAN	172.20.7.34	san

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[illegible]

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

LogRhythm: *Machine Learning Forensics*



INPUT

REAL-TIME FORENSIC DATA COLLECTION

Security Events

System Logs

Other Machine Data

Flow Data

Audit Logs

Application Logs

REAL-TIME FORENSIC DATA GENERATION

Endpoint Monitoring

Network Monitoring

File/ Registry Integrity

Process Activity

Network Comms

User Activity

DPI/ Application ID

Layer 7 Flow

Deep Packet Analytics

Full Packet Capture

ANALYTICS

PROCESSING

Time Normalization

Uniform Data Classification

Metadata Extraction & Tagging

Threat & Risk Contextualization

MACHINE ANALYTICS

Machine Learning

Behavioral Profiling

Statistical Analysis

Whitelisting

Blacklisting

Advanced Correlation

FORENSIC ANALYTICS

Contextual Search

Unstructured Search

Visualization

Pivot / Drill Down

MACHINE DATA INTELLIGENCE (MDI) FABRIC

LogRhythm Labs Research & Intelligence

OUTPUT

ACTIONABLE INTELLIGENCE

Risk Prioritized Alarms

Real Time Dashboards

Reports

INCIDENT RESPONSE

Case Collaboration

Evidence Locker

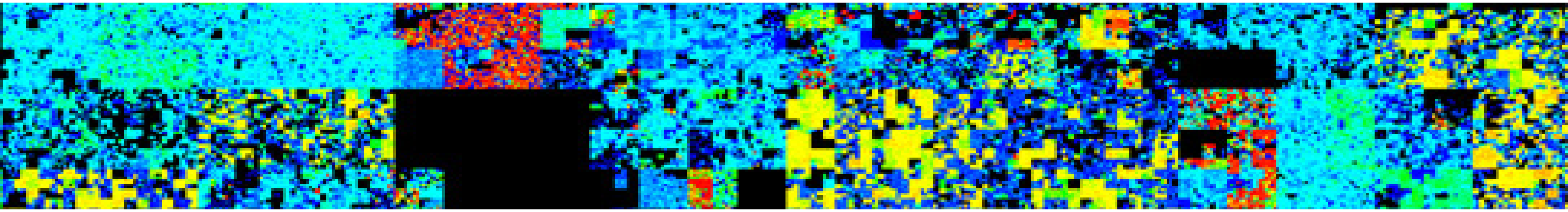
Incident Tracking & Metrics

Automated Response

LogRhythm's *Security Intelligence Platform*

Energising *Cybersecurity* with "Biometrics & Forensics"

1 – Background: CyberCrime & Terrorism	2 – 21stC Profiling & Tracking: "Bad Guys"	3 – Real-Time Security & Surveillance
4 –Integrated Cyber Biometrics: Pre-Attack	5 – Cyber Digital Forensics : Post-Attack	**6 – Cyber-Bio: Security Sector Scenarios**
7 – Biometric User Authentication for "IoT"	8 – Cyber-Bio Vision: Practical Solutions	9 – YOUR TOP 10 Actions & RoadMap

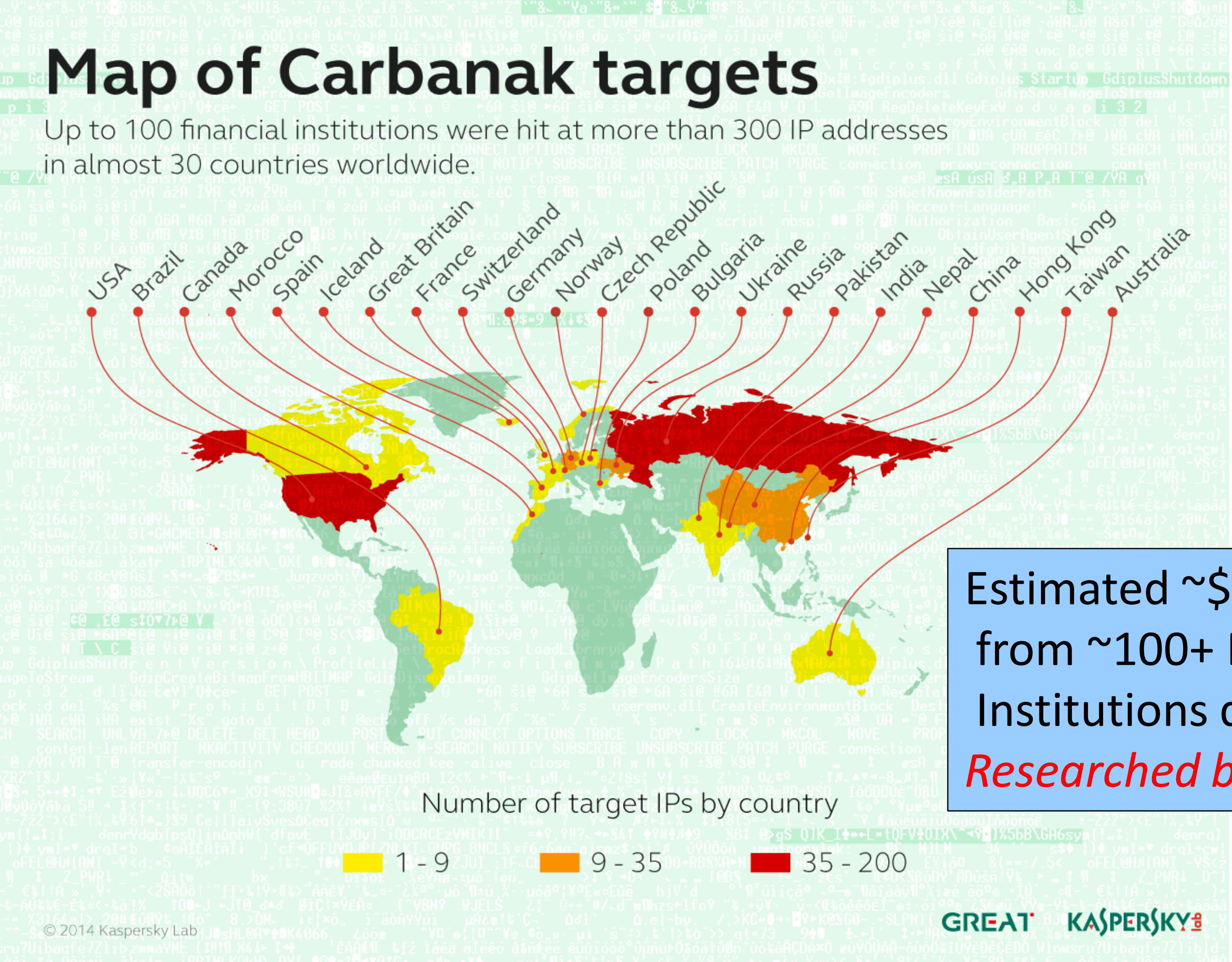


(6) Cyber-Bio: *Security Threat Scenarios*

- Banks/Finance: Fraud, DDOS, Insider Threats
- Government/Parliament: “Fake IDs” & File Theft
- Defence/Military: Cyber-Espionage & Attacks
- Travel/Tourism: Beach Resorts & Travel Hubs
- Culture/Sports: Major Events & Competitions
- Energy/Utilities: Nuclear Theft, Explosions
- Retail/Malls/Campus: Armed Attacks & Siege
- Healthcare/Pharma: “Fake Drugs & Records”

...ALL Generic *Cyber-Bio Threats* apply to ALL Business Sectors & Critical Infrastructure!

Cyber "Banking Theft"– Carbanak



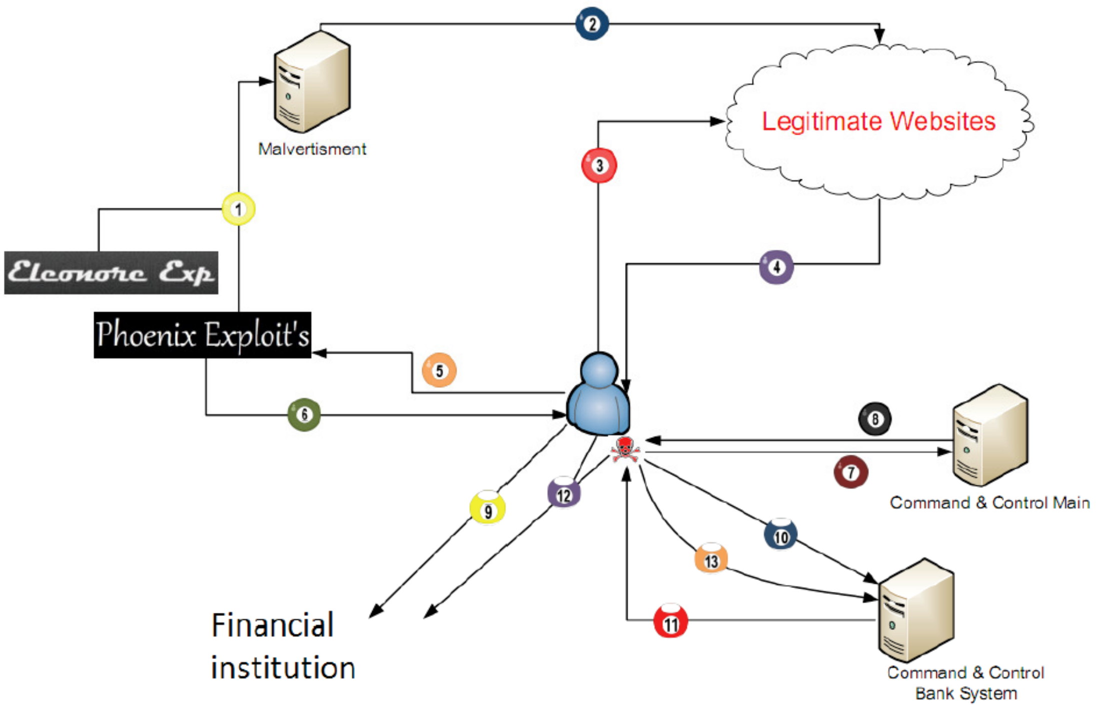
Map of Carbanak targets

Up to 100 financial institutions were hit at more than 300 IP addresses in almost 30 countries worldwide.

Estimated ~$1Billion stolen from ~100+ Banks & Financial Institutions during 2013/2014

Researched by "Kaspersky Labs"

Process Flow of CyberCriminal Attack on Major UK *Financial Institution*: 2010



1. Uploads malicious advertisements to legitimate and fraud advertisements servers
2. The malicious advertisements published among the legitimate websites
3. User accesses to an infected website
4. The website content contains redirection to the malicious Exploit Kit
5. The user is redirected to the malicious Exploit Kit
6. The user's PC exploited, the payload was downloaded successfully
7. The Trojan reports for a new bot to the C&C
8. The C&C sends instruction to the Trojan
9. User access to financial institution
10. The Trojan reports for the user activities
11. The C&C sends commands to the Trojan to manipulate user bank transactions
12. Trojan manipulates User's bank transaction
13. Trojan reports the C&C about successful/failed transaction

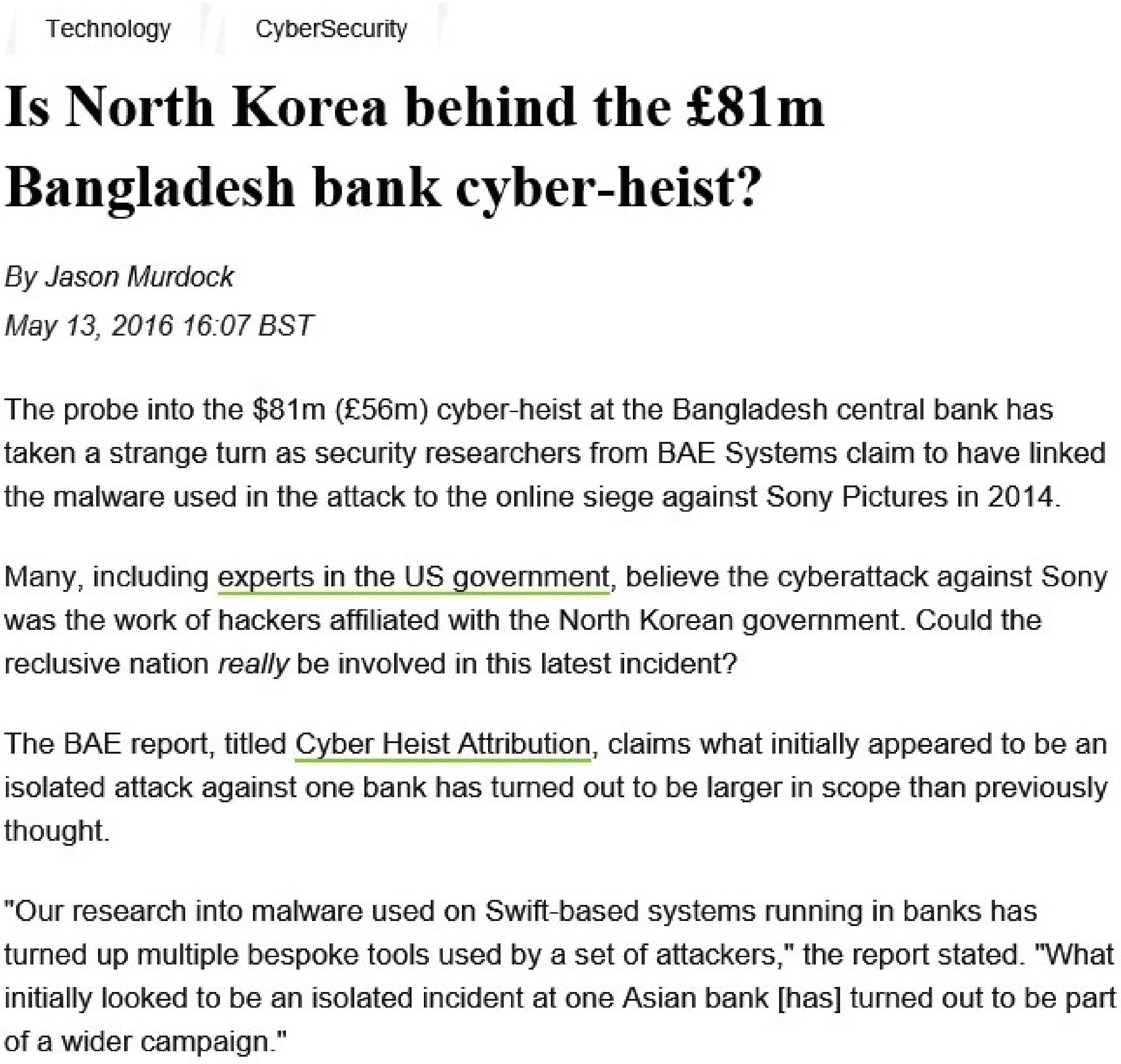
Source: White Paper by M86 Security: Aug 2010

M86 SECURITY

Such Cyber Attacks, with variations, take place regularly in *Banking & Financial Services*. *During Summer 2014 more than 83Million Accounts were "hacked" @ JP Morgan Chase-*

- It is estimated that more than $450Bllion/Year is lost through CyberCrime -

May 2016 : $81m Bank Cyber-Heist



Technology CyberSecurity

Is North Korea behind the £81m Bangladesh bank cyber-heist?

By Jason Murdock

May 13, 2016 16:07 BST

The probe into the $81m (£56m) cyber-heist at the Bangladesh central bank has taken a strange turn as security researchers from BAE Systems claim to have linked the malware used in the attack to the online siege against Sony Pictures in 2014.

Many, including experts in the US government, believe the cyberattack against Sony was the work of hackers affiliated with the North Korean government. Could the reclusive nation *really* be involved in this latest incident?

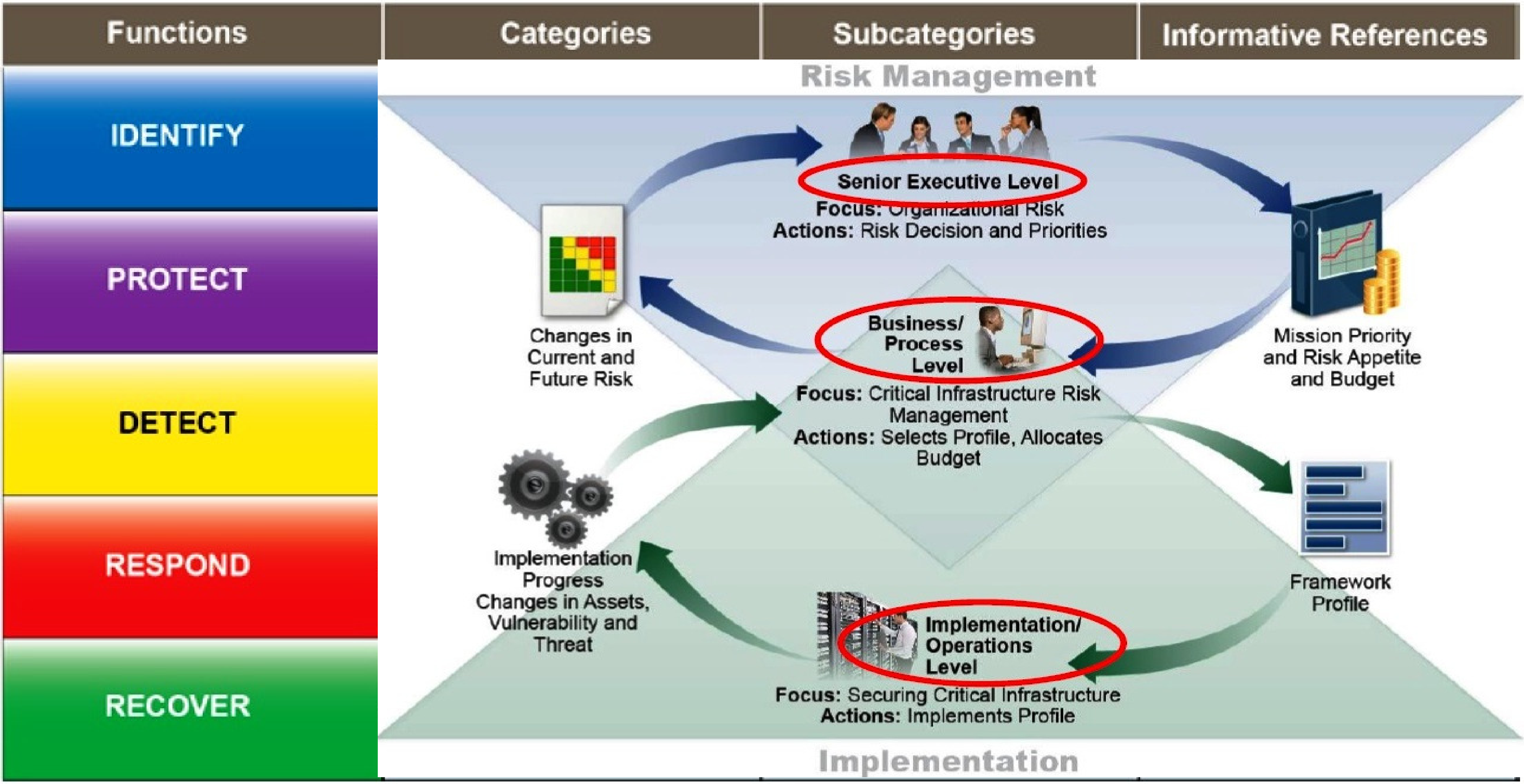
The BAE report, titled Cyber Heist Attribution, claims what initially appeared to be an isolated attack against one bank has turned out to be larger in scope than previously thought.

"Our research into malware used on Swift-based systems running in banks has turned up multiple bespoke tools used by a set of attackers," the report stated. "What initially looked to be an isolated incident at one Asian bank [has] turned out to be part of a wider campaign."

