* 21stC Cybersecurity Trends (1) *

“Integrated Security”

- Securing the Internet of Things –

Dr David E. Probert

***VAZA* International**

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

32nd International East/West Security Conference

“Integrated Cyber-Physical Security and Securing the Enterprise Internet of Things”
- Madrid, Spain: 26th–27th Oct 2915 -
© *Dr David E. Probert* : *www.VAZA.com* ©

21stC кибербезопасности Тенденции (1)

интегрированная безопасность

- Защита Интернет вещей -

Dr David E. Probert

VAZA International

Cybersecurity Trends – *“Dual Themes”*

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

* 21stC Cybersecurity Trends (1) *

“Integrated Security”

- Securing the Internet of Things –

Dr David E. Probert

VAZA International

Dedicated to

32nd International East/West Security Conference

“Integrated Cyber-Physical Security and Securing the Enterprise Internet of Things”

- Madrid, Spain: 26th–27th Oct 2015 -

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

1

- *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”*

* 21stC Cybersecurity Trends (2) *

“Advanced Cybersecurity”

- Artificial Intelligence & Machine Learning -

Dr David E. Probert

VAZA International

Dedicated to

32nd International East/West Security Conference

“Advanced Enterprise Cybersecurity – Artificial Intelligence & Machine Learning”

Madrid, Spain: 26th – 27th Oct 2015

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

1

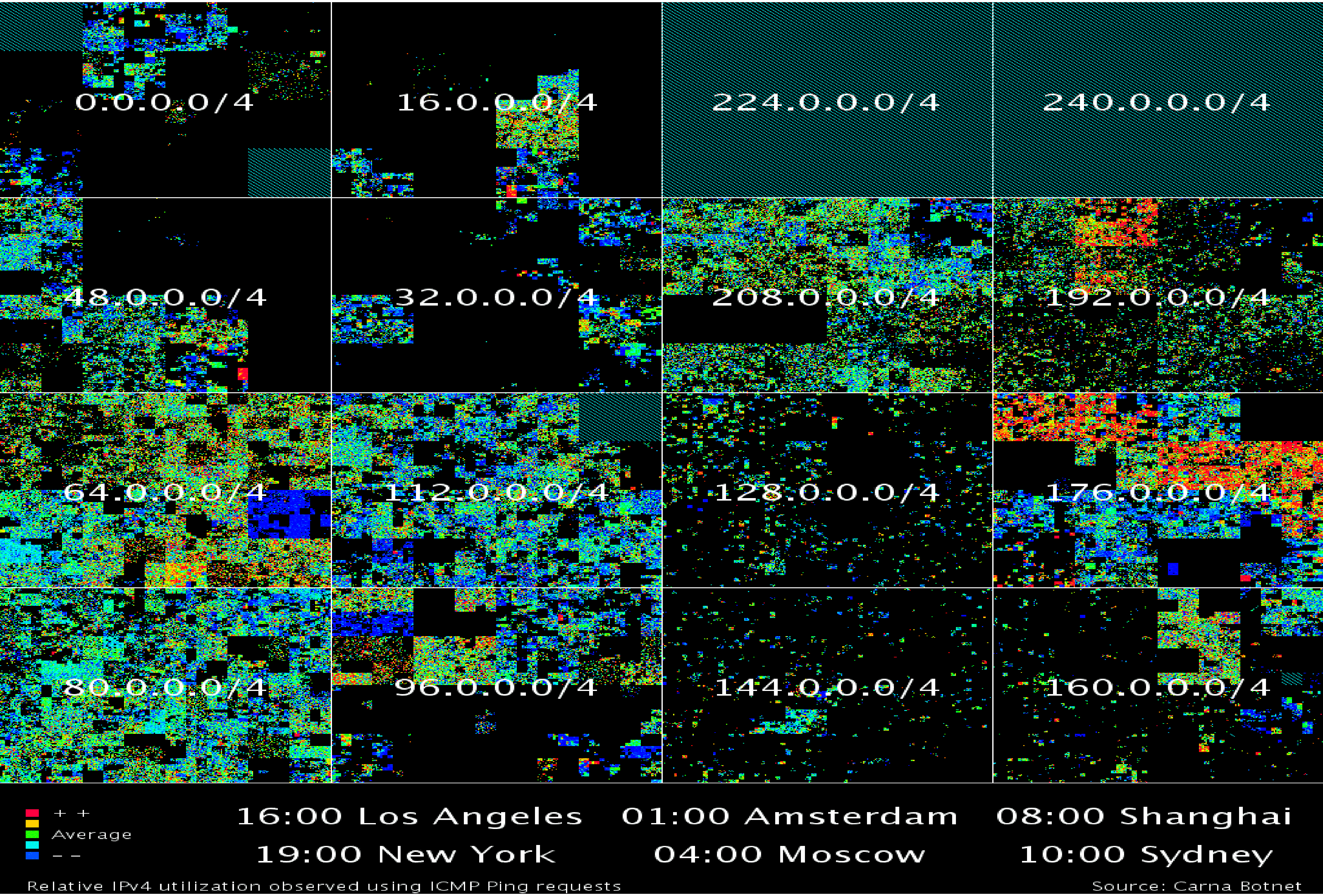
- *Transition from 20thC Security to Hybrid AI-Based 21stC Cyber Models*
- *Using AI & Machine Learning to protect your Enterprise Operations*
- *Developing YOUR Action Plans for Advanced Cybersecurity Solutions!*

“Intelligence”: ”Real-Time Self-Adaptive Cybersecurity” ***11:15 – 27th Oct 2015***

Download Slides: www.valentina.net/Madrid2015/

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

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



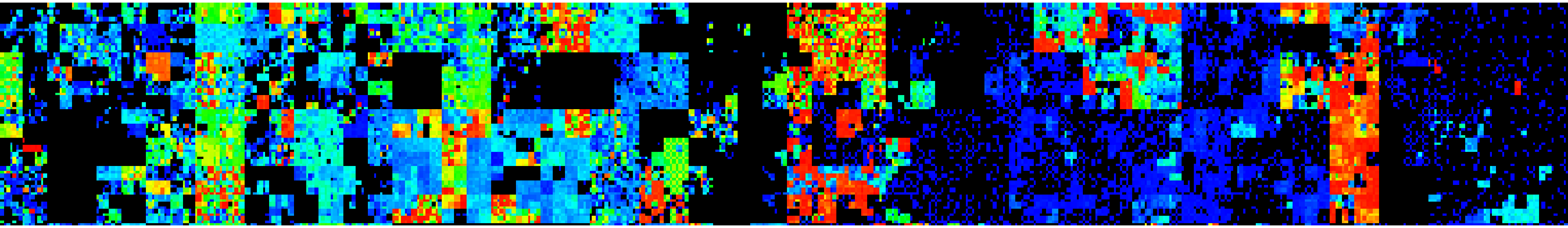
Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet

Global IPv4 Internet Servers: 24/7

21stC Cybersecurity (1) – *"Integrated Security"*

1 – Background: *"21sr Security Landscape"*	2 – Cybersecurity: Players & Threats	3 – Cyber-Physical Threat Scenarios
4 –Banking & Finance: Hybrid Cybersecurity	5 – CSO: Board Level Security Integration	6 – The Enterprise Internet of Things (IoT)
7 – Cyber-Physical Threats from the "IoT"	8 – Practical Solutions for IoT Security	9 –YOUR TOP 10 Actions & RoadMap



Background: *21stC Security Landscape*

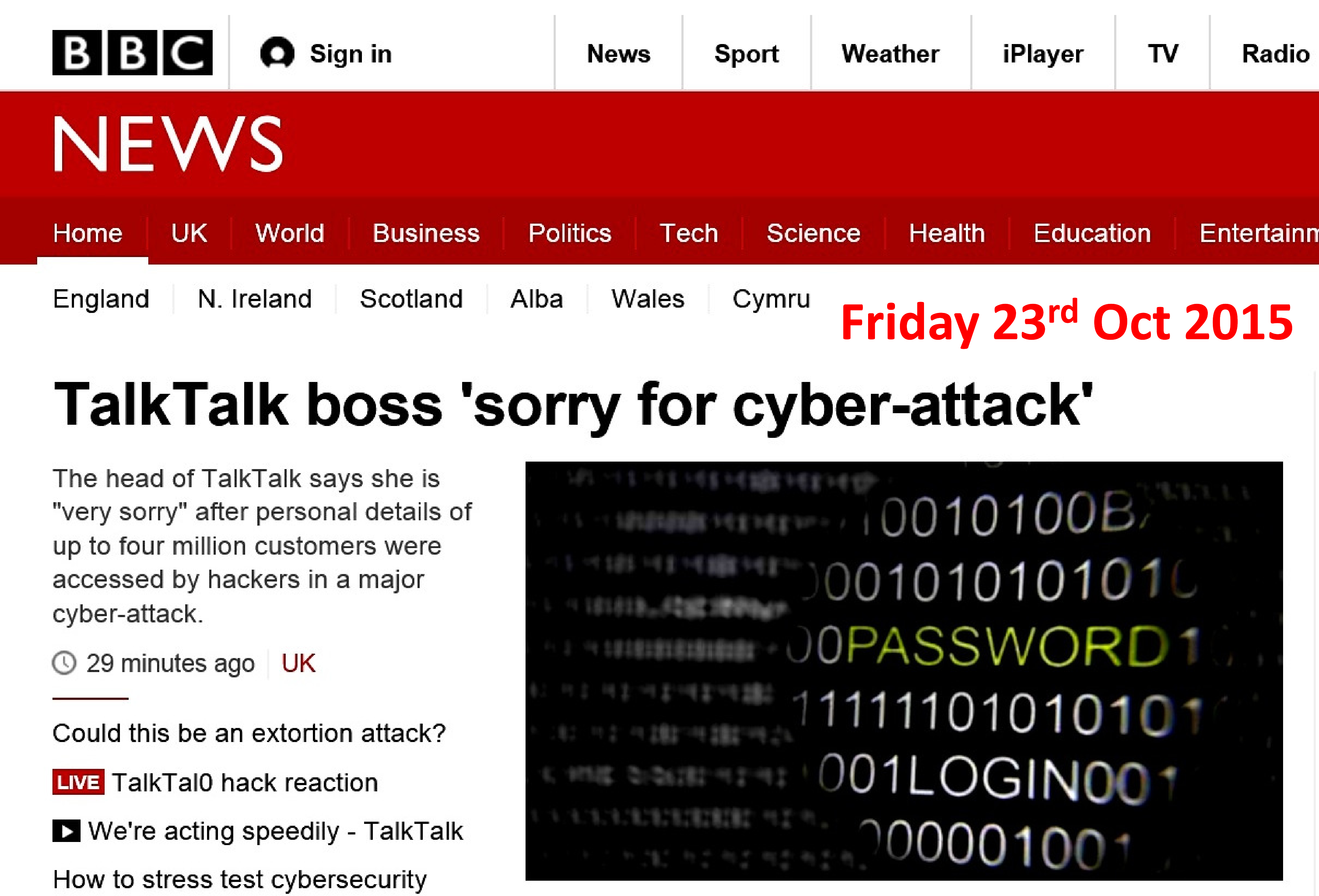
- Convergence of Physical & Cybersecurity Ops
- "Cyber" migrates from IT Dept to Main Board
- Global Real-Time Targeted Cyber Attacks – 24/7
- Transition from 20thC Tools (Firewalls & Anti-virus) to 21stC Tools (AI & Machine Learning)
- Emergence of Corporate "Internet of Things"
- Evolution of Smart Devices, Cities & Economy
- Dramatic increase in Cybercrime & CyberTerror

21stC Cybersecurity *"Threats & Trends"*

- *20 Year* Evolution of CyberCrime & CyberTerror: *1995-2015*

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

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



Friday 23rd Oct 2015

TalkTalk boss 'sorry for cyber-attack'

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

29 minutes ago | UK

Could this be an extortion attack?

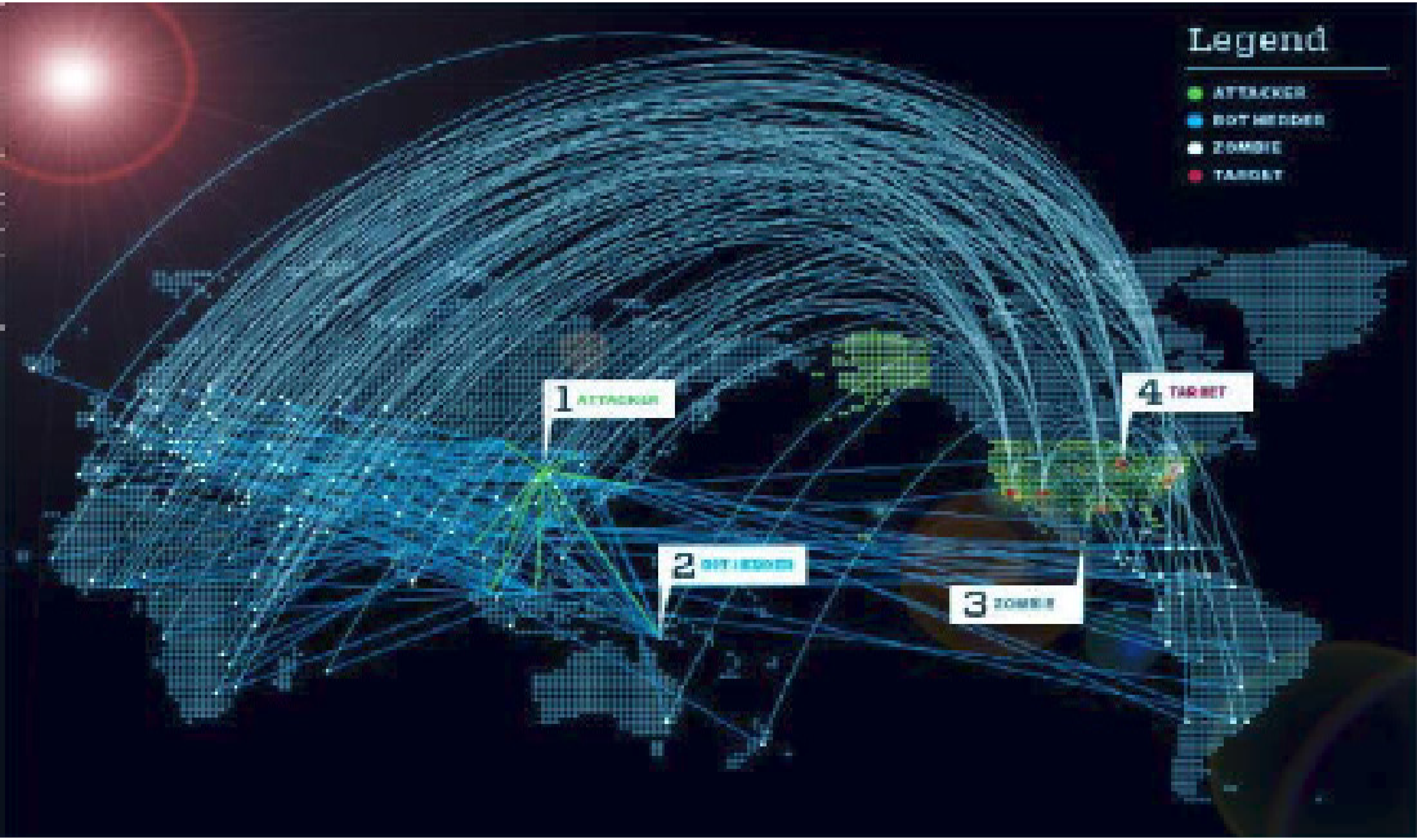
LIVE TalkTal0 hack reaction

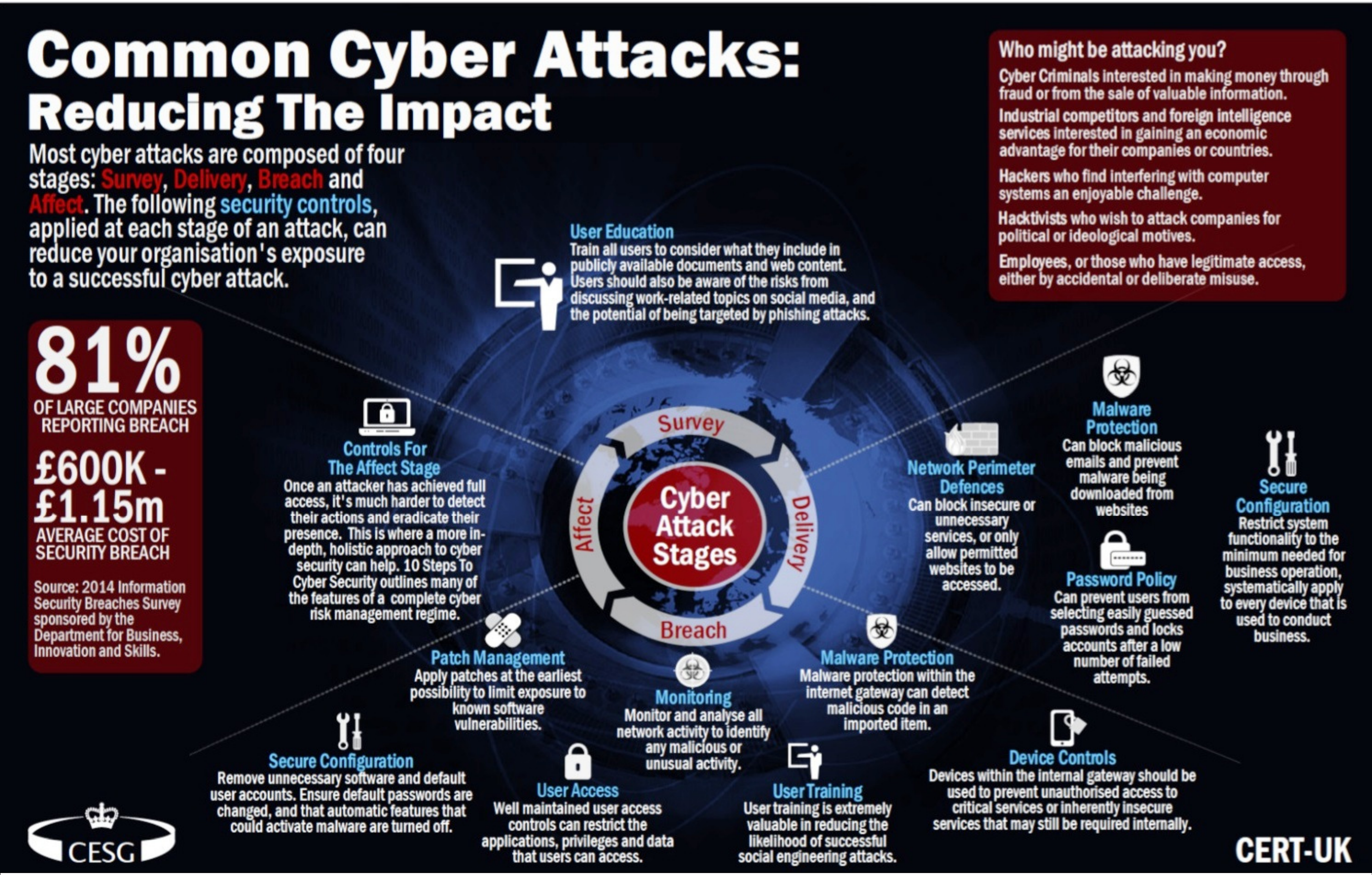
▶ We're acting speedily - TalkTalk

How to stress test cybersecurity

Major Cyber-Attack UK Internet Service Provider

Typical Global *"Botnet"* Cyber Attack





Common Cyber Attacks: Reducing The Impact

Most cyber attacks are composed of four stages: Survey, Delivery, Breach and Affect. The following security controls, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

81% OF LARGE COMPANIES REPORTING BREACH

£600K - £1.15m AVERAGE COST OF SECURITY BREACH

Source: 2014 Information Security Breaches Survey sponsored by the Department for Business, Innovation and Skills.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

User Education
Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Controls For The Affect Stage
Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help. 10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.

Network Perimeter Defences
Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection
Can block malicious emails and prevent malware being downloaded from websites

Password Policy
Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Secure Configuration
Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

Patch Management
Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring
Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection
Malware protection within the internet gateway can detect malicious code in an imported item.

Secure Configuration
Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access
Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training
User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls
Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

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

Command & Control (C2) *Malware* Servers

- *"Global 21st Century **Cyber-Colonisation**"* -

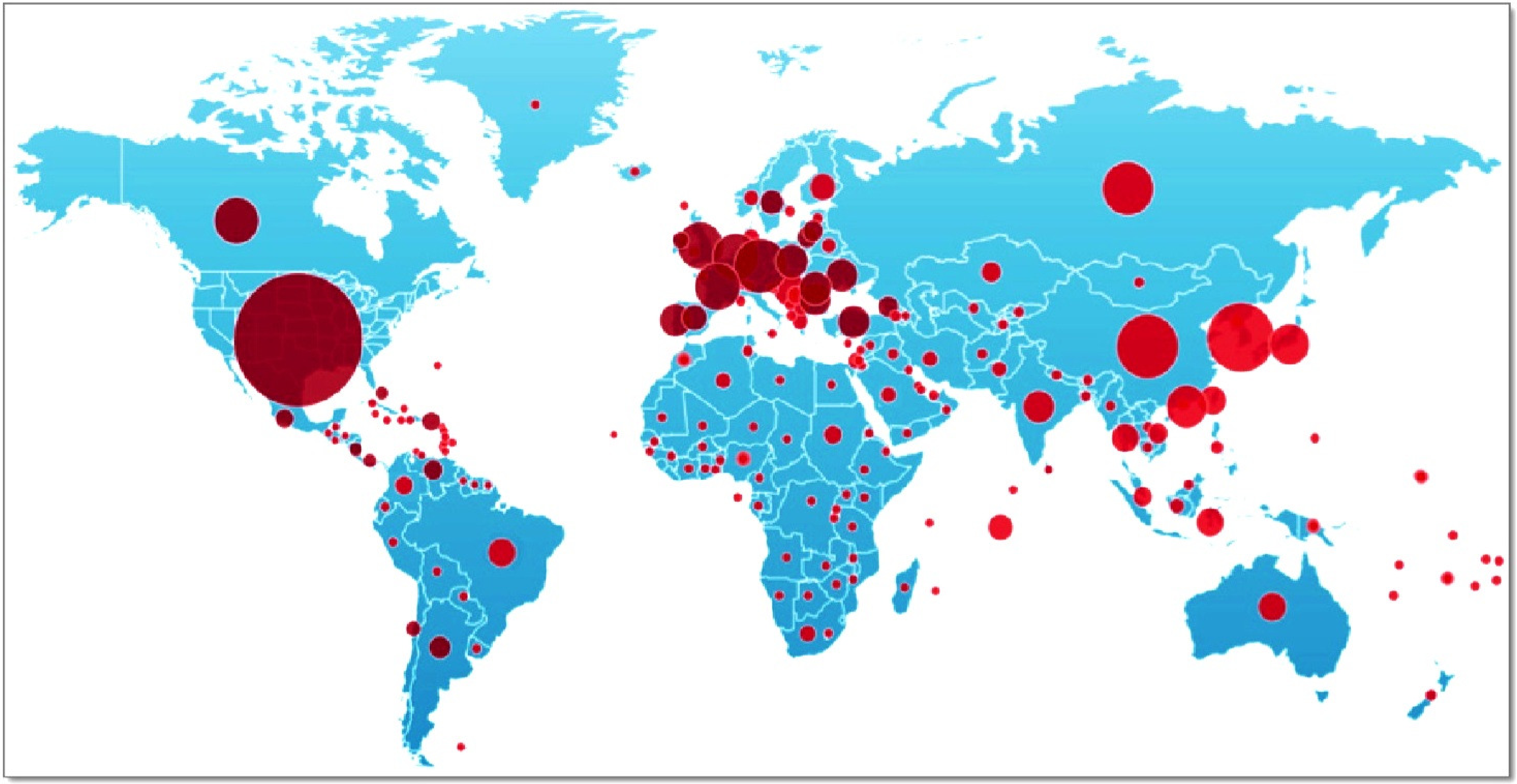
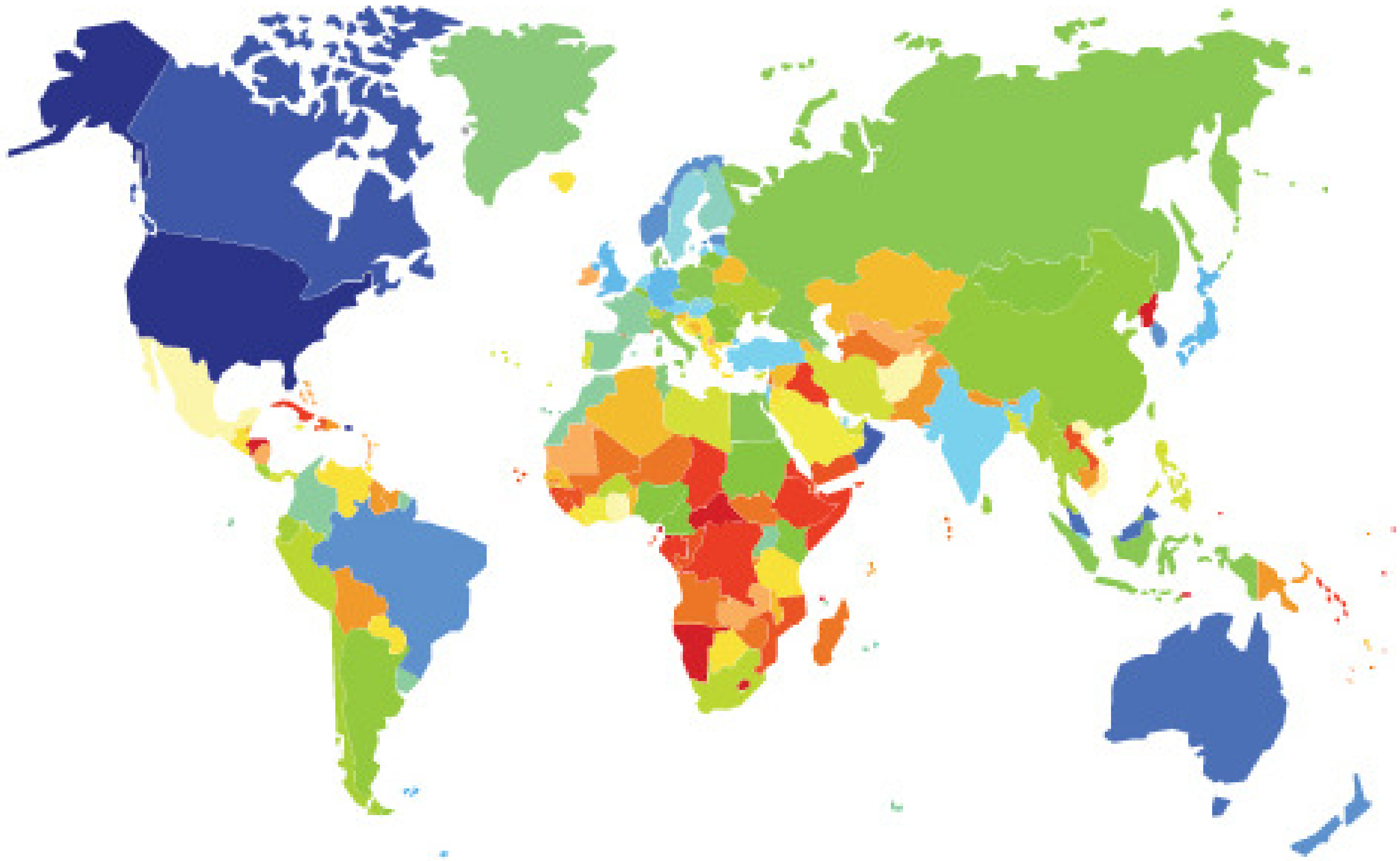


Image: www.fireeye.com – FireEye Inc (c)

UN/ITU – Global Cybersecurity Index (Dec 2014)



ABIresearch

ITU

Global Cybersecurity Index

National Cybersecurity Commitment HIGHEST LOWEST

Typical C2 ***Malware*** Signatures

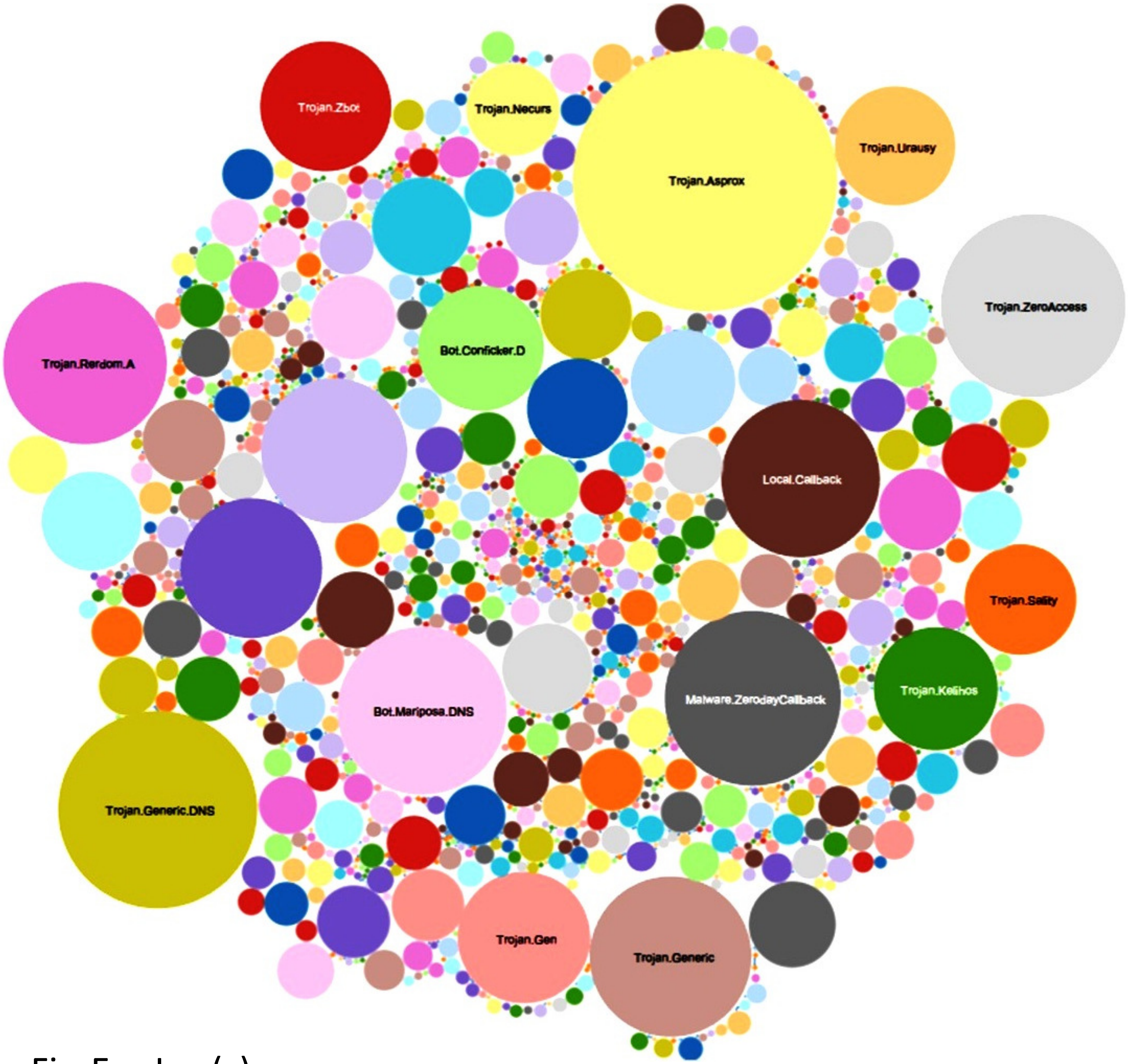
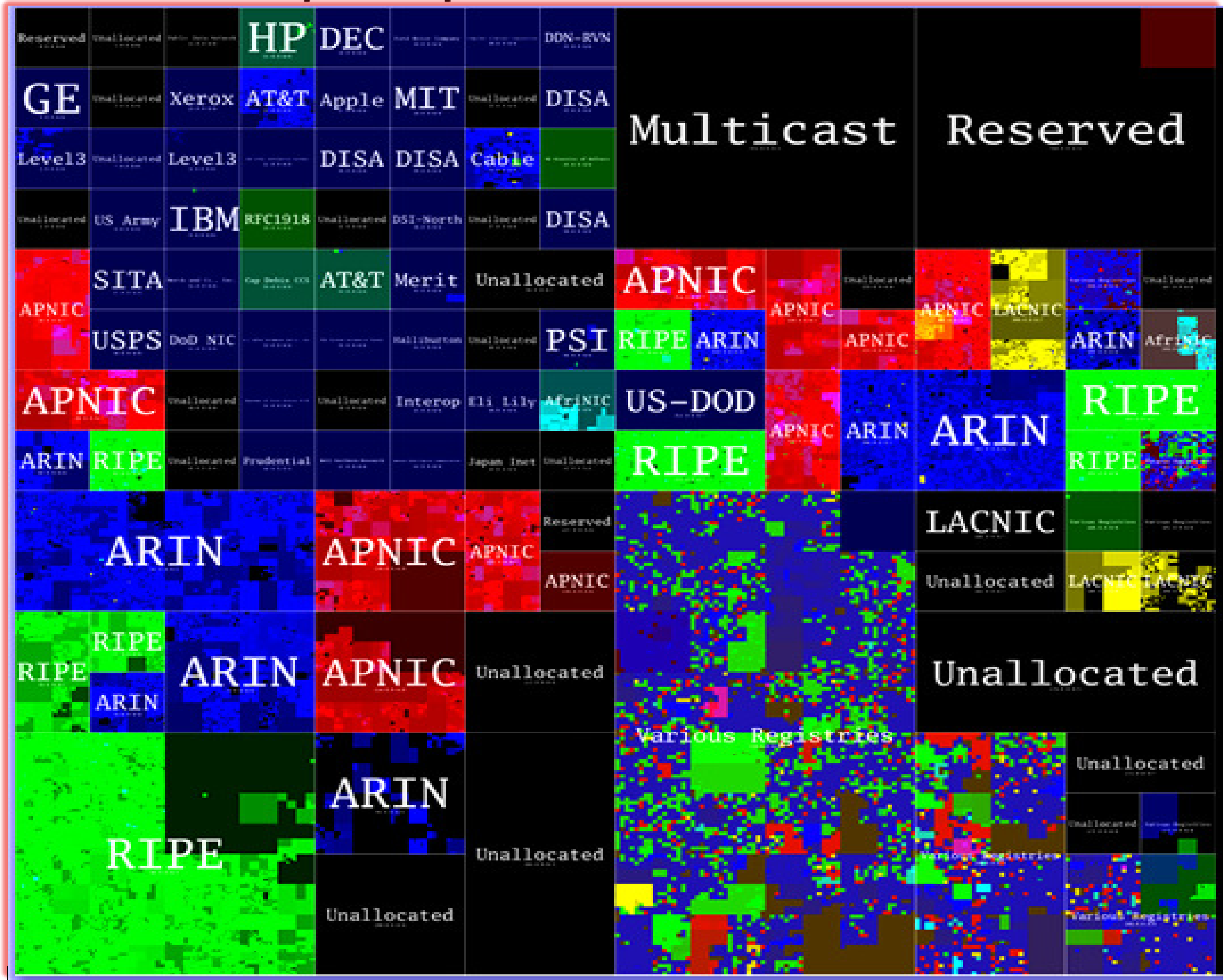