International Business Times
- 13th May 2016 -

NIST *Cybersecurity* Framework

National Institute of Standards & Technology



Functions | Categories | Subcategories | Informative References

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Risk Management

Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget

Implementation Progress Changes in Assets, Vulnerability and Threat

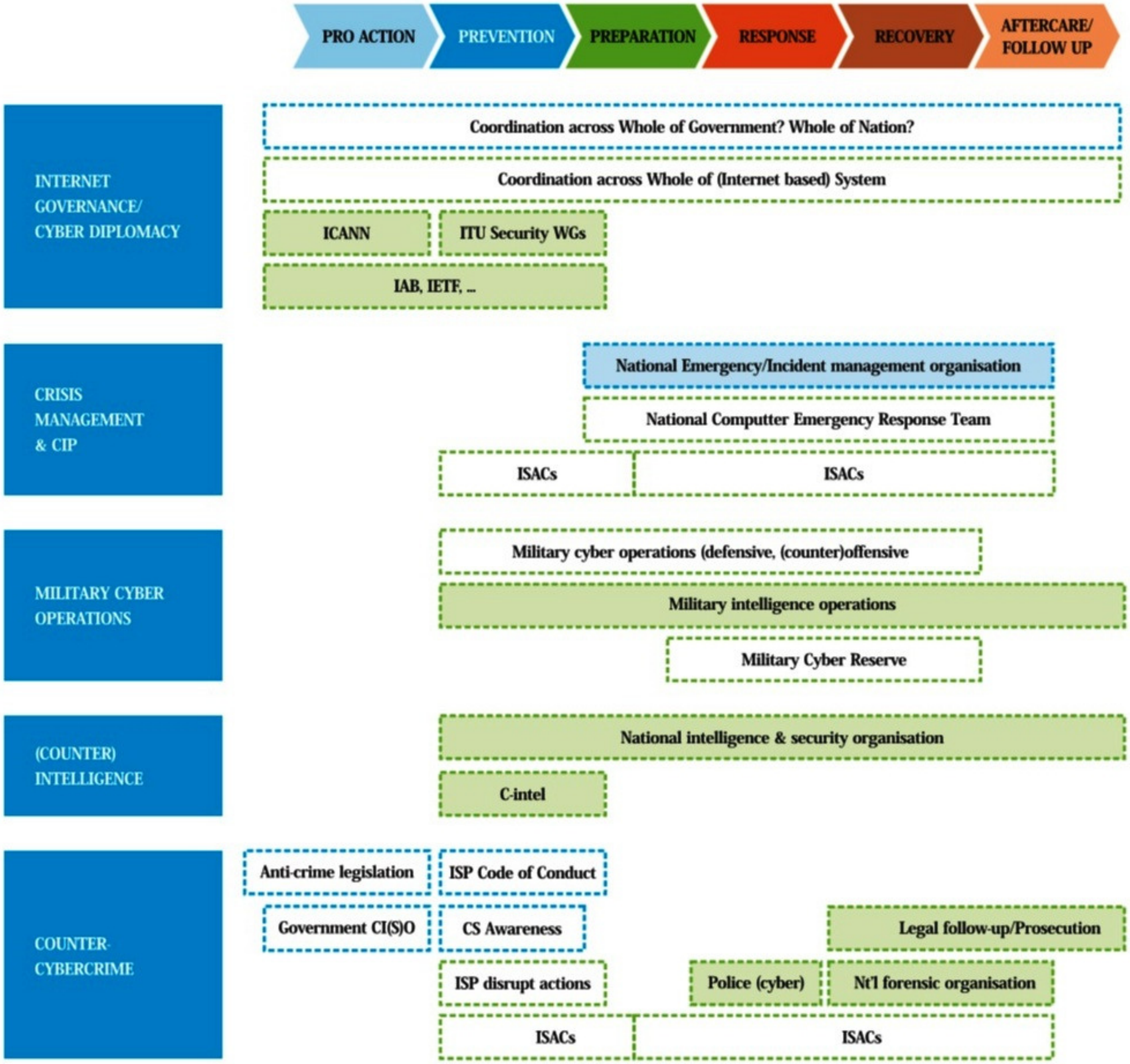
Framework Profile

Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

Web: www.nist.gov/cyberframework/

NATO *Cybersecurity* Framework Manual



PRO ACTION | PREVENTION | PREPARATION | RESPONSE | RECOVERY | AFTERCARE/ FOLLOW UP

INTERNET GOVERNANCE/ CYBER DIPLOMACY

Coordination across Whole of Government? Whole of Nation?

Coordination across Whole of (Internet based) System

ICANN

ITU Security WGs

IAB, IETF, ...

CRISIS MANAGEMENT & CIP

National Emergency/Incident management organisation

National Computter Emergency Response Team

ISACs

ISACs

MILITARY CYBER OPERATIONS

Military cyber operations (defensive, (counter)offensive

Military intelligence operations

Military Cyber Reserve

(COUNTER) INTELLIGENCE

National intelligence & security organisation

C-intel

COUNTER-CYBERCRIME

Anti-crime legislation

ISP Code of Conduct

Government CI(S)O

CS Awareness

Legal follow-up/Prosecution

ISP disrupt actions

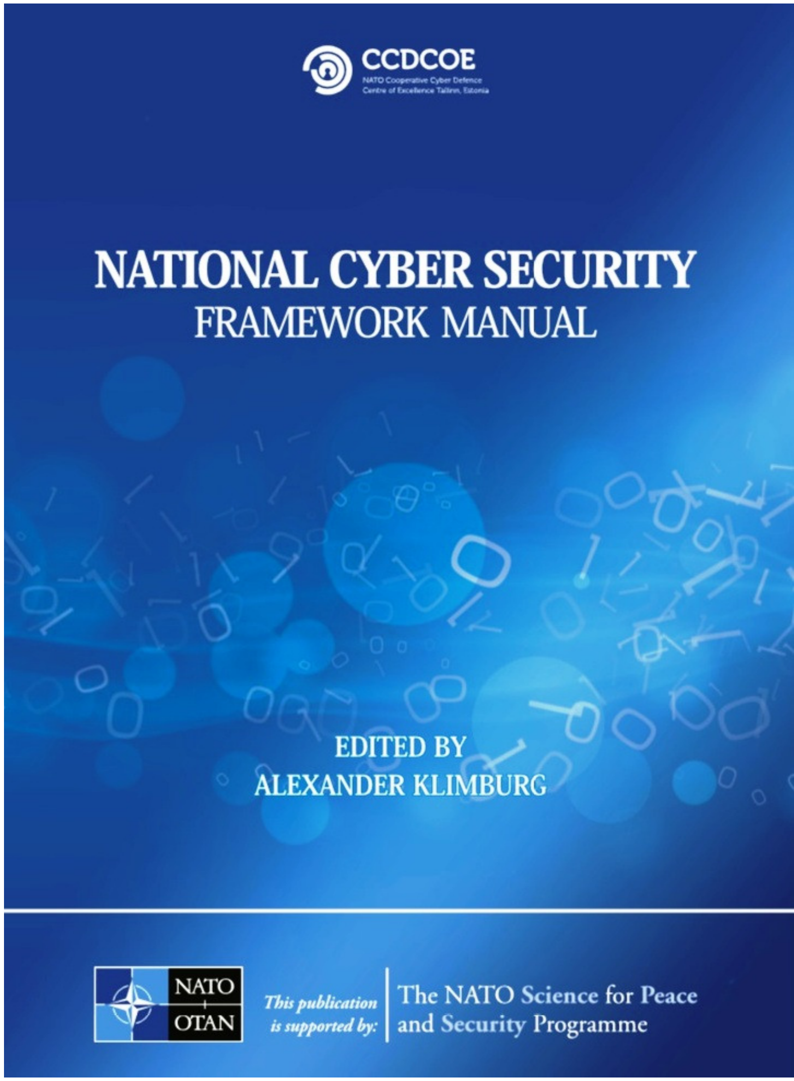
Police (cyber)

Nt'l forensic organisation

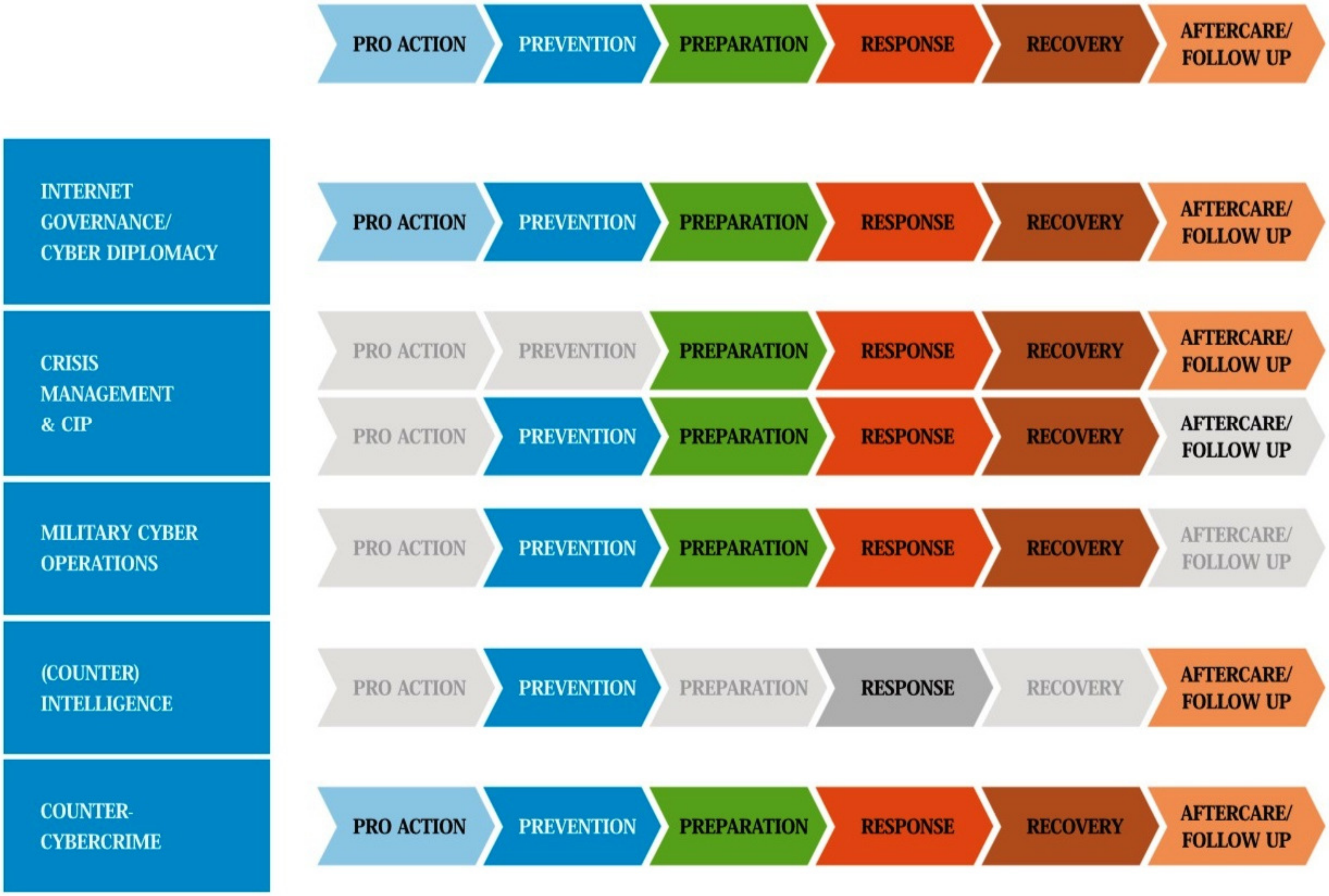
ISACs

ISACs

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


CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
NATIONAL CYBER SECURITY
FRAMEWORK MANUAL
EDITED BY
ALEXANDER KLIMBURG
NATO OTAN
This publication is supported by:
The NATO Science for Peace and Security Programme

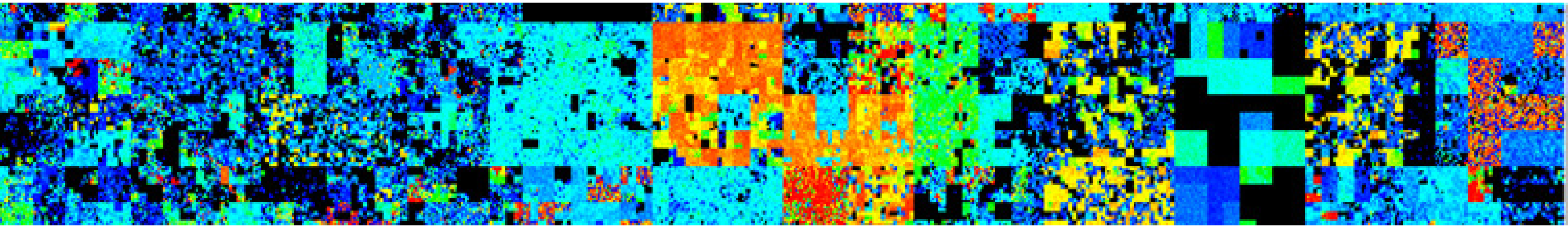
NATO *Cyber* Framework: *The Five Mandates and Six Elements of the Cybersecurity Cycle*



	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
INTERNET GOVERNANCE/ CYBER DIPLOMACY	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
CRISIS MANAGEMENT & CIP	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
MILITARY CYBER OPERATIONS	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
(COUNTER) INTELLIGENCE	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP
COUNTER-CYBERCRIME	PRO ACTION	PREVENTION	PREPARATION	RESPONSE	RECOVERY	AFTERCARE/ FOLLOW UP

Energising *Cybersecurity* with "Biometrics & Forensics"

1 – Background: CyberCrime & Terrorism	2 – 21stC Profiling & Tracking: "Bad Guys"	3 – Real-Time Security & Surveillance
4 –Integrated Cyber Biometrics: Pre-Attack	5 – Cyber Digital Forensics : Post-Attack	6 – Cyber-Bio: Security Sector Scenarios
7 – Biometric User Authentication for "IoT"	8 – Cyber-Bio Vision: Practical Solutions	9 – YOUR TOP 10 Actions & RoadMap



(7) Biometric ID Authentication: “IoT”

- Biometric Security provides Crucial Cyber-Defence for the **“Internet of Things” – “IoT”:**
  - Bio-ID & Authentication for ALL Secure “IoT” Devices
  - Real-Time Bio Profiling & Behavioural Modelling
  - Rapid Intrusion Alerts for “IoT” Networks & Assets
  - Bio ID Access for Secure Cloud Data & Apps
  - Mobile “IoT” Asset Tracking with Bio ID Security

...ALL Secure “IoT” Devices should be Biometric Protected to *Mitigate ID Theft and Fraud!...*

2015-2025: Migration from IPv4 to IPv6

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

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

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

Cyber-Physical Threats from the “IoT”

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

Internet of Things: *Phases of Evolution*

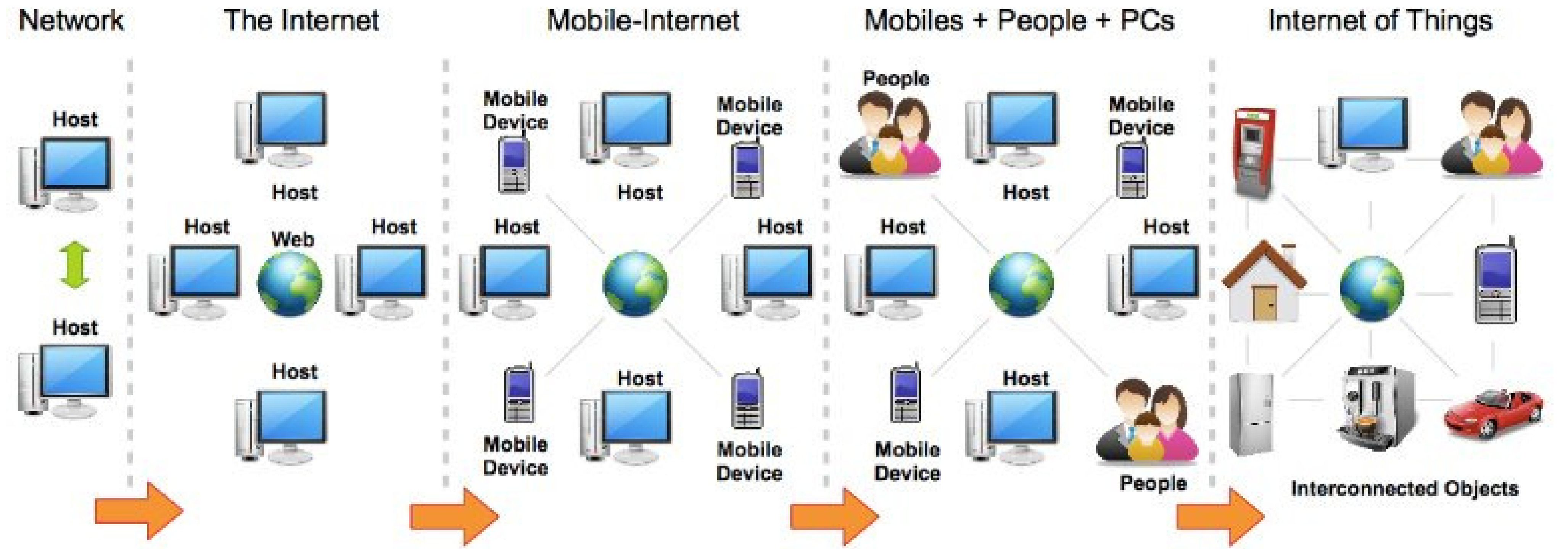
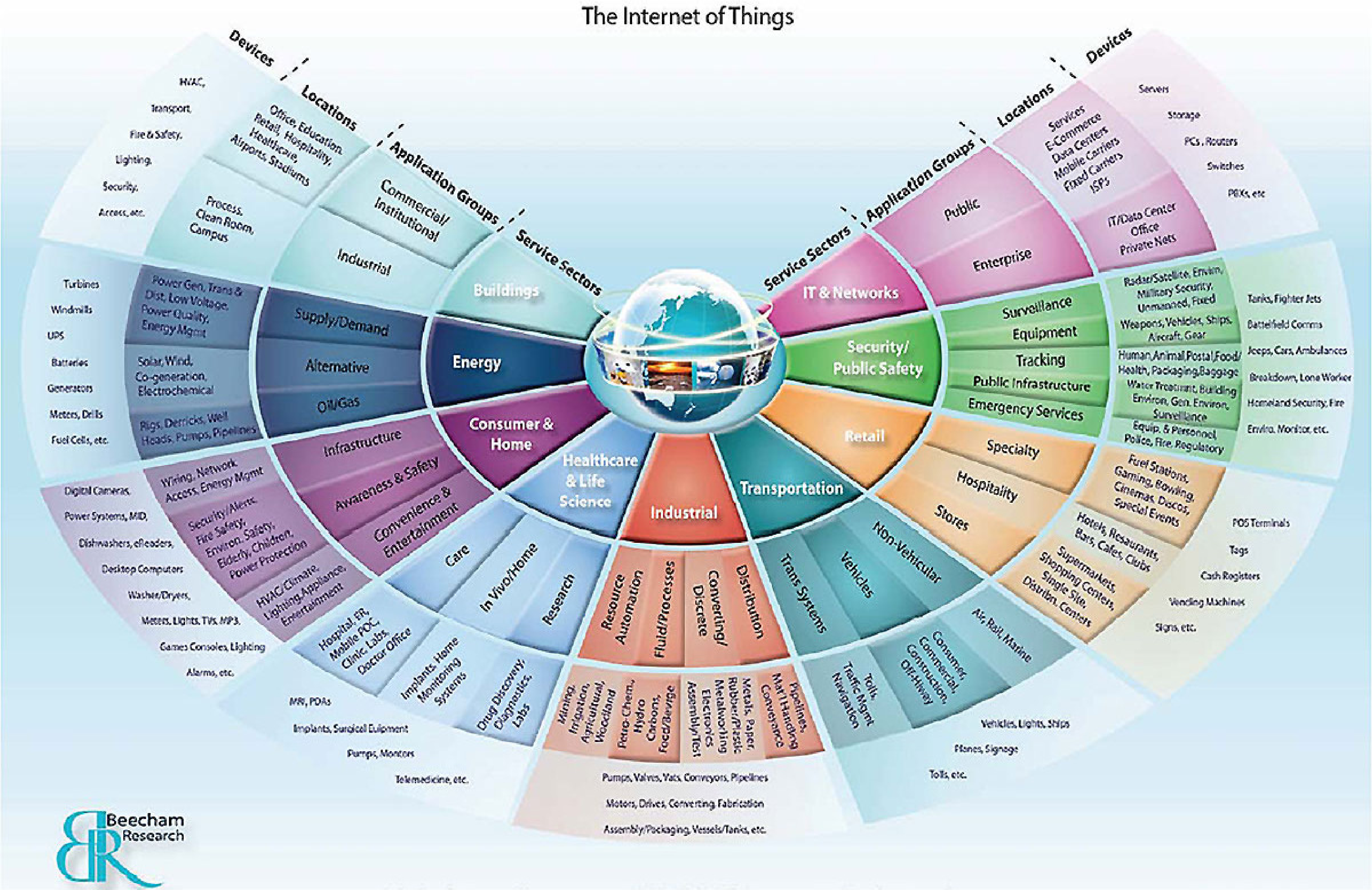