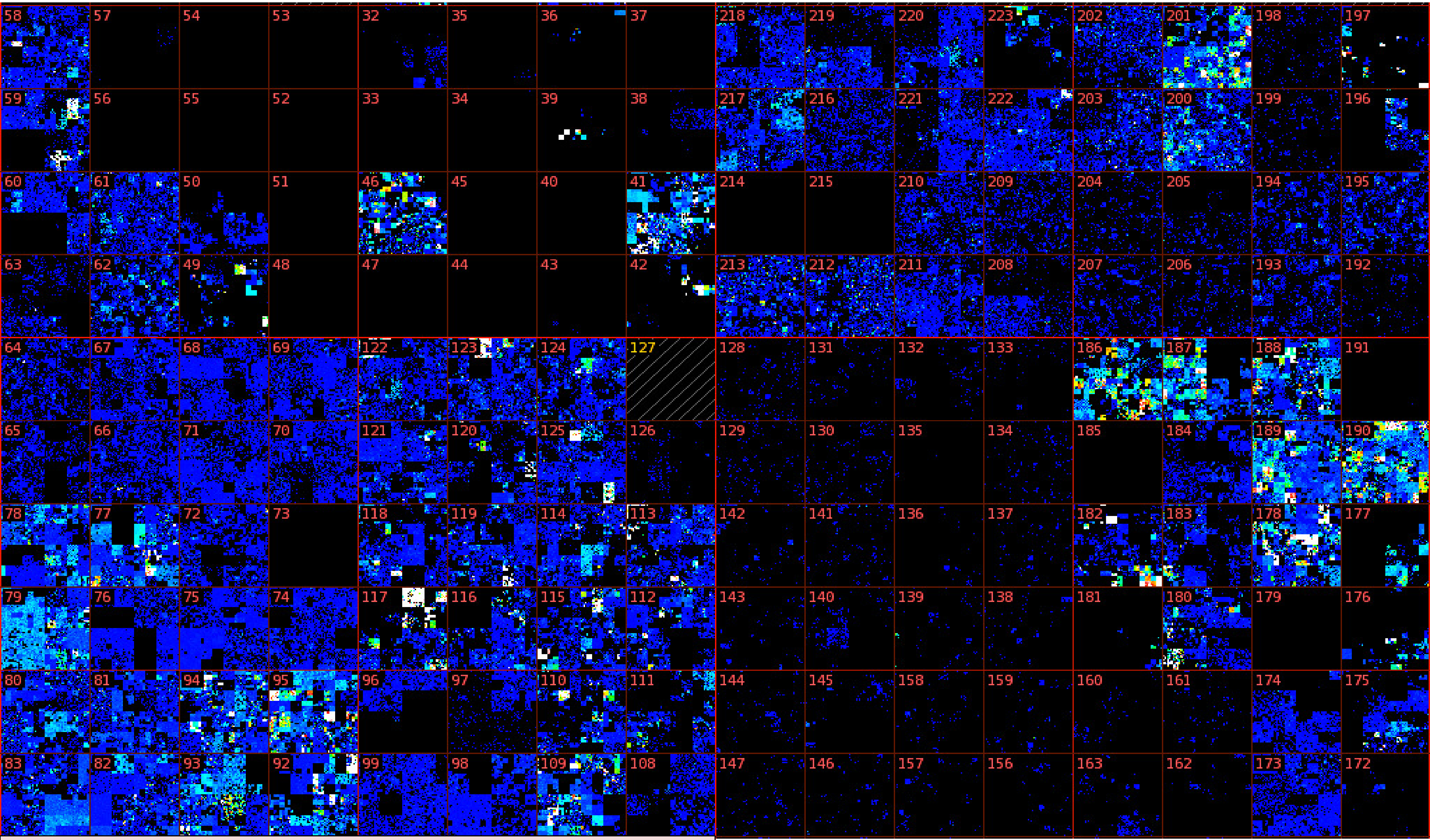
Image: www.fireeye.com – FireEye Inc (c)

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



...From 20thC Physical World To 21stC Cyberspace! ...

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



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

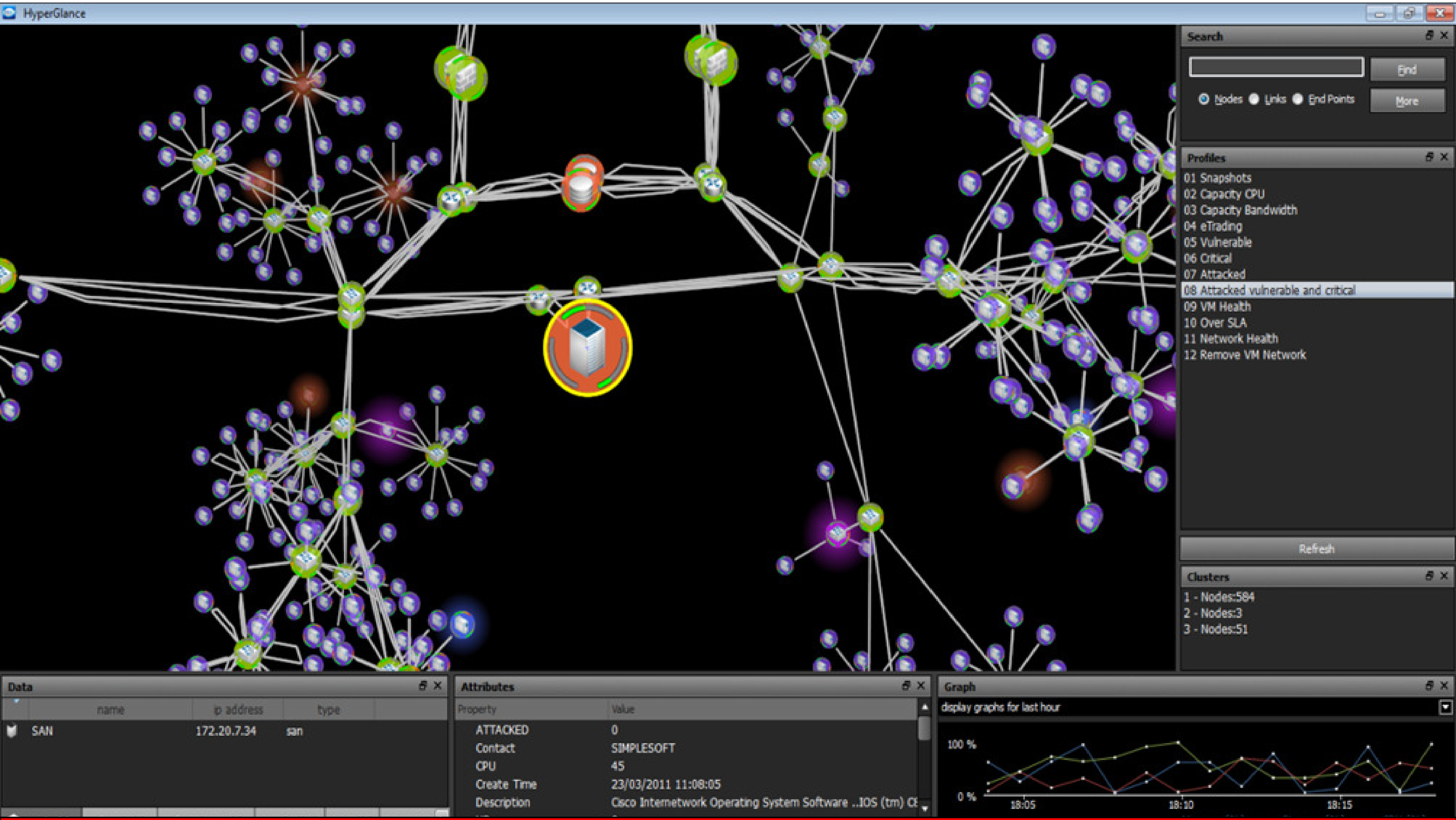
Contrast between our Physical & Cyber Worlds

Convergence to 21stC "Intelligent Worlds" will take time!

Physical World = "Space"	Cyber World = "Time"
Top-Down	Bottom-Up
Dynamic	Self-Organising
Secrecy	Transparency
Territorial – "Geographical Space"	Global – "Real-Time"
Government Power	Citizen Power
Control	Freedom
Direct	Proxy
Padlocks & Keys	Passwords & Pins
Convergent	Divergent
Hierarchical	Organic
Carbon Life	Silicon Life
Tanks & Missiles	Cyber Weapons & "Botnets"
Mass Media	Social Media

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

Smart 3D Network Modelling: *Hyperglance*



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

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

Data

name	ip address	type
SAN	172.20.7.34	san

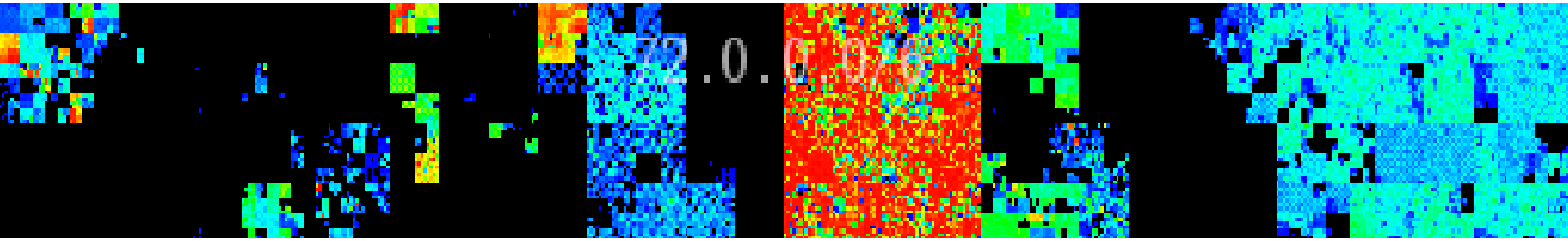
Attributes

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

Hyperglance Real-Time IT Modelling & Visualisation Software - Intergence.Com - *Cambridge, UK*

21stC Cybersecurity (1) – *“Integrated Security”*

1 – Background: *“21stC Security Landscape”*	2 – Cybersecurity :Players and Targets	3 – Cyber-Physical Threat Scenarios
4 –Banking & Finance: Hybrid Cybersecurity	5 – CSO: Board Level Security Integration	6 – The Enterprise Internet of Things (IoT)
7 – Cyber-Physical Threats from the “IoT”	8 – Practical Solutions for IoT Security	9 – YOUR TOP 10 Actions & RoadMap



Cybersecurity: *Players and Targets*

- **"Bad Guys Threats":** Cyber-Criminals, Cyber-Terrorists, Political Activists, Cyber-Espionage.
- **"Good Guy Targets":** Critical Information Sectors – Financial Services, Government, Military, Energy, Transportation, Telecommunications, Social Media, Healthcare, Education......

......**Targets** are often high-traffic websites with massive databases of financial & political interest – such as **Banks, Social Media & Government**

CyberCrime, CyberTerrorism & Espionage

- ***Profit:*** Cybercrime is generally for commercial gain and profit with focus on Financial Service Sector. It is now carried out on an *“Industrial Scale”* by IT Technically skilled criminal specialists as Global eCrime Business!

- ***Power:*** CyberTerror by Groups such as ISIS is executed to assert their “power”, develop their “brand” as well as to attract new “followers” through social media.

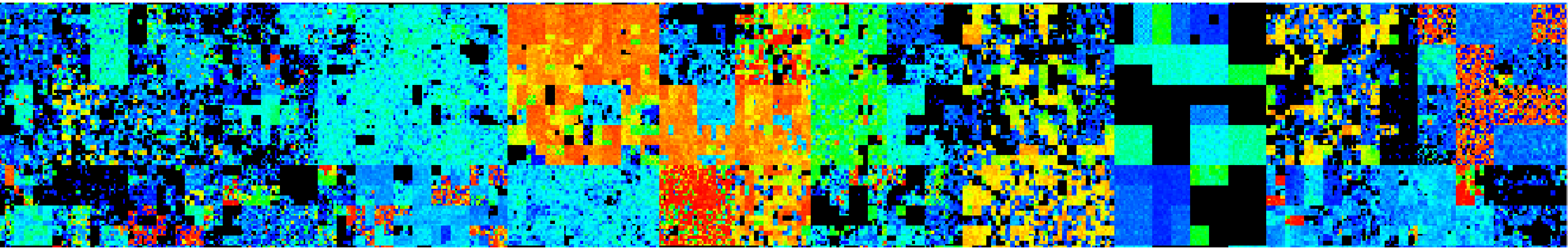
- ***Espionage:*** CyberEspionage Groups are now emerging to penetrate both commercial, government and military organisations around the globe.

Main Cyber Players and their Motives

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

21stC Cybersecurity (1) – *"Integrated Security"*

1 – Background: *"21stC Security Landscape"*	2 – Cybersecurity: Players & Targets	3 – Cyber-Physical Threat Scenarios
4 –Banking & Finance: Hybrid Cybersecurity	5 – CSO: Board Level Security Integration	6 – The Enterprise Internet of Things (IoT)
7 – Cyber-Physical Threats from the "IoT"	8 – Practical Solutions for IoT Security	9 – YOUR TOP 10 Actions & RoadMap



Cyber-Physical Threat Scenarios

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

"Cyber 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

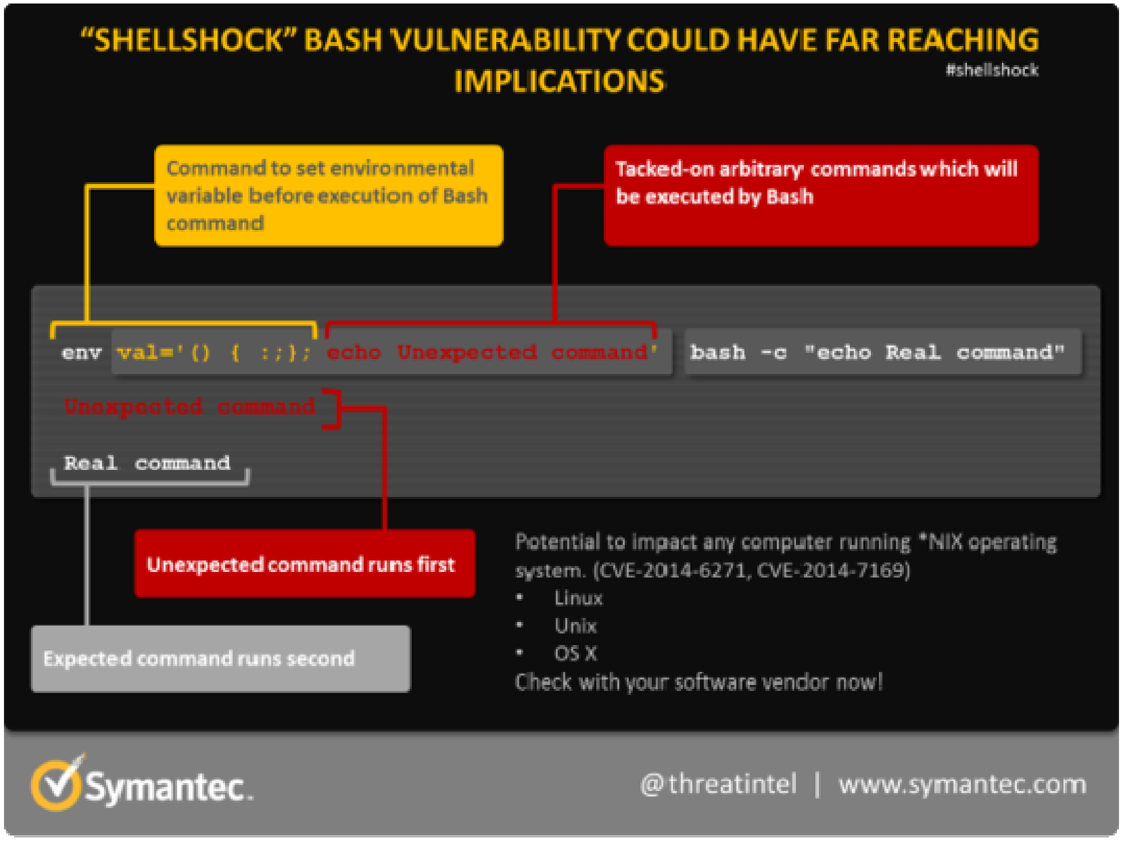
  - *Fake Maintenance Staff or Contractors:* A relatively easy way for criminals to access secure facilities, particularly in remote regions or developing countries is to fake their personnel IDs and CVs as being legitimate ICT maintenance staff or contractors

  - *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!

Recent Cyber Threats & Security Flaws

- *SHELLSHOCK* – Discovered *24th Sept 2014* – Security flaw in "Bash Software" that is present in the Apple Mac OS X, Unix and Linux. Allows execution of malicious code that could allow access to private data and remote control of server for orchestrated DDOS "BOT" attacks to targeted victim networks.



"SHELLSHOCK" BASH VULNERABILITY COULD HAVE FAR REACHING IMPLICATIONS

#shellshock

Command to set environmental variable before execution of Bash command

Tacked-on arbitrary commands which will be executed by Bash

```
env val='() { :;}; echo Unexpected command' bash -c "echo Real command"
Unexpected command
Real command
```

Unexpected command runs first

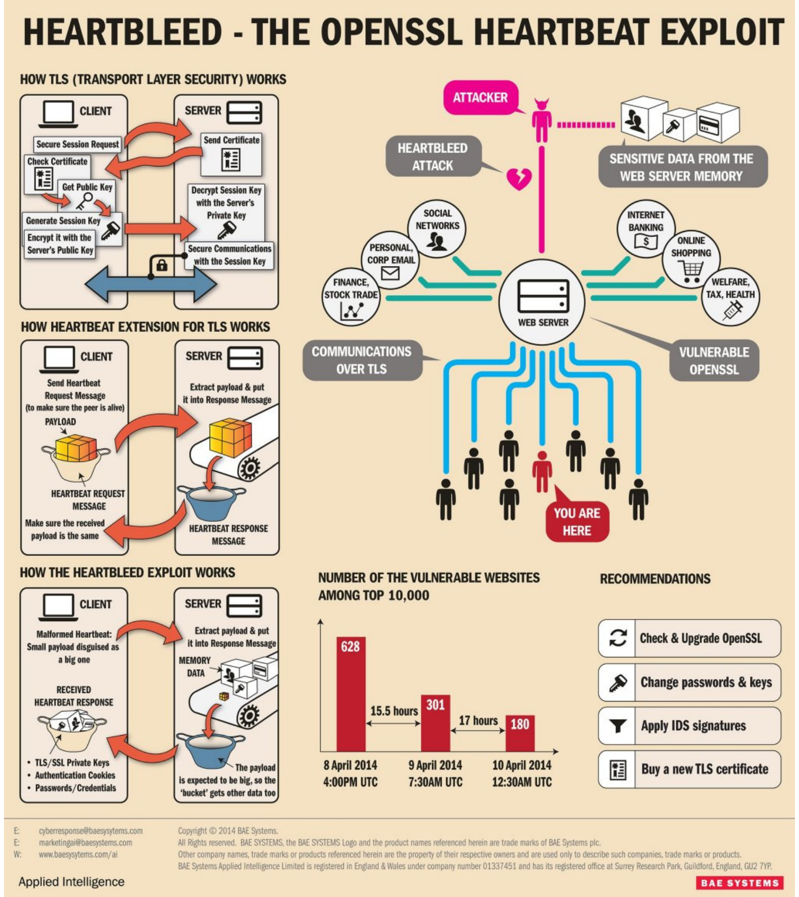
Expected command runs second

Potential to impact any computer running *NIX operating system. (CVE-2014-6271, CVE-2014-7169)

- Linux
- Unix
- OS X

Check with your software vendor now!

Symantec.
@threatintel | www.symantec.com



HEARTBLEED - THE OPENSSL HEARTBEAT EXPLOIT

HOW TLS (TRANSPORT LAYER SECURITY) WORKS

CLIENT
SERVER
Secure Session Request
Send Certificate
Check Certificate
Get Public Key
Decrypt Session Key with the Server's Private Key
Generate Session Key
Encrypt it with the Server's Public Key
Secure Communications with the Session Key

HOW HEARTBEAT EXTENSION FOR TLS WORKS

CLIENT
SERVER
Send Heartbeat Request Message (to make sure the peer is alive)
PAYLOAD
HEARTBEAT REQUEST MESSAGE
Make sure the received payload is the same
Extract payload & put it into Response Message
HEARTBEAT RESPONSE MESSAGE

HOW THE HEARTBLEED EXPLOIT WORKS

CLIENT
SERVER
Malformed Heartbeat: Small payload disguised as a big one
RECEIVED HEARTBEAT RESPONSE
• TLS/SSL Private Keys
• Authentication Cookies
• Passwords/Credentials
Extract payload & put it into Response Message
MEMORY DATA
The payload is expected to be big, so the 'bucket' gets other data too

ATTACKER
HEARTBLEED ATTACK
SENSITIVE DATA FROM THE WEB SERVER MEMORY
SOCIAL NETWORKS
PERSONAL, CORP EMAIL
FINANCE, STOCK TRADE
INTERNET BANKING
ONLINE SHOPPING
WELFARE, TAX, HEALTH
WEB SERVER
COMMUNICATIONS OVER TLS
VULNERABLE OPENSSL
YOU ARE HERE

NUMBER OF THE VULNERABLE WEBSITES AMONG TOP 10,000

628
15.5 hours
301
17 hours
180
8 April 2014 4:00PM UTC
9 April 2014 7:30AM UTC
10 April 2014 12:30AM UTC

RECOMMENDATIONS

- Check & Upgrade OpenSSL
- Change passwords & keys
- Apply IDS signatures
- Buy a new TLS certificate

E: cyberresponse@baesysytems.com
E: marketingai@baesystems.com
W: www.baesysytems.com/ai

Applied Intelligence

BAE SYSTEMS

- *HEARTBLEED* – Discovered *April 2014* in OpenSSL Cryptography Library (widely used in Transport Layer Security – TLS) as a buffer over-read security flaw. When exploited this allows the theft of users private encryption "keys", as well as passwords & session cookies

Commercialisation of *“Cyber Toolkits”*

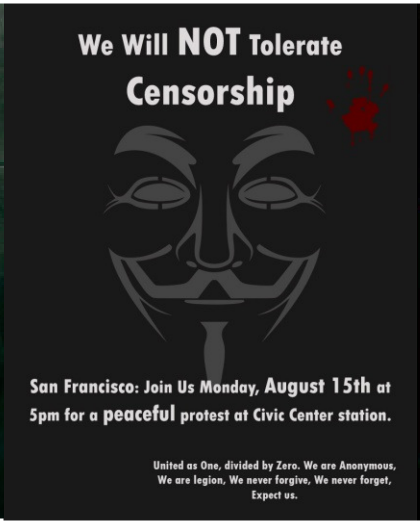
- Industrialisation and Mainstreaming of Cyber Attacks:
  - *(1) Researchers & Cyber Software Creators of Malicious Codes* : Often creative talented computer scientists that have turned their skills to tools for illegal penetration & control of secure systems
  - *(2) “Botnet” - Farmers & Herders* : They are responsible for the illegal international distribution and infection of target “zombie” networked laptops PCs & Servers within homes and offices. The malicious codes (malware such as viruses & trojans) are spread through spam emails, infected websites and “backdoor” attacks.
  - *(3) “Commercial Botnet Dealers”* : They sell access to herds of “zombie” infected machines. The embedded malicious code can be triggered to stimulate “Denial of Service (DDoS)” attacks on target servers & websites. The aim is usually to maximise economic and political damage upon the targeted nation and associated businesses.

…..For further information see the ITU “BotNet” Mitigation Toolkit(2008)

Hybrid Cyber-Physical Hacktivism

"Anonymous" Attacks on BART - Aug 2011

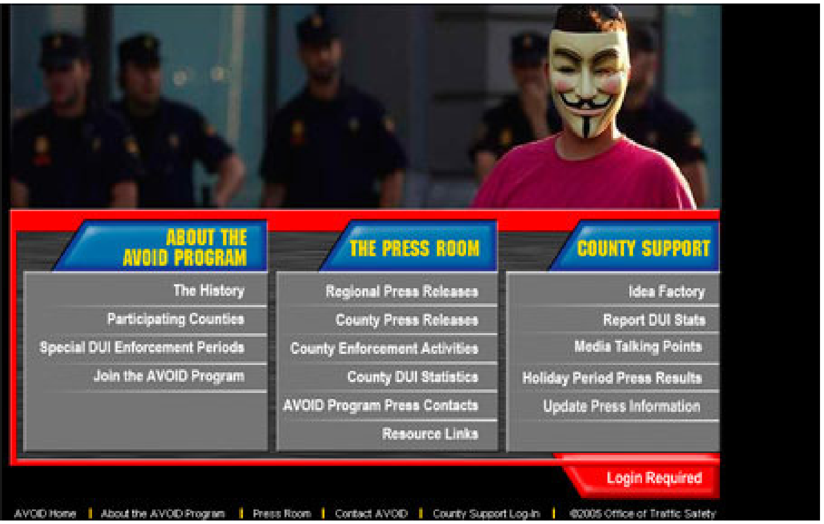
❖ *Physical Protests* by International *Hacktivist* Group – *"Anonymous"* - coupled with multiple Web-Site *Cyber Attacks* following incident on *Bay Area Transit Network - BART – San Francisco*



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.



"Historic" Cyber Attack Case Studies

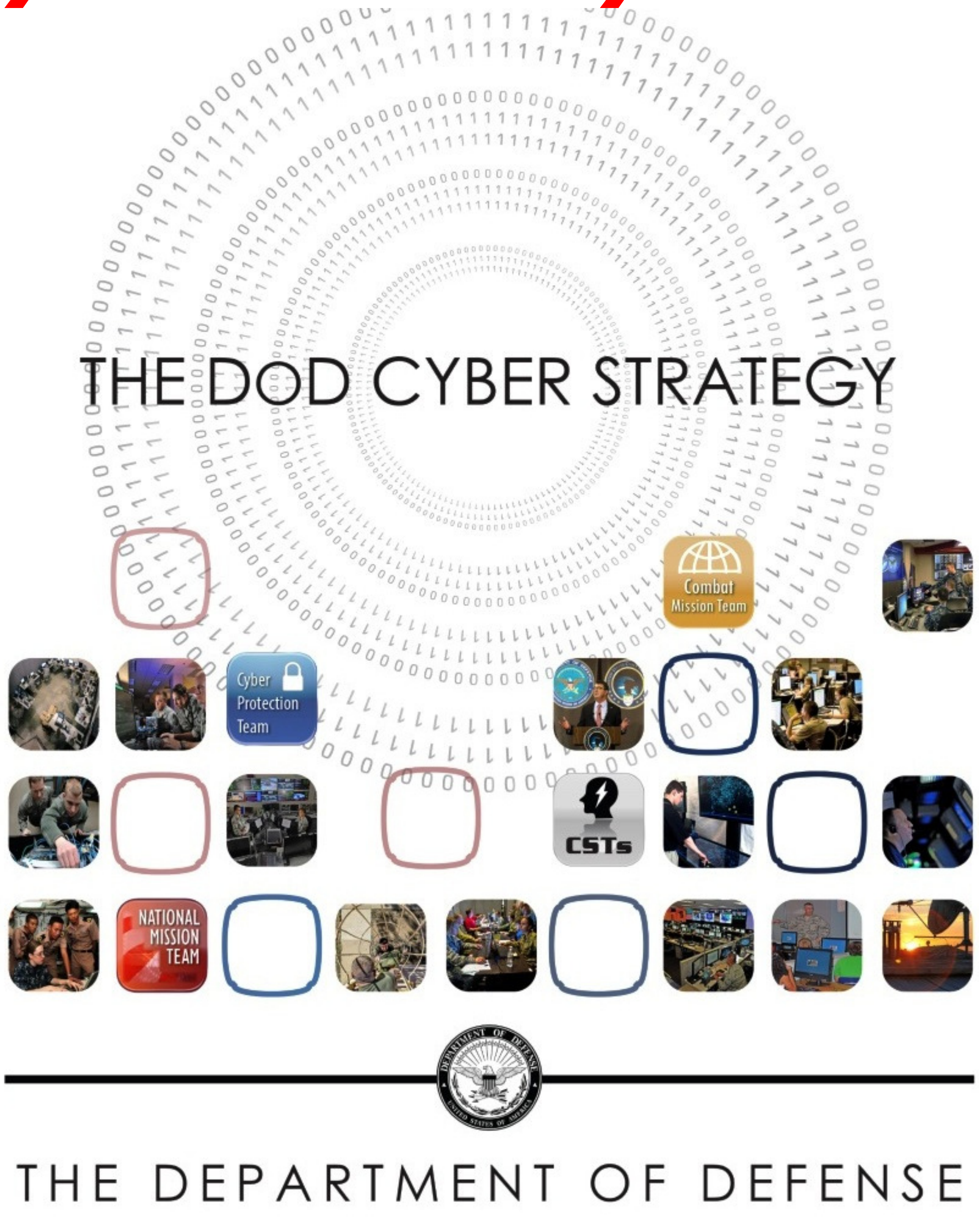
- *Estonia : May 2007*
  - Targeted at Government & Banking Servers – and immobilised national & commercial economic infrastructure for several days. This was one of the earliest "historic" massive DDos attacks (Distributed Denial of Service) from unknown proxy sources.
- *Georgia : August 2008*
  - Targeted at Government Servers including Parliament & Ministry of Foreign Affairs, and the National & Commercial Banking Network from anonymous proxy sources.
- *South Korea : July 2009*
  - Targets included the Defence Ministry, Presidential Offices, National Assembly, and Korea Exchange Banks. This attack was also simultaneously targeted at various high-profile US Sites & Servers such as the NY Stock Exchange, White House & Pentagon.
- *Iran, Indonesia & India : June 2010*
  - Computer worm known as *Stuxnet* discovered in Industrial Logic Controllers in several countries including Iran , Indonesia and India. Stuxnet was the 1st known sophisticated "Designer" Cyber Malware targeted on specific industrial SCADA Systems (Supervisory Control And Data Acquisition). Duqu Malware (2011) is related to Stuxnet.
- *Middle East : May 2012*
  - Sophisticated Modular Computer Malware known as *Flame* or Skywiper is discovered infecting computer networks in Middle Eastern Countries including Iran, Saudi Arabia, Syria, Egypt,& Israel

……Small scale penetrations & cyber attacks continue on an almost 24/7 against almost ALL countries including government & critical national & industrial infrastructure (CNI)

Growing National *Cybersecurity* Focus

THE DEPARTMENT OF DEFENSE CYBER STRATEGY

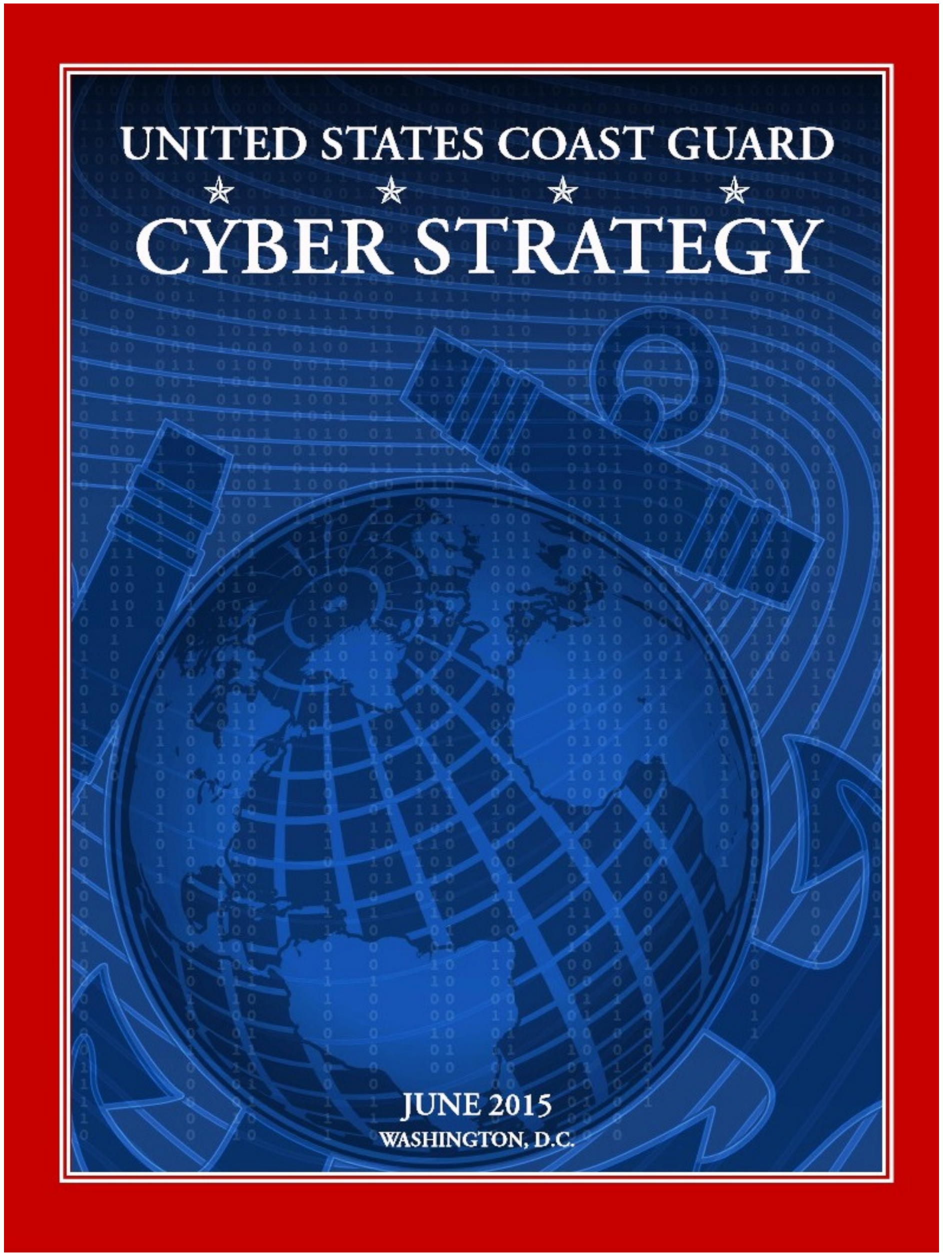
April 2015



THE DOD CYBER STRATEGY

THE DEPARTMENT OF DEFENSE

Cybersecurity Sector Plans: *Government*



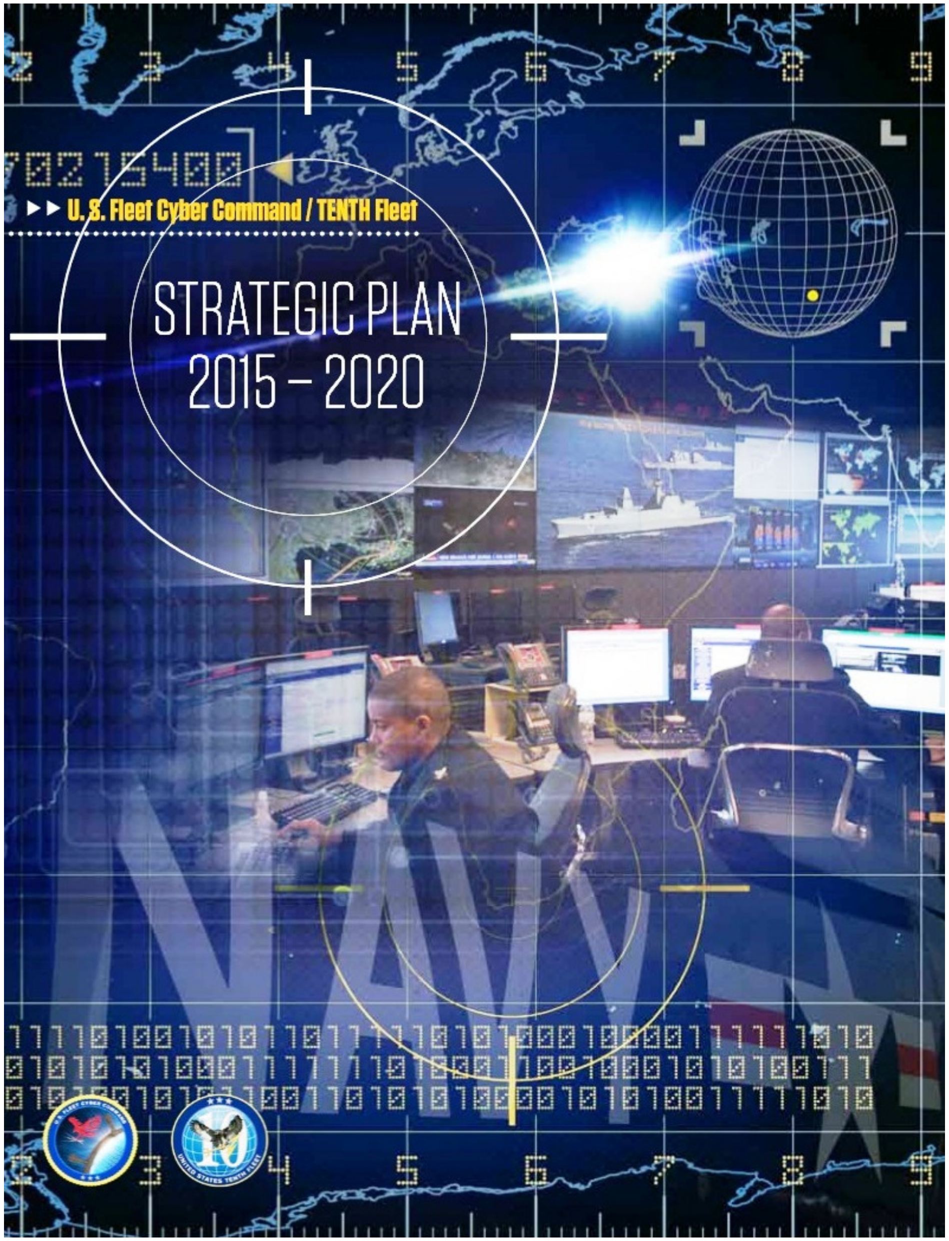
UNITED STATES COAST GUARD

★ ★ ★ ★

CYBER STRATEGY

JUNE 2015

WASHINGTON, D.C.

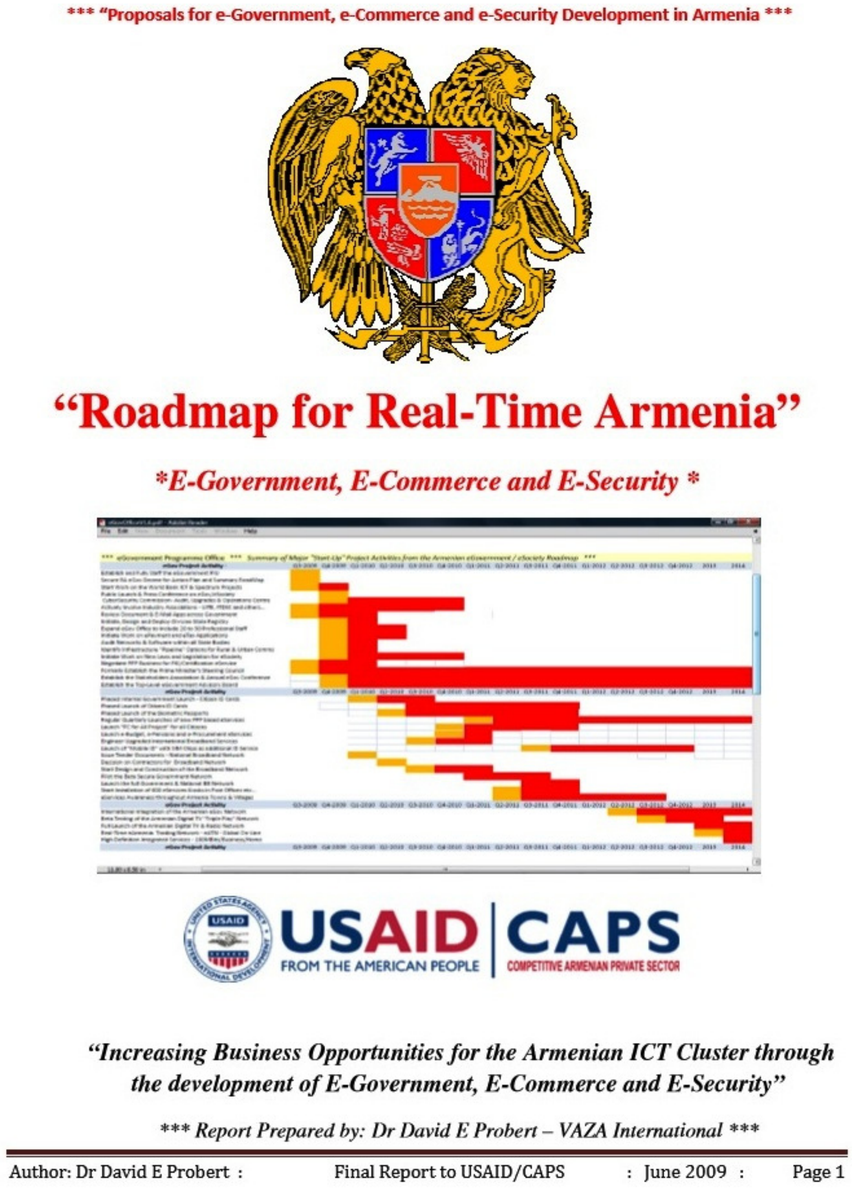


▸▸ U.S. Fleet Cyber Command / TENTH Fleet

STRATEGIC PLAN

2015 – 2020

Cybersecurity for Armenia and Georgia



*** "Proposals for e-Government, e-Commerce and e-Security Development in Armenia ***

"Roadmap for Real-Time Armenia"

*E-Government, E-Commerce and E-Security *

USAID FROM THE AMERICAN PEOPLE | CAPS COMPETITIVE ARMENIAN PRIVATE SECTOR

"Increasing Business Opportunities for the Armenian ICT Cluster through the development of E-Government, E-Commerce and E-Security"

**** Report Prepared by: Dr David E Probert – VAZA International ****

Author: Dr David E Probert : Final Report to USAID/CAPS : June 2009 : Page 1

*** "Real-Time" Georgia : Securing Government & Enterprise Operations ***

"Real-Time Georgia"

Securing Government & Enterprise Operations

Dr David E Probert

VAZA International

1st Georgian IT Innovation Conference

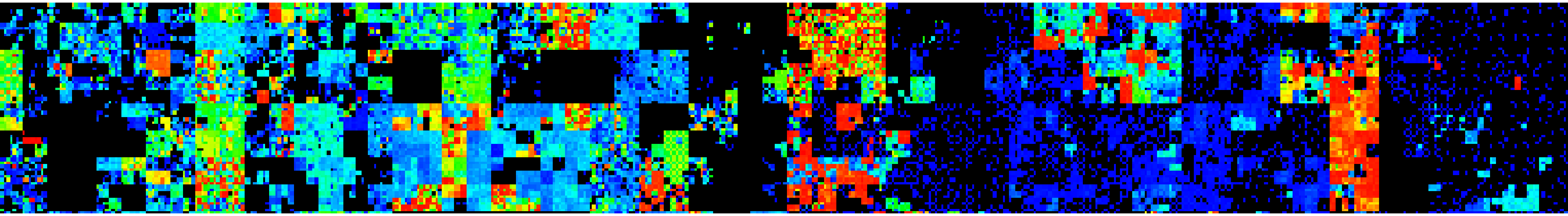
Tbilisi : 29th & 30th October 2008

1 Author : Dr David E Probert Copyright : www.vaza.com – Oct 2008

Link: www.valentina.net/vaza/CyberDocs/

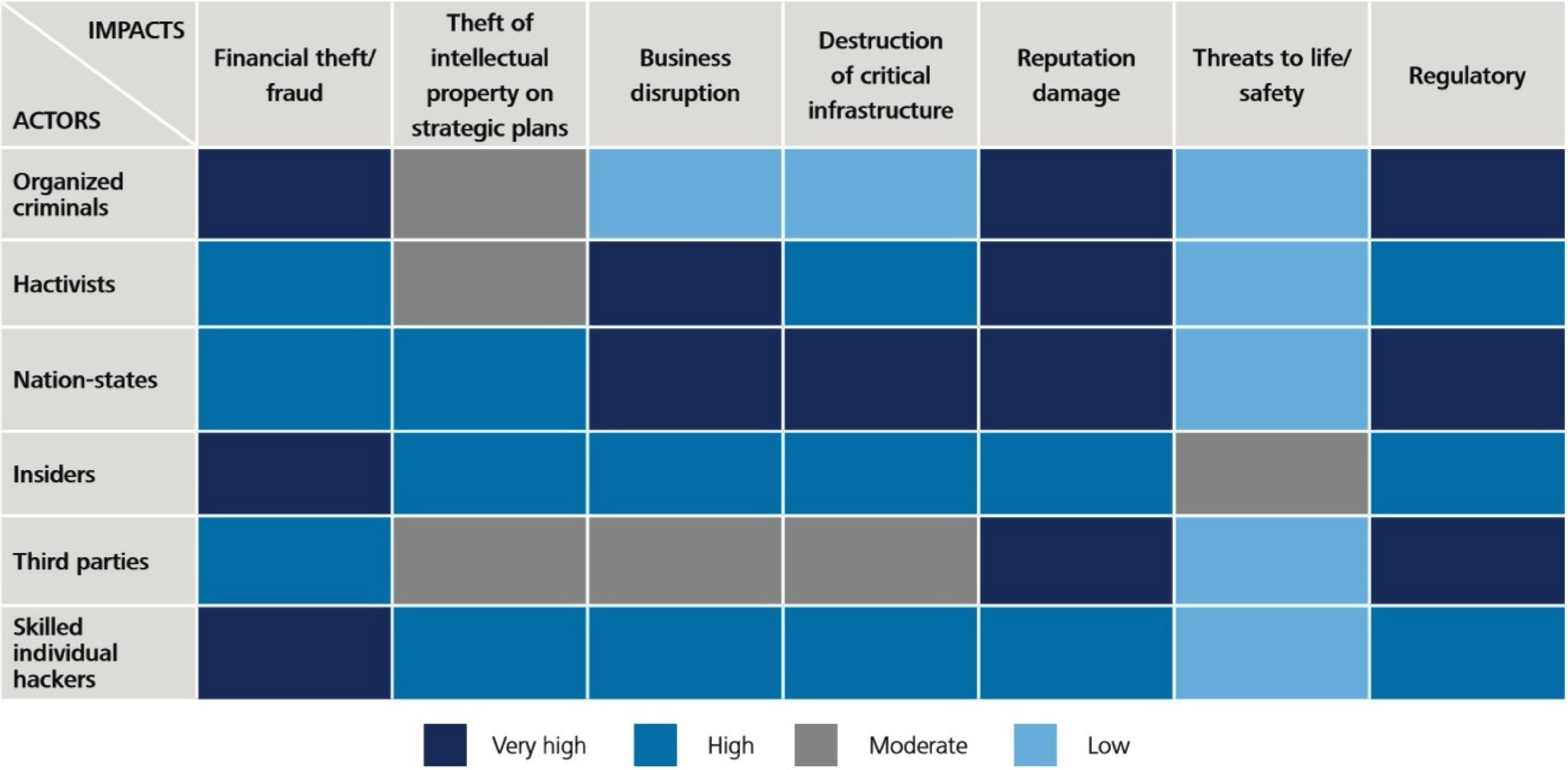
21stC Cybersecurity (1) – *“Integrated Security”*

1 – Background: *“21stC Security Landscape”*	2 – Cybersecurity: Players & Targets	3 – Cyber-Physical Threat Scenarios
4 –Banking & Finance: Hybrid Cybersecurity	5 – CSO: Board Level Security Integration	6 – The Enterprise Internet of Things (IoT)
7 –Cyber-Physical Threats from the “IoT”	8 – Practical Solutions for IoT Security	9 – **YOUR TOP 10 Actions & RoadMap**



Cybersecurity Threats & Risks for the Banking & Finance Sector

A typical cyber risk heat map for the banking sector



IMPACTS / ACTORS	Financial theft/ fraud	Theft of intellectual property on strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life/ safety	Regulatory
Organized criminals	■	▨	□	□	■	□	■
Hactivists	▣	▨	■	▣	■	□	▣
Nation-states	▣	▣	■	■	■	□	■
Insiders	■	▣	▣	▣	▣	▨	▣
Third parties	▣	▨	▨	▨	■	□	■
Skilled individual hackers	■	▣	▣	▣	▣	□	▣

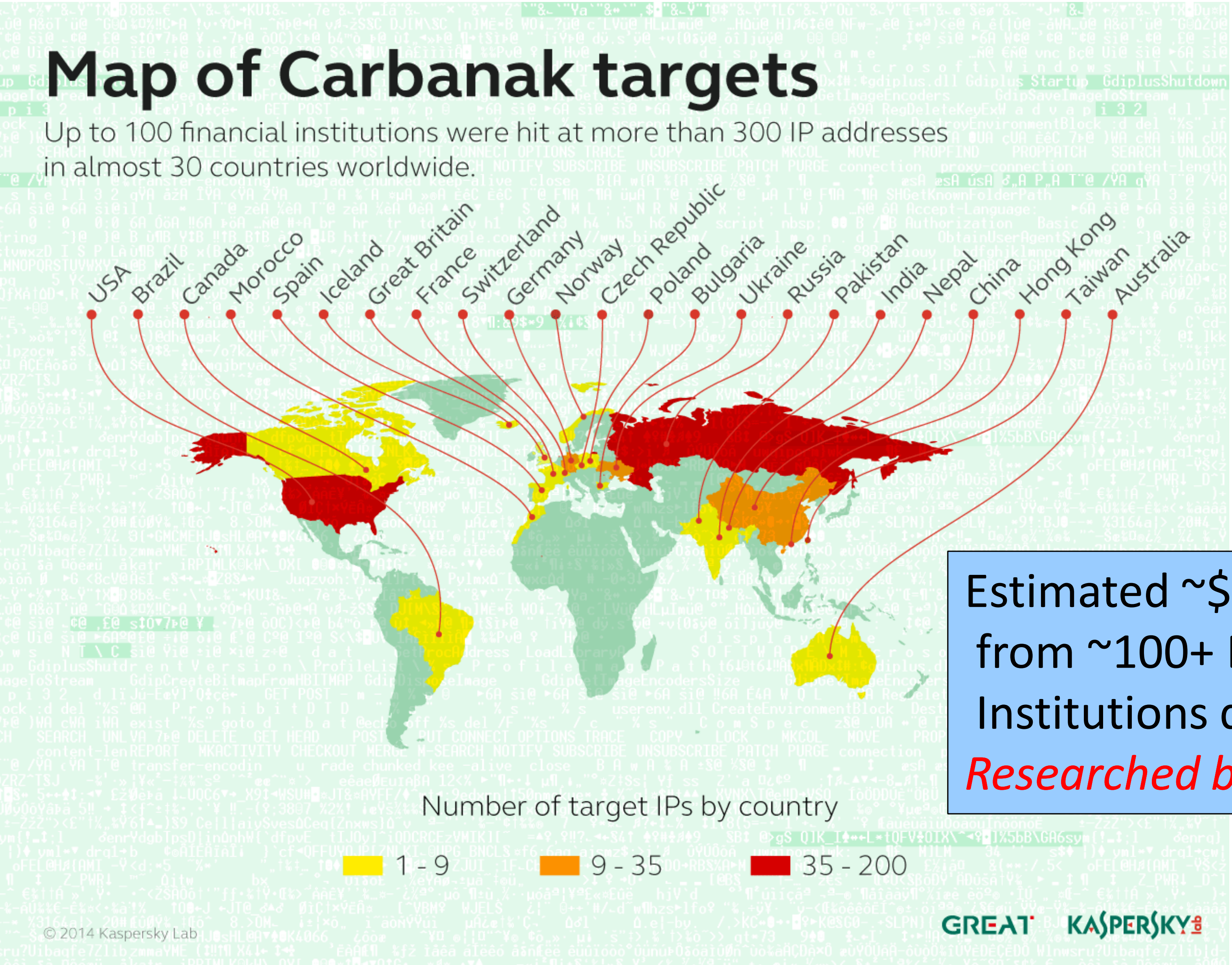
■ Very high ▣ High ▨ Moderate □ Low

Source: Deloitte Center for Financial Services analysis

Banking & Finance: *Cyber-Physical Threats*

- *Banks & Financial Institutions* are prime targets for Cybercriminals & Cyberterrorists since they are at the heart of ALL National Economies!
- *Access* to Accounts is usually indirect through phishing scams, infected websites with malicious scripts, and personal ID Theft.
- *On-Line bank transfers* are also commonly used for international money laundering of funds secured from illegal activities
- *Instant Money Transfer Services* are preferred for crimes such as the classic "Advanced Fee Scam" as well as Lottery and Auction Scams
- An increasing problem is *Cyber-Extortion* instigated through phishing
- *National & Commercial Banks* have also been targets of DDOS cyber attacks from politically motivated and terrorist organisations
- *Penetration Scans:* Banks are pivotal to national economies and will receive penetration scans and attempted hacks on a regular basis.
- *On-Line Banking* networks including ATMs, Business and Personal Banking are at the "sharp end" of financial security and require great efforts towards end-user authentication & transaction network security

Cyber “Banking Theft”– Carbanak



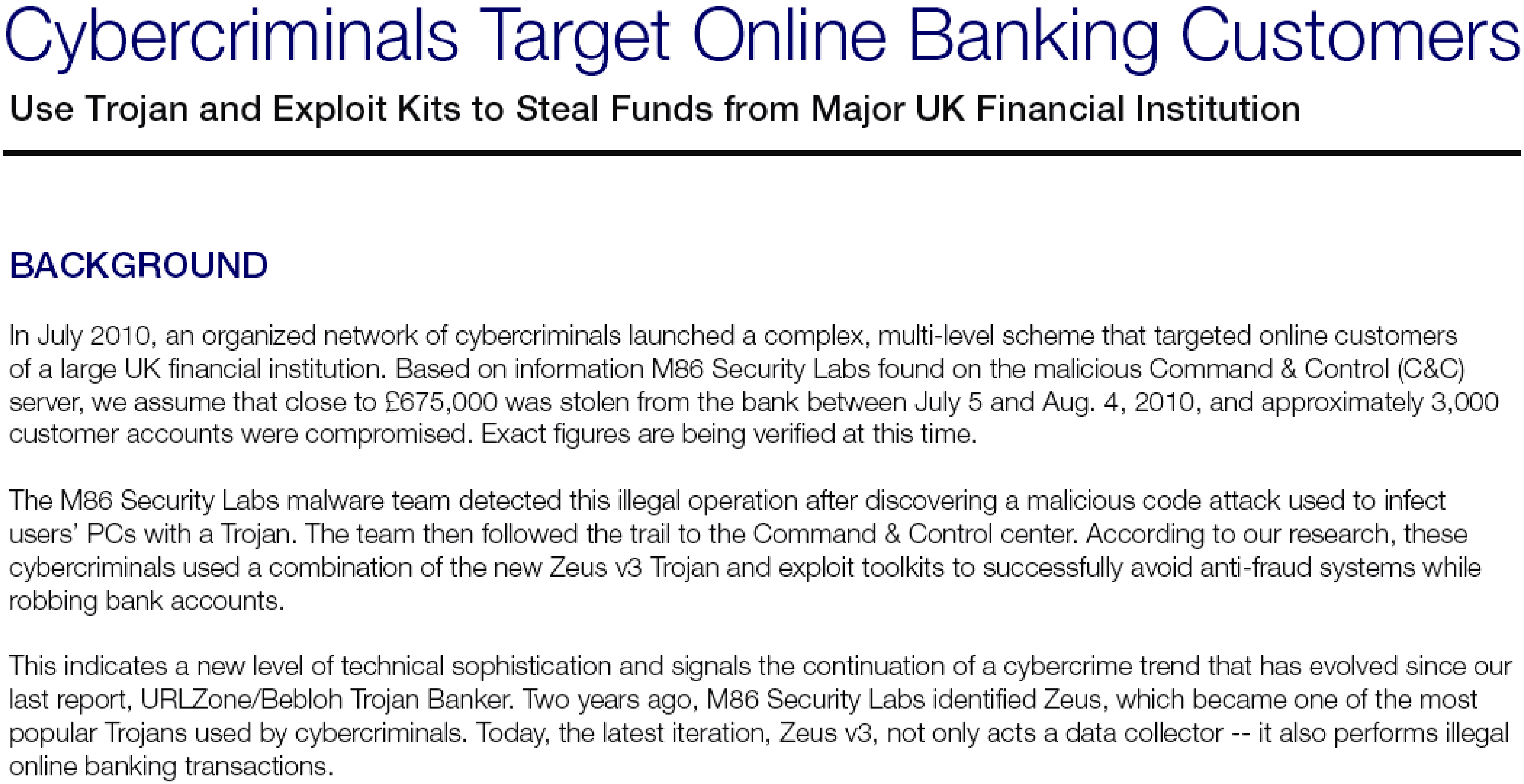
Map of Carbanak targets

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”

Cybercriminals Target *Major UK Bank*



Cybercriminals Target Online Banking Customers

Use Trojan and Exploit Kits to Steal Funds from Major UK Financial Institution

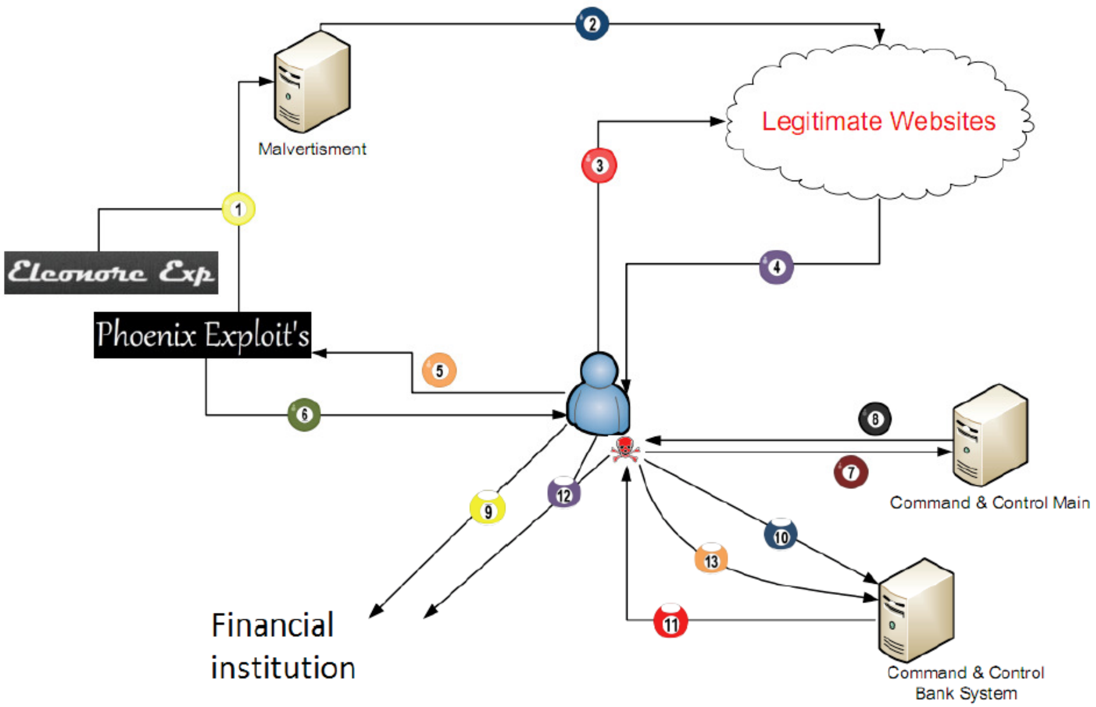
BACKGROUND

In July 2010, an organized network of cybercriminals launched a complex, multi-level scheme that targeted online customers of a large UK financial institution. Based on information M86 Security Labs found on the malicious Command & Control (C&C) server, we assume that close to £675,000 was stolen from the bank between July 5 and Aug. 4, 2010, and approximately 3,000 customer accounts were compromised. Exact figures are being verified at this time.