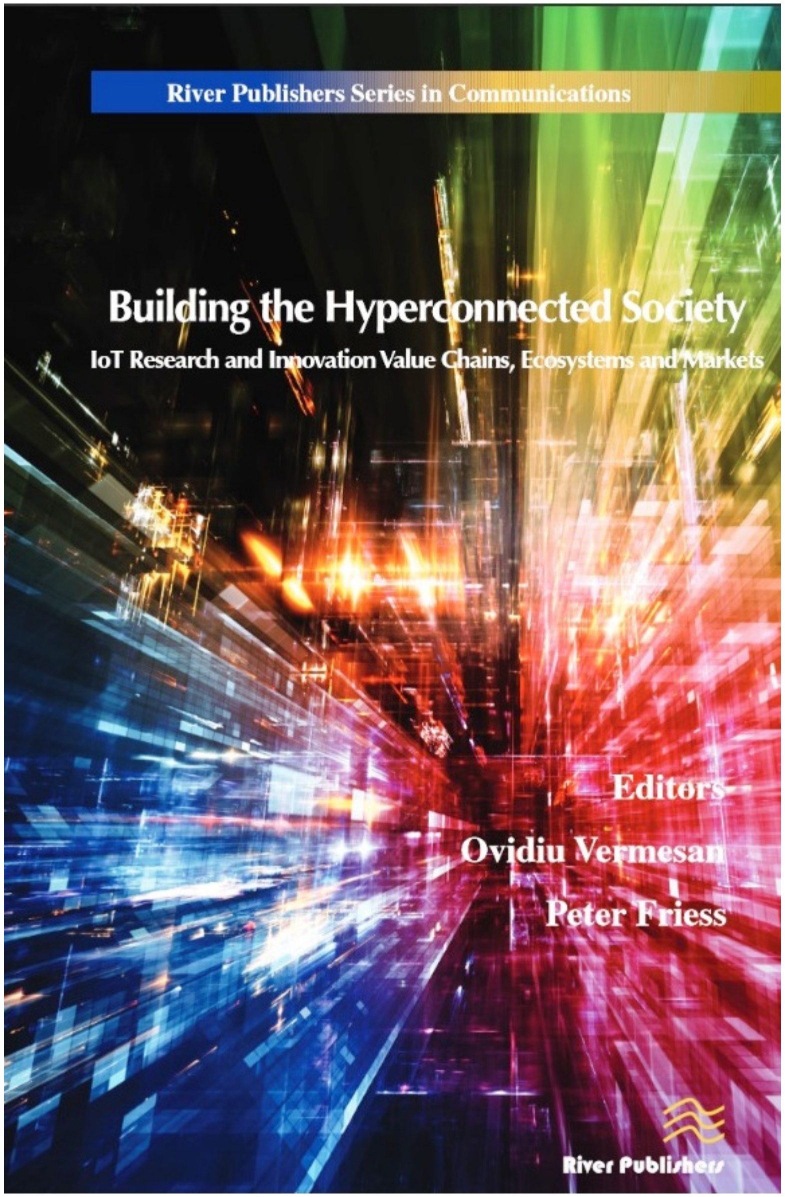
Fig. 1. Evolution of the Internet in five phases. The evolution of Internet begins with connecting two computers together and then moved towards creating World Wide Web by connecting large number of computers together. The mobile-Internet emerged by connecting mobile devices to the Internet. Then, peoples'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

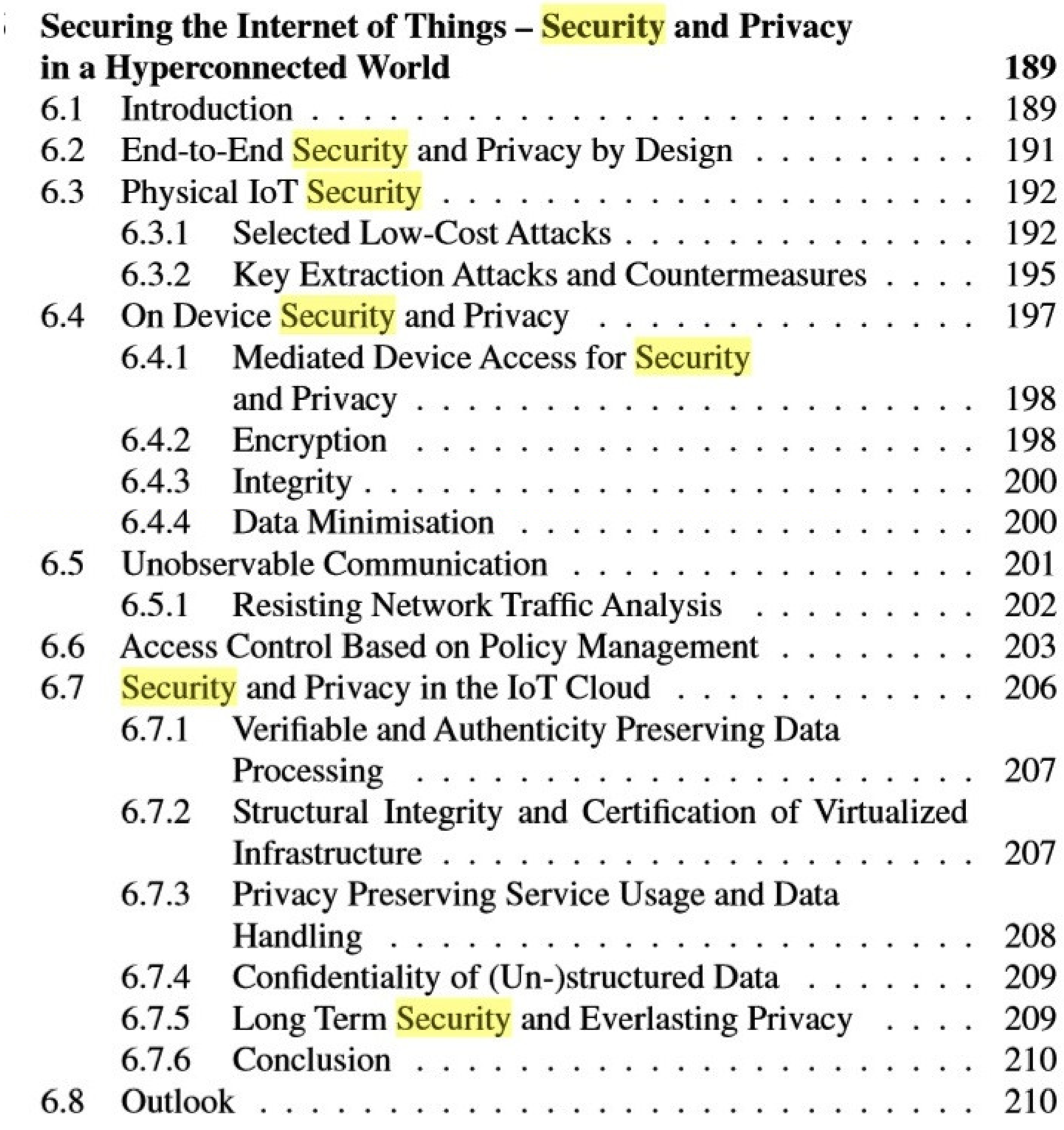
Internet of Things: *Spans ALL Sectors*


The Internet of Things
Devices
Locations
Application Groups
Service Sectors
HVAC,
Transport,
Fire & Safety,
Lighting,
Security,
Access, etc.
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Process, Clean Room, Campus
Commercial/ Institutional
Industrial
Buildings
Turbines
Windmills
UPS
Batteries
Generators
Meters, Drills
Fuel Cells, etc.
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Solar, Wind, Co-generation, Electrochemical
Rigs, Derricks, Well Heads, Pumps, Pipelines
Supply/Demand
Alternative
Oil/Gas
Energy
Digital Cameras,
Power Systems, MID,
Dishwashers, eReaders,
Desktop Computers
Washer/Dryers,
Meters, Lights, TVs, MP3,
Games Consoles, Lighting
Alarms, etc.
Wiring, Network Access, Energy Mgmt
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
HVAC/Climate, Lighting,Appliance, Entertainment
Infrastructure
Awareness & Safety
Convenience & Entertainment
Consumer & Home
MRI, PDAs
Implants, Surgical Eqipment
Pumps, Monitors
Telemedicine, etc.
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
Implants, Home Monitoring Systems
Drug Discovery, Diagnostics, Labs
Care
In Vivo/Home
Research
Healthcare & Life Science
Pumps, Valves, Vats, Conveyors, Pipelines
Motors, Drives, Converting, Fabrication
Assembly/Packaging, Vessels/Tanks, etc.
Mining, Irrigation, Agricultural, Woodland
Petro-Chem, Hydro Carbons, Food/Bevrge
Metalworking Electronics Assembly/Test
Metals, Paper, Rubber/Plastic
Pipelines, Mat'l Handling Conveyance
Resource Automation
Fluid/Processes
Converting/ Discrete
Distribution
Industrial
Vehicles, Lights, Ships
Planes, Signage
Tolls, etc.
Tolls, Traffic Mgmt Navigation
Consumer, Commercial, Construction, Off-Hiway
Air, Rail, Marine
Trans Systems
Vehicles
Non-Vehicular
Transportation
POS Terminals
Tags
Cash Registers
Vending Machines
Signs, etc.
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hotels, Resaurants, Bars, Cafes, Clubs
Supermarkets, Shopping Centers, Single Site, Distribn. Centers
Specialty
Hospitality
Stores
Retail
Tanks, Fighter Jets
Battlefield Comms
Jeeps, Cars, Ambulances
Breakdown, Lone Worker
Homeland Security, Fire
Enviro. Monitor, etc.
Radar/Satellite, Envirn, Military Security, Unmanned, Fixed
Weapons, Vehicles, Ships, Aircraft, Gear
Human,Animal,Postal,Food/ Health, Packaging,Baggage
Water Treatment, Building Environ, Gen. Environ, Surveillance
Equip. & Personnel, Police, Fire, Regulatory
Surveillance
Equipment
Tracking
Public Infrastructure
Emergency Services
Security/ Public Safety
Servers
Storage
PCs, Routers
Switches
PBXs, etc
Services E-Commerce Data Centers Mobile Carriers Fixed Carriers ISPs
IT/Data Center Office Private Nets
Public
Enterprise
IT & Networks
Beecham Research

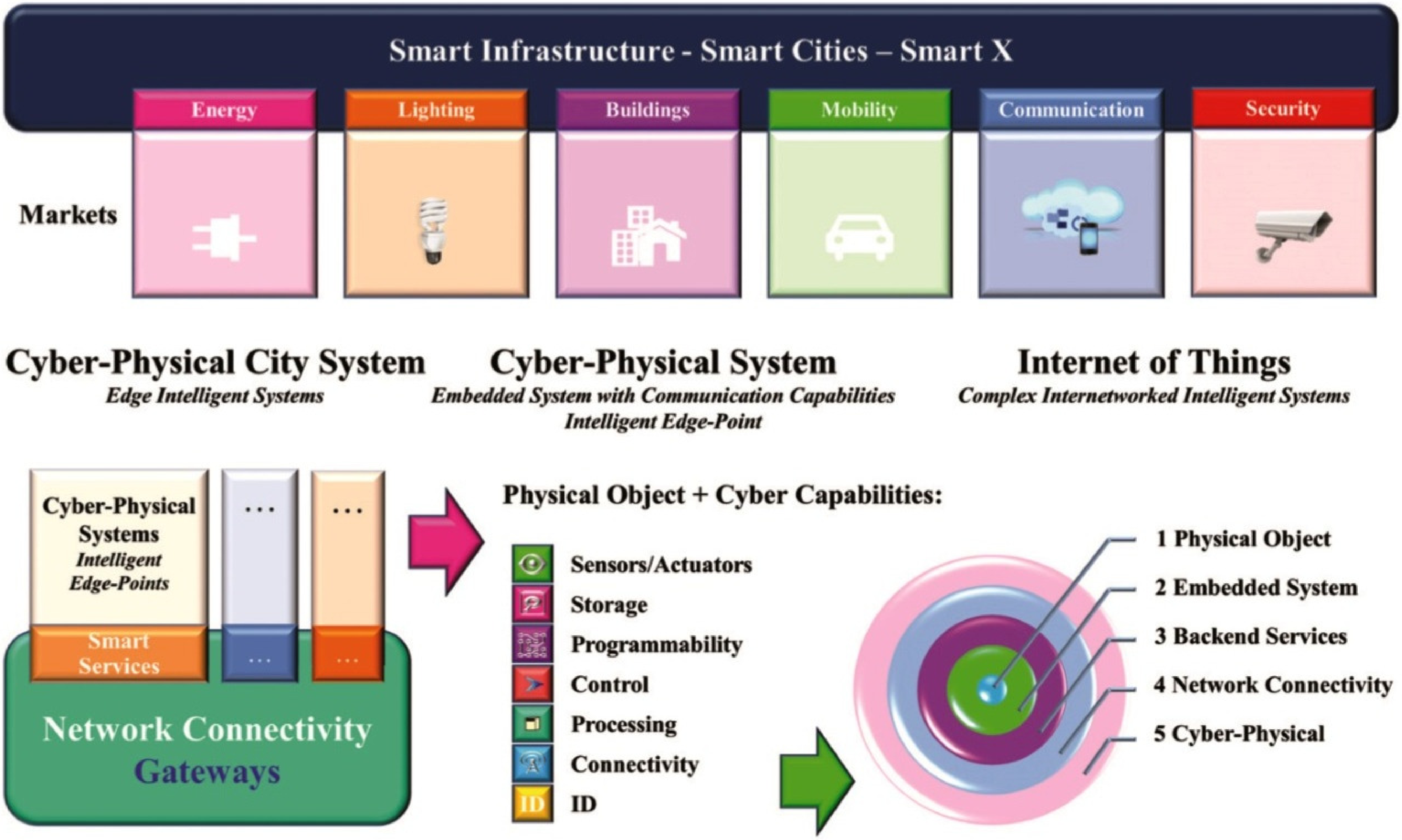
- Security for the *Internet of Things* -

Security & Privacy in Hyperconnected Society


River Publishers Series in Communications
Building the Hyperconnected Society
IoT Research and Innovation Value Chains, Ecosystems and Markets
Editors
Ovidiu Vermesan
Peter Friess
River Publishers


Securing the Internet of Things – Security and Privacy in a Hyperconnected World **189**

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 ID

1 Physical Object

2 Embedded System

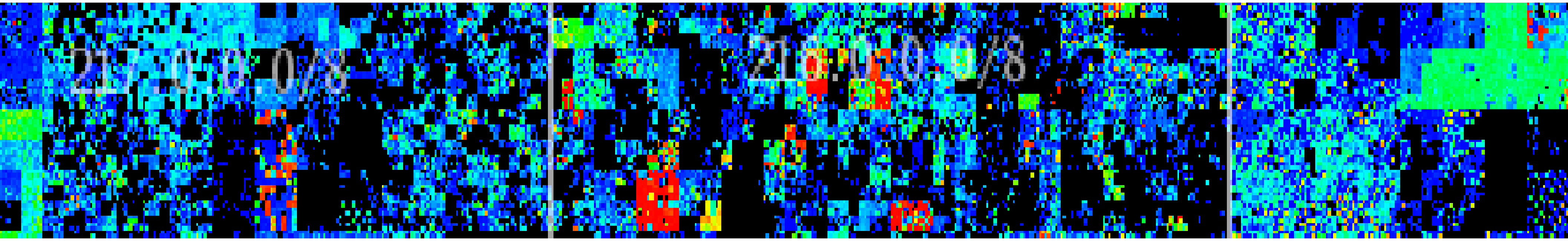
3 Backend Services

4 Network Connectivity

5 Cyber-Physical

Energising *Cybersecurity* with "Biometrics & Forensics"

1 – Background: CyberCrime & Terrorism	2 – 21stC Profiling & Tracking: "Bad Guys"	3 – Real-Time Security & Surveillance
4 –Integrated Cyber Biometrics: Pre-Attack	5 – Cyber Digital Forensics : Post-Attack	6 – Cyber-Bio: Security Sector Scenarios
7 –Biometric User Authentication for "IoT"	8 – Cyber-Bio Vision: Practical Solutions	9 – YOUR TOP 10 Actions & RoadMap

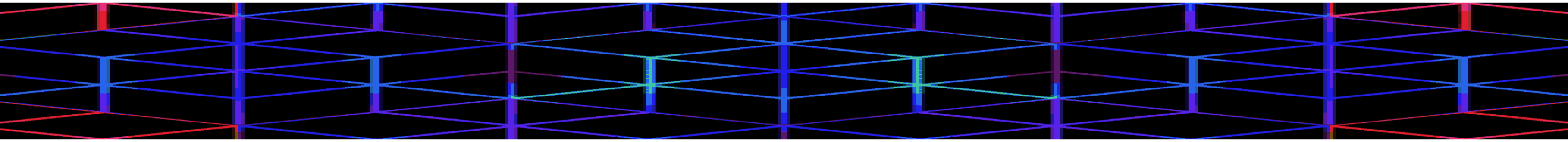


(8) Cyber-Bio Vision: *Practical Solutions*

- Integrated ***Cyber-Biometric Solutions*** will be progressively deployed during the next 5 to 10 years:
  - **Scenario 2020:** *Business & Government* – Staff Access to Facilities, "IoT" Devices, Networks, Data Bases & Assets
  - **Scenario 2025**: *Cities & Urban Regions* – Tracking "Bad Guy" Criminal Profiles (Bio, Cyber, SIM, CCTV, "Cell")
  - **Scenario 2040:** *Global Cyber-Bio Security* – ePassports, Bio-ID Cards, Bio-Border Controls, Bio-Signature, Access to National Transport Hubs, Sports & Cultural Events

....Eventually *ALL Access* to Secure Facilities, Financial & Legal Transactions, Major Sports Events, Concerts & Transport Hubs will require *YOUR Biometric-ID*!...

Our CyberVision: *2020 - 2040*

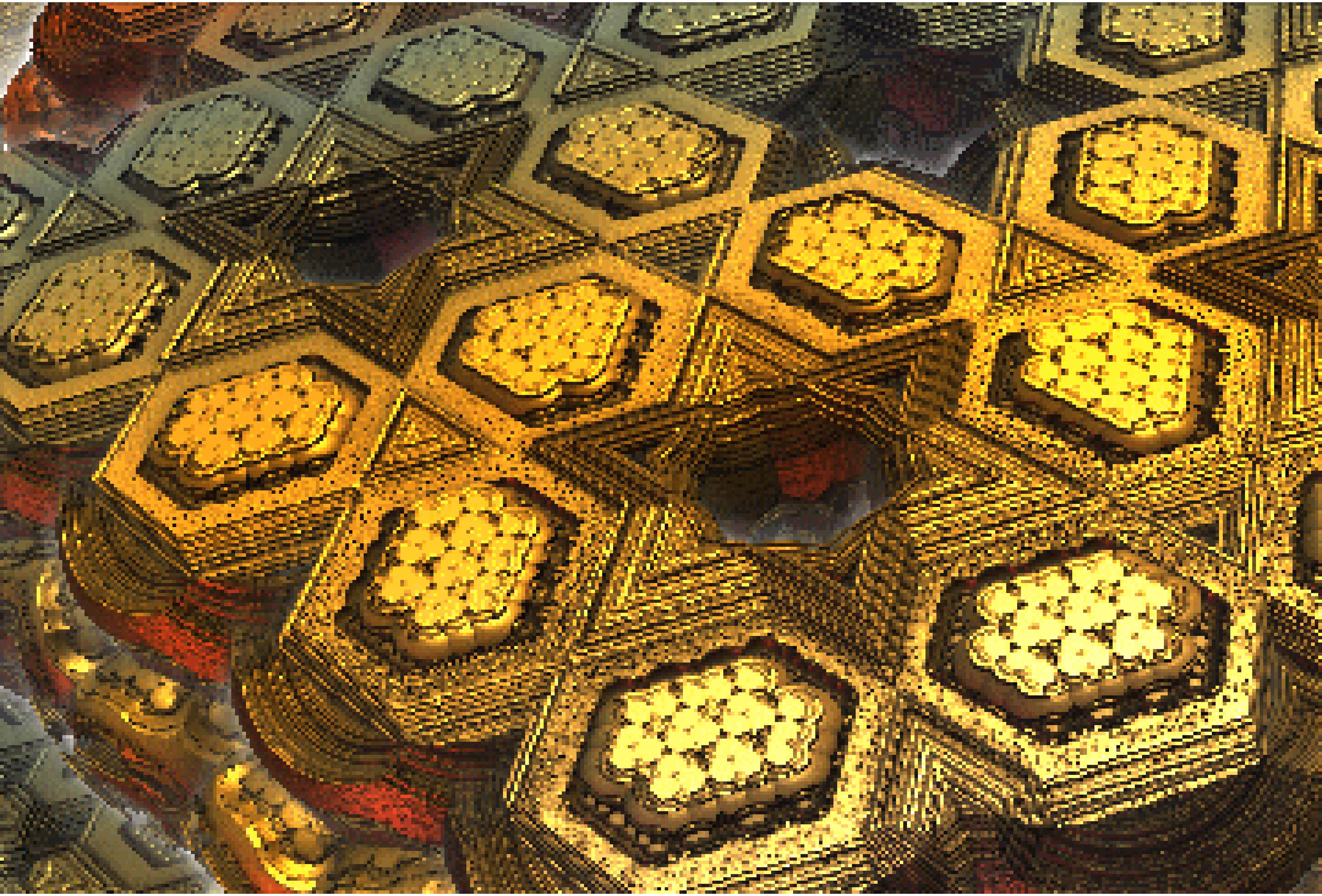


- **Scenario 2020 – *Adaptive Security-IoT*:** Managed Integration of IoT, *Cyber* & Physical Ops under CSO Management!

- **Scenario 2025 – *Intelligent Security*:** Transition to Real-Time Artificial Intelligence & Machine Learning based Enterprise Cybersecurity Tools & Biometric ID & Forensic Solutions

- **Scenario 2040** – ***Neural Security:*** Self-Organising, Intelligent Bio-Cyber Solutions with AI Profiling, Tracking & Surveillance!