The M86 Security Labs malware team detected this illegal operation after discovering a malicious code attack used to infect users' PCs with a Trojan. The team then followed the trail to the Command & Control center. According to our research, these cybercriminals used a combination of the new Zeus v3 Trojan and exploit toolkits to successfully avoid anti-fraud systems while robbing bank accounts.

This indicates a new level of technical sophistication and signals the continuation of a cybercrime trend that has evolved since our last report, URLZone/Bebloh Trojan Banker. Two years ago, M86 Security Labs identified Zeus, which became one of the most popular Trojans used by cybercriminals. Today, the latest iteration, Zeus v3, not only acts a data collector -- it also performs illegal online banking transactions.

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

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 -

Cybersecurity for *Banking & Finance*

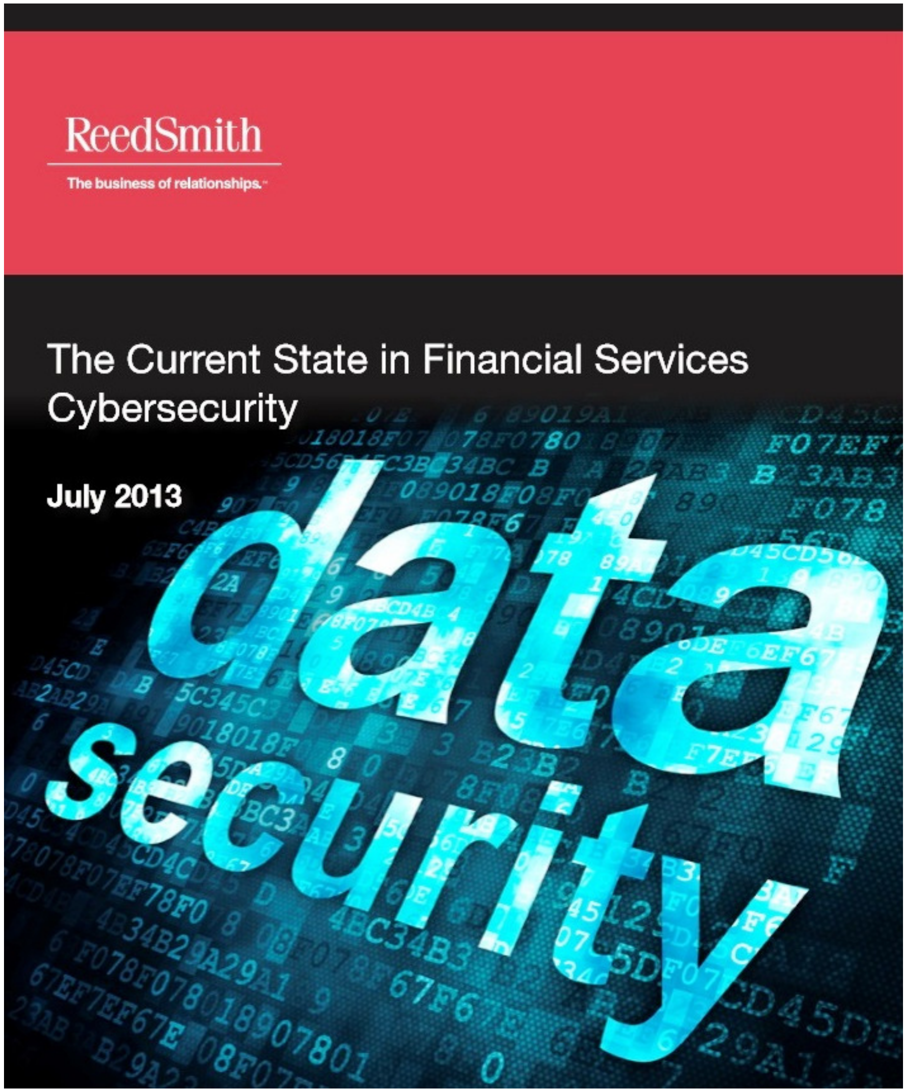
NEW YORK STATE ★ DEPARTMENT OF FINANCIAL SERVICES ★

EXCELSIOR

New York State

Department of Financial Services

Report on Cyber Security in the Banking Sector



ReedSmith

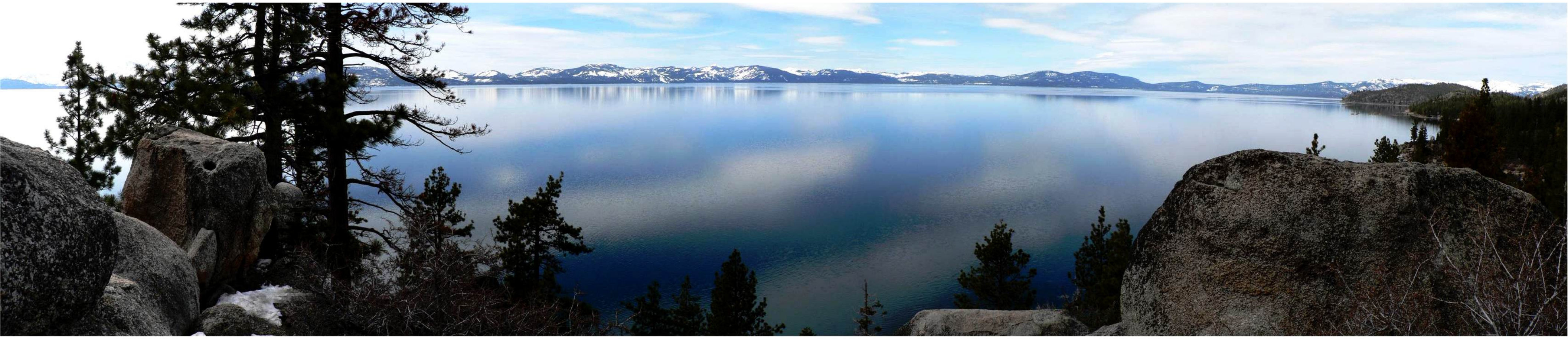
The business of relationships.

The Current State in Financial Services Cybersecurity

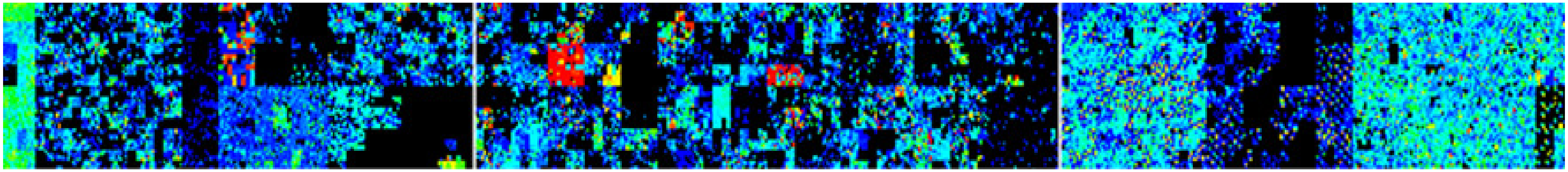
July 2013

data security

21stC Cybersecurity (1) – *"Integrated Security"*



1 – Background: *"21stC Security Landscape"*	2 – Cybersecurity: Players & Targets	3 – Cyber-Physical Threat Scenarios
4 –Banking & Finance: Hybrid Cybersecurity	**5 – CSO: Board Level Security Integration**	6 – The Enterprise Internet of Things (IoT)
7 –Cyber-Physical Threats from the "IoT"	8 – Practical Solutions for IoT Security	9 – YOUR TOP 10 Actions & RoadMap



CSO: *Board Level Security Integration*

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

Traditional *"Physical Security"* Defences in the context of "Cybersecurity"

- ***Compliance:*** Investments in establishing and upgrading cybersecurity defences against cybercrime means that all physical security and associated operational staff should also be reviewed for compliance with policies, and audited to international standards

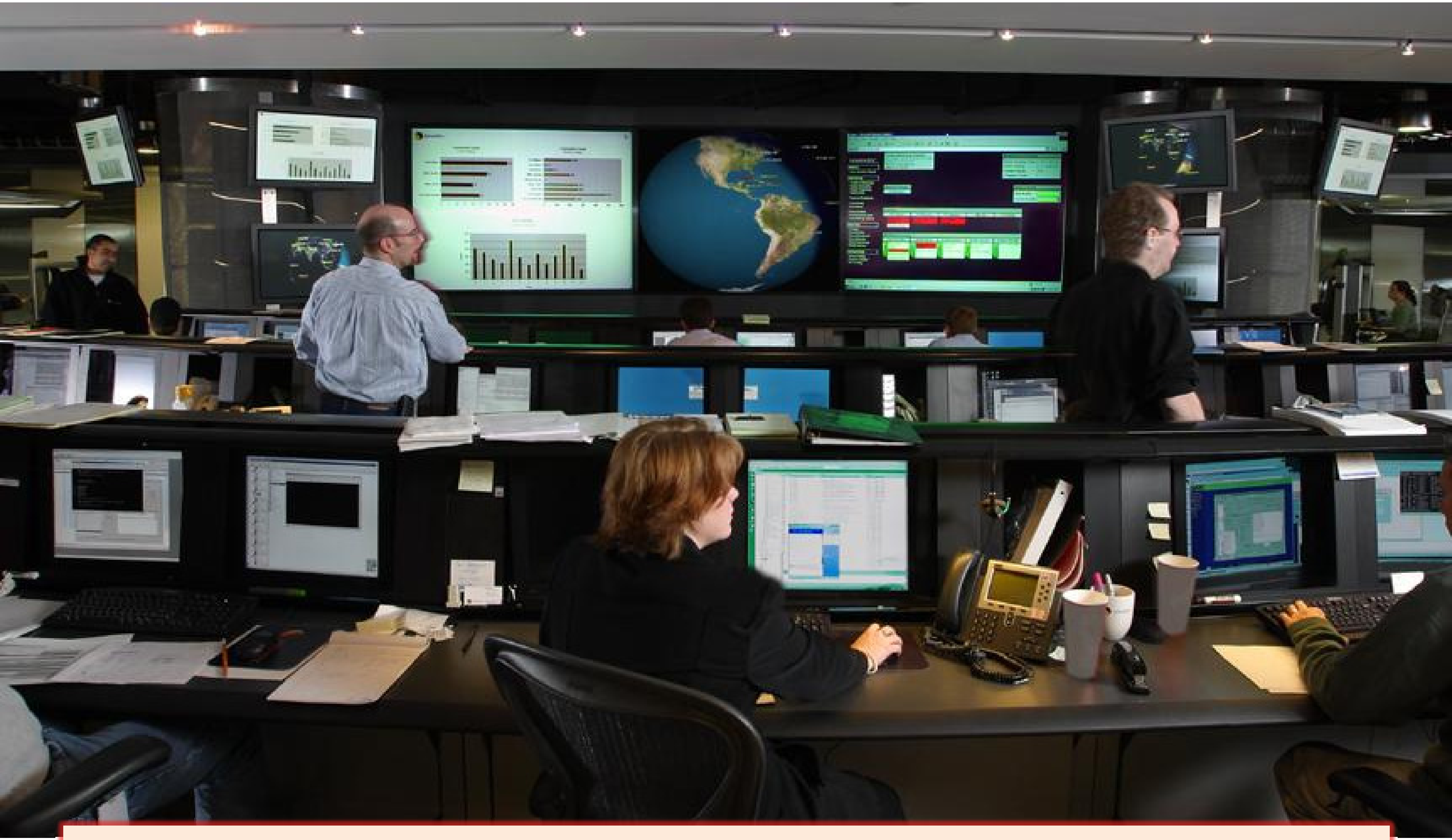
- ***Integration:*** Physical and Cybersecurity operations should be linked "step-by-step" at the command and control level in the main government or enterprise operations centre.

- ***Physical Security*** for critical service sectors such as governments, airports, banks, telecommunications, education, energy, healthcare and national defence should be included within the strategy and policies for Cybersecurity and vice versa

- ***Upgrades:*** In order to maximise security, Government and Businesses need to upgrade and integrate resources & plans for both physical & cybersecurity during the next years.

- ***Roadmap:*** I'd recommend developing a focused total security action plan and roadmap (Physical & Cyber) for each critical sector within YOUR National Economy & Enterprises

Cyber: Integrated Command & Control



- ***Security Operations Command Centre for Global Security Solutions Enterprise***

Cyber Integration with *Physical Security Operations*

- *Cybersecurity* for Government, Business & Critical Service Sectors should be tightly integrated with operational physical security solutions including:

1) *Advanced CCTV* Camera Surveillance of the Secure Government & Critical Facilities
2) *Exterior ANPR* (Automatic Number Plate Recognition) Systems for Car Parking & Entrances
3) Integration of the Cyber *CERT/CSIRT* with physical CCTV & Alarm Control Centres
4) *Personnel RFID* and/or biometrics office & campus access controls
5) Professionally trained *security personnel & guards* – 24/7 – for top security facilities
6) Implemented facility *security policy* for staff, visitors and contractors
7) *Intelligent perimeter* security controls for campuses and critical service facilities such as airports, power stations, refineries, military bases, hospitals and government institutions
8) *On-Line Audit trails* and Electronic Log-Files for secure Physical Facilities
9) Focus upon in-depth *physical security* for computer server rooms, data storage & archives

All critical information infrastructures on multi-building campus sites such as airports, universities, hospitals, military bases, leisure resorts & government agencies require
"Integrated 4D Cyber-Physical Security Operations" = "SMART SECURITY"

Critical Energy Industry Sector : *"Cybersecurity for Automated Industrial Control & Safety Systems"*

Protection against "Stuxnet" type designer malware that attacks SCADA systems

Integration of Physical and Cyber Security

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

Physical Security Operations

Cyber Security Operations

Shared

Alerts

Smart Security = ***Virtual Integration***

Corporate CSO-led Security Team

ONE – Shopping List!

Integrated Management,
Training, Standards, Plans

ONE – Architecture!

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

Integrated Cyber & Physical Security: *"The Shopping List"*

...Smart Security for Business & Government is a Multi-Year Programme!

1) ***Cybersecurity Team*:** Establishment of a CERT/CSIRT & Professionally Qualified Cybersecurity Team within your Business or Government Organisation
2) ***CNI:*** Long Term Critical Infrastructure Protection (CNI) – Protect Critical Info Assets!
3) ***System Upgrades*:** Technical Infrastructure Upgrades including Hardware, Software, Databases, Secure Network Links, Biometrics & RFID
4) ***Back-Up*:** Disaster Recovery, Business Continuity and Back-Up Systems
5) ***Physical* :** Physical Security Applications – CCTV, Alarms, Control Centre
6) ***Awareness Campaign*:** Business-Wide Campaign for Cybersecurity Awareness
7) ***Training*:** Cybersecurity Skills, Certification & Professional Training Programme
8) ***Encryption*:** Implement Data Encryption for Business Critical Info
9) ***Rules & Policies:*** Develop and Communicate Cyber & Physical Security Policies for ALL Staff & Contractors to cover topics such as Wi-Fi and "Bring your Own Device (BYOD)"

......It is also recommended to develop an economic "Cost-Benefit" analysis and detailed Business Case in order to justify Cybersecurity Investment for your Board of Directors!

"Cyber – Physical Security Operations"

Convergence to Smart Resilient Security Solutions

- ***IP Networks:*** Physical security and associated Operational Solutions are increasingly based upon sophisticated electronic networked solutions, including biometrics, smart CCTV, intelligent perimeter fences, embedded active & passive RFID Devices and networked real-time sensors

- ***Convergence:*** CSO-led Management operations for "Physical Security" and "Cybersecurity" will steadily converge & become integrated during the next few years from staff, assets, resources & operational budget perspectives = ***"Smart Resilient Security"***

- ***Smart Security in 3 Phases:*** Cyber-Physical Security Integration will evolve over 5 -10 years

  *1st Phase – Virtual Operational Integration - **CSO** managed Security Team*

  *2nd Phase – Integrated Architectures and Standards – **ONE** Cyber-Physical Model*

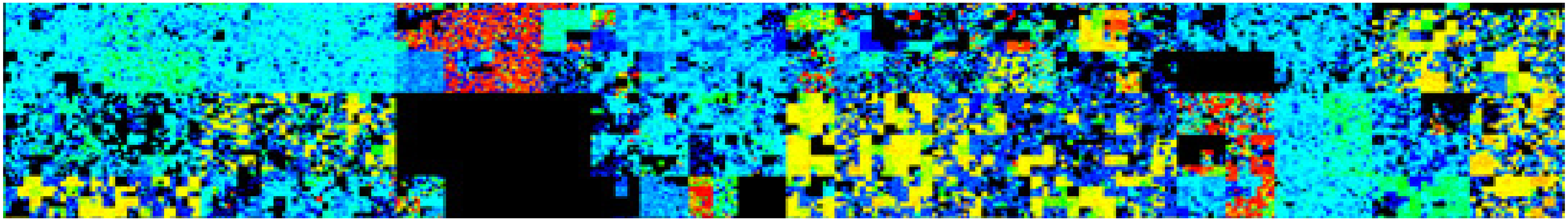
  *3rd Phase – Embedded Intelligent Integration of **ALL** Devices - Internet of Things*

- ***Business Benefits:*** The benefits of integrating cyber and physical security for both Business and Governments are reduced running costs, reduced penetration risk, and increased early warning of co-ordinated cyber-physical security attacks, whether from criminals, hackers or terrorists.

……the "Cyber-Vardzia" White Paper for Georgia discusses Cybersecurity and Physical security in some depth, as well as their convergence and integration!

21stC Cybersecurity (1) – *“Integrated Security”*

1 – Background: *“21stC Security Landscape”*	2 – Cybersecurity: Players & Targets	3 – Cyber-Physical Threat Scenarios
4 –Banking & Finance: Hybrid Cybersecurity	5 – CSO: Board Level Security Integration	**6 – The Enterprise Internet of Things (IoT)**
7 – Cyber-Physical Threats from the “IoT”	8 – Practical Solutions for IoT Security	9 – YOUR TOP 10 Actions & RoadMap



Enterprise *"Internet of Things"-* IoT

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

“Internet of Things”: *Our Definitions*

A *dynamic global network infrastructure*

with *self configuring capabilities*

based on *standard and interoperable communication protocols*

where *physical and virtual “things”*

have *identities, physical attributes, and virtual personalities*

use *intelligent interfaces*,

and are *seamlessly integrated*

into *the information network.*

Internet of Things: *Phases of Evolution*

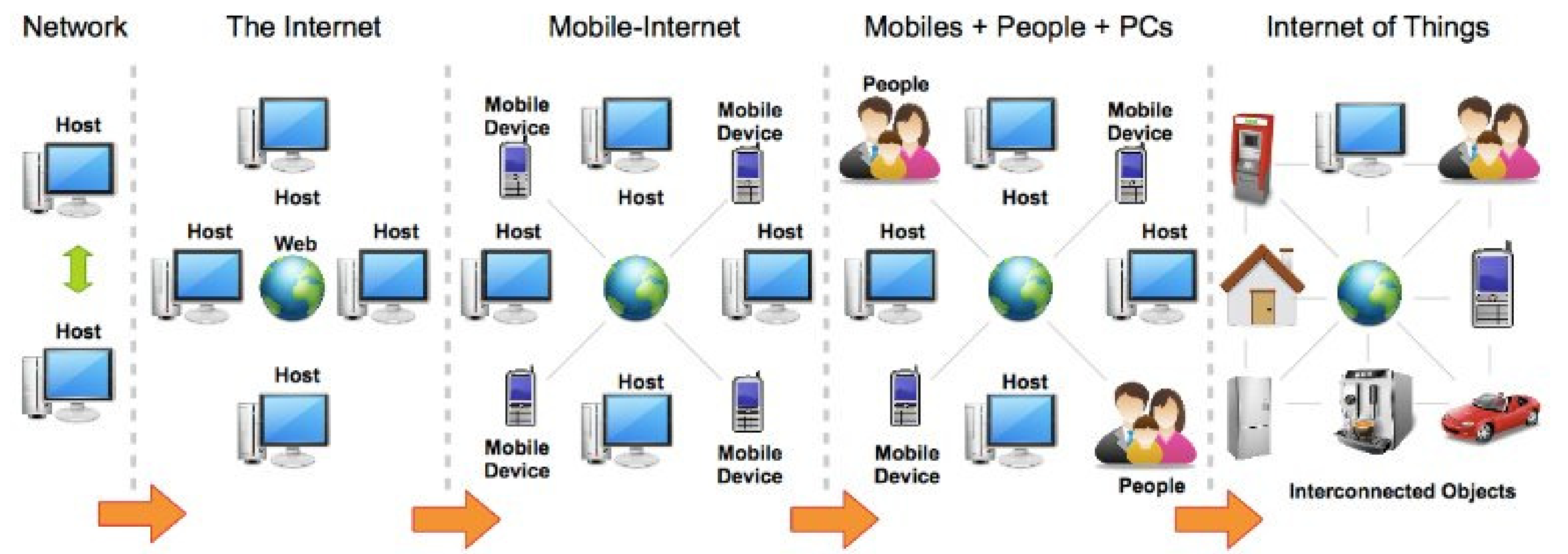
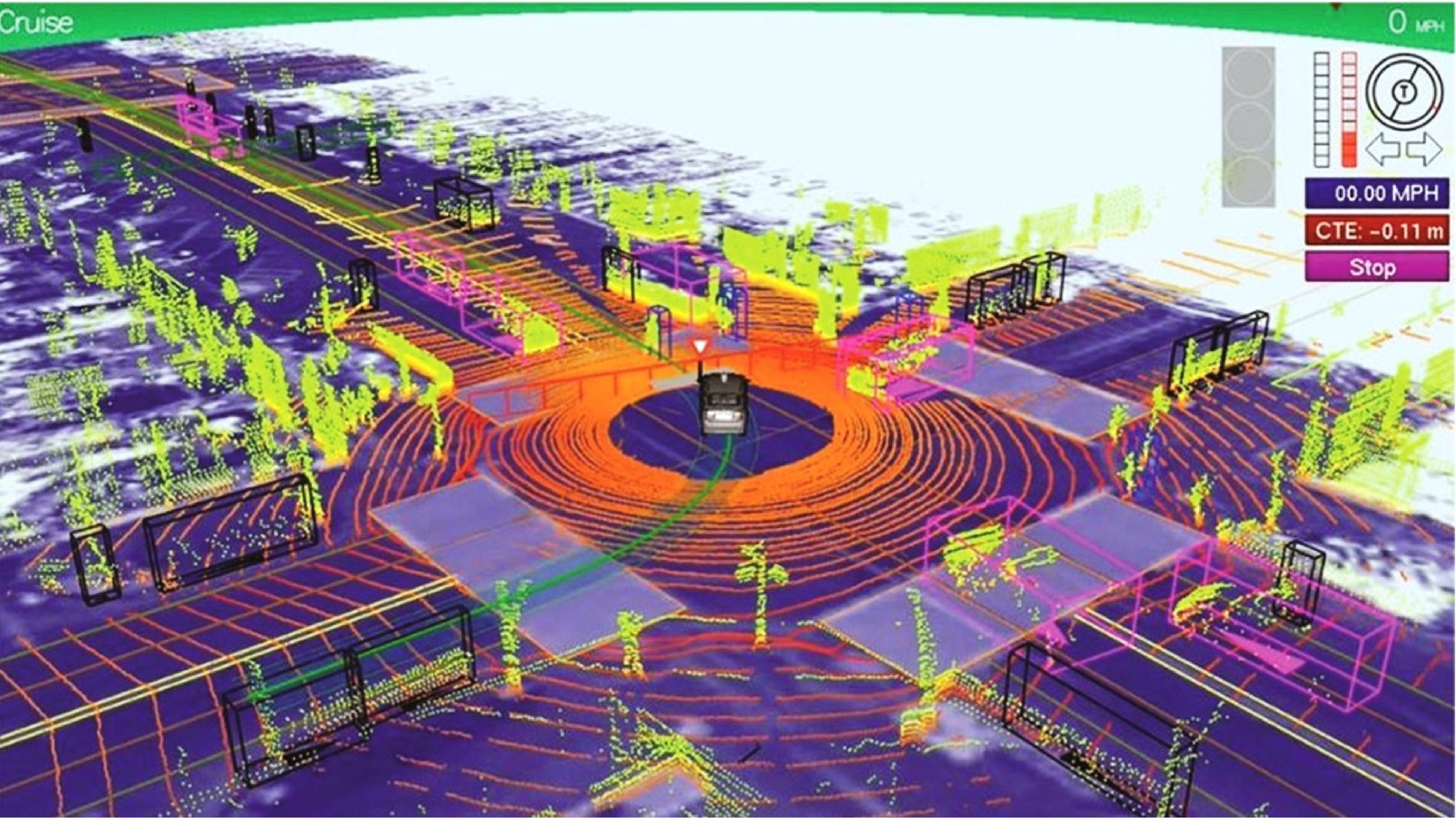


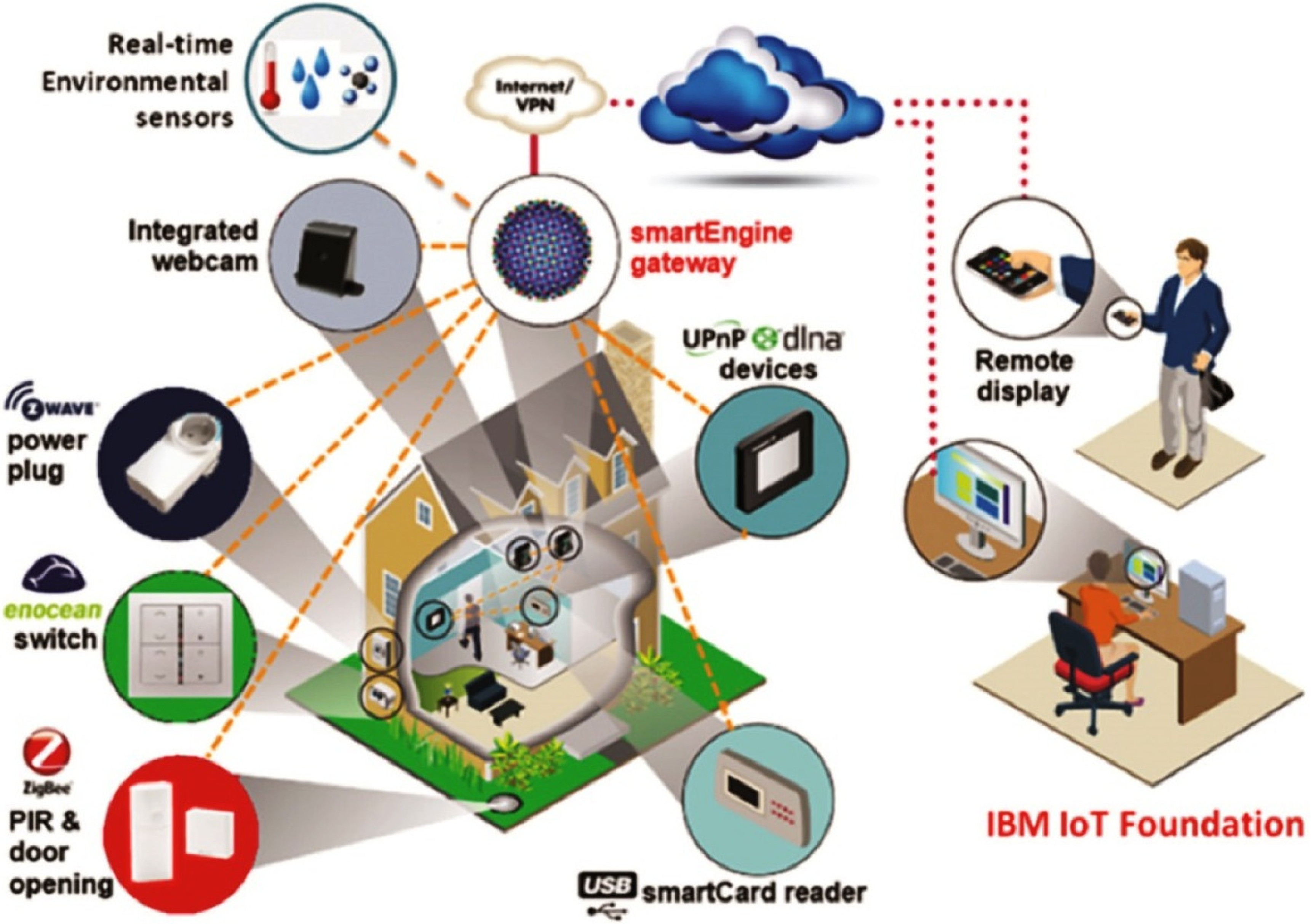
Fig. 1. Evolution of the Internet in five phases. The evolution of Internet begins with connecting two computers together and then moved towards creating World Wide Web by connecting large number of computers together. The mobile-Internet emerged by connecting mobile devices to the Internet. Then, peoples'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

“IoT Devices”: *Wristbands and Watches*

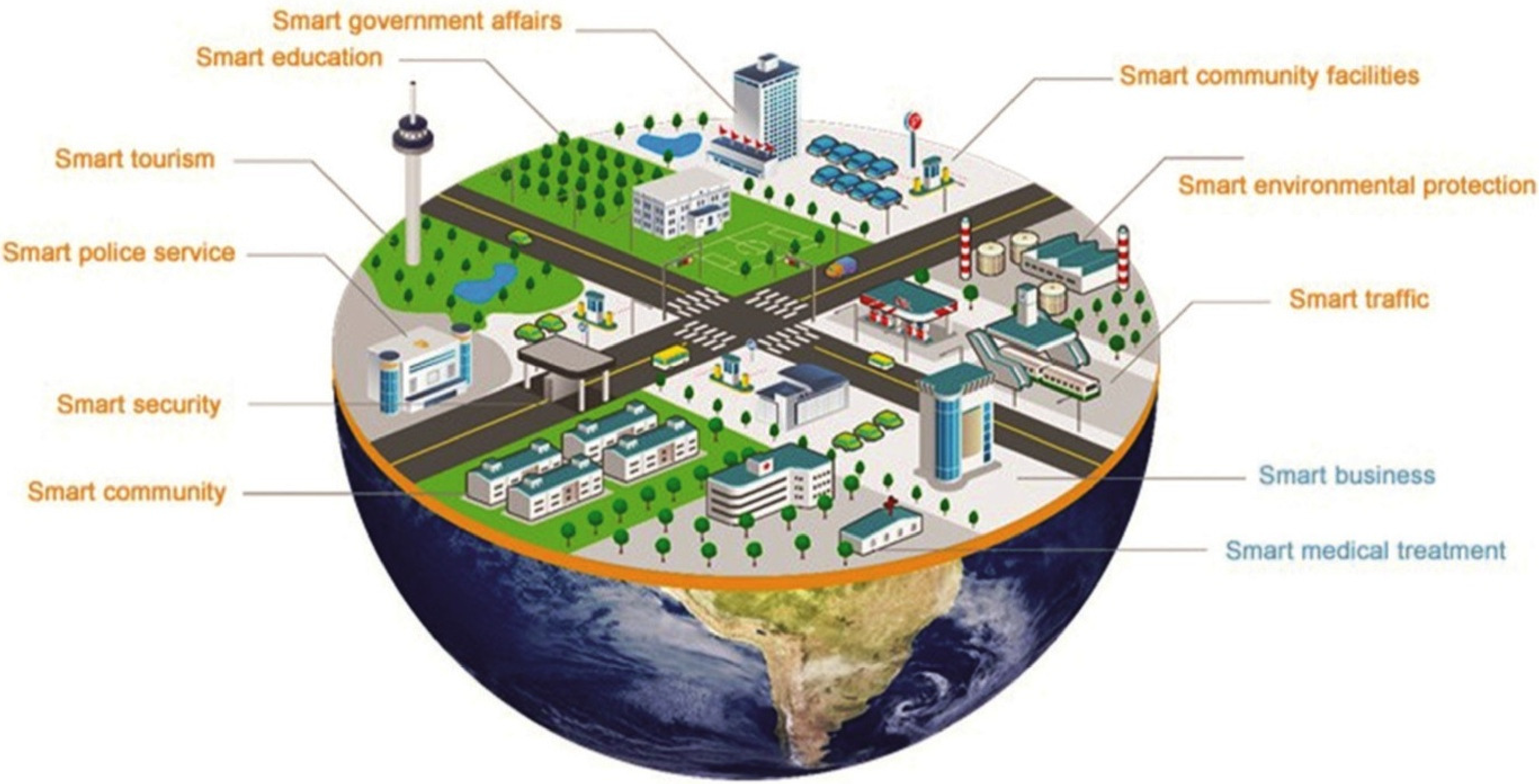
“Google Car”: *Computer Vision View*



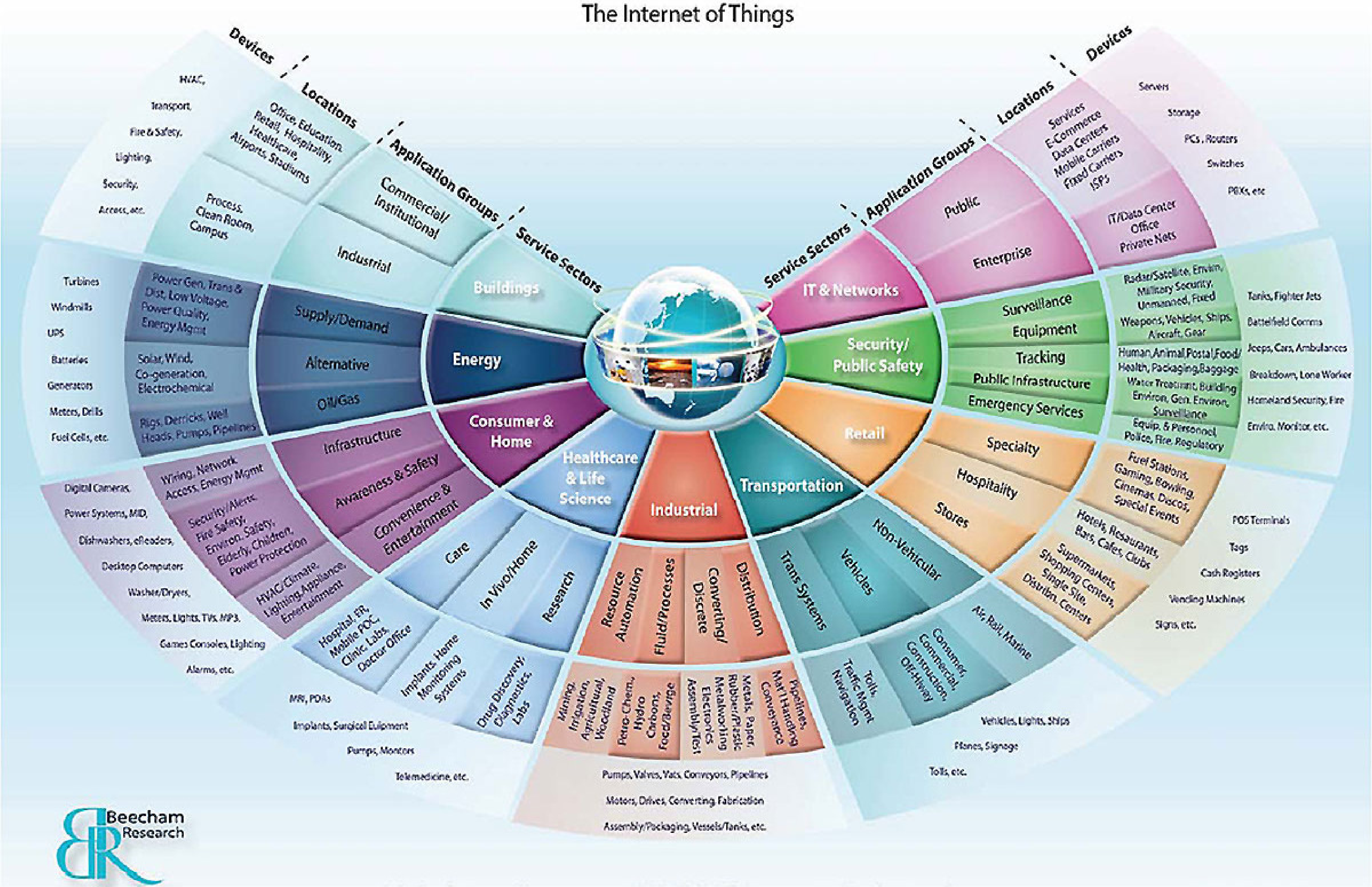
"IoT" Connectivity in the Home: IBM



Smart City: *Scaled "IoT" Architectures*

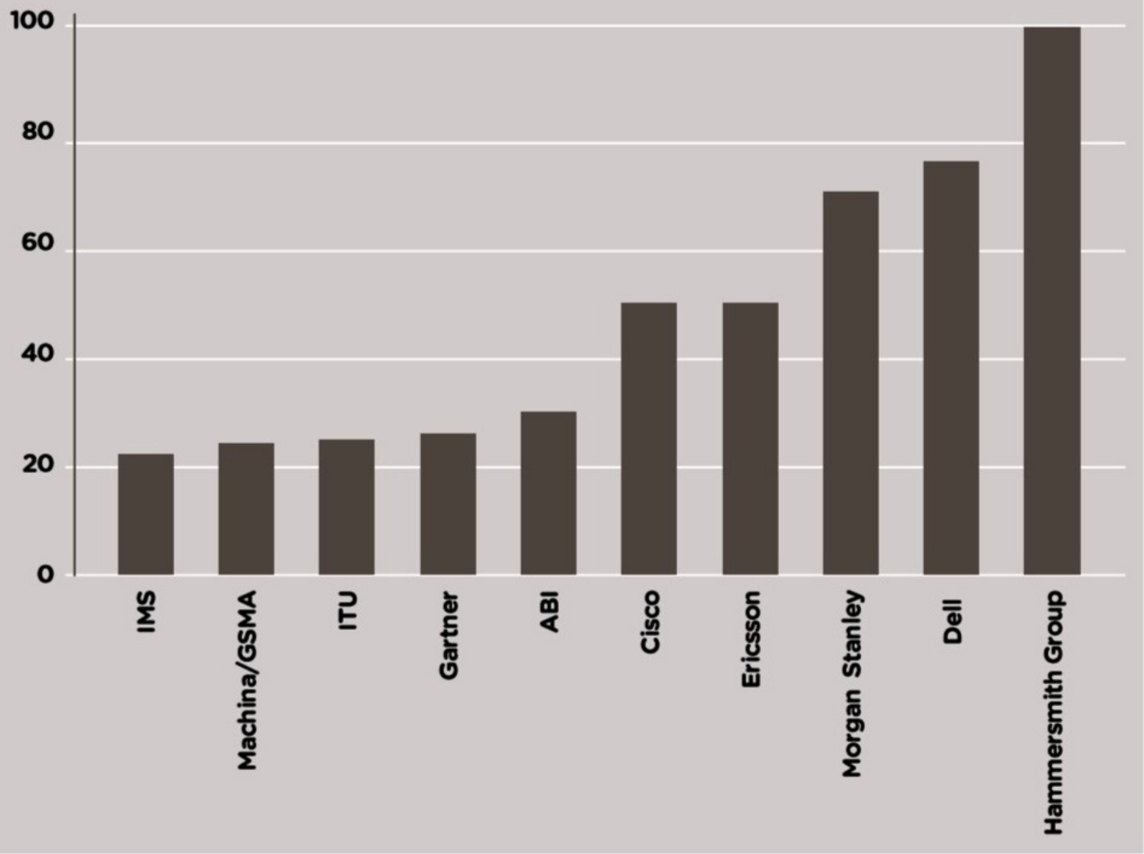


Internet of Things: *Spans ALL Sectors*


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

2020 Estimates for "IoT" Connectivity

Figure 3:
Industry estimates for connected devices (billions) in 2020[2]

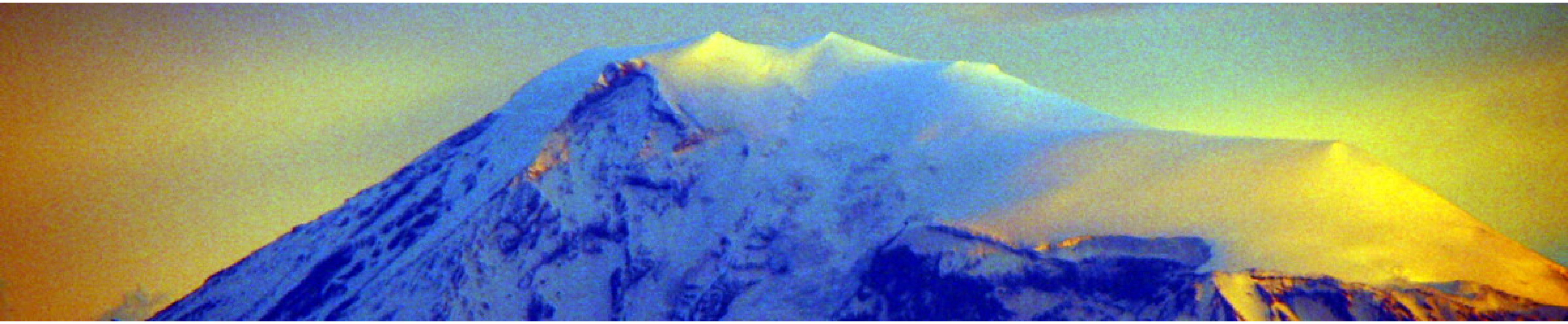


[1] 'Internet of Things Connections Counter', Cisco Systems, 2014

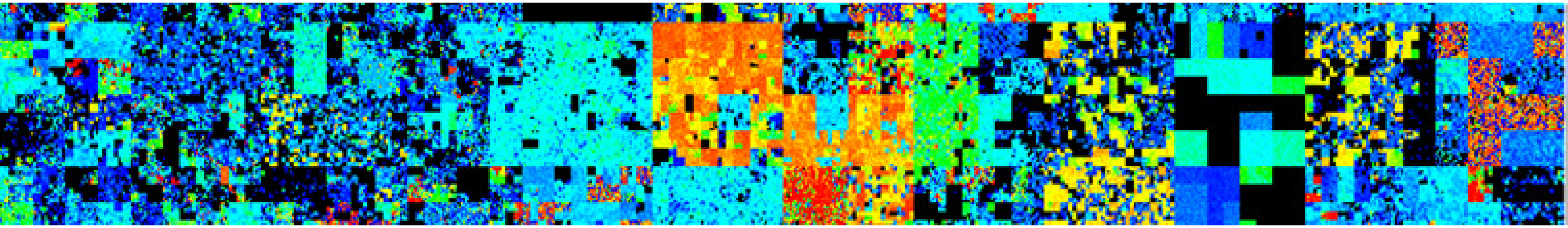
[2] http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10; https://www.abiresearch.com/market-research/product/1016390-over-30-billion-wireless-connected-devices/; 'Forecast: The Internet of Things, Worldwide 2013', Gartner, 2013; 'The State of Broadband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

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

21stC Cybersecurity (1) – *"Integrated Security"*



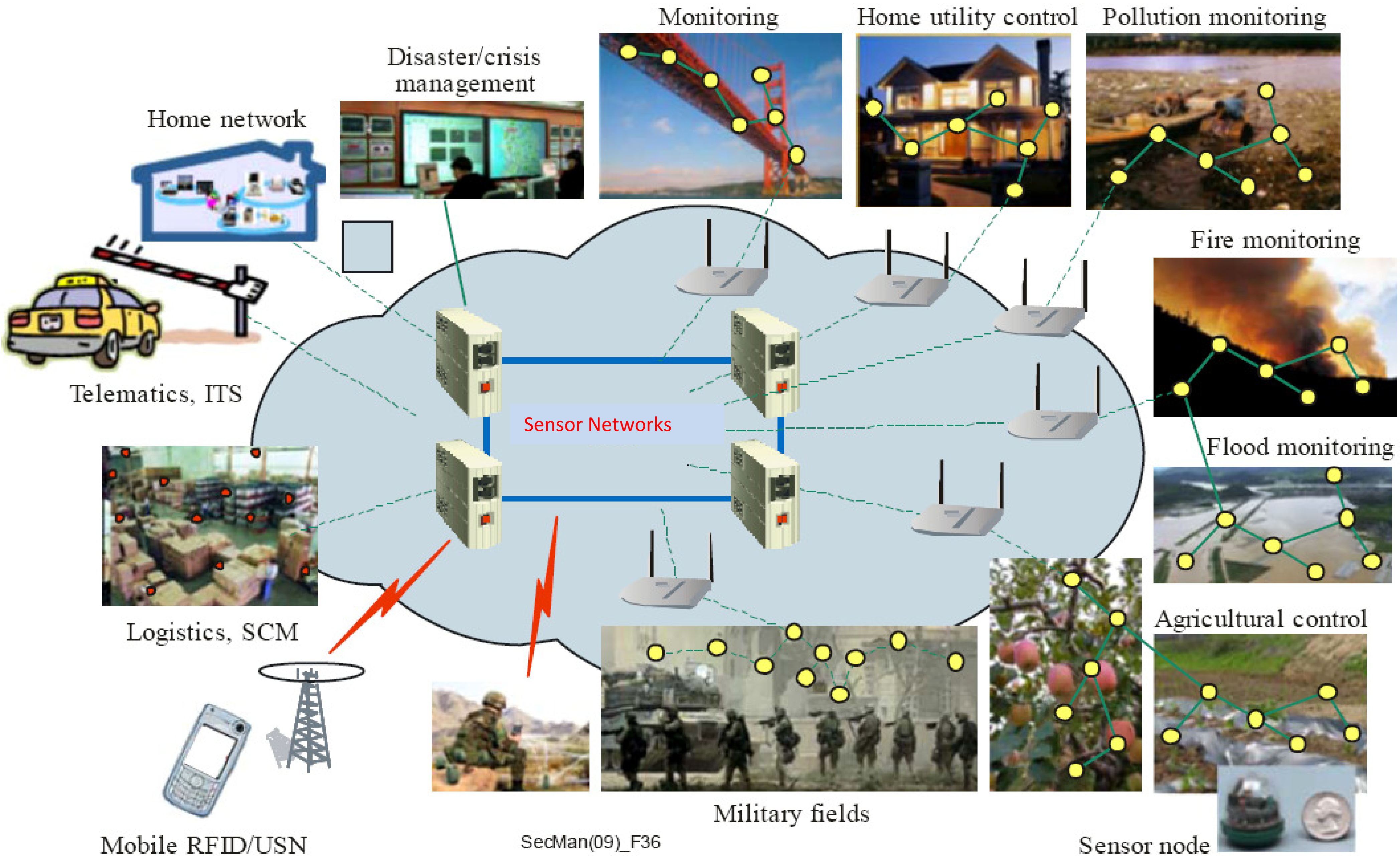
1 – Background: *"21stC Security Landscape"*	2 – Cybersecurity: Players & Targets	3 – Cyber-Physical Threat Scenarios
4 –Banking & Finance: Hybrid Cybersecurity	5 – CSO: Board Level Security Integration	6 – The Enterprise Internet of Things (IoT)
7 – Cyber-Physical Threats from the "IoT"	8 – Practical Solutions for IoT Security	9 – YOUR TOP 10 Actions & RoadMap



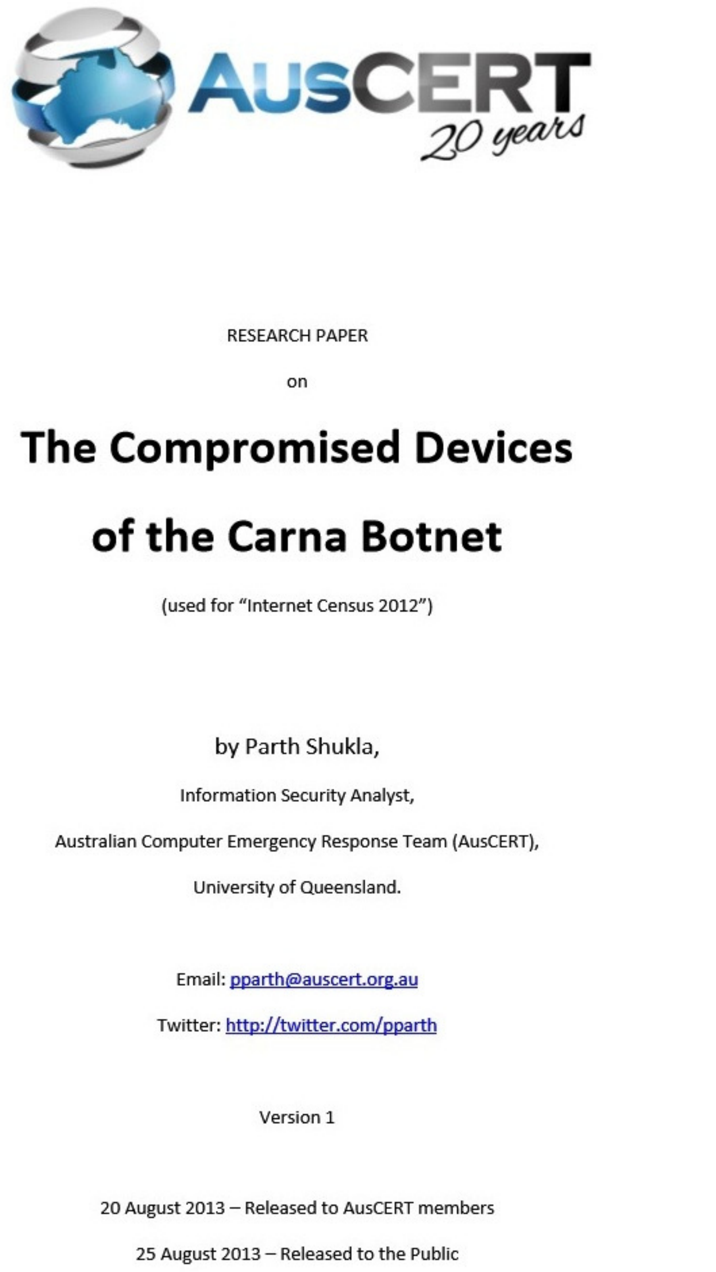
Cyber-Physical Threats from the “IoT”

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

Cybersecurity for Critical Sector Environmental Networks: *"Internet of Things"*



"Integrated Cyber-Physical Security and Securing the Enterprise Internet of Things"
- Madrid, Spain: 26th–27th Oct 2915 -
© *Dr David E. Probert : www.VAZA.com* ©



AusCERT 20 years

RESEARCH PAPER

on

The Compromised Devices of the Carna Botnet

(used for "Internet Census 2012")

by Parth Shukla,

Information Security Analyst,

Australian Computer Emergency Response Team (AusCERT),

University of Queensland.

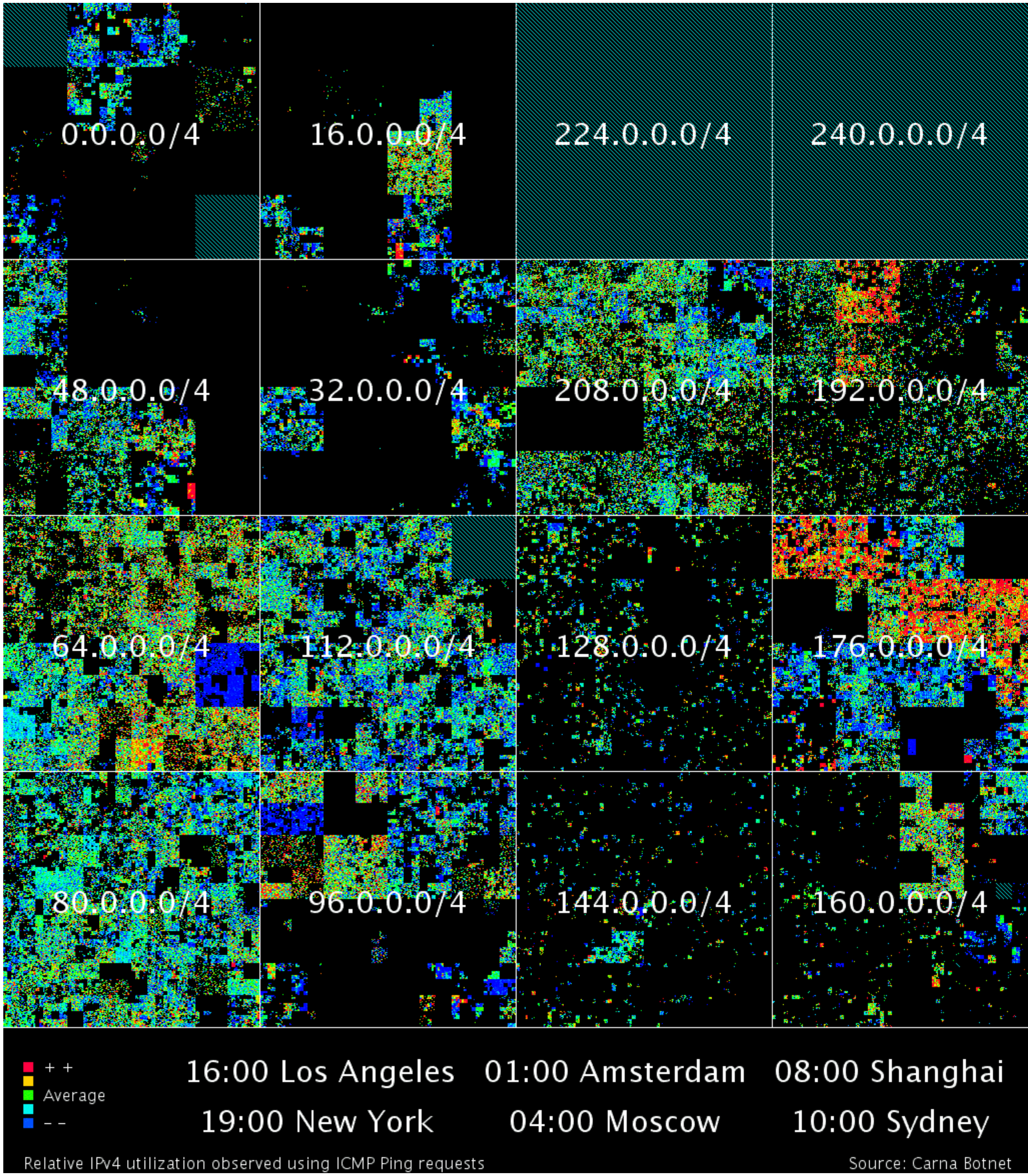
Email: pparth@auscert.org.au

Twitter: http://twitter.com/pparth

Version 1

20 August 2013 – Released to AusCERT members

25 August 2013 – Released to the Public

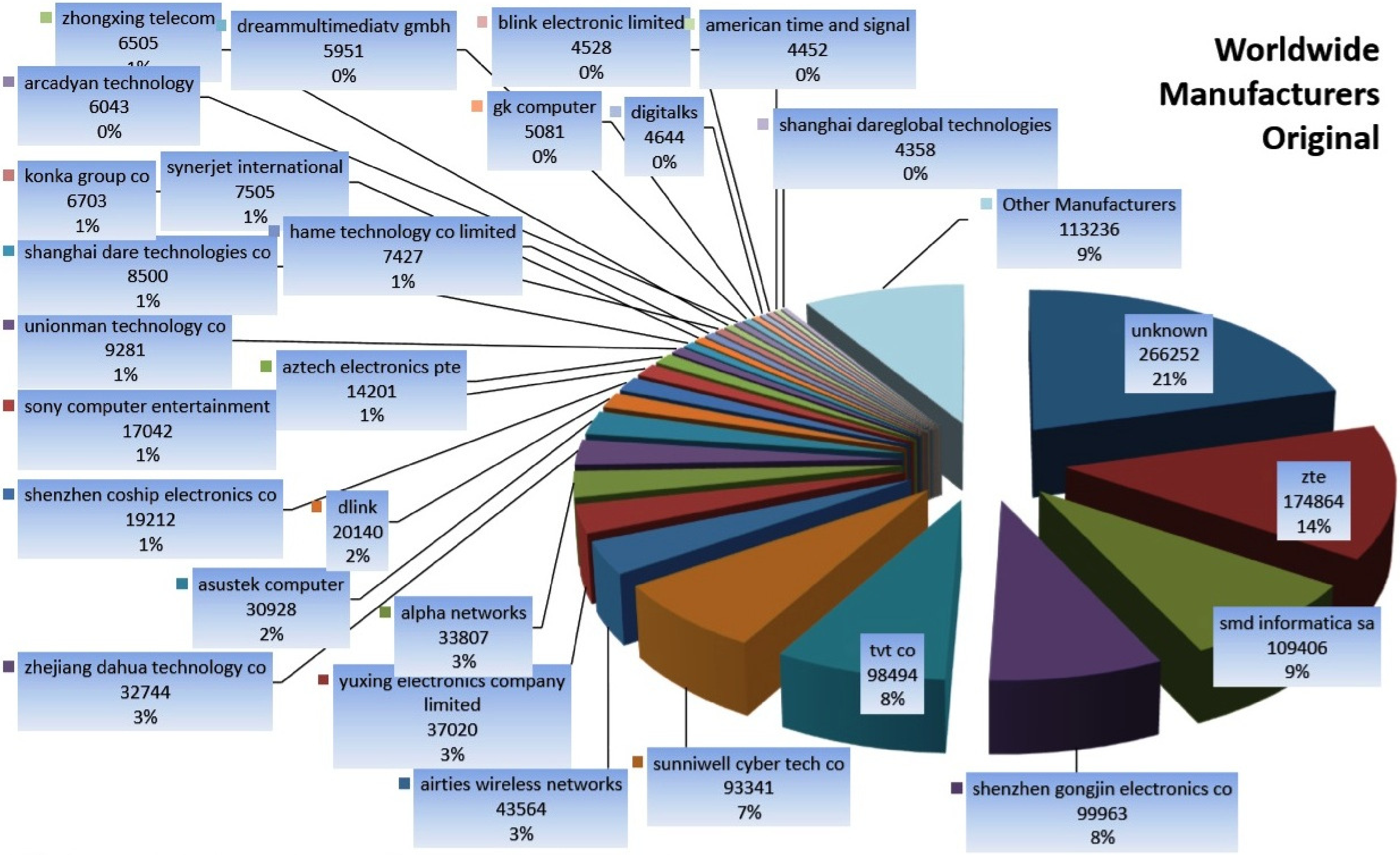


Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet

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

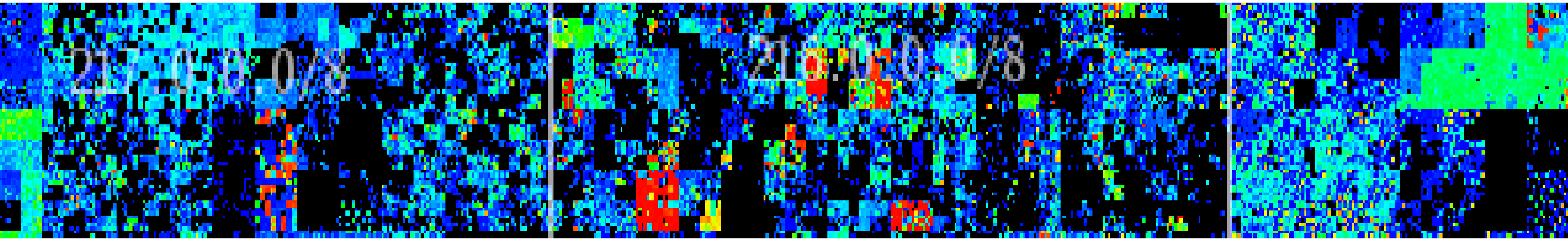
Vulnerable Legacy Devices: “IoT”



Worldwide
Manufacturers
Original

21stC Cybersecurity (1) – *"Integrated Security"*

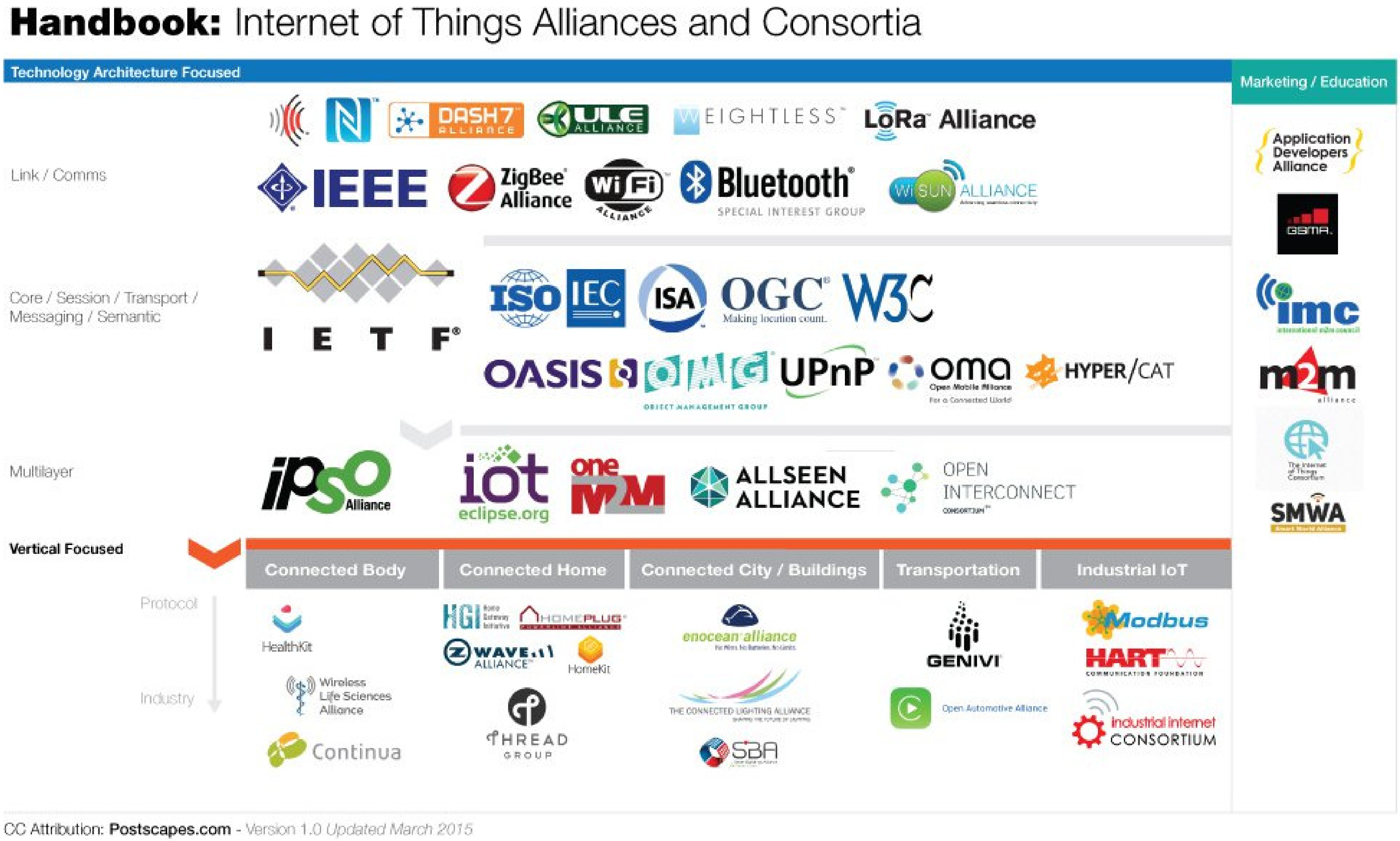
1 – Background: *"21stC Security Landscape"*	2 – Cybersecurity: Players & Targets	3 – Cyber-Physical Threat Scenarios
4 –Banking & Finance: Hybrid Cybersecurity	5 – CSO: Board Level Security Integration	6 – The Enterprise Internet of Things (IoT)
7 –Cyber-Physical Threats from the "IoT"	**8 – Practical Solutions for "IoT" Security**	9 – YOUR TOP 10 Actions & RoadMap



Practical Security Solutions for the “IoT”