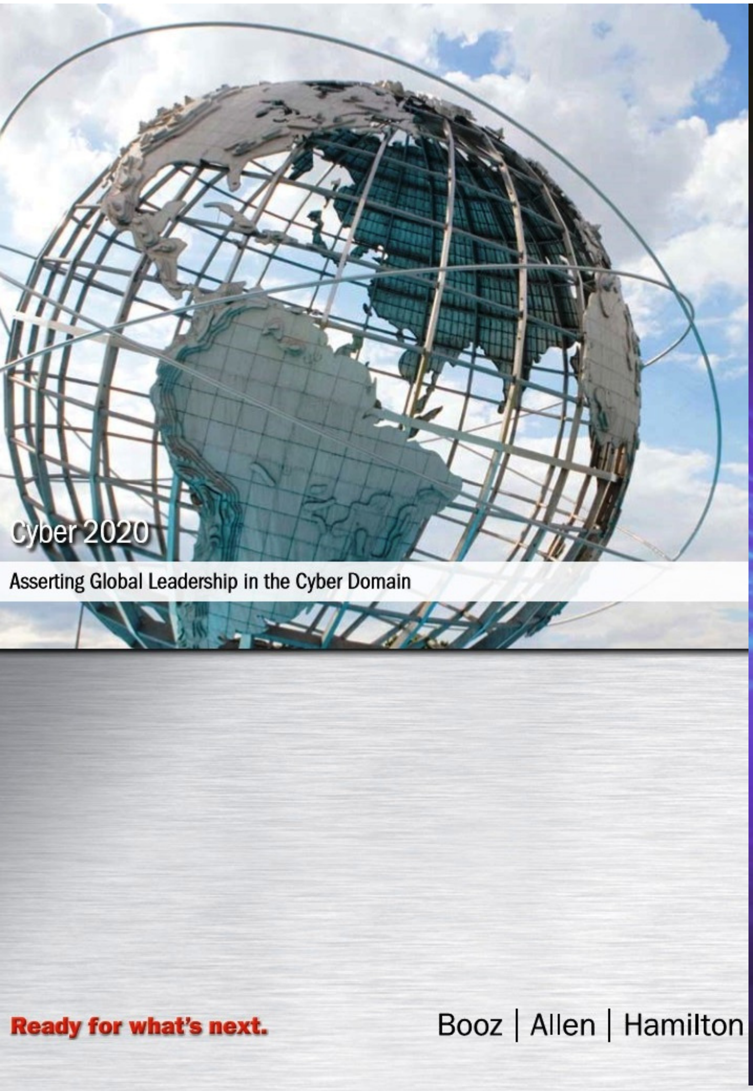
Cyberspace 2020 – *"Adaptive Security"*



Scenario 2020: Adaptive Security - IoT

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

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

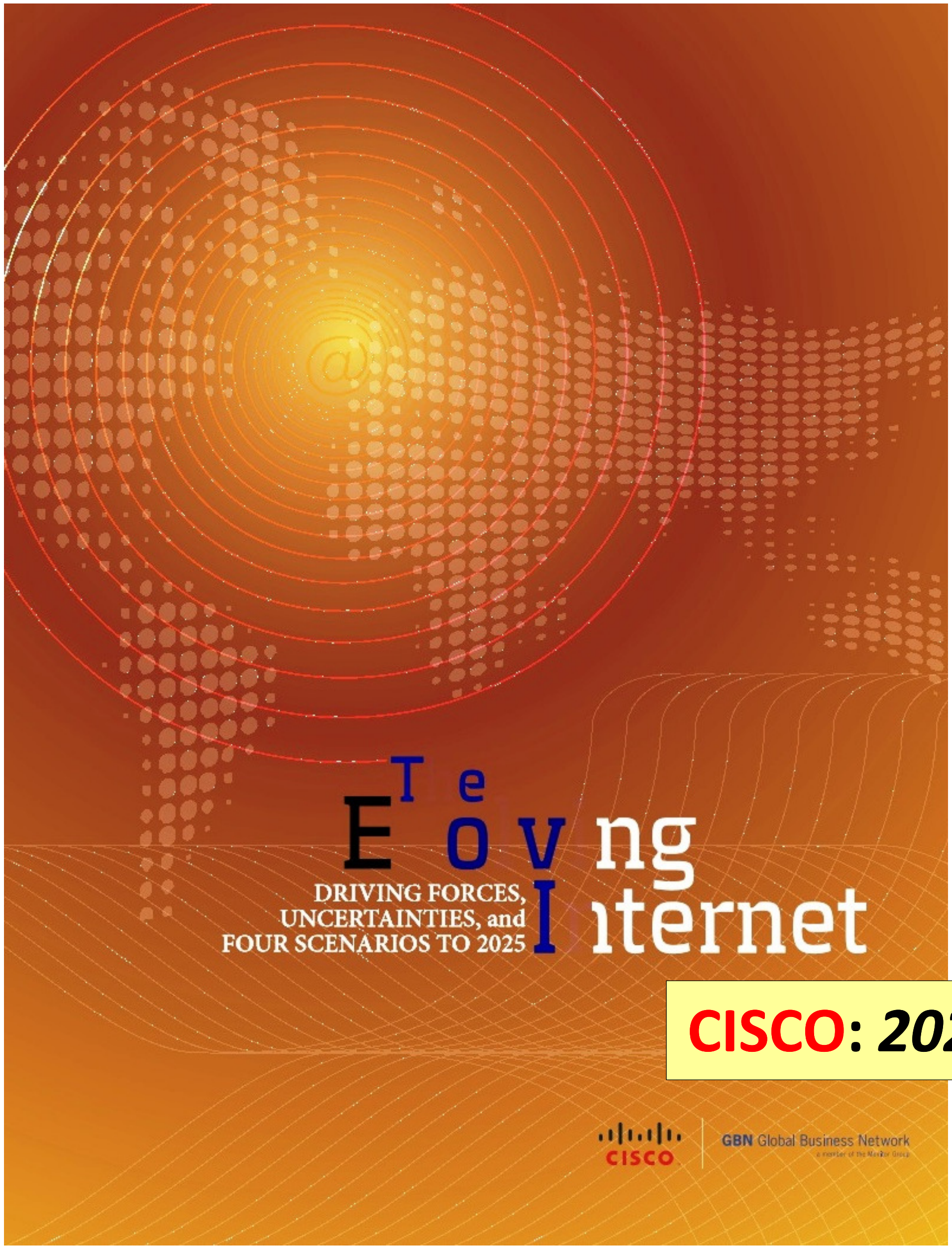
Department of Defence
Defence Science and
Technology Organisation

Cyber 2020 Vision

DSTO cyber science and technology plan

DSTO | Science and Technology for Safeguarding Australia

Technology Visions: Scenario *2025*



The Evolving Internet

DRIVING FORCES, UNCERTAINTIES, and FOUR SCENARIOS TO 2025

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

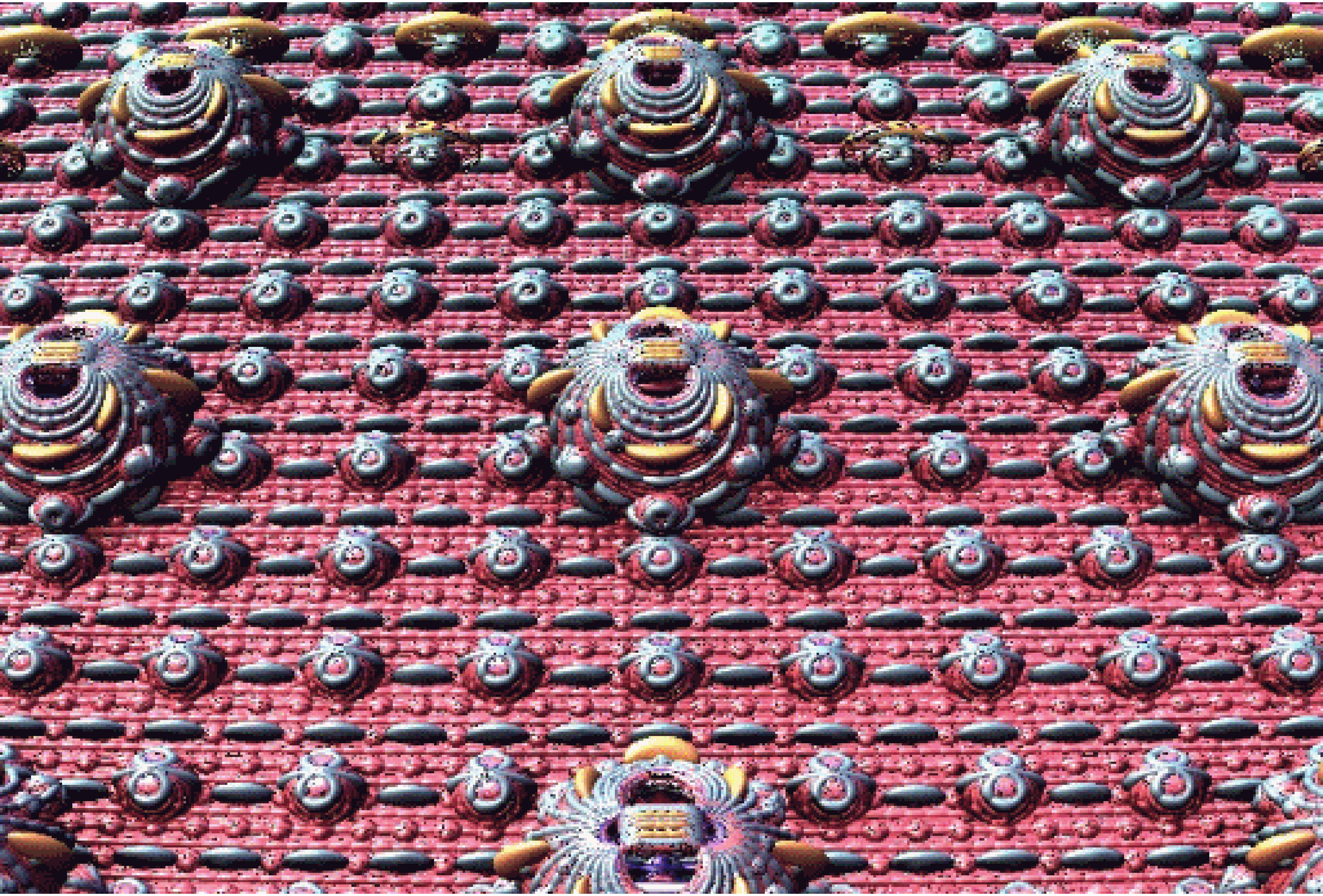
This document is a part of our "Telecom & Over-The-Top" category which includes in 2014:
- a dataset in Excel,
- a state-of-the-art report in PowerPoint,
- six market reports in Word, each with its synopsis in PowerPoint
- Privileged access to our lead OTT analysts

www.idate.org

DIGIWORLD by IDATE

CISCO: *2025* Scenarios: IDATE

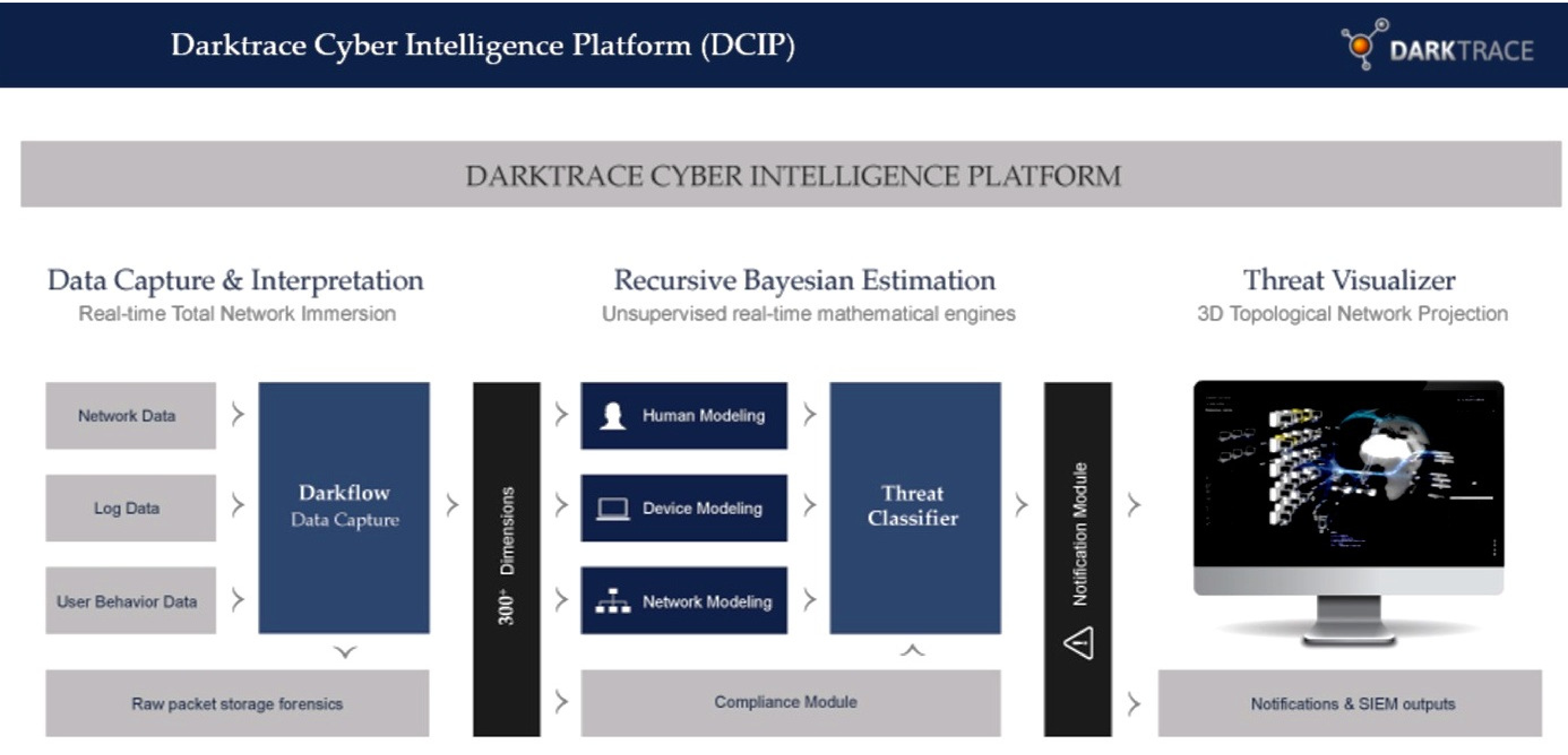
Cyberspace 2025 – *Intelligent Security”*



Scenario 2025: Intelligent Security

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

Darktrace: *Cyber Intelligence Platform*



Darktrace Cyber Intelligence Platform (DCIP)

DARKTRACE

DARKTRACE CYBER INTELLIGENCE PLATFORM

Data Capture & Interpretation
Real-time Total Network Immersion

- Network Data
- Log Data
- User Behavior Data

Darkflow
Data Capture

Raw packet storage forensics

300+ Dimensions

Recursive Bayesian Estimation
Unsupervised real-time mathematical engines

- Human Modeling
- Device Modeling
- Network Modeling

Threat Classifier

Compliance Module

Notification Module

Threat Visualizer
3D Topological Network Projection

Notifications & SIEM outputs

Self-Learning Enterprise Immune System: *"Behavioural Biometrics Model"*

Cyberspace 2025: *Microsoft Scenarios*

*** Plateau – Peak – Canyon ***

Microsoft

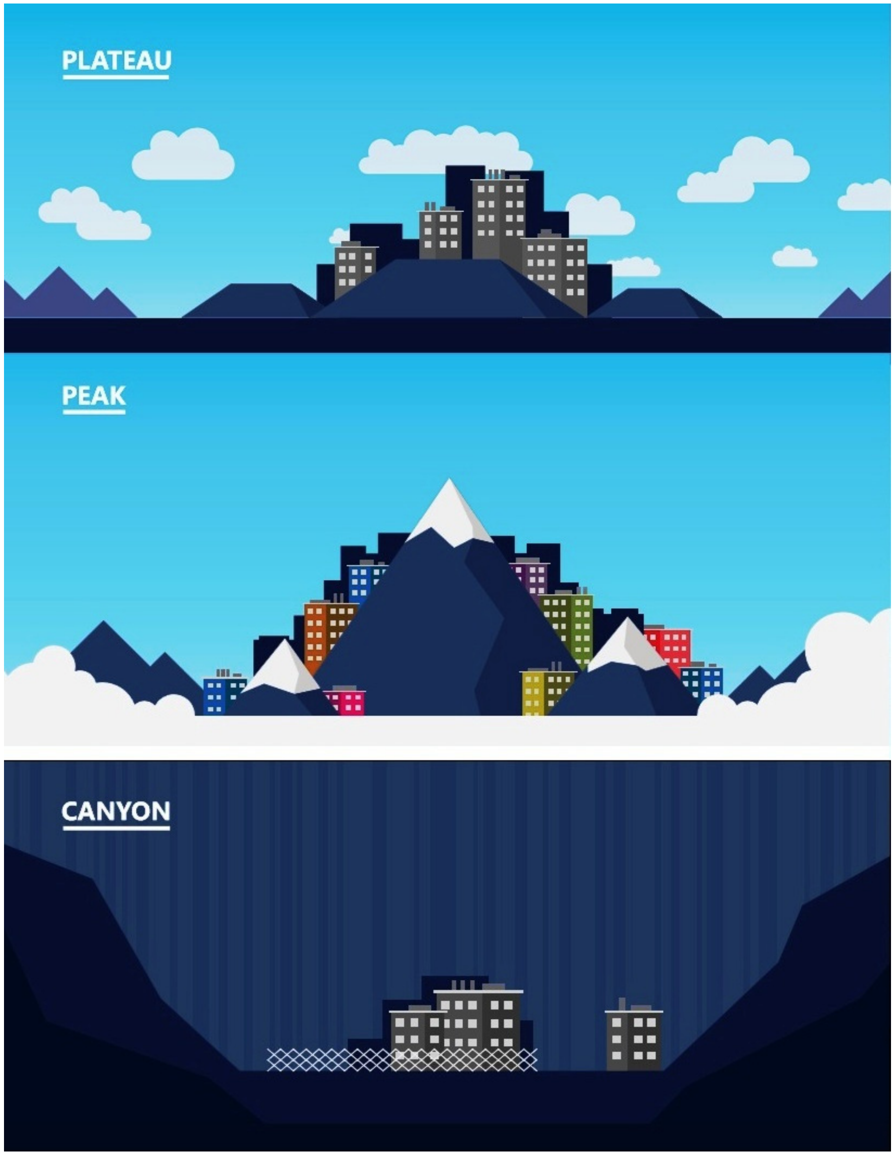
CYBERSPACE 2025

TODAY'S DECISIONS, TOMORROW'S TERRAIN

NAVIGATING THE FUTURE OF CYBERSECURITY POLICY

AUTHORS
David Burt
Aaron Kleiner
J. Paul Nicholas
Kevin Sullivan

JUNE 2014



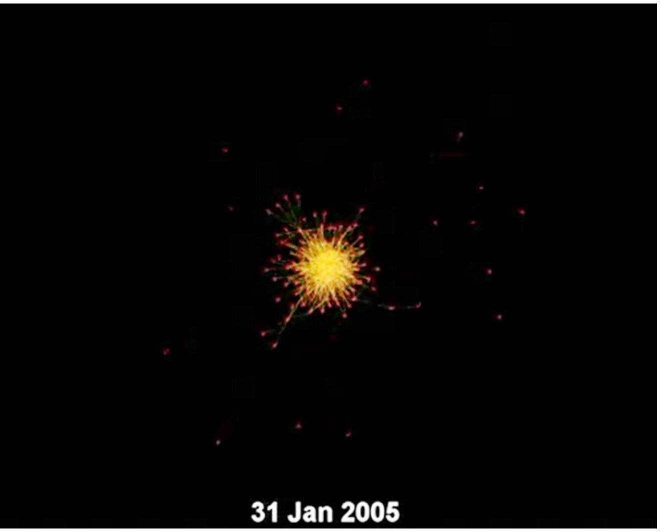
Cyberspace 2040 – "Neural Security"

Scenario 2040: Neural Security

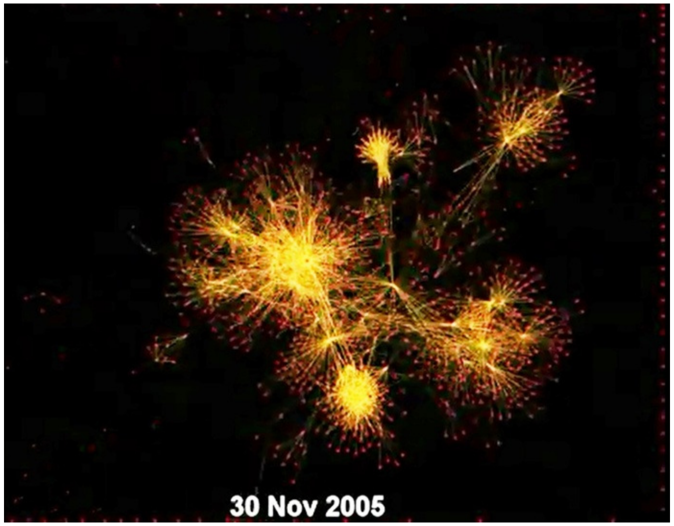
- ..25 Year Time Window - **1990 <– 2015 -> 2040**
- Full Implementation of Intelligent & Adaptive Cybersecurity across the Extended Enterprise
- Autonomous "Alerts" and Real-Time AI-based Cyber Event, Traffic & User Modelling
- New Scaled Architectures and Operational Standards for "Smart Systems" –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