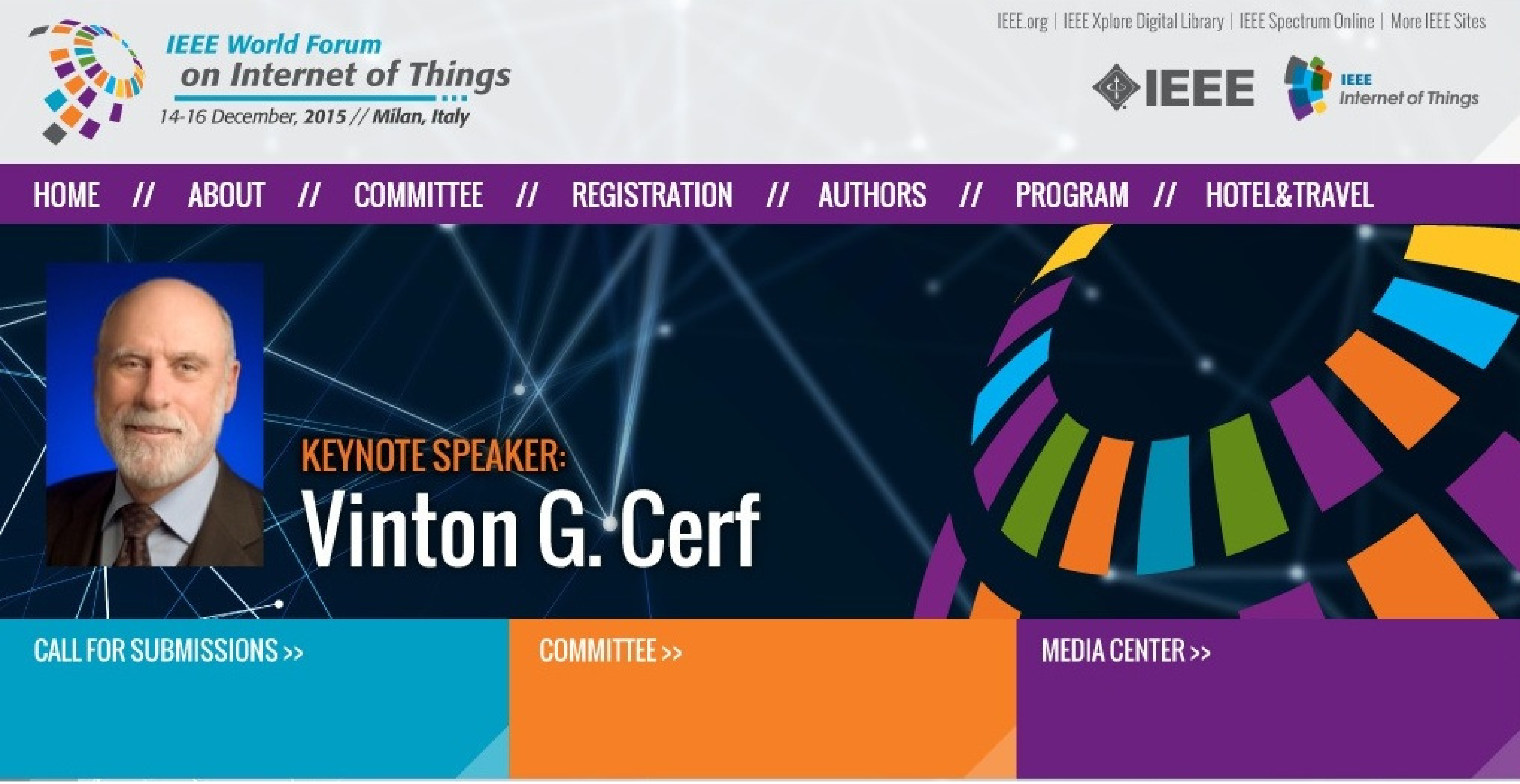
- **European Union - IERC:** Extensive “IoT” research during the last 5 years including security.
- **IEEE IoT Community, Journal & Conference :** Recent international focus upon IoT Security Standards and Engineering Practical Solutions.
- **Advanced Cyber Tools:** Sustainable IoT Network Security requires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

Internet of Things: *Business Alliances*


Handbook: Internet of Things Alliances and Consortia
Technology Architecture Focused
Marketing / Education
Link / Comms
DASH7 ALLIANCE
ULE ALLIANCE
WEIGHTLESS
LoRa Alliance
IEEE
ZigBee Alliance
Wi Fi ALLIANCE
Bluetooth SPECIAL INTEREST GROUP
Wi SUN ALLIANCE
Core / Session / Transport / Messaging / Semantic
I E T F
ISO
IEC
ISA
OGC Making location count.
W3C
OASIS
OMG OBJECT MANAGEMENT GROUP
UPnP
oma Open Mobile Alliance For a Connected World
HYPER/CAT
Multilayer
IPSO Alliance
iot eclipse.org
oneM2M
ALLSEEN ALLIANCE
OPEN INTERCONNECT CONSORTIUM
Vertical Focused
Connected Body
Connected Home
Connected City / Buildings
Transportation
Industrial IoT
Protocol
Industry
HealthKit
Wireless Life Sciences Alliance
Continua
HGI Home Gateway Initiative
HOMEPLUG POWERLINE ALLIANCE
Z-WAVE ALLIANCE
HomeKit
THREAD GROUP
enocean alliance
THE CONNECTED LIGHTING ALLIANCE
SBA
GENIVI
Open Automotive Alliance
Modbus
HART COMMUNICATION FOUNDATION
Industrial Internet CONSORTIUM
Application Developers Alliance
GSMA
imc international m2m council
m2m alliance
The Internet of Things Consortium
SMWA
CC Attribution: Postscapes.com - Version 1.0 Updated March 2015

IEEE World Forum: "Internet of Things"

14th-15th December 2015 – Milan, Italy



IEEE.org | IEEE Xplore Digital Library | IEEE Spectrum Online | More IEEE Sites

IEEE World Forum on Internet of Things

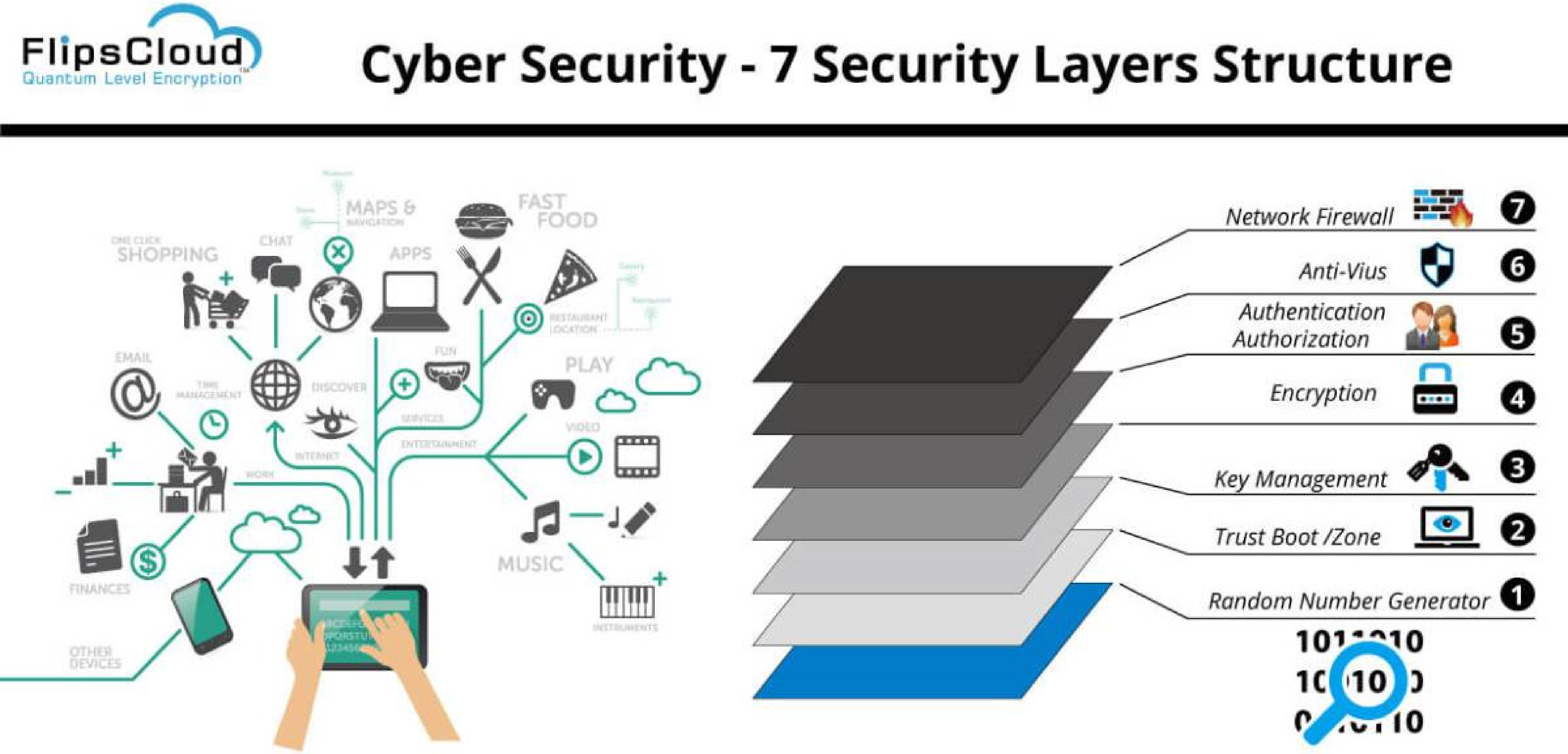
14-16 December, 2015 // Milan, Italy

HOME // ABOUT // COMMITTEE // REGISTRATION // AUTHORS // PROGRAM // HOTEL&TRAVEL

KEYNOTE SPEAKER:
Vinton G. Cerf

CALL FOR SUBMISSIONS >> COMMITTEE >> MEDIA CENTER >>

IoT Cybersecurity: *7-Level Architecture*



Reports: Securing the *"Internet of Things"*

Capgemini Consulting

SOGETI
High Tech

Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT

Deloitte Review

ISSUE 17 | 2015

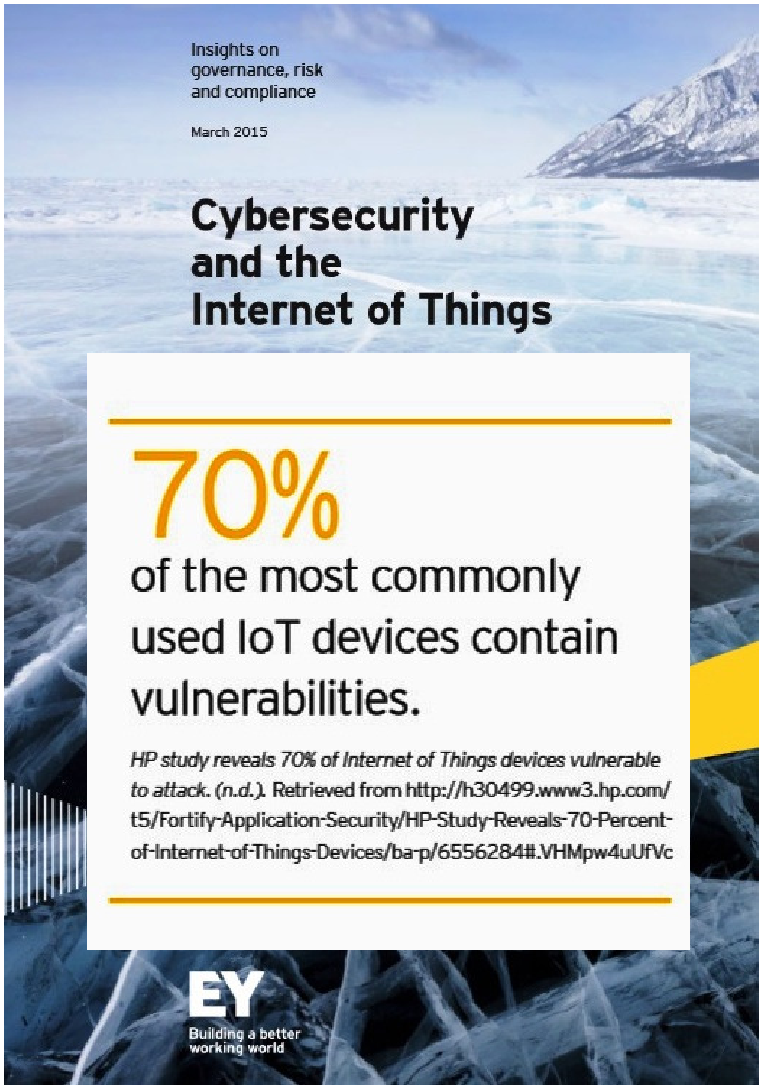
Complimentary article reprint

Safeguarding the Internet of Things

Being secure, vigilant, and resilient in the connected age

BY IRFAN SAIF, SEAN PEASLEY, AND ARUN PERINKOLAM
> ILLUSTRATION BY ALEX NABAUM

Consultant Reports: *Internet of Things*



Insights on
governance, risk
and compliance

March 2015

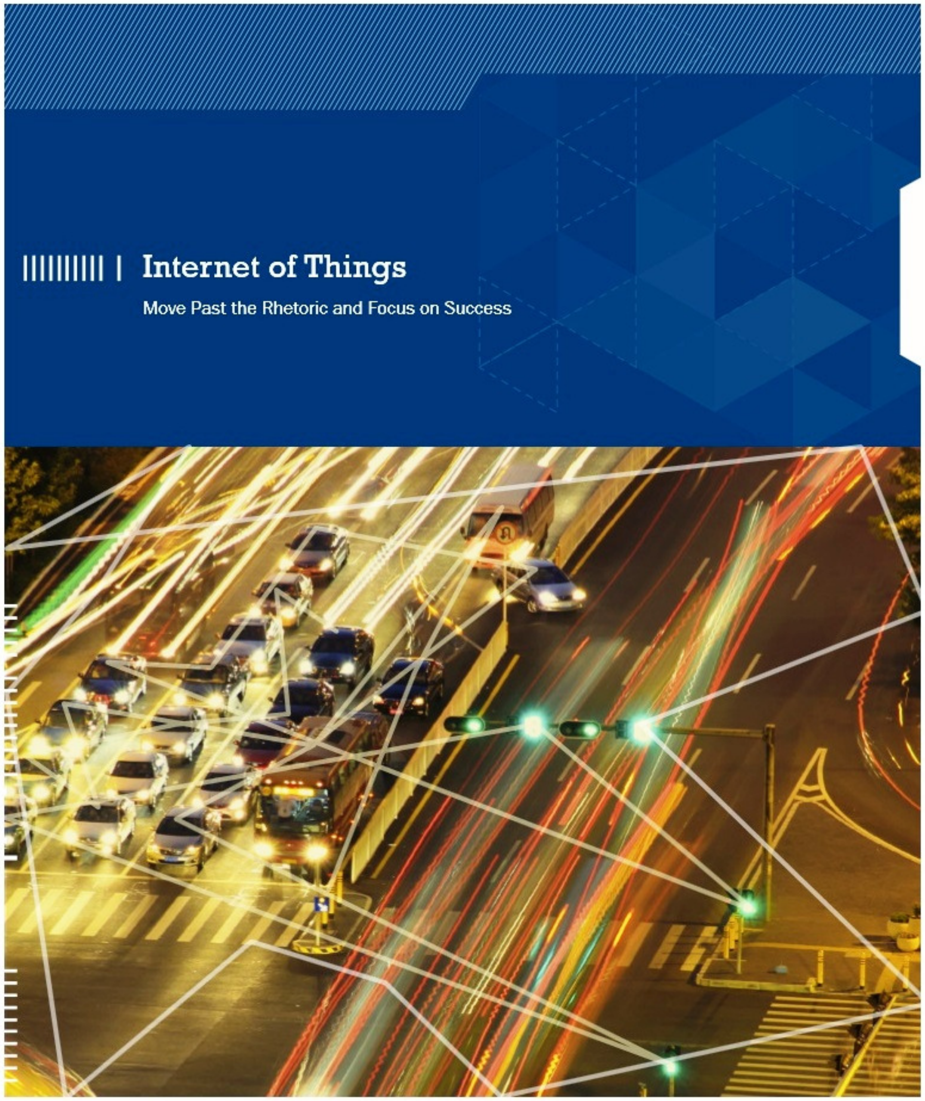
Cybersecurity
and the
Internet of Things

70%
of the most commonly used IoT devices contain vulnerabilities.

HP study reveals 70% of Internet of Things devices vulnerable to attack. (n.d.). Retrieved from http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VHMpw4uUfVc

EY
Building a better
working world

Ernst and Young Global Limited



Internet of Things

Move Past the Rhetoric and Focus on Success

Innovate Forw

Booz, Allen and Hamilton

Hamilton

Ernst and Young *Cybersecurity Reports(1)*

Insights on
governance, risk
and compliance

December 2014

Achieving resilience in the cyber ecosystem

EY
Building a better
working world

Insights on
governance, risk
and compliance

March 2015

Cybersecurity and the Internet of Things

EY
Building a better
working world

Insights on
governance, risk
and compliance
January 2014

Privacy trends 2014
Privacy protection in the age of technology

EY
Building a better
working world

Web: www.ey.com *- Ernst & Young Global Limited*

Ernst and Young *Cybersecurity Reports(2)*

Insights on governance, risk and compliance

October 2014

Cyber program management

Identifying ways to get ahead of cybercrime

EY

Building a better working world

Insights on governance, risk and compliance

November 2014

Cyber threat intelligence – how to get ahead of cybercrime

EY

Building a better working world

Insights on governance, risk and compliance

October 2014

Get ahead of cybercrime

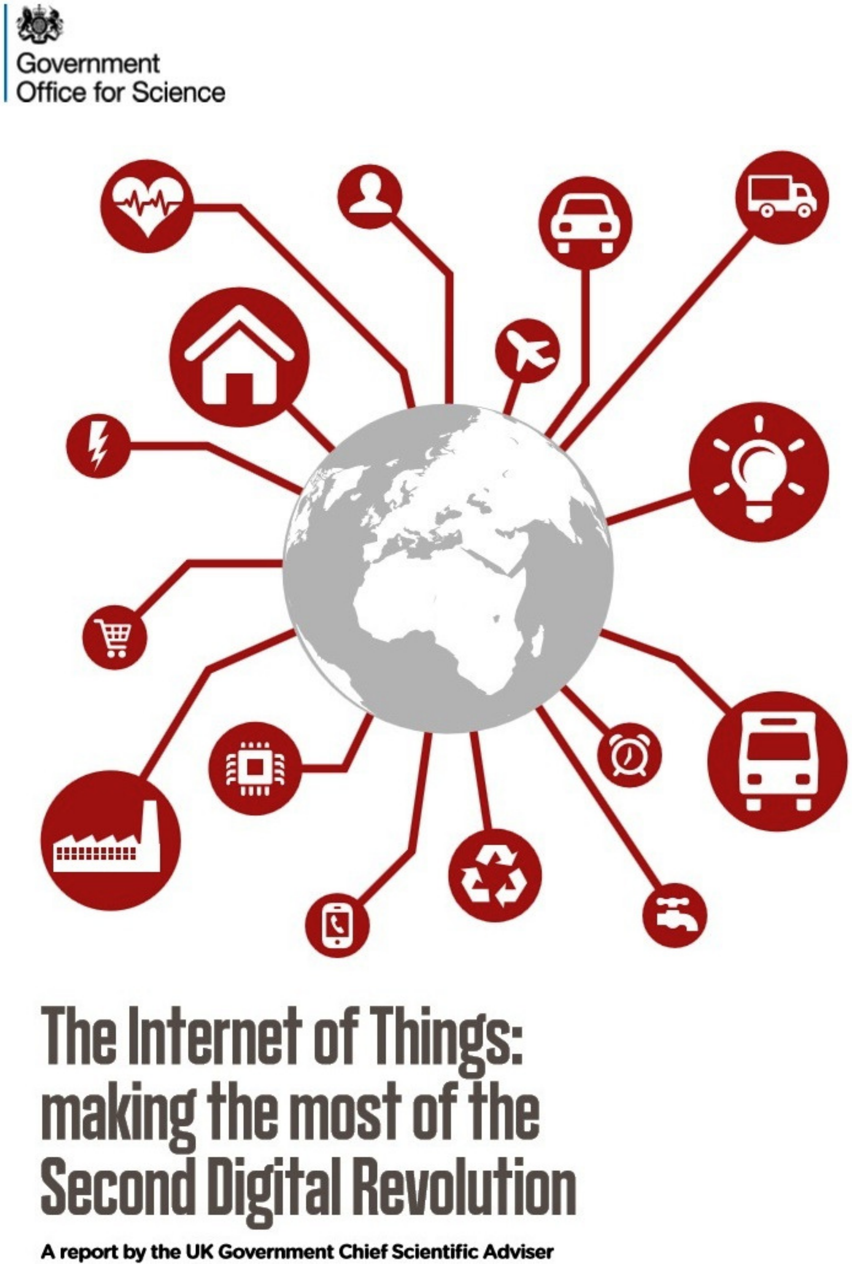
EY's Global Information Security Survey 2014

EY

Building a better working world

Web: www.ey.com *- Ernst & Young Global Limited*

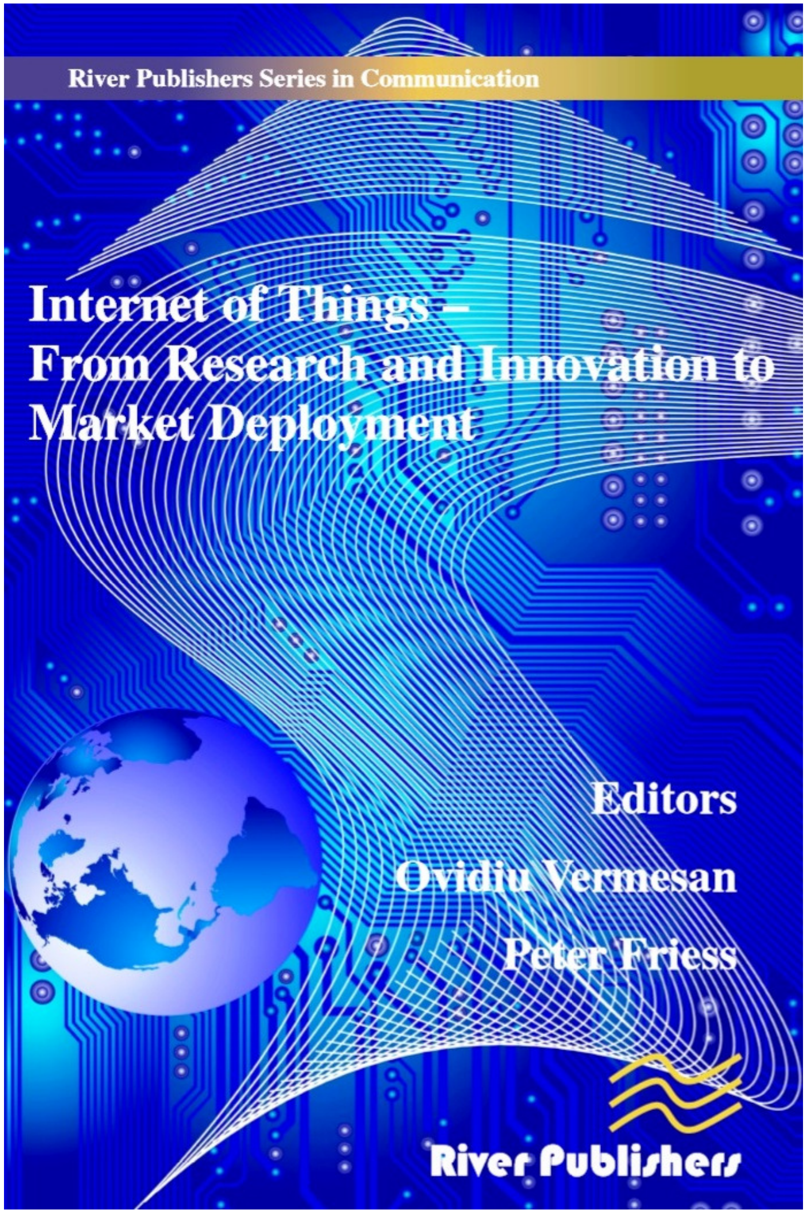
Useful Publications on *“Internet of Things”*



Government
Office for Science

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

A report by the UK Government Chief Scientific Adviser



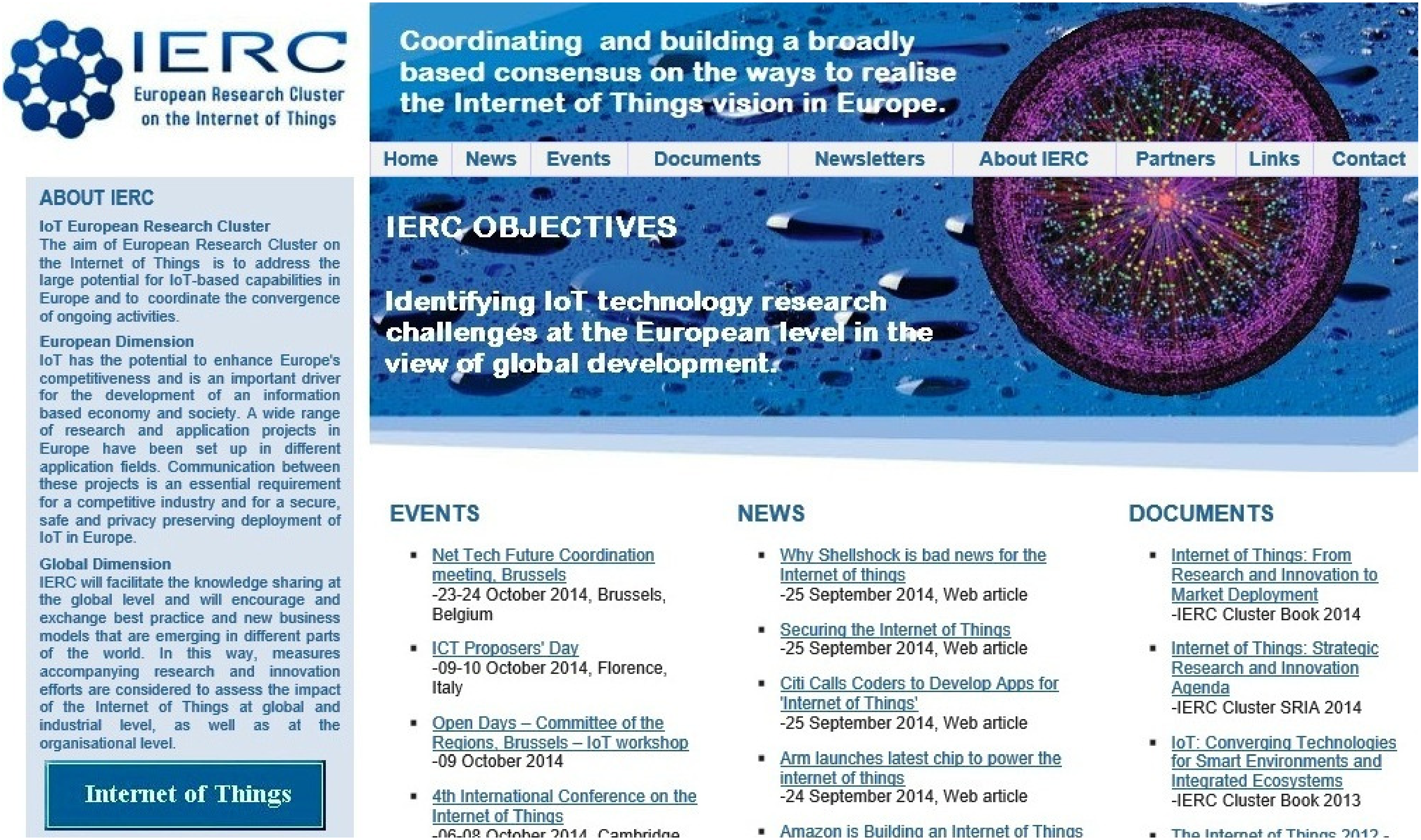
River Publishers Series in Communication

Internet of Things –
From Research and Innovation to
Market Deployment

Editors
Ovidiu Vermesan
Peter Friess

River Publishers

European Research Cluster: *Internet of Things*



IERC

European Research Cluster on the Internet of Things

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

ABOUT IERC

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

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

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

IERC OBJECTIVES

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

EVENTS

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

NEWS

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

DOCUMENTS

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

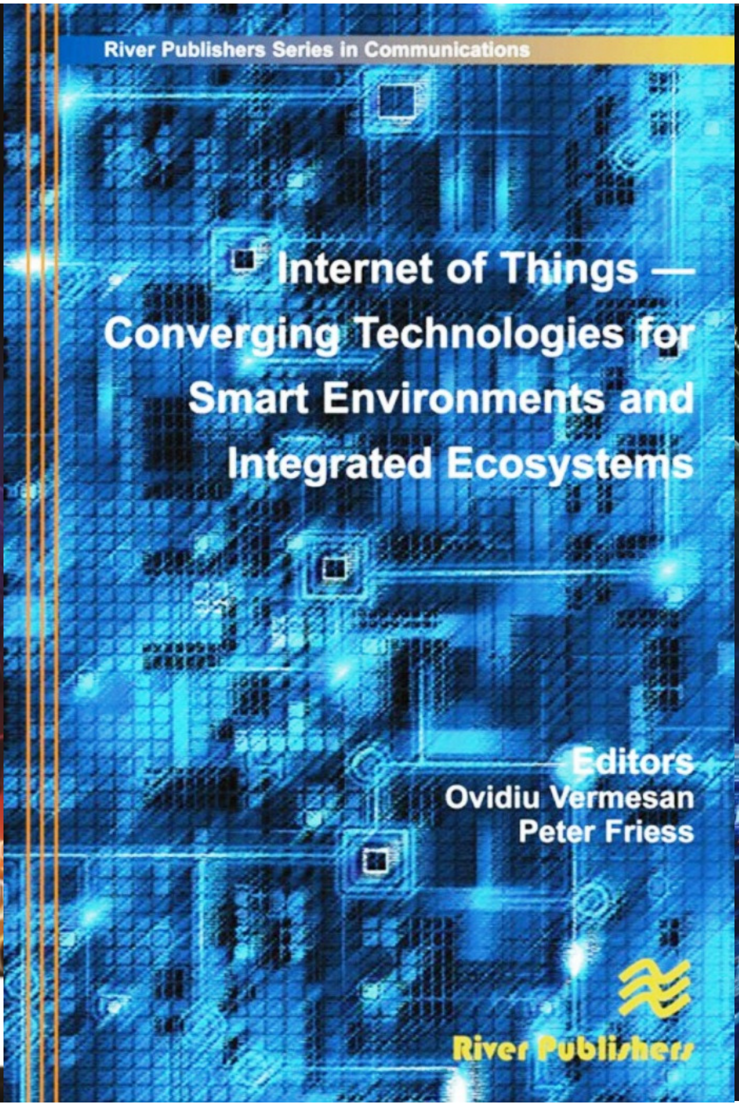
IERC – Research Cluster Reports on *"Smart Systems" & the Internet of Things*

The Internet of Things 2012

New Horizons

CASAGRAS2
an EU Framework 7 Project

IERC
European Research Cluster on the Internet of Things

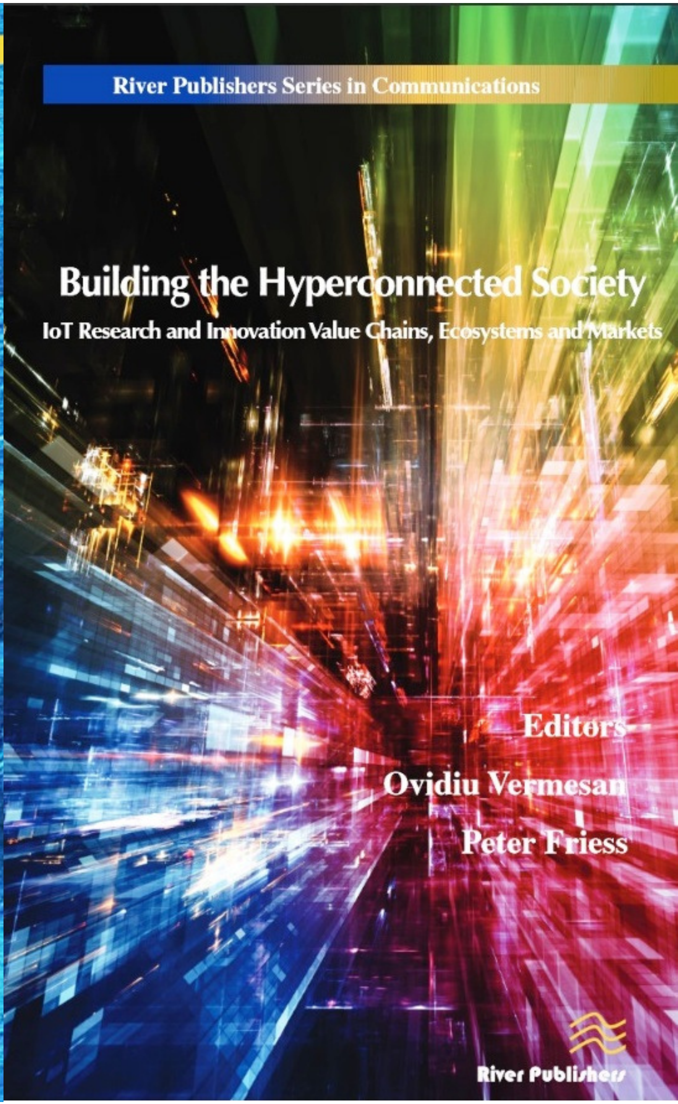


River Publishers Series in Communications

Internet of Things – Converging Technologies for Smart Environments and Integrated Ecosystems

Editors
Ovidiu Vermesan
Peter Friess

River Publishers



River Publishers Series in Communications

Building the Hyperconnected Society

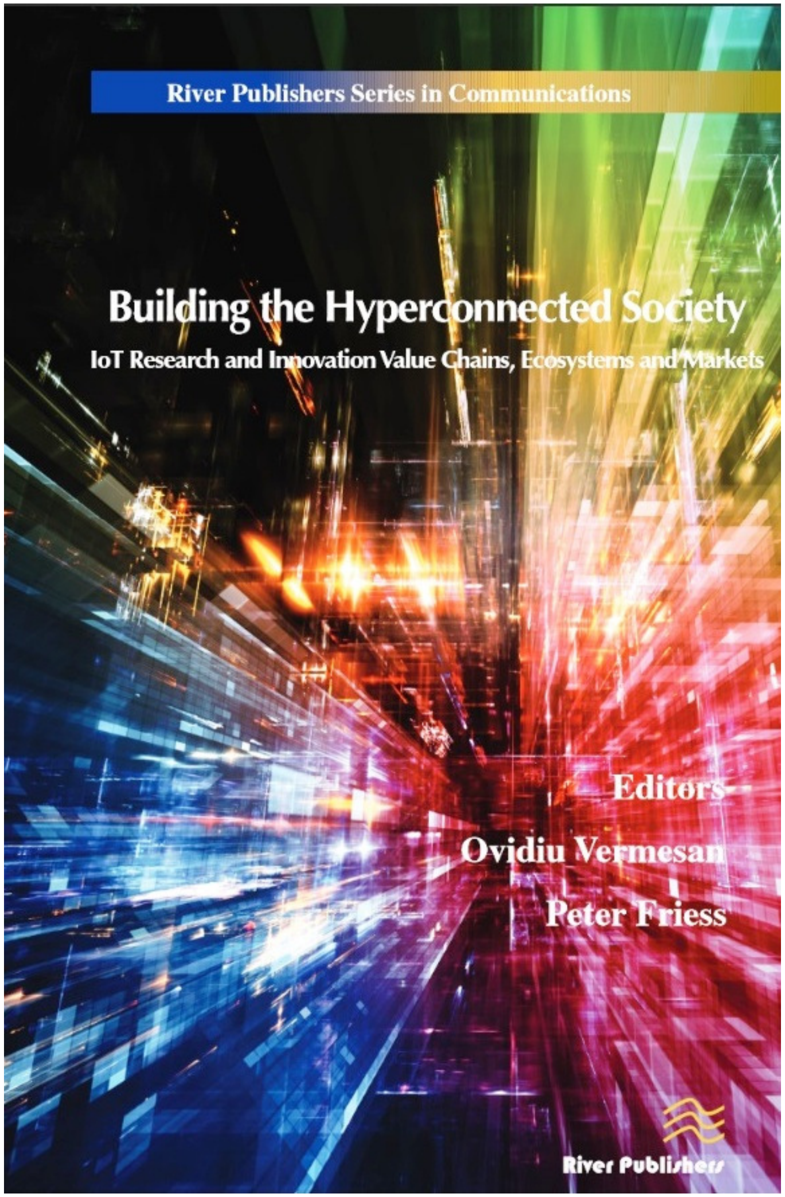
IoT Research and Innovation Value Chains, Ecosystems and Markets

Editors
Ovidiu Vermesan
Peter Friess

River Publishers

- Security the Internet of Things -

Security & Privacy in Hyperconnected Society



River Publishers Series in Communications

Building the Hyperconnected Society

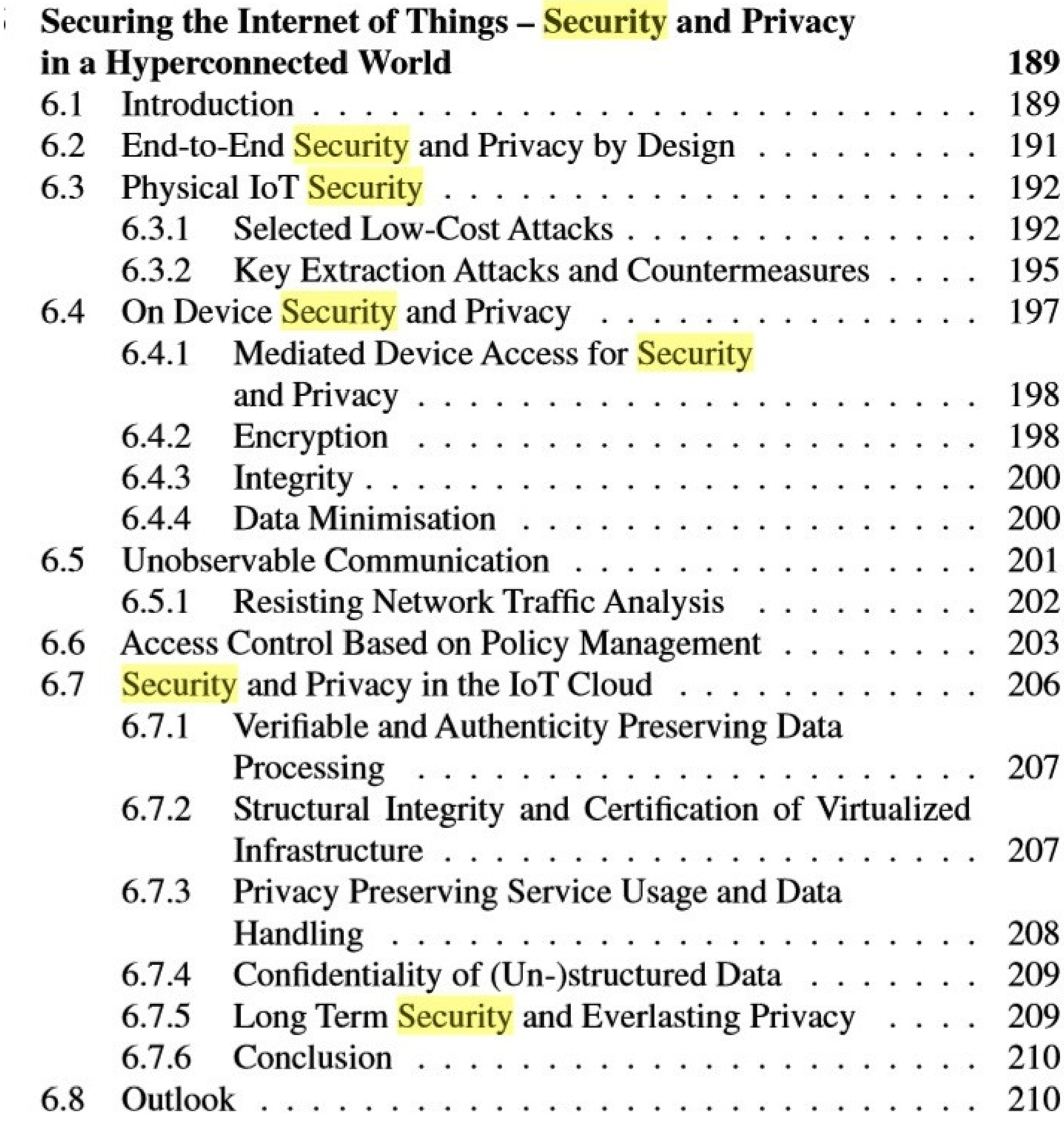
IoT Research and Innovation Value Chains, Ecosystems and Markets

Editors

Ovidiu Vermesan

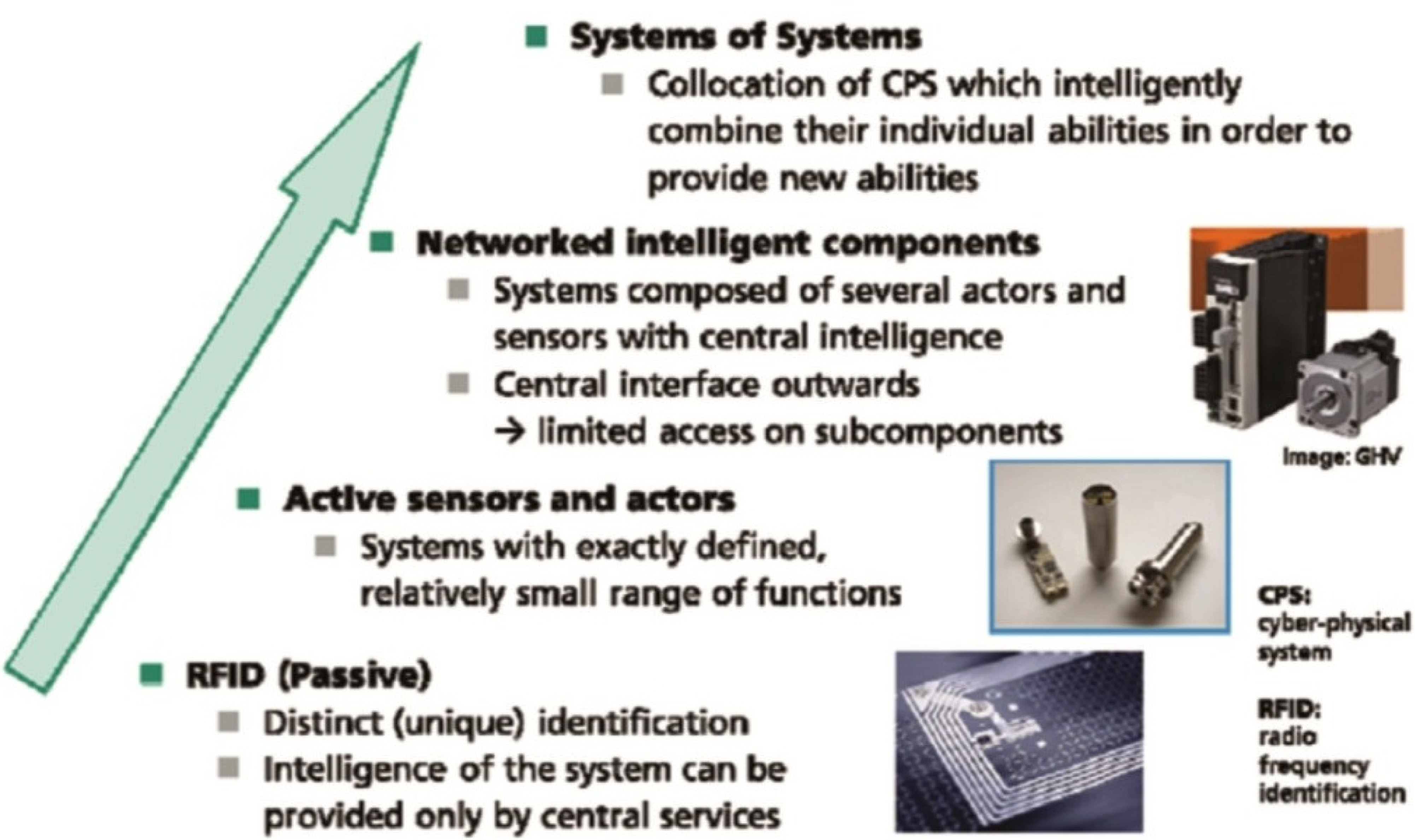
Peter Friess

River Publishers



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

Evolution of *"Cyber-Physical"* Solutions



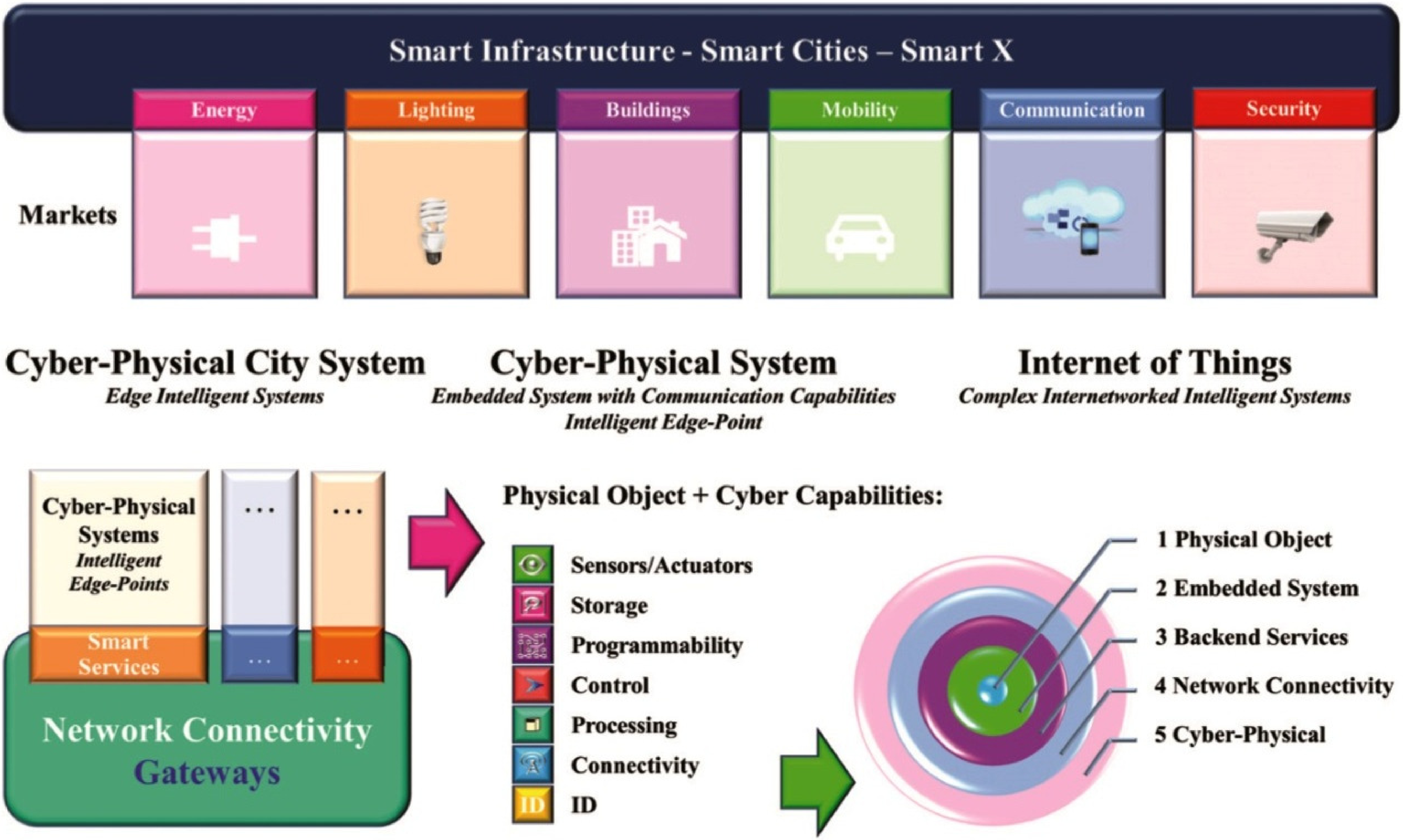
- **Systems of Systems**
  - Collocation of CPS which intelligently combine their individual abilities in order to provide new abilities
- **Networked intelligent components**
  - Systems composed of several actors and sensors with central intelligence
  - Central interface outwards → limited access on subcomponents
- **Active sensors and actors**
  - Systems with exactly defined, relatively small range of functions
- **RFID (Passive)**
  - Distinct (unique) identification
  - Intelligence of the system can be provided only by central services

Image: GHV

CPS: cyber-physical system

RFID: radio frequency identification

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



Smart Infrastructure - Smart Cities – Smart X

Markets

Energy

Lighting

Buildings

Mobility

Communication

Security

Cyber-Physical City System
Edge Intelligent Systems

Cyber-Physical System
Embedded System with Communication Capabilities
Intelligent Edge-Point

Internet of Things
Complex Internetworked Intelligent Systems

Cyber-Physical Systems *Intelligent Edge-Points*

Smart Services

. . .

. . .

Network Connectivity

Gateways

Physical Object + Cyber Capabilities:

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

1 Physical Object

2 Embedded System

3 Backend Services

4 Network Connectivity

5 Cyber-Physical

Cyber-Physical System Modules for "IoT"

Cyber-Physical System

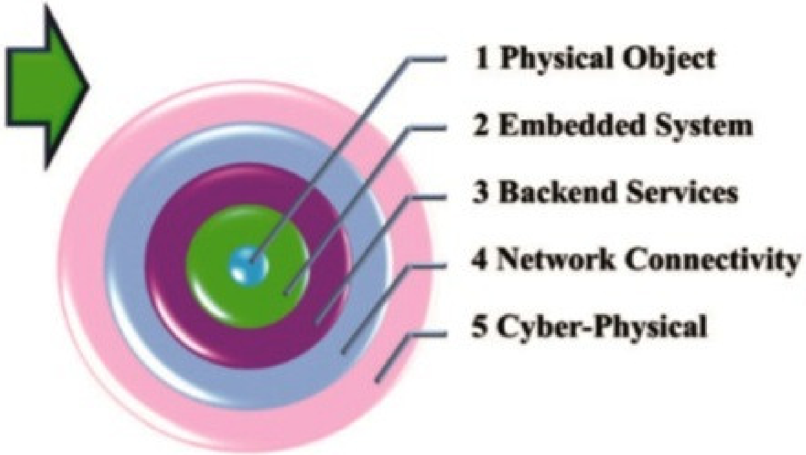
Embedded System with Communication Capabilities
Intelligent Edge-Point

Physical Object + Cyber Capabilities:

- 🟩 Sensors/Actuators
- 🟪 Storage
- 🟪 Programmability
- 🟥 Control
- 🟩 Processing
- 🟦 Connectivity
- 🟨 ID

Internet of Energy

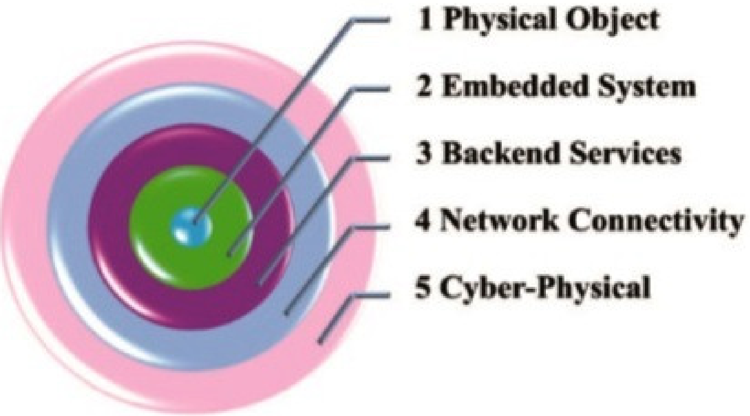
Internetworked Intelligent Systems



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

Internet of Lighting

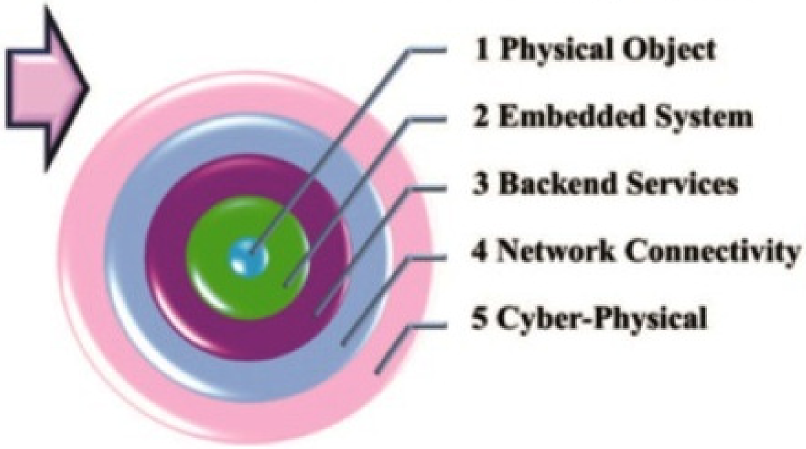
Internetworked Intelligent Systems



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

Internet of Buildings

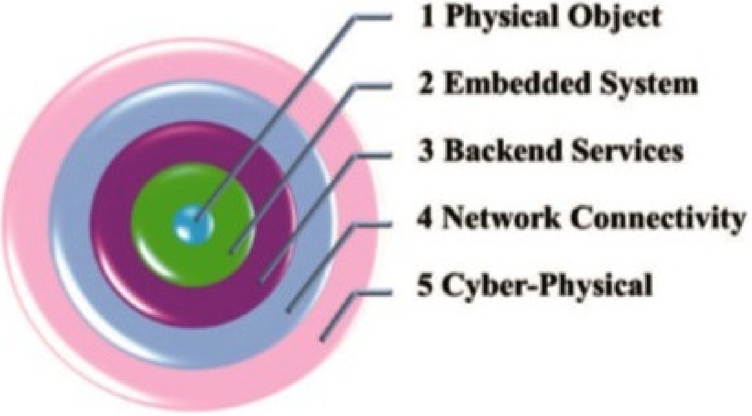
Internetworked Intelligent Systems



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

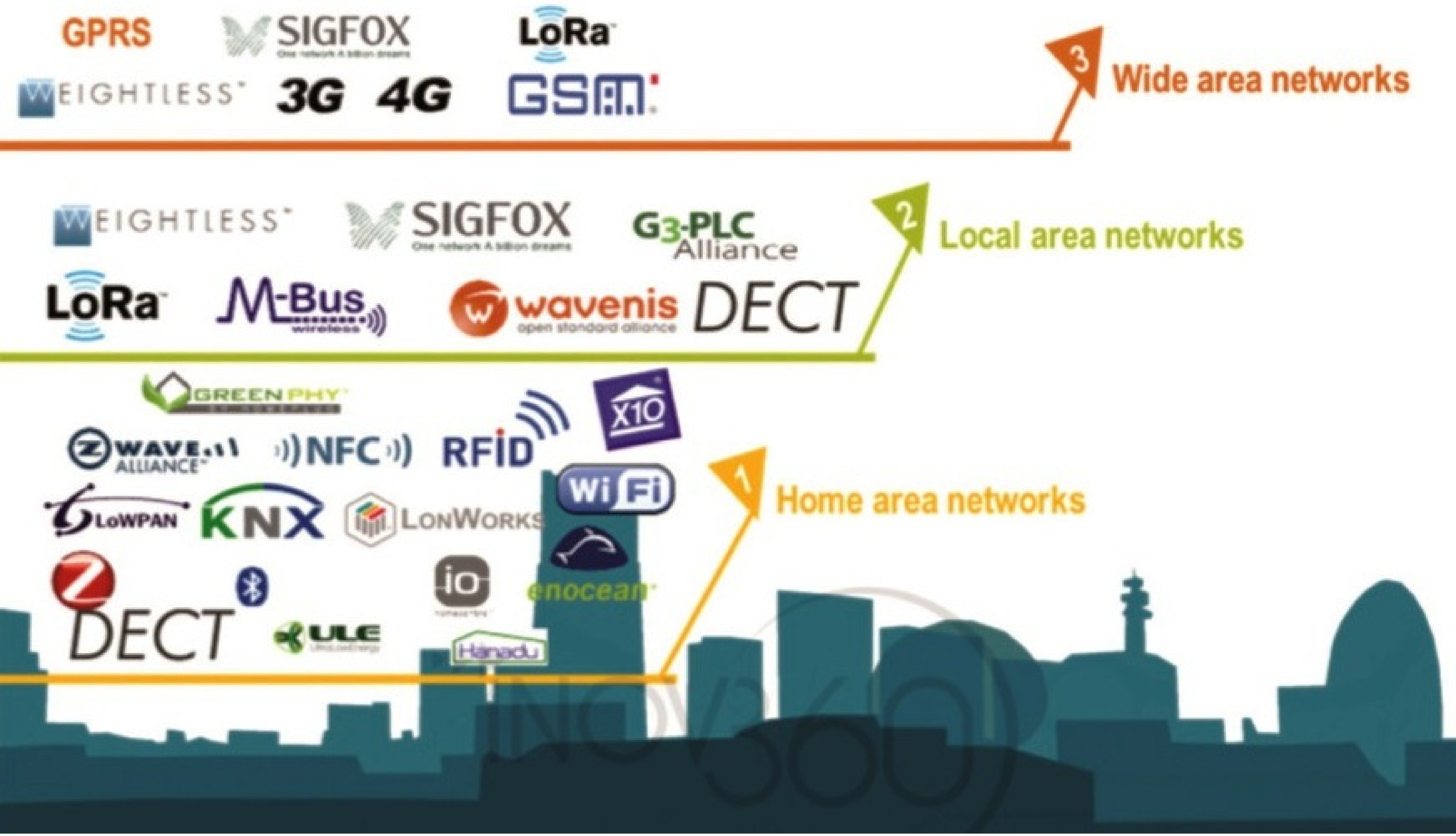
Internet of Vehicles

Internetworked Intelligent Systems

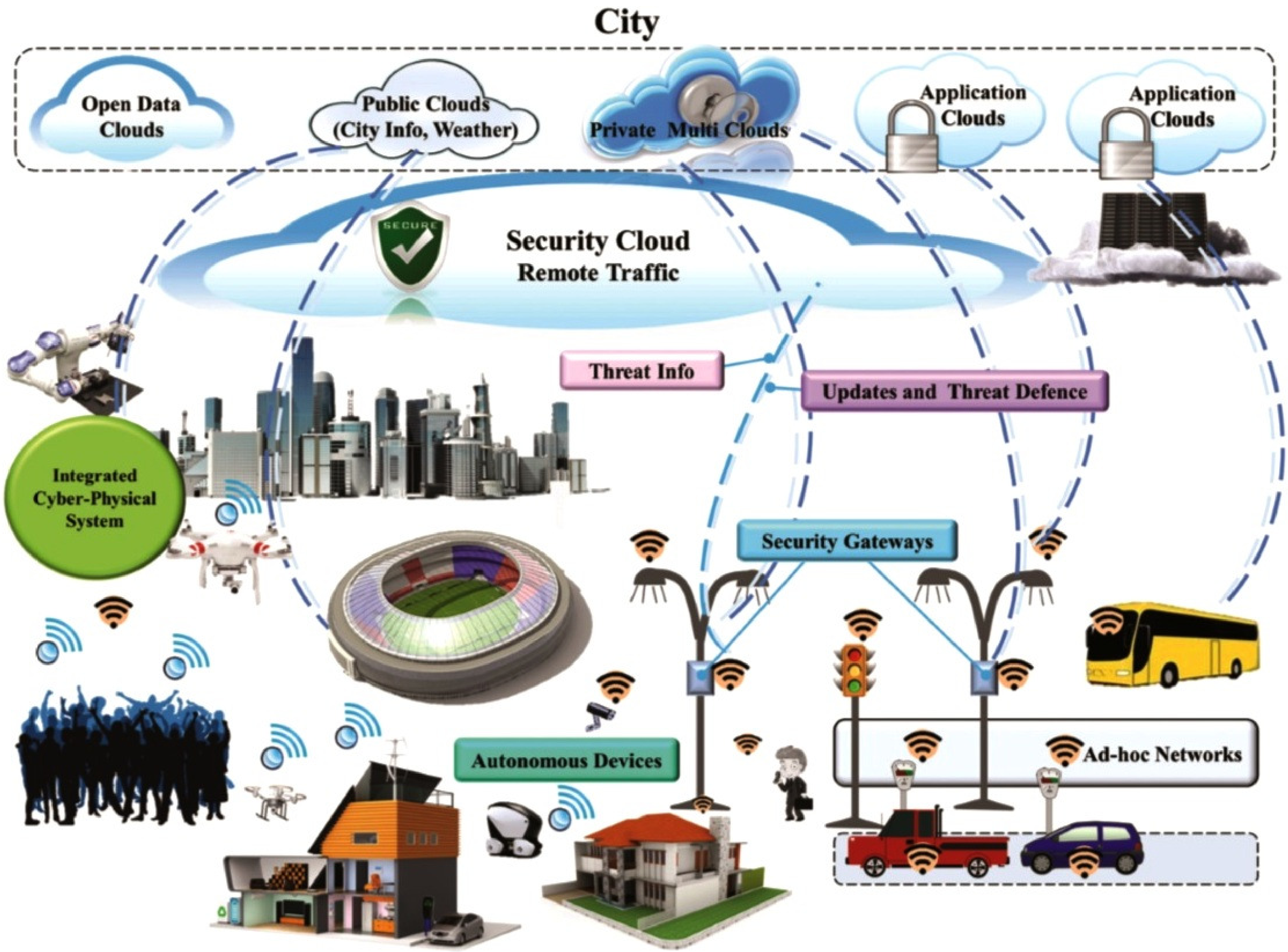


1 Physical Object
2 Embedded System
3 Backend Services
4 Network Connectivity
5 Cyber-Physical

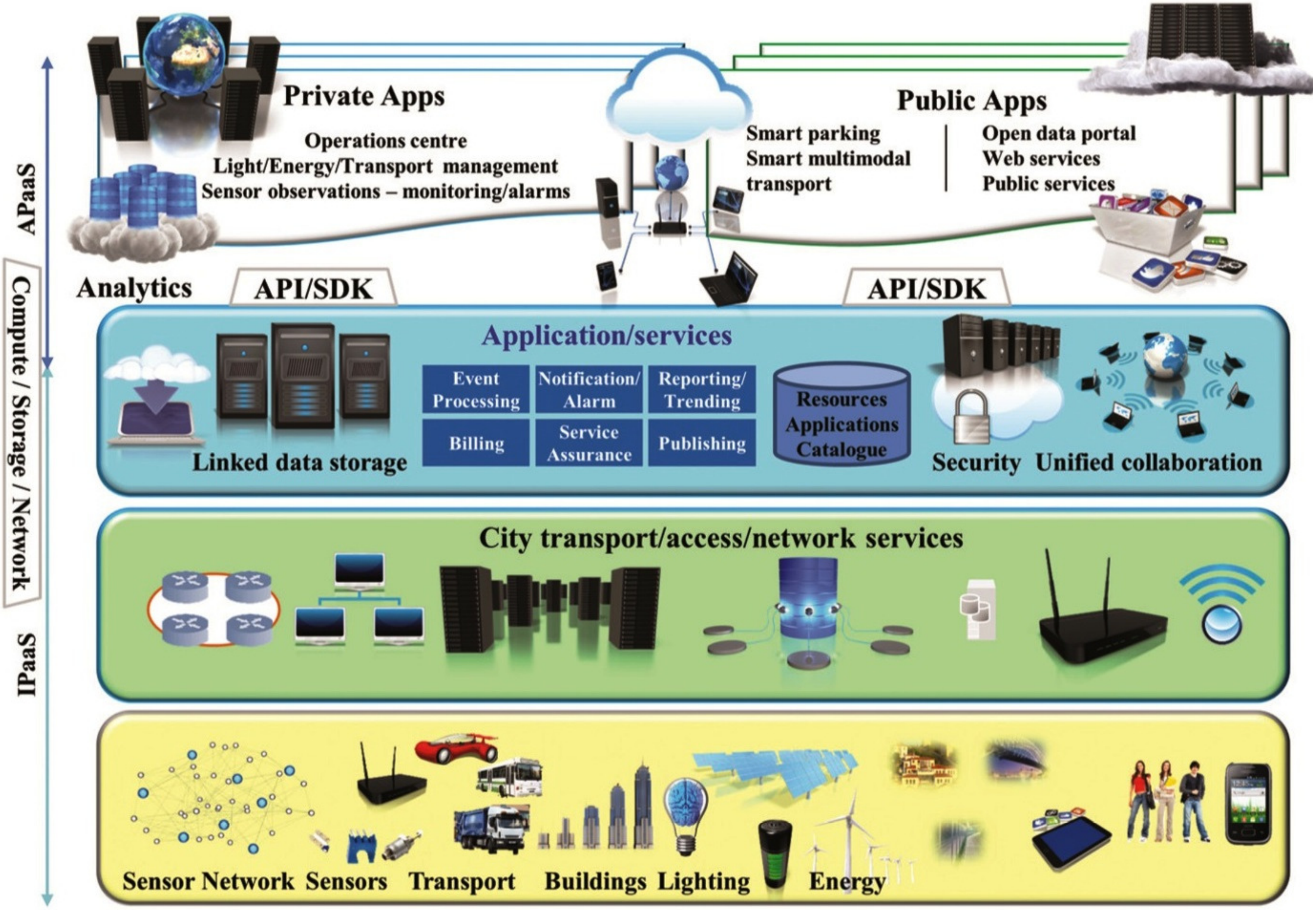
"IoT": Communications Standards



Smart City: *Multi-Layer Security Framework*

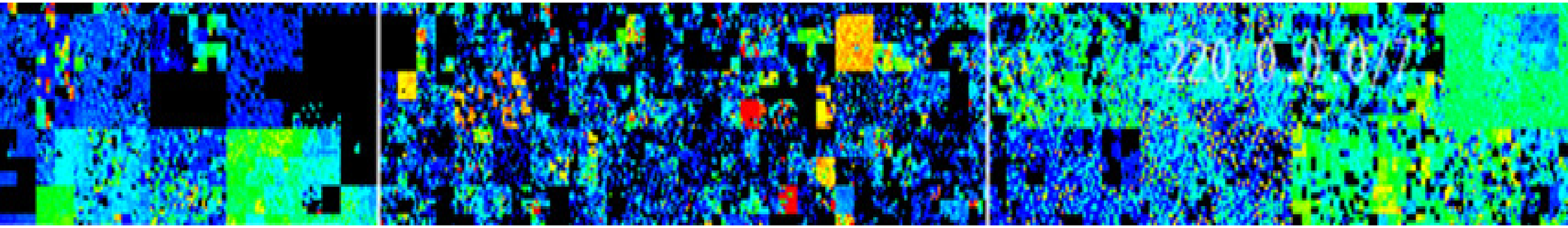


Smart City: *Multi-Layered Architecture*



21stC Cybersecurity (1) – *"Integrated Security"*

1 – Background: *"21stC Security Landscape"*	**2 – Cybersecurity: Players & Targets**	**3 – Cyber-Physical Threat Scenarios**
4 –Banking & Finance: Hybrid Cybersecurity	**5 – CSO: Board Level Security Integration**	**6 – The Enterprise Internet of Things (IoT)**
7 – Cyber-Physical Threats from the "IoT"	**8 – Practical Solutions for IoT Security**	**9 – YOUR TOP 10 Actions & RoadMap**



YOUR TOP 10 *Integrated Security Actions*

1) CSO – Chief Security Officer's Team – Board Level Roles & Responsibilities
2) Professional Training – Suggest Top-Level CISSP Certification for Team
3) Implement International Security Standards (ISO/IEC- 27000)
4) Develop Professional CERT Team
5) Profile YOUR Security Staff and Contractors for Possible Risks

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

Later, in the 2nd Presentation, we'll review **Advanced Cybersecurity Developments**

Cybersecurity Trends (1): "Integrated Security"

International East-West Security Conference: Madrid, Spain

Thank-You!...