Multi-Year Evolution of Wiki-Web

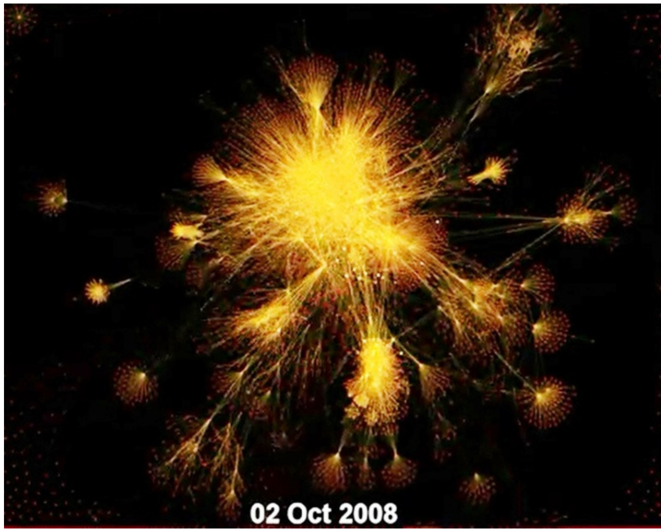
Complex Adaptive System : “Wiki.tudelft.nl”



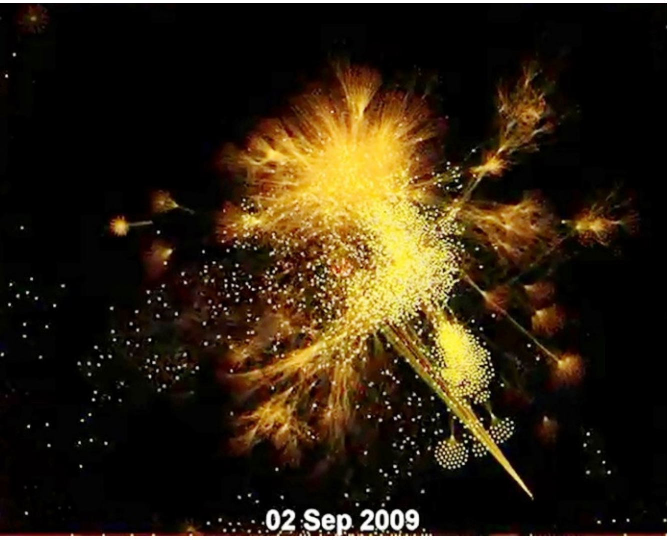
31 Jan 2005



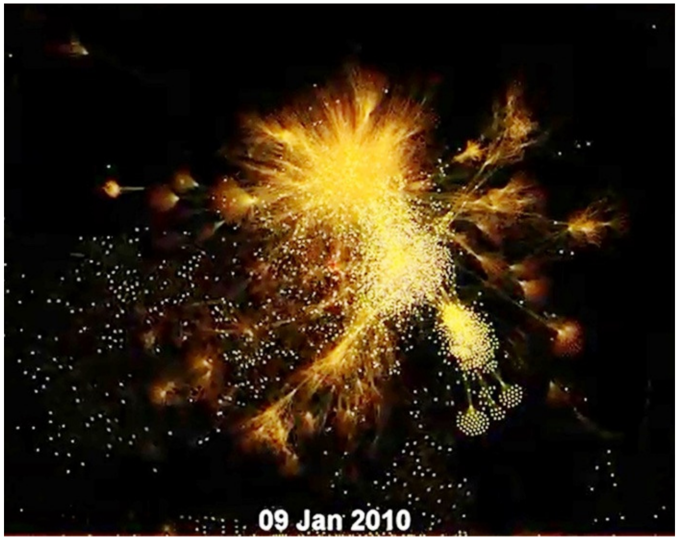
30 Nov 2005



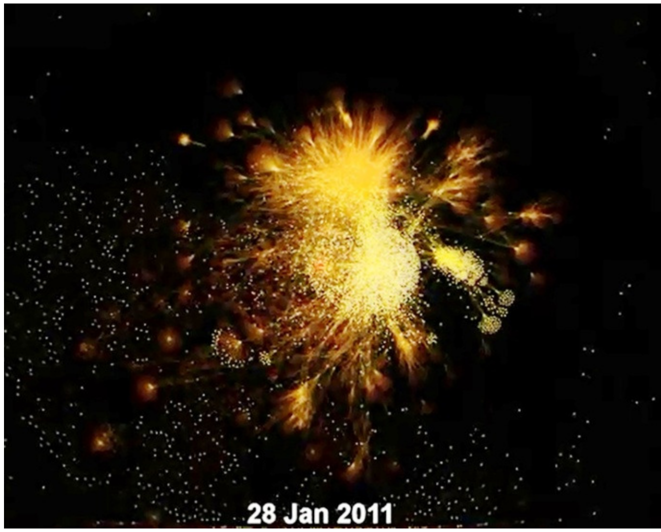
02 Oct 2008



02 Sep 2009



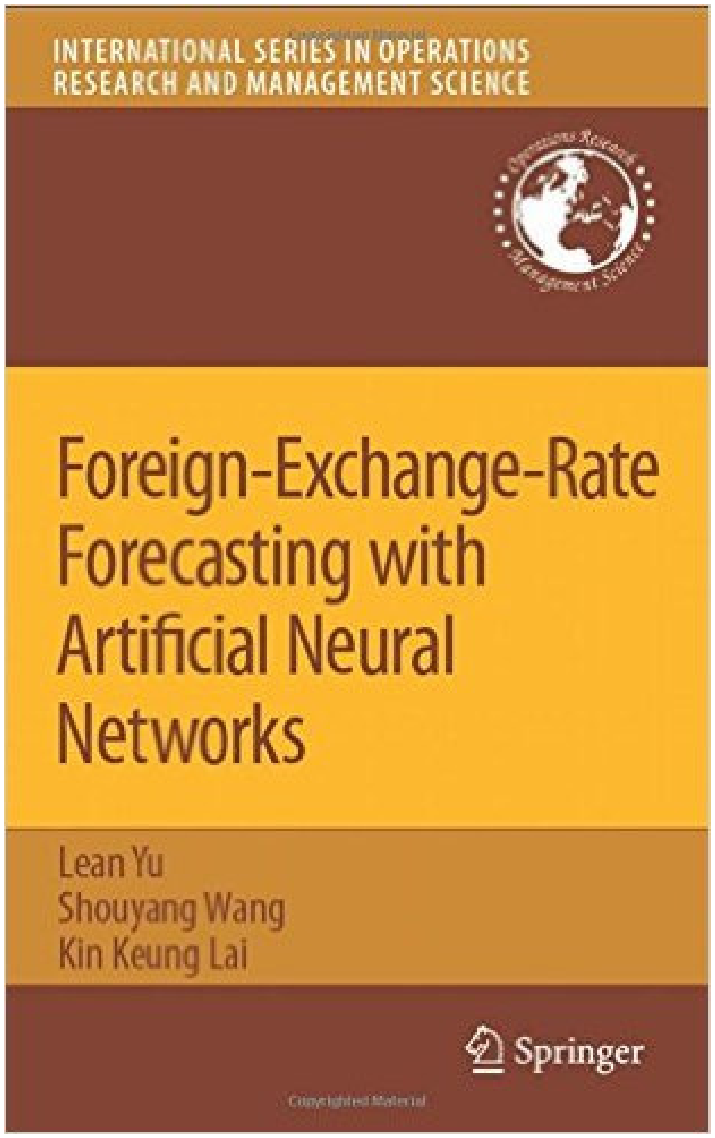
09 Jan 2010

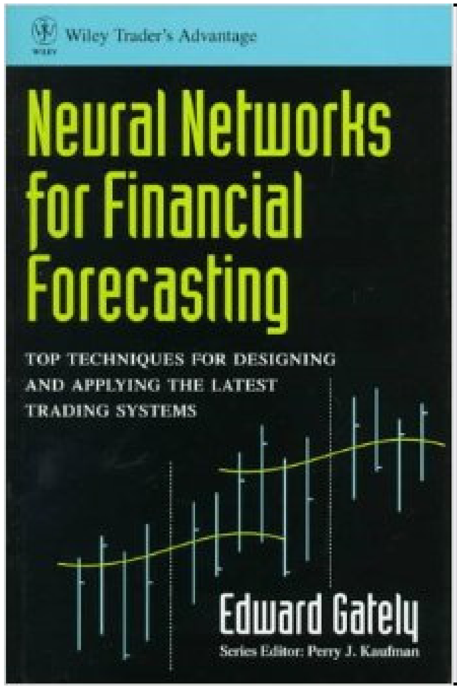


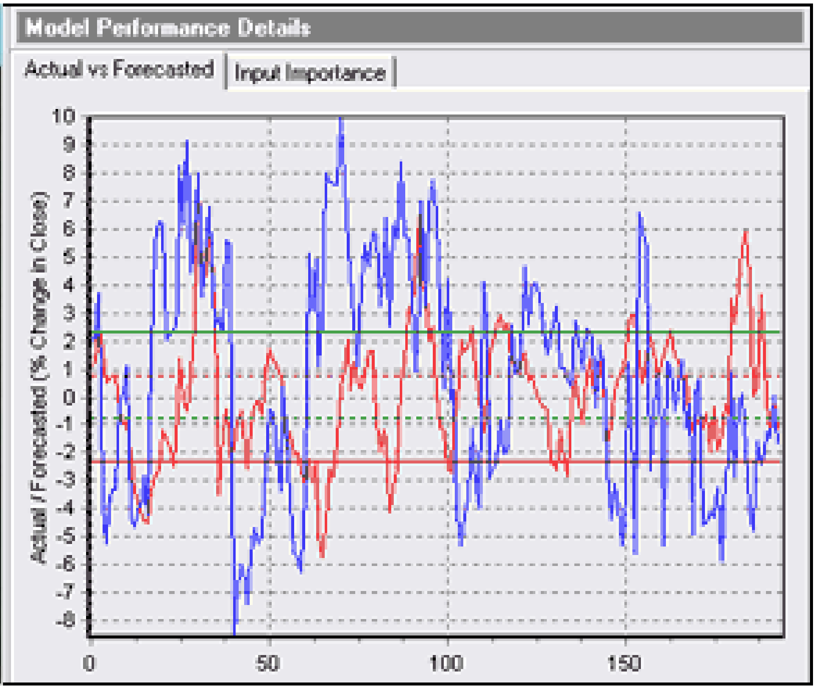
28 Jan 2011

Delft University of Technology - Netherlands

Artificial Neural Networks applied to Real-Time Foreign Exchange Dealing


INTERNATIONAL SERIES IN OPERATIONS RESEARCH AND MANAGEMENT SCIENCE
Operations Research Management Science
Foreign-Exchange-Rate Forecasting with Artificial Neural Networks
Lean Yu
Shouyang Wang
Kin Keung Lai
Springer
Copyrighted Material


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



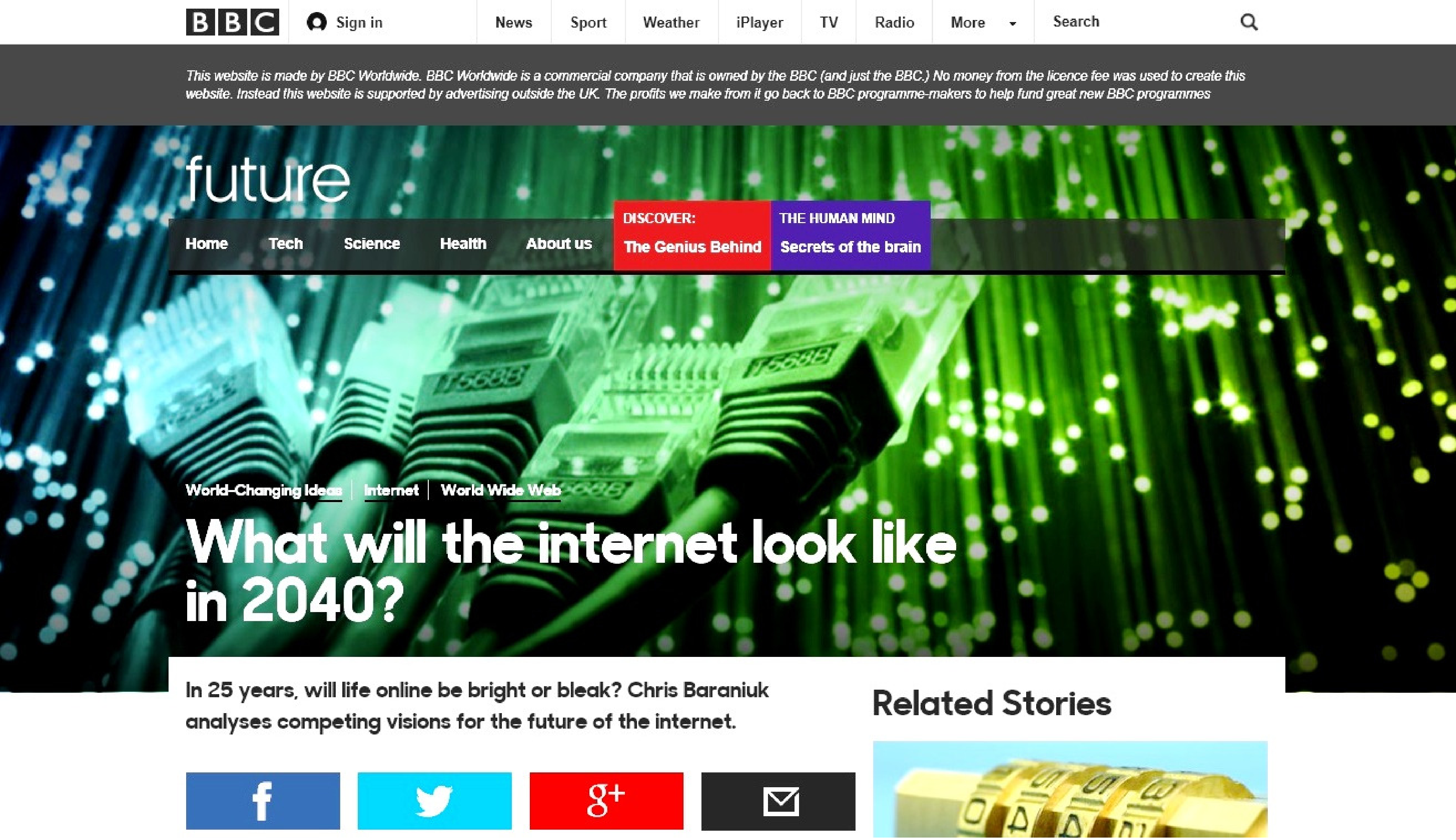
Algorithmic Computer Trading using Real-Time Neural Nets & Statistical Maths Tools have been used for 20+ Years!

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

Worldwide Real-Time Financial Trading

@Light Speed – 24/7 – Global Networks

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:* UK Ministry of Defence - MOD

MINISTRY OF DEFENCE

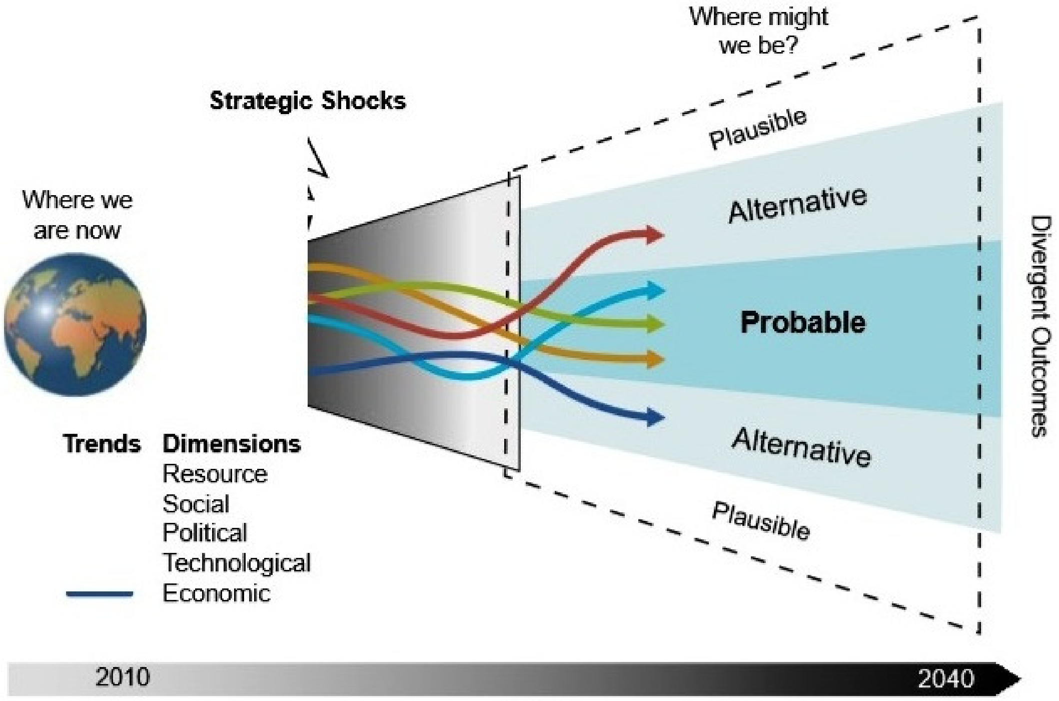
Ministry of Defence

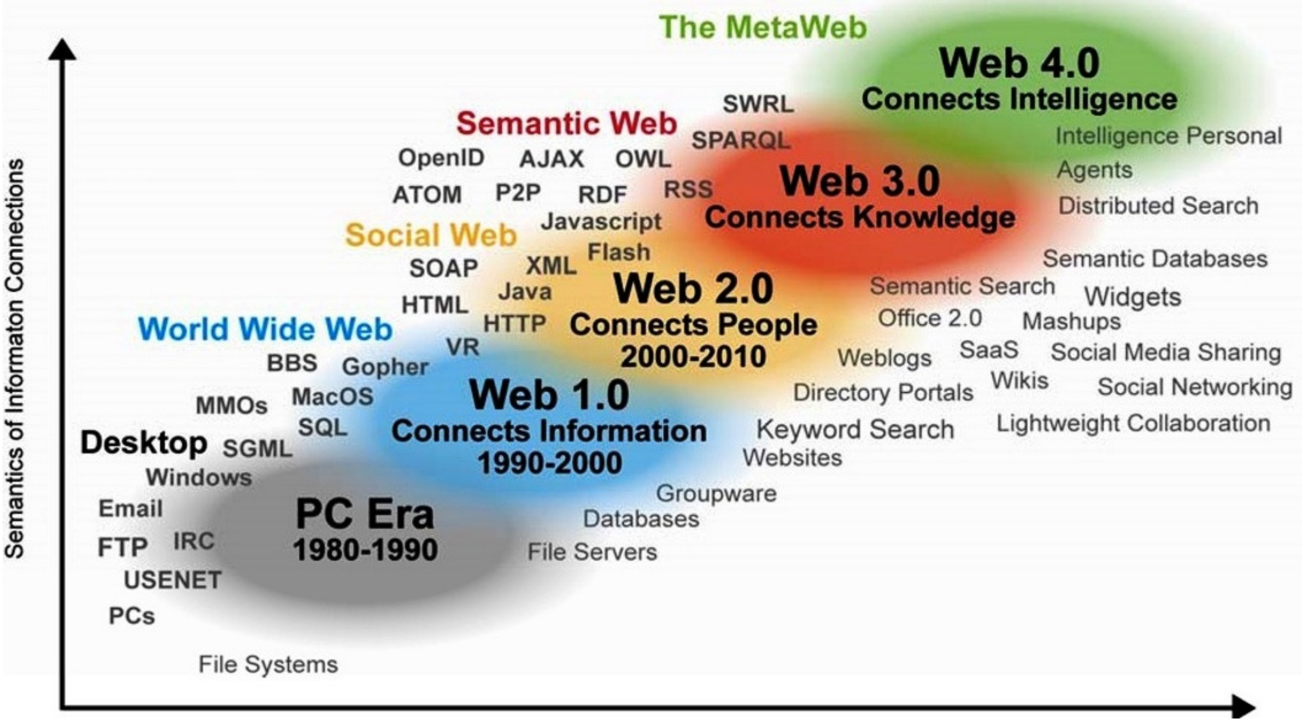
Strategic Trends Programme

Global Strategic Trends - Out to 2040

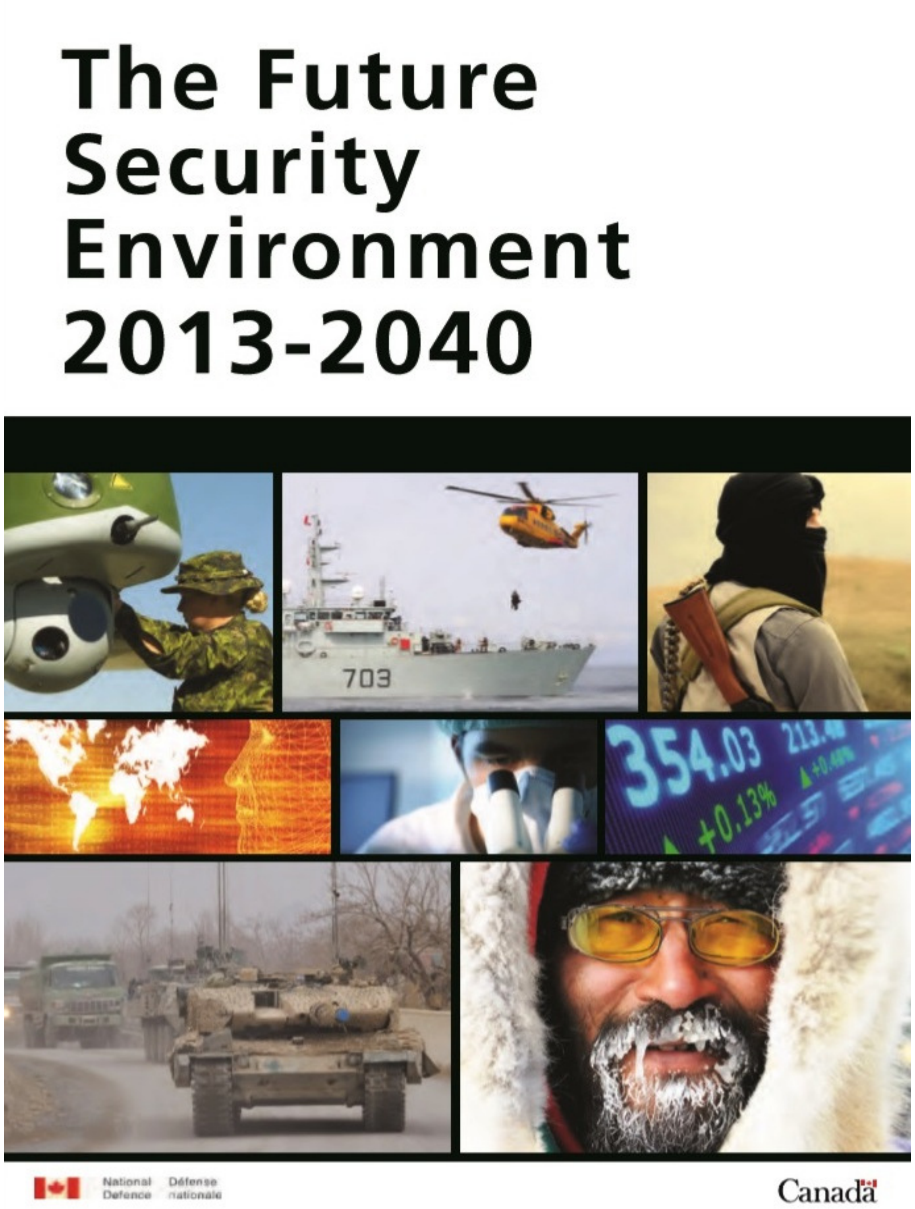
Fourth Edition

D C D C





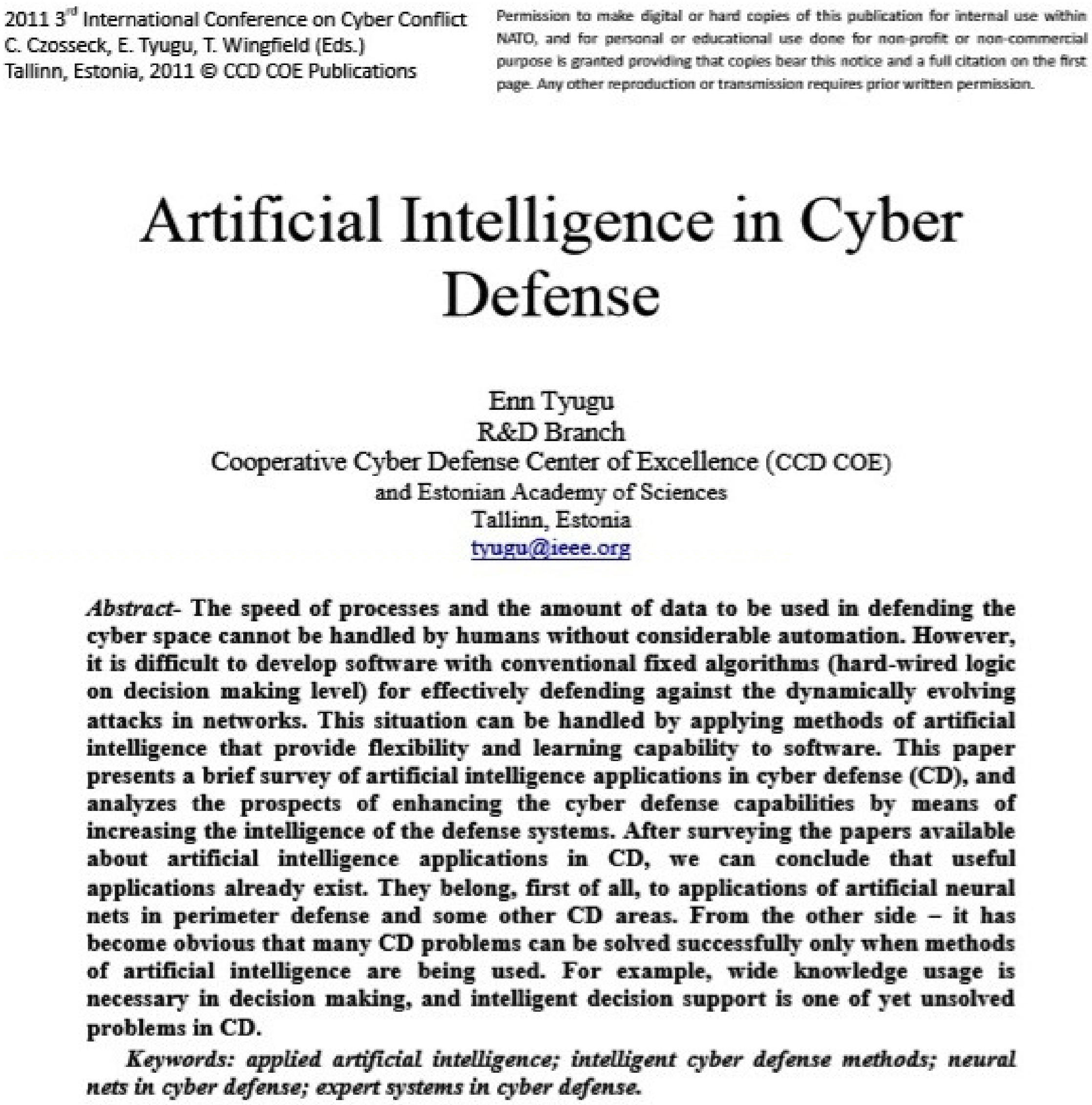
Scenario 2040: Cyber Defense – NATO & Canada



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

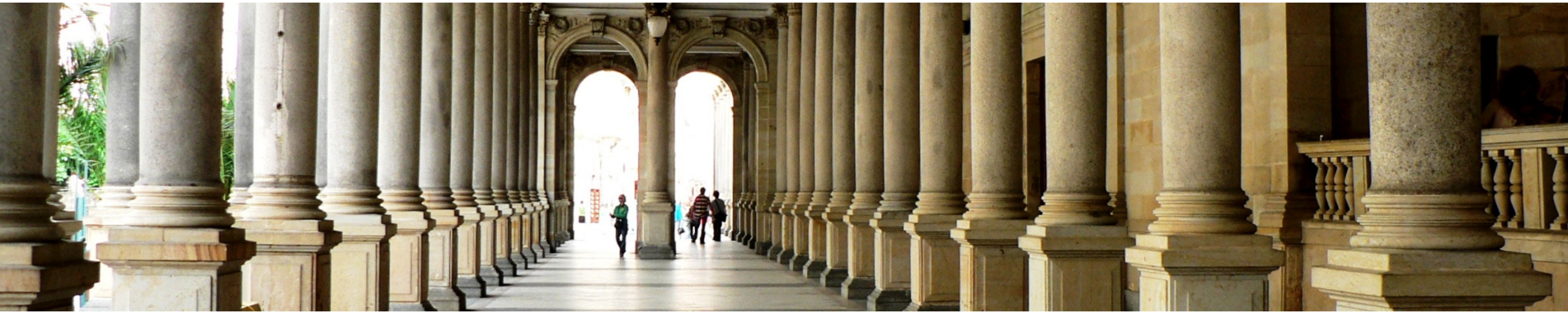
Artificial Intelligence in Cyber Defense

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

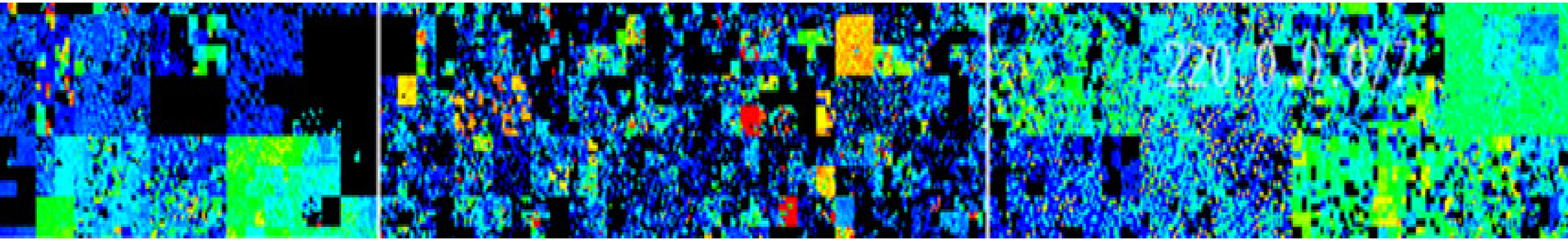
Abstract- The speed of processes and the amount of data to be used in defending the cyber space cannot be handled by humans without considerable automation. However, it is difficult to develop software with conventional fixed algorithms (hard-wired logic on decision making level) for effectively defending 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.

Energising *Cybersecurity* with "Biometrics & Forensics"



1 – Background: CyberCrime & Terrorism	2 – 21stC Profiling & Tracking: "Bad Guys"	3 – Real-Time Security & Surveillance
4 –Integrated Cyber Biometrics: Pre-Attack	5 – Cyber Digital Forensics : Post-Attack	6 – Cyber-Bio: Security Sector Scenarios
7 –Biometric User Authentication for "IoT"	8 – Cyber-Bio Vision: Practical Solutions	**9 – YOUR TOP 10 Actions & RoadMap**



(9) YOUR Top 10 Cyber-Bio Actions

1) Assign CSO – Chief Security Officer with Cyber-Biometric Action Plan
2) Professional Cyber-Biometric & Cyber-Forensics Training – CISSP
3) Implement International Security Standards (ISO/IEC- Biometrics)
4) Open Discussions with Biometric & Cyber-Forensic Solution Vendors
5) Profile YOUR Security Staff and Contractors for Possible Risks

6) ICT: Hire Qualified Cyber-Bio 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 Cyber-Bio-Forensics Security Integration
9) Professional Association Membership for Team Networking & Skill Building - IPSA
10) Cyber Legal Protection – Check *Your* Legacy Contracts for Cyber-Bio Trading Risks

Now ***YOUR*** Business will be ***"Energised"*** with **Cyber Biometrics & Digital Forensics!**

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

Edinburgh Napier UNIVERSITY

UNIVERSITY OF SURREY

WARWICK THE UNIVERSITY OF WARWICK

Security Lancaster | Lancaster University

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Queen's University Belfast

UNIVERSITY OF Southampton

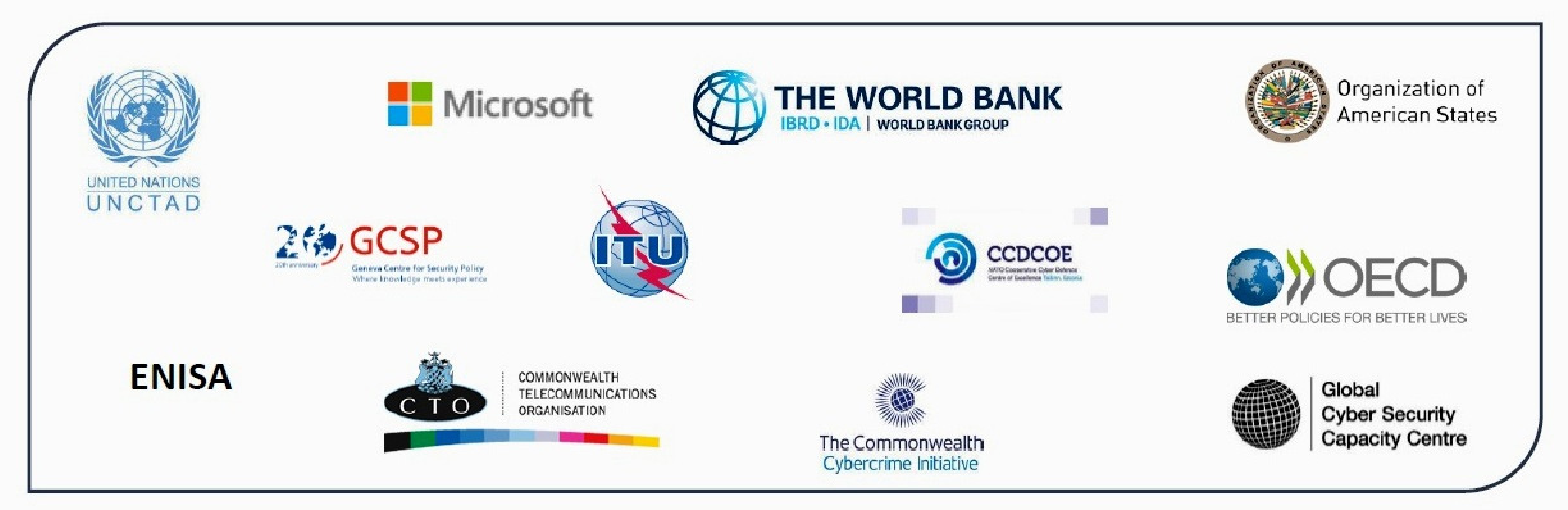
UNIVERSITY OF OXFORD

Cranfield UNIVERSITY

UCL

UNIVERSITY of York

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

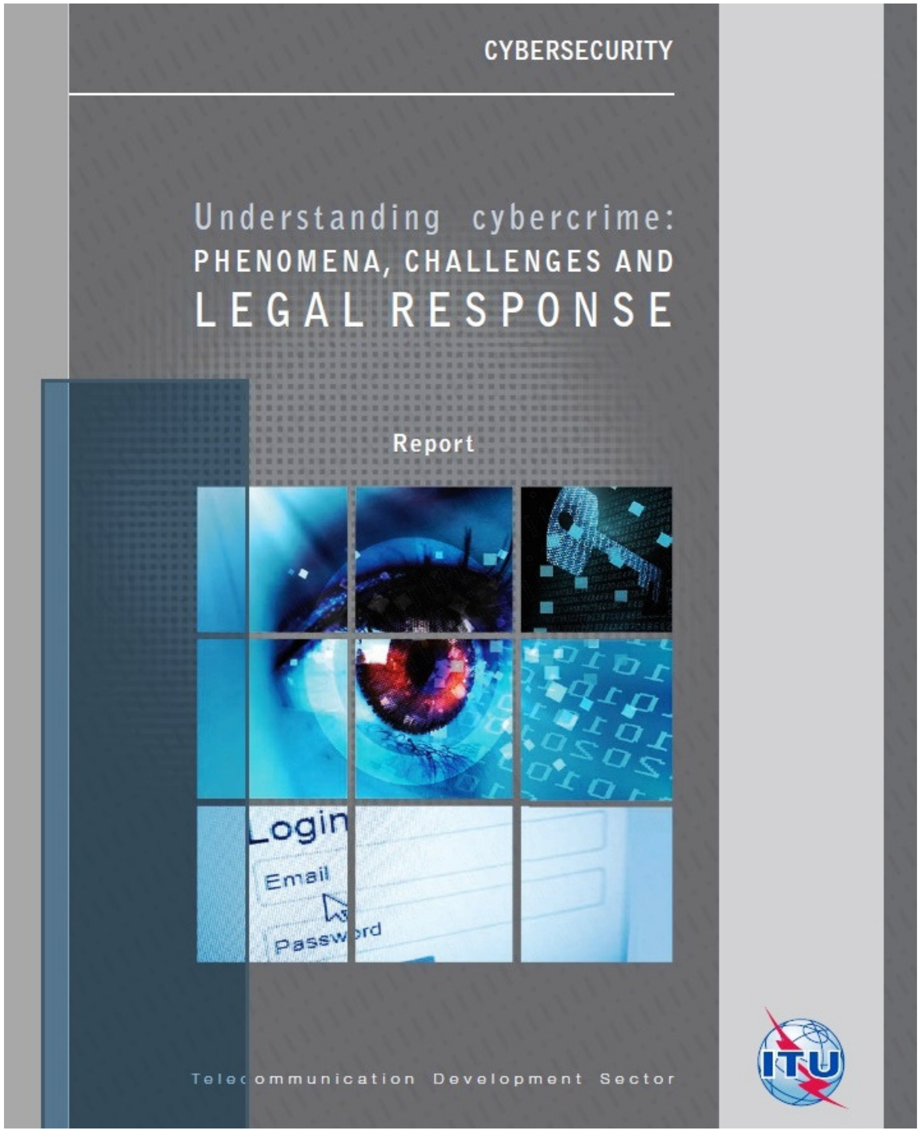

UNITED NATIONS
UNCTAD
Microsoft
THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP
Organization of American States
20 GCSP
Geneva Centre for Security Policy
Where knowledge meets experience
ITU
CCDCOE
OECD
BETTER POLICIES FOR BETTER LIVES
ENISA
CTO
COMMONWEALTH TELECOMMUNICATIONS ORGANISATION
The Commonwealth Cybercrime Initiative
Global Cyber Security Capacity Centre

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

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

- UN/ITU *CyberSecurity* Agenda -

Understanding CyberCrime (Eng/Rus)



CYBERSECURITY

Understanding cybercrime:
PHENOMENA, CHALLENGES AND
LEGAL RESPONSE

Report

Telecommunication Development Sector

КИБЕРБЕЗОПАСНОСТЬ

Понимание киберпреступности:
ЯВЛЕНИЕ, ЗАДАЧИ И
ЗАКОНОДАТЕЛЬНЫЙ ОТВЕТ

Отчет

Login
Email
Password

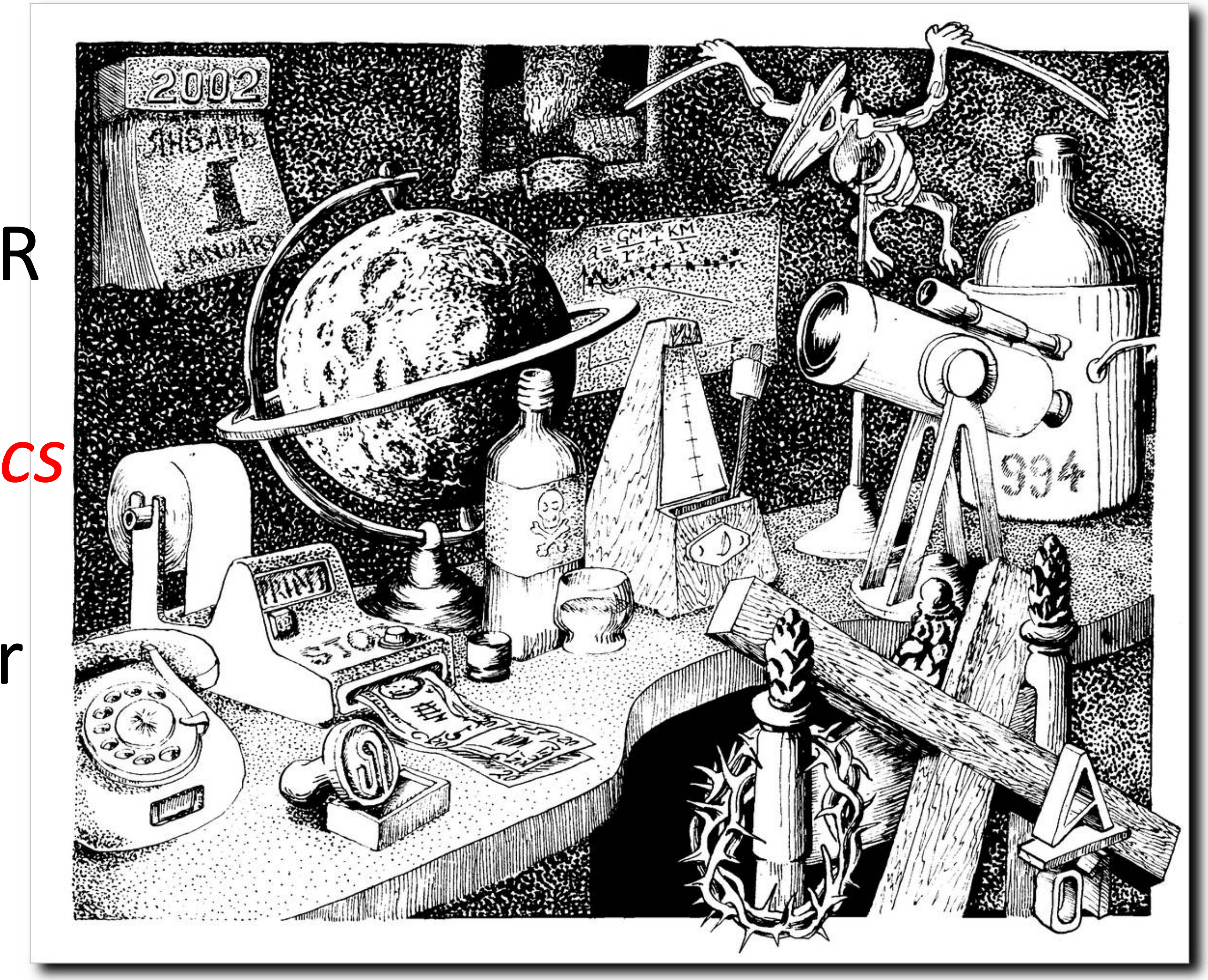
Сектор развития электросвязи

ITU

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

"Real-Time Defence" from Cyber Attacks"

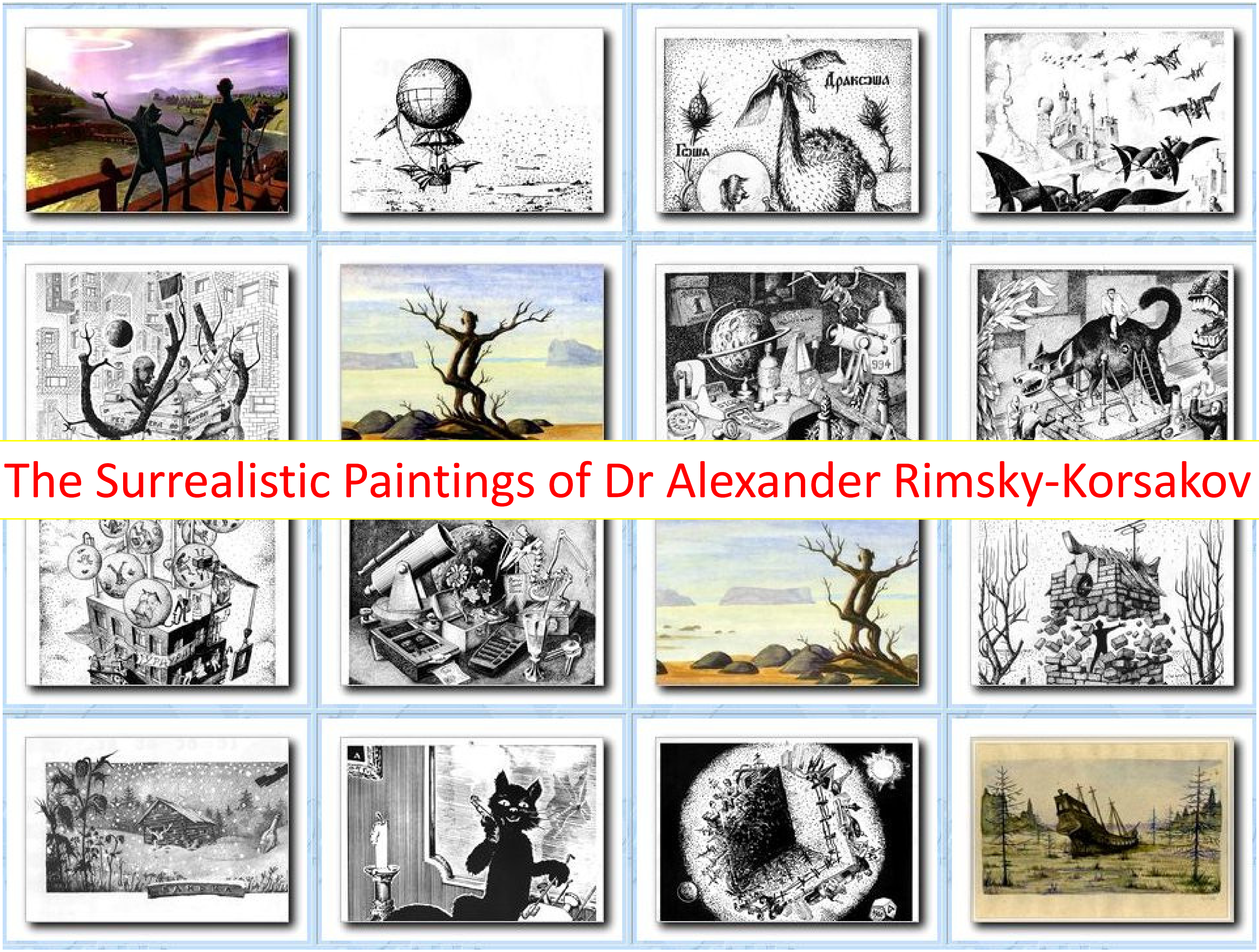
.......Energising YOUR Cybersecurity with *Biometrics & Forensics* will Increase your Defence from Cyber Threats & Attacks!



"The Director's Desk – Scientific Institute" - 2002

Pen & Ink Drawing by Alexander Rimski-Korsakov

The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov



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

Energising Cybersecurity with "Biometrics & Forensics"

International East-West Security Conference: Prague

Thank-You!...

Download Presentation Slides:

www.Valentina.net/Prague2016/

East-West Security Conference – Prague 2016

- Biometrics & Cyber Forensics - *Slides (PDF)* -

The Crucial Role of Cybersecurity in the - *"War on Terror"* -

Dr David E. Probert

VAZA International

Dedicated to Grand-Daughters – Abigail and Alice – *Securing their Future Life!*

33rd International East/West Security Conference

The Crucial Role of Cybersecurity
in the "War on Terrorism"
- Prague, Czech Republic: 6th-7th June 2016 -
© *Dr David E. Probert : www.VAZA.com* ©

1

...Energising ***YOUR*** Cybersecurity with *"Biometrics & Forensics"*

Dr David E. Probert

VAZA International

Dedicated to Grand-Sons: Ethan, Matthew & Roscoe – *Energising their Security!*

33rd International East/West Security Conference

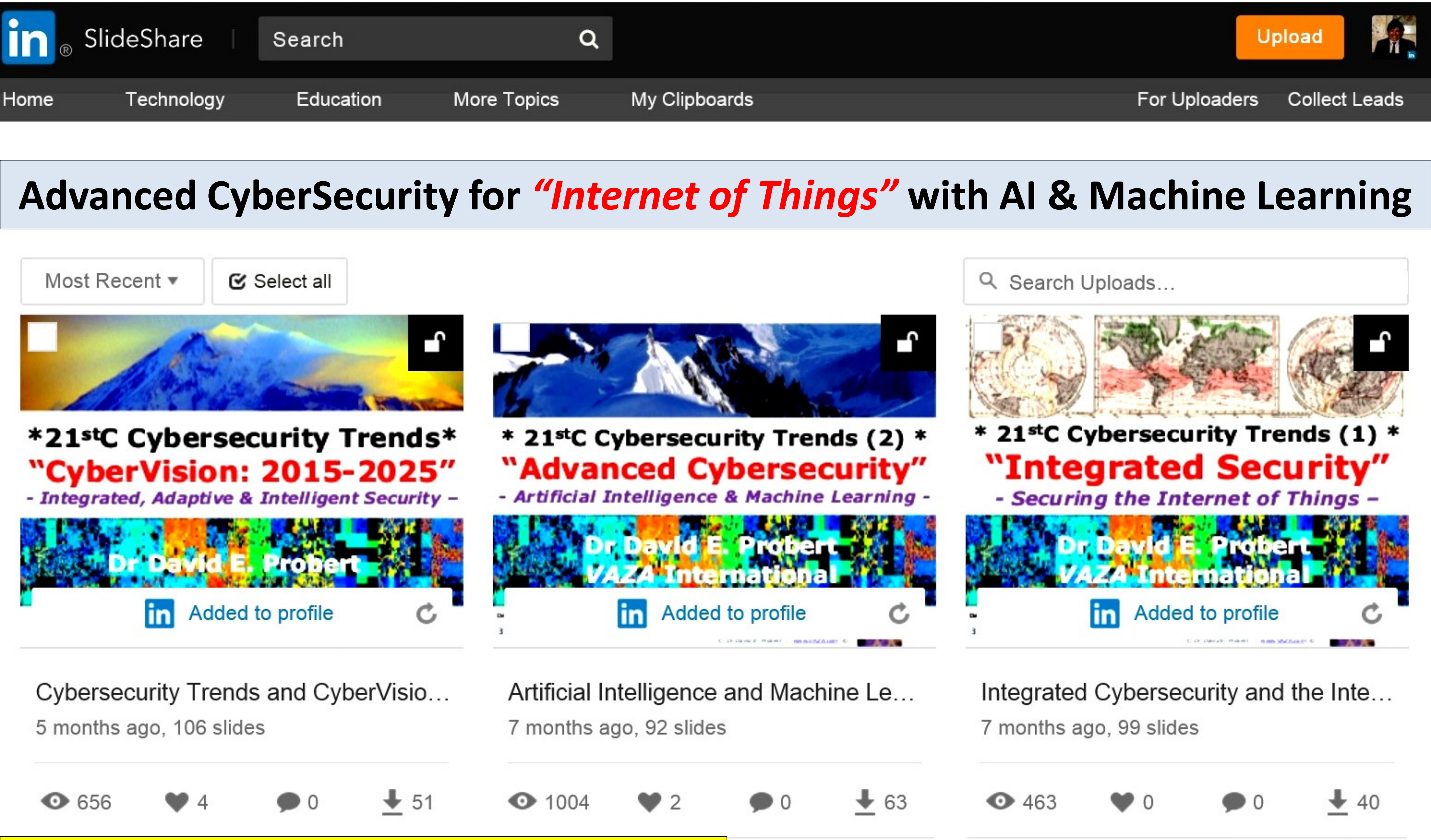
Energising YOUR Cybersecurity with
"Biometrics & Digital Forensics"
- Prague, Czech Republic: 6th-7th June 2016 -
© *Dr David E. Probert : www.VAZA.com* ©

1

Theme (1) – "Cyber War on Terror" **Theme (2) – "Biometrics & Forensics"**

Download Link: *www.valentina.net/Prague2016/*

Advanced Security & CyberVision 2025



Advanced CyberSecurity for *"Internet of Things"* with AI & Machine Learning

21stC Cybersecurity Trends
"CyberVision: 2015-2025"
- Integrated, Adaptive & Intelligent Security –
Dr David E. Probert

Cybersecurity Trends and CyberVisio…
5 months ago, 106 slides
👁 656 ♥ 4 💬 0 ⬇ 51

* 21stC Cybersecurity Trends (2) *
"Advanced Cybersecurity"
- Artificial Intelligence & Machine Learning -
Dr David E. Probert
VAZA International

Artificial Intelligence and Machine Le…
7 months ago, 92 slides
👁 1004 ♥ 2 💬 0 ⬇ 63

* 21stC Cybersecurity Trends (1) *
"Integrated Security"
- Securing the Internet of Things –
Dr David E. Probert
VAZA International

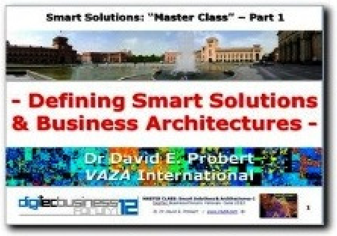
Integrated Cybersecurity and the Inte…
7 months ago, 99 slides
👁 463 ♥ 0 💬 0 ⬇ 40

Web: www.slideshare.net/DrDavidProbert/

Download Presentation Slides:
www.Valentina.net/Prague2016/

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

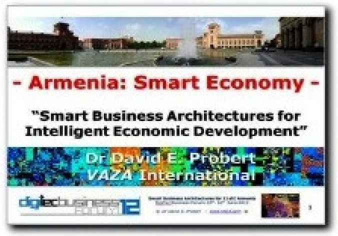
"Master Class - Smart Theory & Practice

Smart Solutions: "Master Class" – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

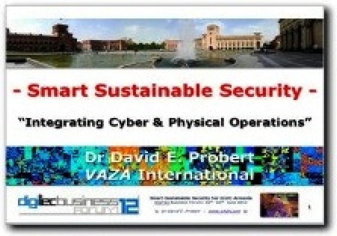
"Master Class 2012 - Smart Design"


- 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 & "Electronic Diaspora" : Securing Government & Enterprise Operations ***

"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

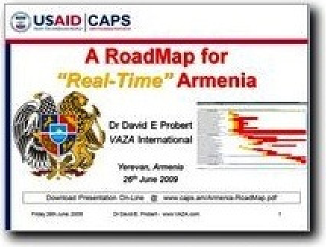
Awesome Armenia: In Photos

"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

Download Presentation On-Line @ www.caps.am/Armenia-RoadMap.pdf

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"

"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

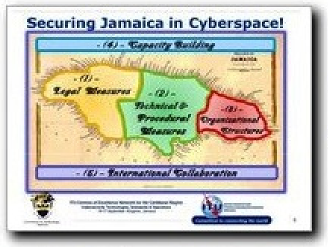
21stC Georgia – "Cyber Vardzia"

"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

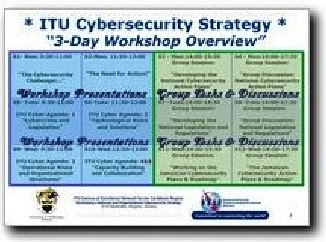
- (1) - Legal Measures

- (2) - Technical & Procedural Measures

- (3) - Organizational Structures

- (5) - International Collaboration

Jamaica: Cybersecurity Technology- Slides


* ITU Cybersecurity Strategy *
"3-Day Workshop Overview"

Workshop Presentations

Group Tasks & Discussions

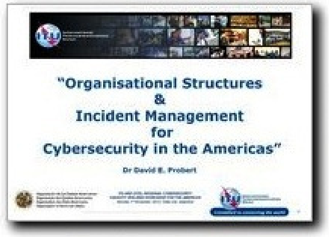
Workshop Presentations

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.

- ***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 -

Smart Solutions: “Master Class” – Part 1

- Defining Smart Solutions & Business Architectures -

Dr David E. Probert
VAZA International

"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 Practice"

Smart Solutions: “Master Class” – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

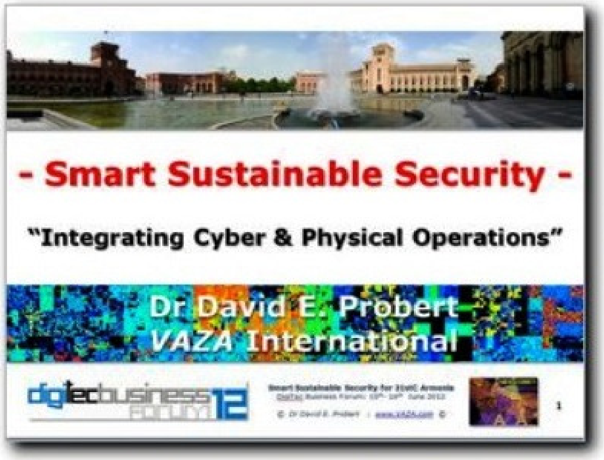
"Master Class - Smart Design"

- Armenia: Smart Economy -

“Smart Business Architectures for Intelligent Economic Development”

Dr David E. Probert
VAZA International

"Armenia: Smart Economy"



- Smart Sustainable Security -

“Integrating Cyber & Physical Operations”

Dr David E. Probert
VAZA International

"Armenia: Smart Sustainable Security"

- Smart Governance -

“Stimulating Innovation & Economic Growth”

Dr David E. Probert
VAZA International

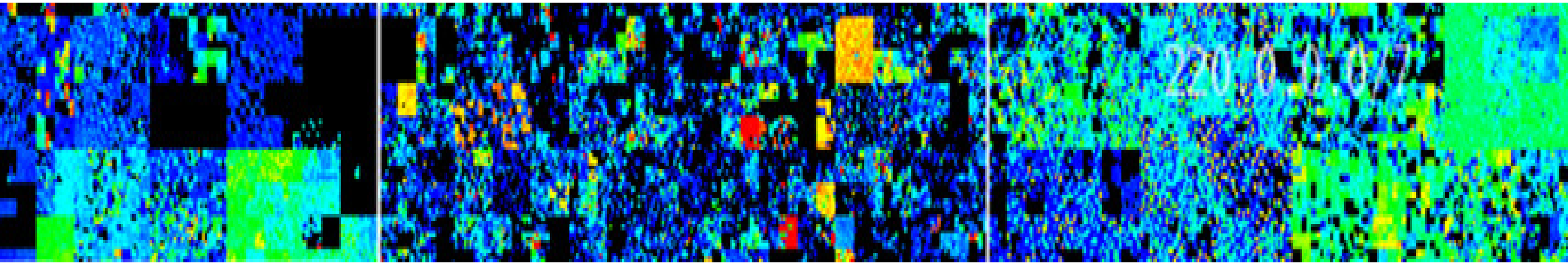
"Armenia: Smart Governance"

Download: www.valentina.net/DigiTec2012/

Energising YOUR Cybersecurity with *"Biometrics & Forensics"*

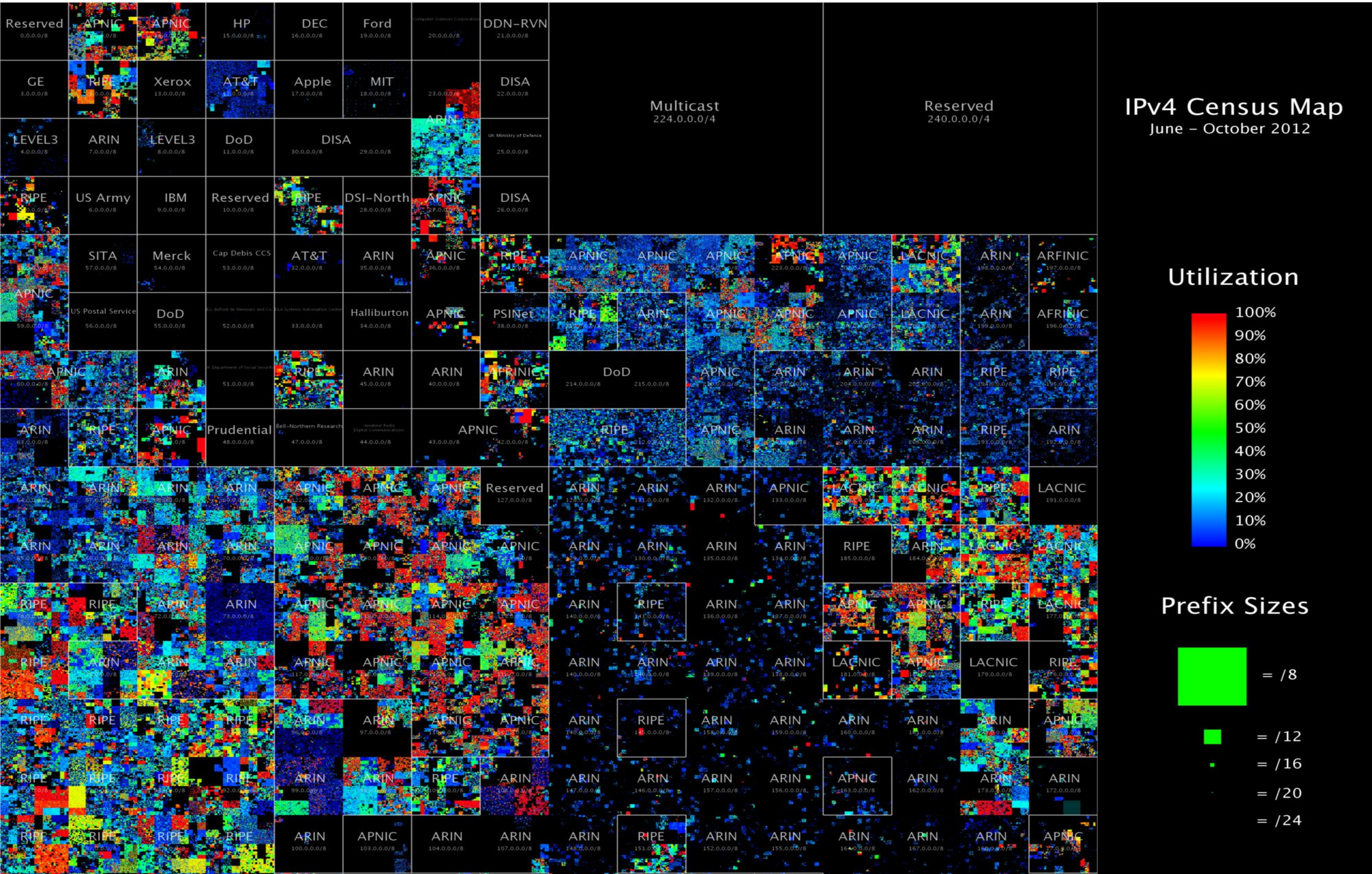
East-West Security Conference: Prague, Czech Republic

BACK-UP SLIDES



IPv4 Census Map

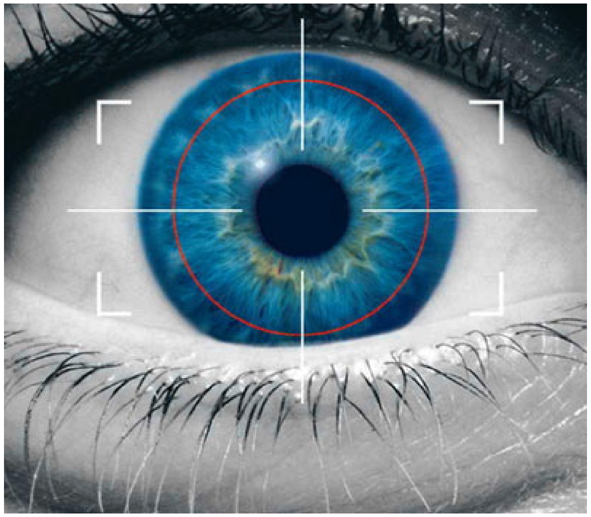
June – October 2012



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

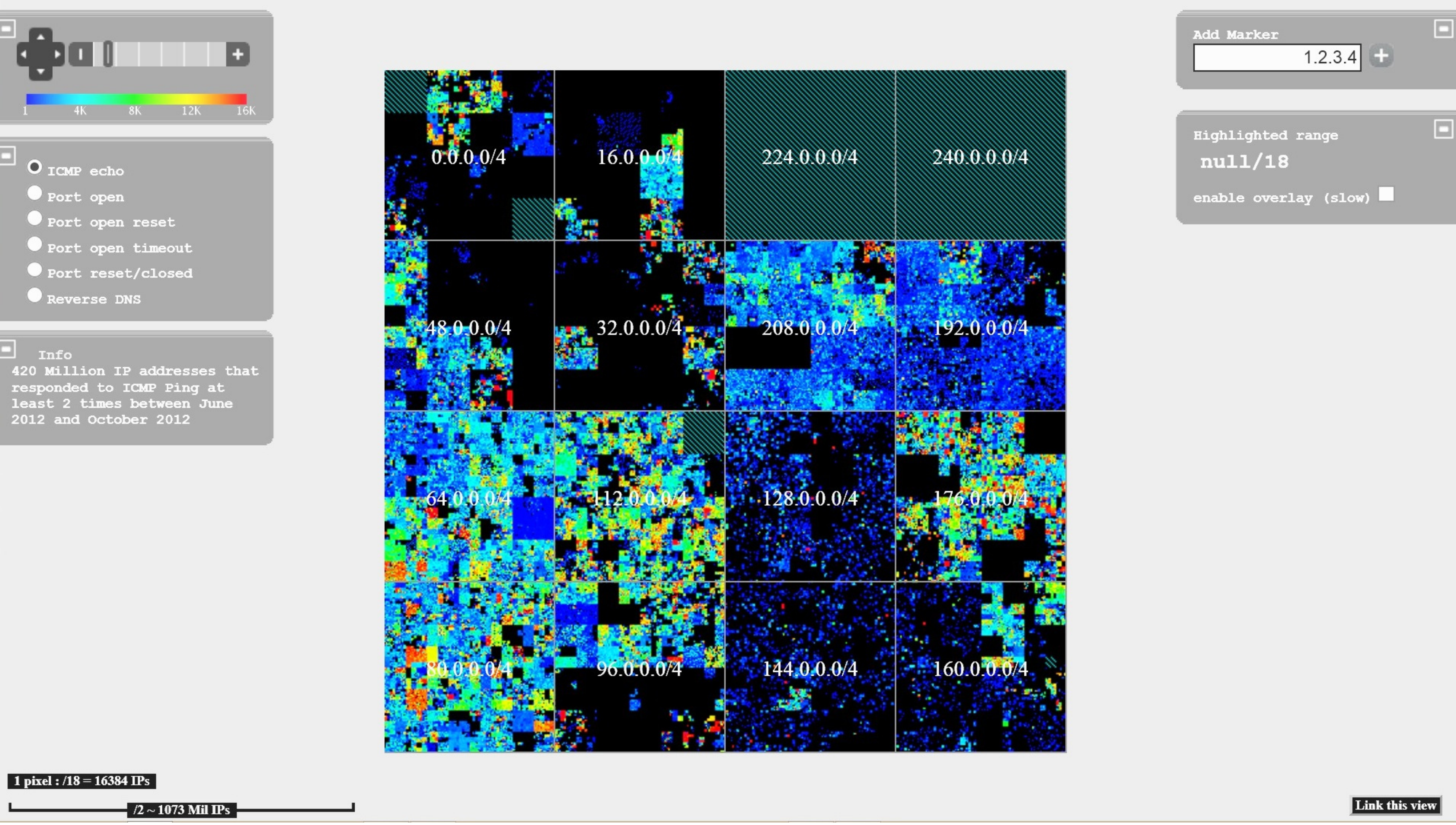
Biometrics & *RFID* Security Applications

- ***Biometrics*** techniques may include:
  - Finger and Palm Prints
  - Retinal and Iris Scans
  - 3D Vein ID
  - Voice Scans & Recognition
  - DNA Database – Criminal Records
  - 3D Facial Recognition



- ***RFID =*** Radio Frequency ID with applications that include:
  - Personal ID Cards for Building, Secure Facility Access
  - Tags for Retail Articles as a Deterrence to Shoplifting
  - Powered RFID Tags for Vehicles to open Doors, Barriers & Switch Lights
  - Plans to use RFID Tags for Perishable Products such as Fruit & Vegetables
  - Asset Tags to manage the movement of High-Value & Strategic Assets
  - Potential for Embedded Intelligent RFID Devices into Humans

Cyberspace Browser: *Internet Census 2012*



● 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

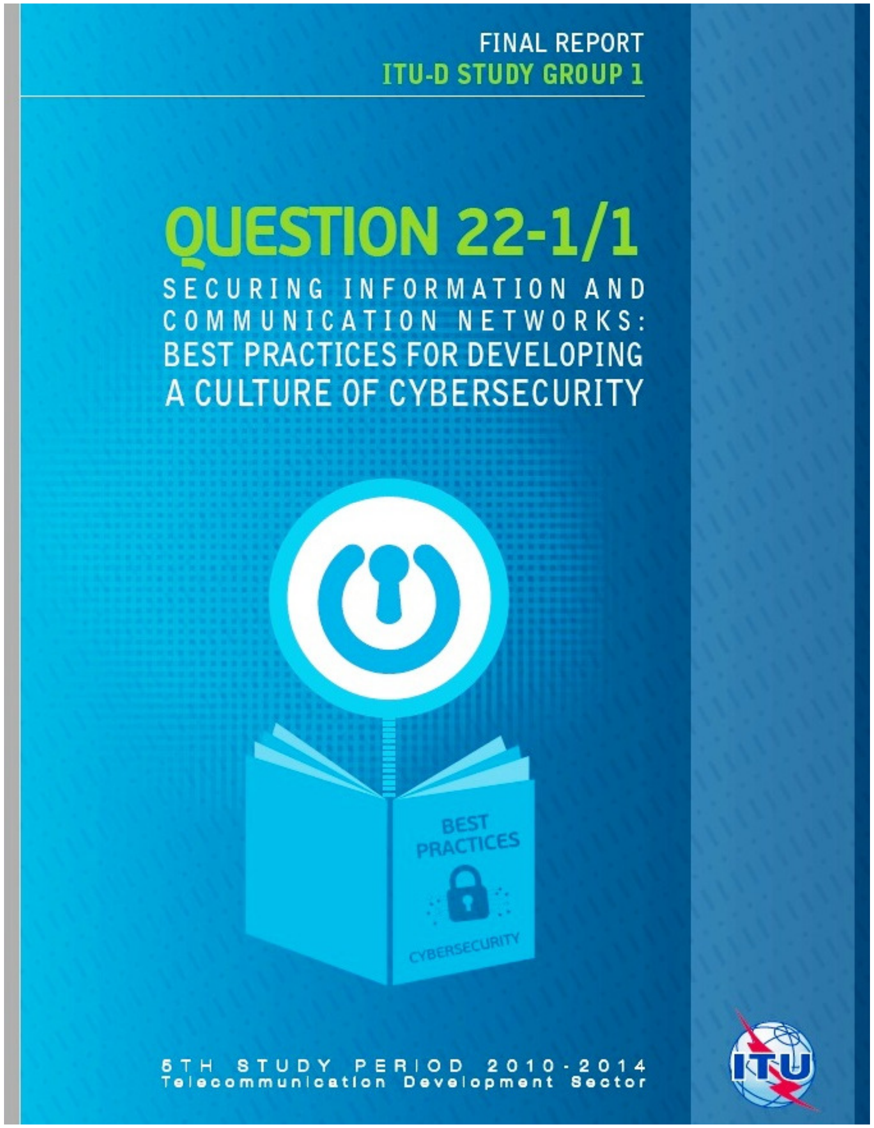
Highlighted range
null/18
enable overlay (slow) □

1 pixel : /18 = 16384 IPs

/2 ~ 1073 Mil IPs

- UN/ITU *CyberSecurity* Agenda -

Best Practice for CyberSecurity Culture

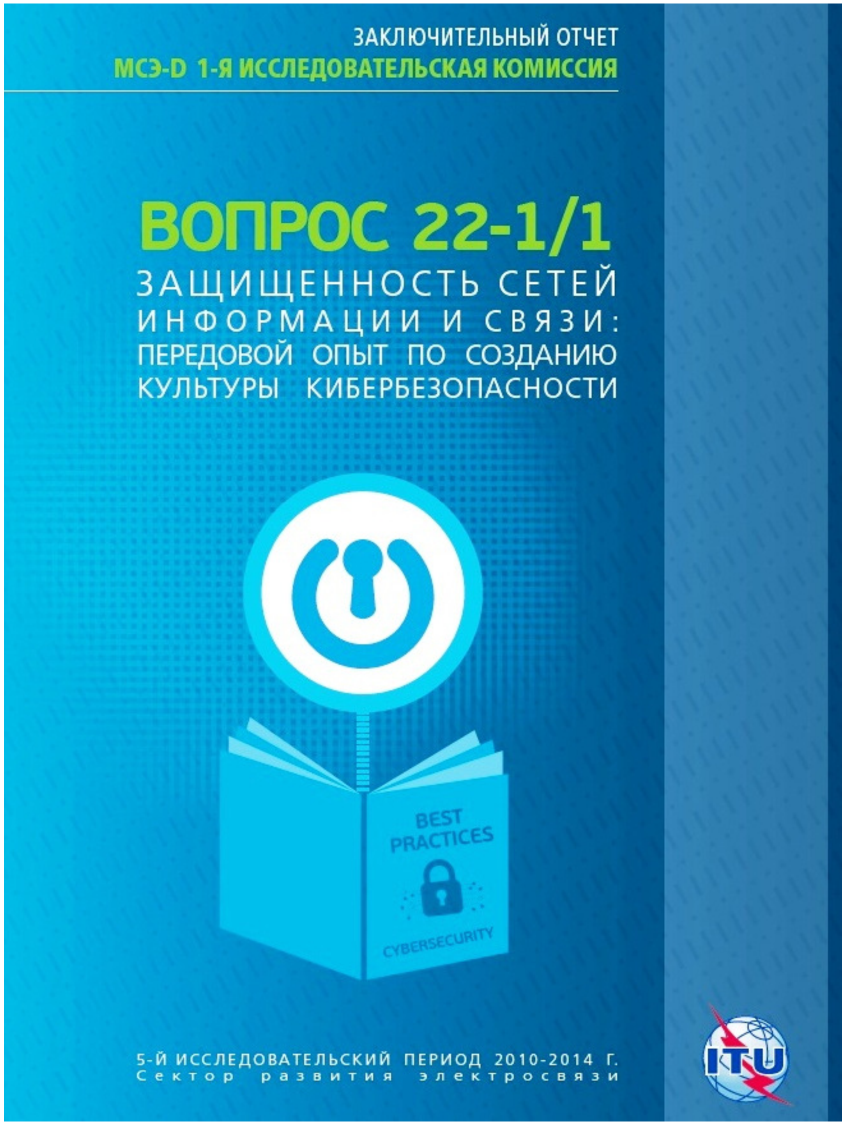


FINAL REPORT
ITU-D STUDY GROUP 1

QUESTION 22-1/1

SECURING INFORMATION AND COMMUNICATION NETWORKS: BEST PRACTICES FOR DEVELOPING A CULTURE OF CYBERSECURITY

5TH STUDY PERIOD 2010-2014
Telecommunication Development Sector



ЗАКЛЮЧИТЕЛЬНЫЙ ОТЧЕТ
МСЭ-D 1-Я ИССЛЕДОВАТЕЛЬСКАЯ КОМИССИЯ

ВОПРОС 22-1/1

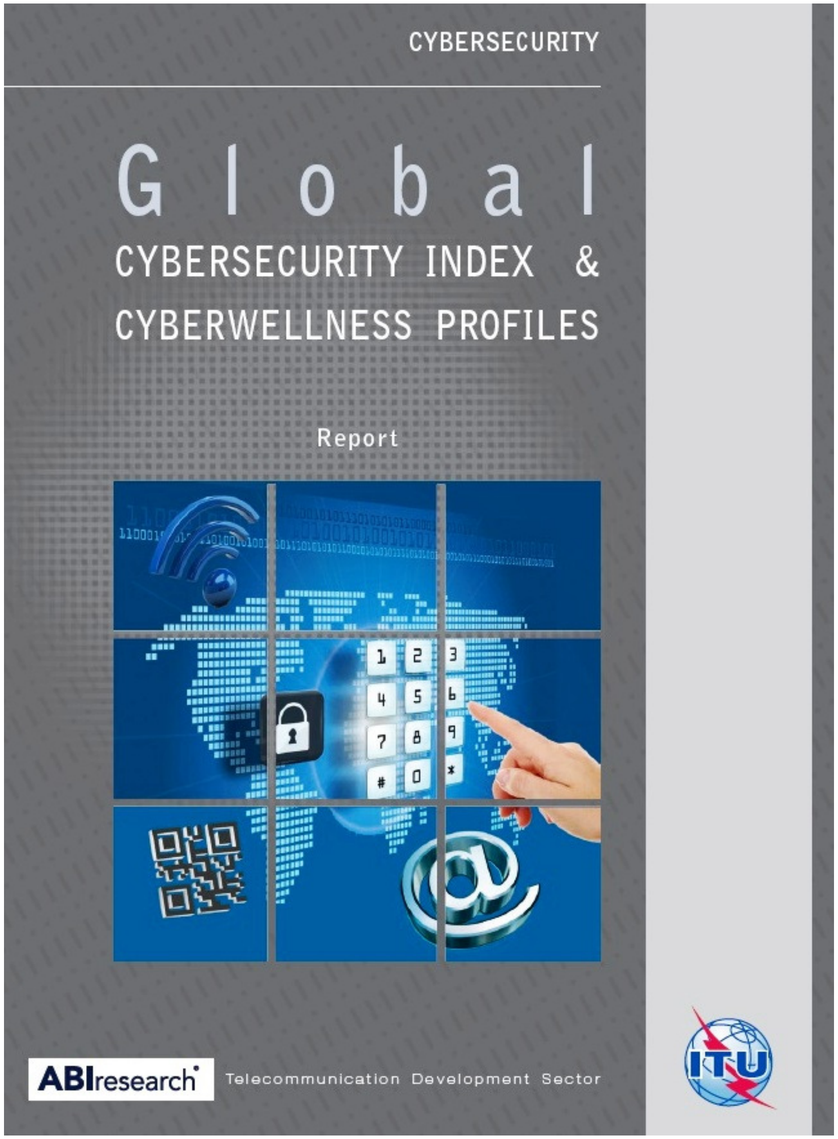
ЗАЩИЩЕННОСТЬ СЕТЕЙ ИНФОРМАЦИИ И СВЯЗИ: ПЕРЕДОВОЙ ОПЫТ ПО СОЗДАНИЮ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ

5-Й ИССЛЕДОВАТЕЛЬСКИЙ ПЕРИОД 2010-2014 Г.
Сектор развития электросвязи

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

- UN/ITU *CyberSecurity* Agenda –

Global CyberSecurity Index (Eng/Rus)



CYBERSECURITY

Global CYBERSECURITY INDEX & CYBERWELLNESS PROFILES

Report

ABIresearch Telecommunication Development Sector

ITU

КИБЕРБЕЗОПАСНОСТЬ

ГЛОБАЛЬНЫЙ ИНДЕКС КИБЕРБЕЗОПАСНОСТИ И ПРОФИЛИ ПО КИБЕРБЛАГОПОЛУЧИЮ

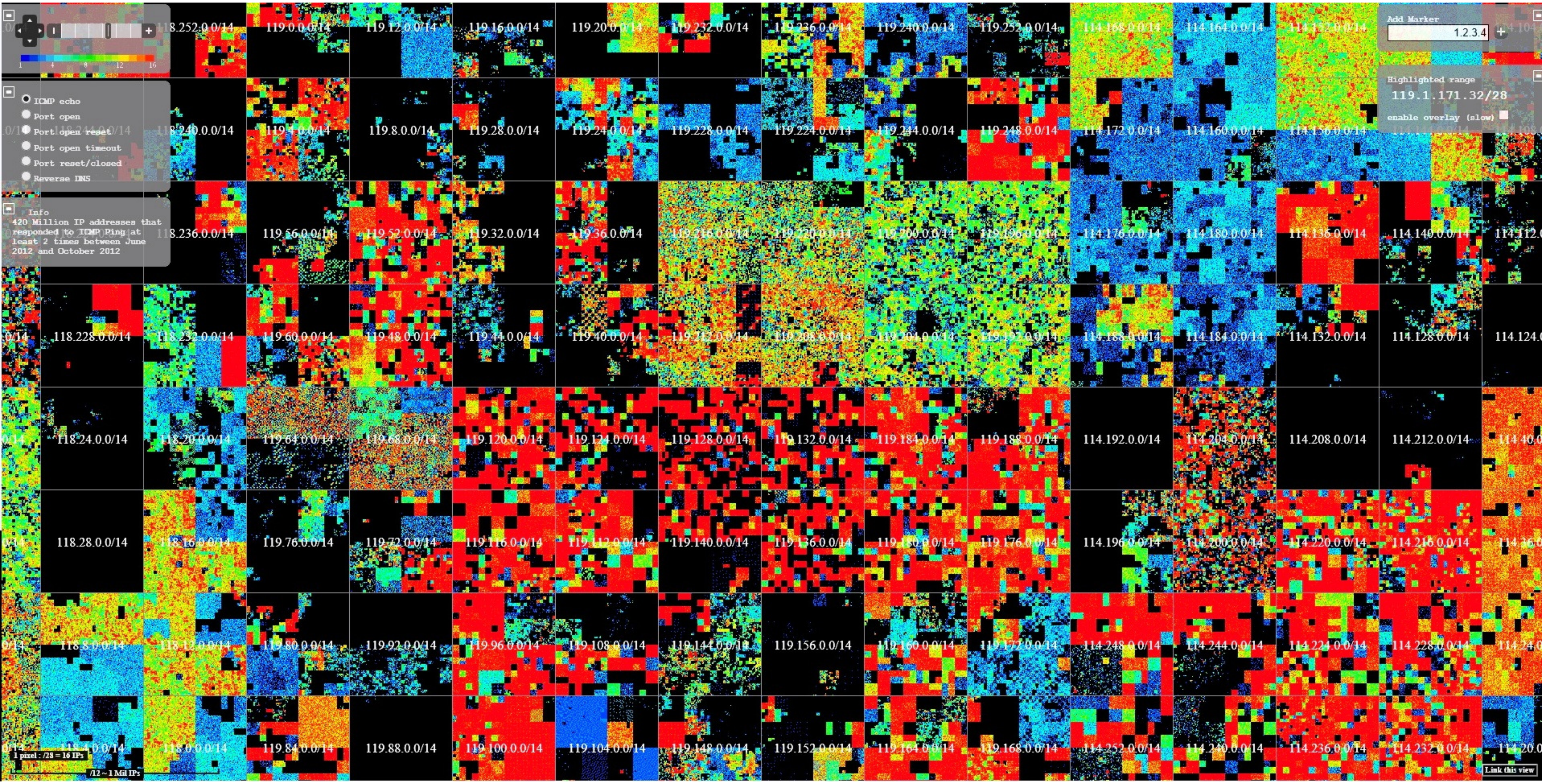
Отчет

ABIresearch Сектор развития электросвязи

ITU

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

Cyberspace (Hilbert Map): *Browser Zoom*



○ 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/