Download Presentation Slides:

www.Valentina.net/Madrid2015/

East-West Security Conference – Spain2015

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

* 21stC Cybersecurity Trends (1) *

"Integrated Security"

- Securing the Internet of Things –

Dr David E. Probert

VAZA International

Dedicated to

32nd International East/West Security Conference

"Integrated Cyber-Physical Security and Securing the Enterprise Internet of Things"
- Madrid, Spain: 26th–27th Oct 2015 -
© *Dr David E. Probert* : www.VAZA.com ©

1

* 21stC Cybersecurity Trends (2) *

"Advanced Cybersecurity"

- Artificial Intelligence & Machine Learning -

Dr David E. Probert

VAZA International

Dedicated to

32nd International East/West Security Conference

"Advanced Enterprise Cybersecurity – Artificial Intelligence & Machine Learning"
Madrid, Spain: 26th – 27th Oct 2915
© Dr David E. Probert : www.VAZA.com ©

1

Theme (1) – "Integrated Security"

Theme (2) – "Advanced Cybersecurity"

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

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

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

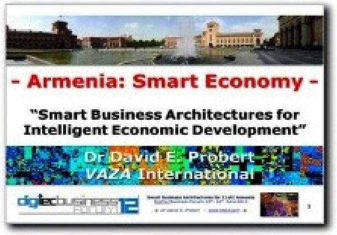
"Master Class - Smart Theory & Practice

Smart Solutions: "Master Class" – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

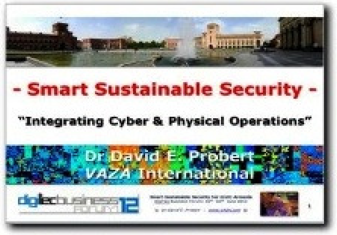
"Master Class 2012 - Smart Design"


- 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

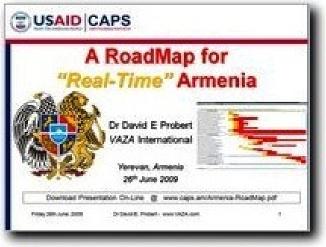
Awesome Armenia: In Photos

"Roadmap for Real-Time Armenia"

E-Government, E-Commerce and E-Security

USAID | CAPS

Roadmap for Real-Time Armenia- Report

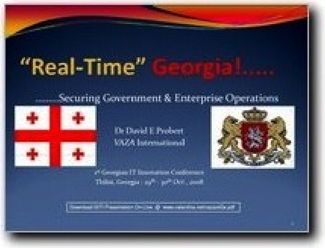

USAID | CAPS

A RoadMap for "Real-Time" Armenia

Dr David E Probert
VAZA International

Yerevan, Armenia
26th June 2009

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"

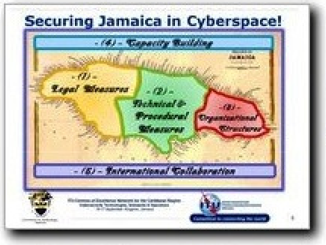
"Integrated Cyber & Physical Security"

for e-Government & e-Georgia

Dr David E. Probert
VAZA International

GITI

21stC Georgia - "CyberVardzia" - Slides


Securing Jamaica in Cyberspace!

- (4) - Capacity Building

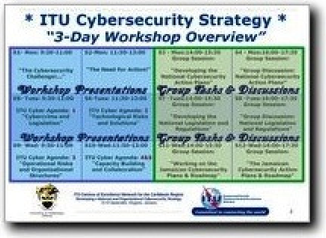
- (1) - Legal Measures

- (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)

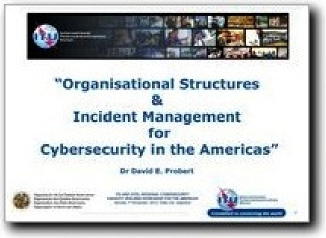
Dr. David Probert is the Founder and Executive Director of VAZA International which focused upon projects, consultancy and workshops primarily in the fields of Cybersecurity, eGovernment and Real-Time Networking Solutions. He has worked on Security Projects for several International Agencies including the ITU, USAID and the European Union in countries including Georgia, Armenia & Jamaica.

Prior to the establishment of VAZA, Dr. Probert was the Chief Technology Officer for a Major UK Security plc which delivered customized networked security solutions for governments, and across sectors such as transportation, healthcare & education.

From 2000 to 2003, Dr. Probert worked as Vice President for Madge Networks where he was responsible for the development of Secure Wireless Networking Products , using advanced authentication techniques.

From 1987 to 1999, he worked for the Digital Equipment Corporation where he held several senior positions including European Director for Value Added Networks & European Director for the Internet Business Group. During this time he represented Digital on the European Board for TERENA (Trans-European Research and Academic Networks Association), and headed up several international projects including the AsiaNet Project for Nuclear & Environmental Security in the Russian Arctic Kola Peninsula. He was also Project Director for the Multi-Media & eCommerce Website for the World's 1st Supersonic Car – ThrustSSC.

"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

digitecbusiness FORUM 12

"Master Class - Smart Theory"

Smart Solutions: "Master Class" – Part 2

- Smart Solutions in Practice for 21stC Armenia -

Dr David E. Probert
VAZA International

digitecbusiness FORUM 12

"Master Class - Smart Practice"

Smart Solutions: "Master Class" – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

digitecbusiness FORUM 12

"Master Class - Smart Design"

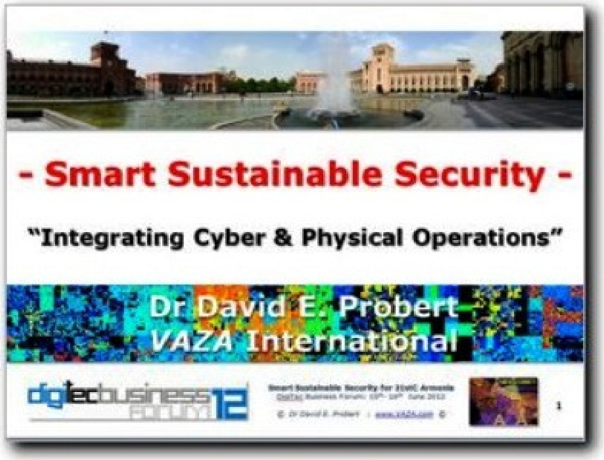
- Armenia: Smart Economy -

"Smart Business Architectures for Intelligent Economic Development"

Dr David E. Probert
VAZA International

digitecbusiness FORUM 12

"Armenia: Smart Economy"



- Smart Sustainable Security -

"Integrating Cyber & Physical Operations"

Dr David E. Probert
VAZA International

digitecbusiness FORUM 12

"Armenia: Smart Sustainable Security"

- Smart Governance -

"Stimulating Innovation & Economic Growth"

Dr David E. Probert
VAZA International

digitecbusiness FORUM 12

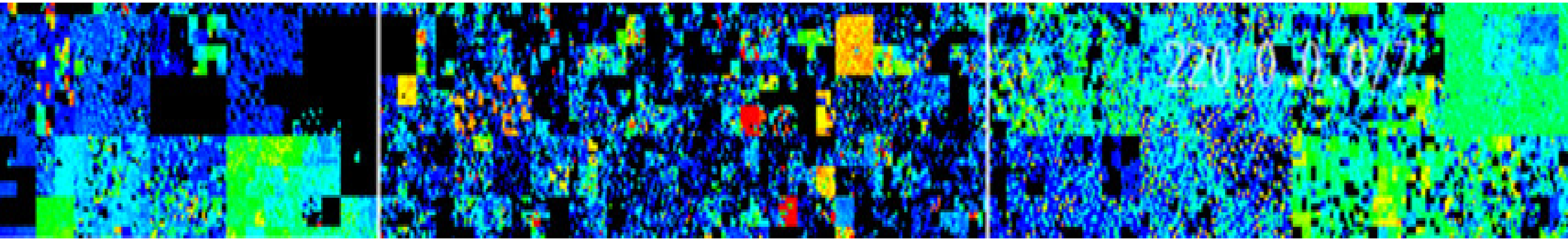
"Armenia: Smart Governance"

Download: www.valentina.net/DigiTec2012/

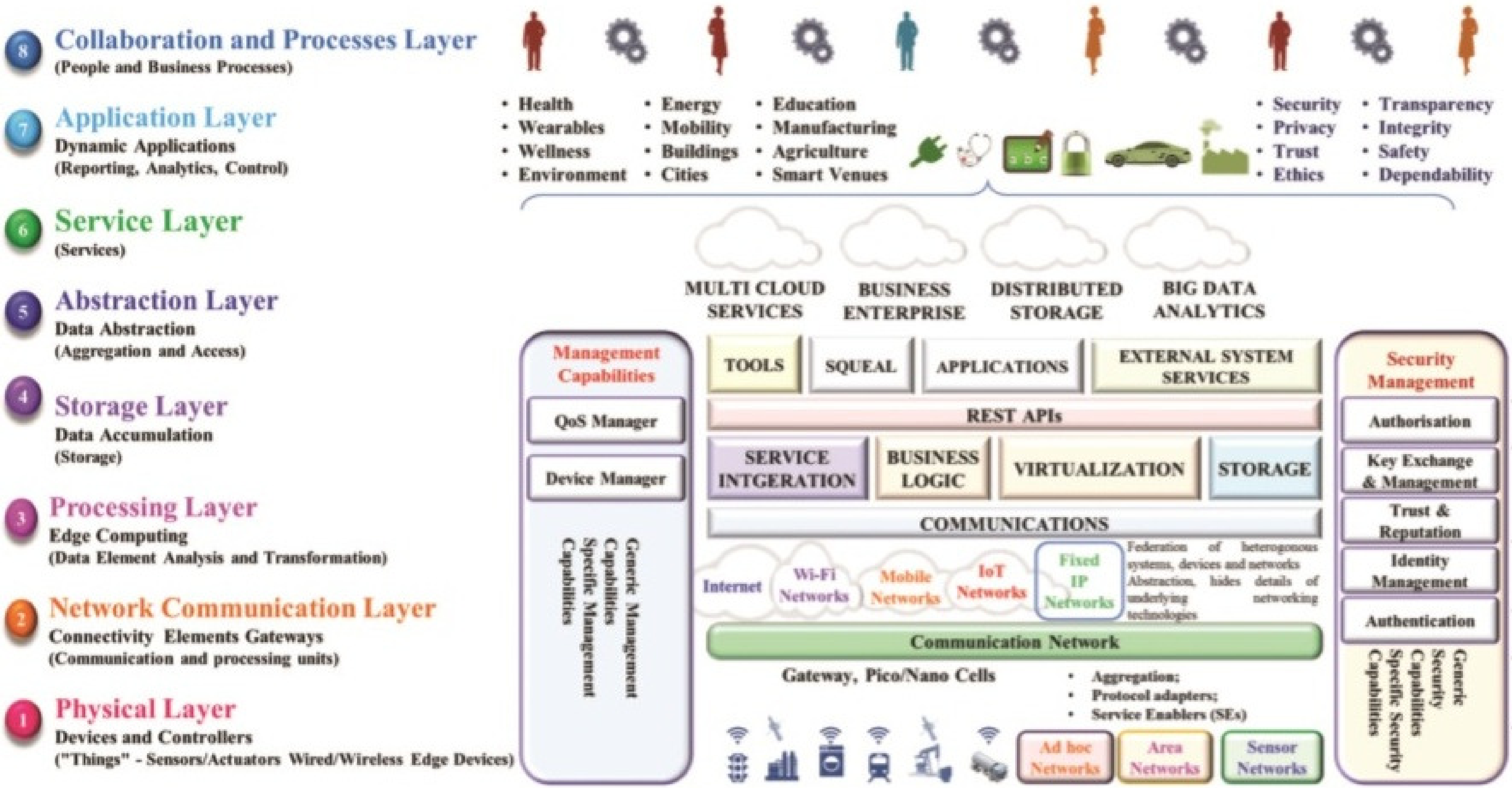
Cybersecurity Trends (1) : “Integrated Security”

International East-West Security Conference: Madrid, Spain

BACK-UP SLIDES



"Internet of Things" *Practical Architecture*



8 **Collaboration and Processes Layer**
(People and Business Processes)

7 **Application Layer**
Dynamic Applications
(Reporting, Analytics, Control)

6 **Service Layer**
(Services)

5 **Abstraction Layer**
Data Abstraction
(Aggregation and Access)

4 **Storage Layer**
Data Accumulation
(Storage)

3 **Processing Layer**
Edge Computing
(Data Element Analysis and Transformation)

2 **Network Communication Layer**
Connectivity Elements Gateways
(Communication and processing units)

1 **Physical Layer**
Devices and Controllers
("Things" - Sensors/Actuators Wired/Wireless Edge Devices)

- Health
- Wearables
- Wellness
- Environment

- Energy
- Mobility
- Buildings
- Cities

- Education
- Manufacturing
- Agriculture
- Smart Venues

- Security
- Privacy
- Trust
- Ethics

- Transparency
- Integrity
- Safety
- Dependability

MULTI CLOUD SERVICES

BUSINESS ENTERPRISE

DISTRIBUTED STORAGE

BIG DATA ANALYTICS

Management Capabilities

QoS Manager

Device Manager

Generic Management Capabilities

Specific Management Capabilities

TOOLS

SQUEAL

APPLICATIONS

EXTERNAL SYSTEM SERVICES

REST APIs

SERVICE INTGERATION

BUSINESS LOGIC

VIRTUALIZATION

STORAGE

COMMUNICATIONS

Internet

Wi-Fi Networks

Mobile Networks

IoT Networks

Fixed IP Networks

Federation of heterogeneous systems, devices and networks
Abstraction, hides details of underlying networking technologies

Communication Network

Gateway, Pico/Nano Cells

- Aggregation;
- Protocol adapters;
- Service Enablers (SEs)

Ad hoc Networks

Area Networks

Sensor Networks

Security Management

Authorisation

Key Exchange & Management

Trust & Reputation

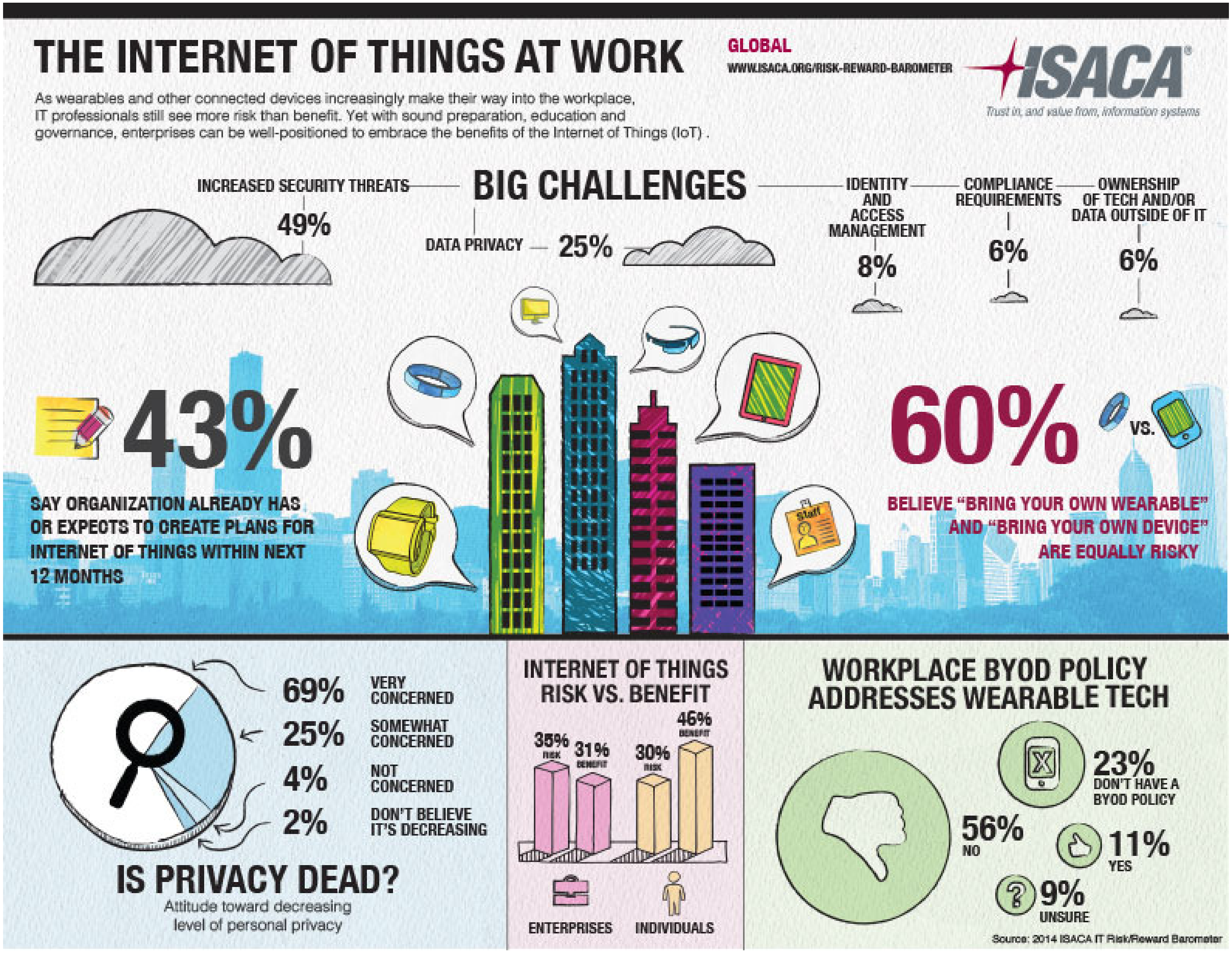
Identity Management

Authentication

Generic Security Capabilities

Specific Security Capabilities

Internet of Things: *Business Reality!*



THE INTERNET OF THINGS AT WORK

GLOBAL

WWW.ISACA.ORG/RISK-REWARD-BAROMETER

ISACA® Trust in, and value from, information systems

As wearables and other connected devices increasingly make their way into the workplace, IT professionals still see more risk than benefit. Yet with sound preparation, education and governance, enterprises can be well-positioned to embrace the benefits of the Internet of Things (IoT) .

BIG CHALLENGES

INCREASED SECURITY THREATS 49%
DATA PRIVACY 25%
IDENTITY AND ACCESS MANAGEMENT 8%
COMPLIANCE REQUIREMENTS 6%
OWNERSHIP OF TECH AND/OR DATA OUTSIDE OF IT 6%
Staff
VS.

43% SAY ORGANIZATION ALREADY HAS OR EXPECTS TO CREATE PLANS FOR INTERNET OF THINGS WITHIN NEXT 12 MONTHS

60% BELIEVE "BRING YOUR OWN WEARABLE" AND "BRING YOUR OWN DEVICE" ARE EQUALLY RISKY

IS PRIVACY DEAD?

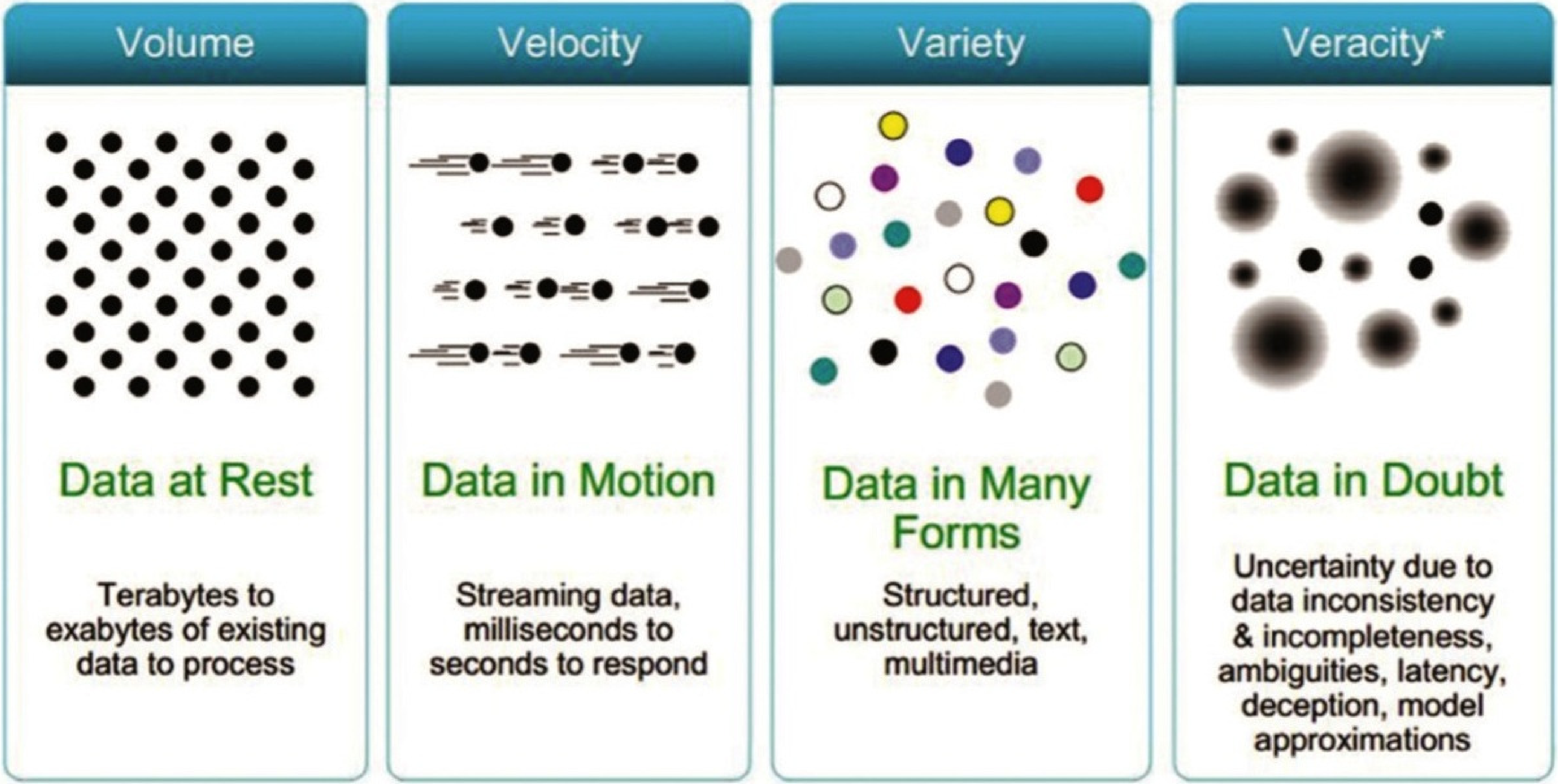
Attitude toward decreasing level of personal privacy

INTERNET OF THINGS RISK VS. BENEFIT

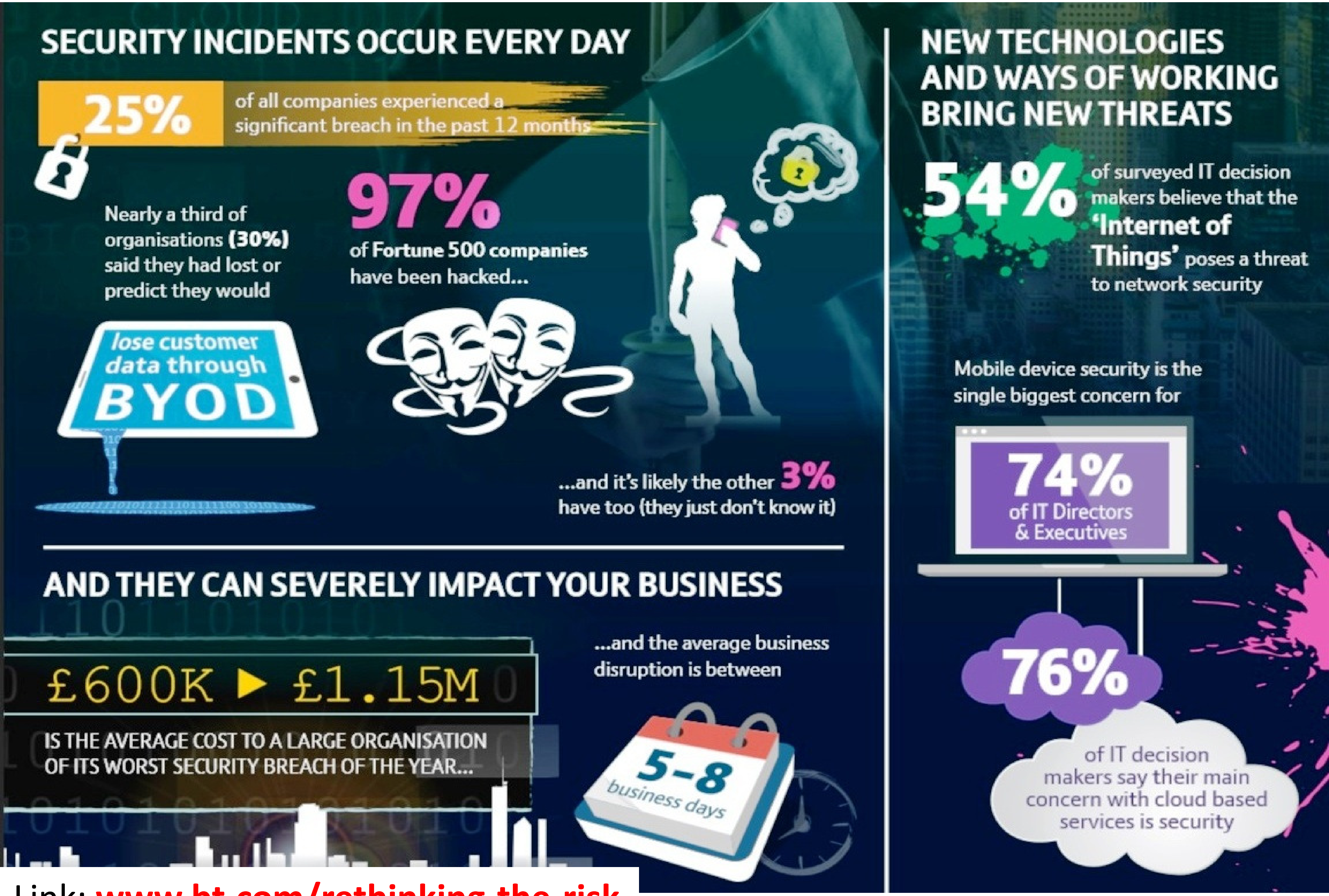
WORKPLACE BYOD POLICY ADDRESSES WEARABLE TECH

Source: 2014 ISACA IT Risk/Reward Barometer

"BIG DATA" Challenges for "IoT"



Volume	Velocity	Variety	Veracity*
Data at Rest	Data in Motion	Data in Many Forms	Data in Doubt
Terabytes to exabytes of existing data to process	Streaming data, milliseconds to seconds to respond	Structured, unstructured, text, multimedia	Uncertainty due to data inconsistency & incompleteness, ambiguities, latency, deception, model approximations



SECURITY INCIDENTS OCCUR EVERY DAY

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

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

lose customer data through **BYOD**

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

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

AND THEY CAN SEVERELY IMPACT YOUR BUSINESS

£600K ▶ £1.15M

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

...and the average business disruption is between

5–8 business days

NEW TECHNOLOGIES AND WAYS OF WORKING BRING NEW THREATS

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

Mobile device security is the single biggest concern for

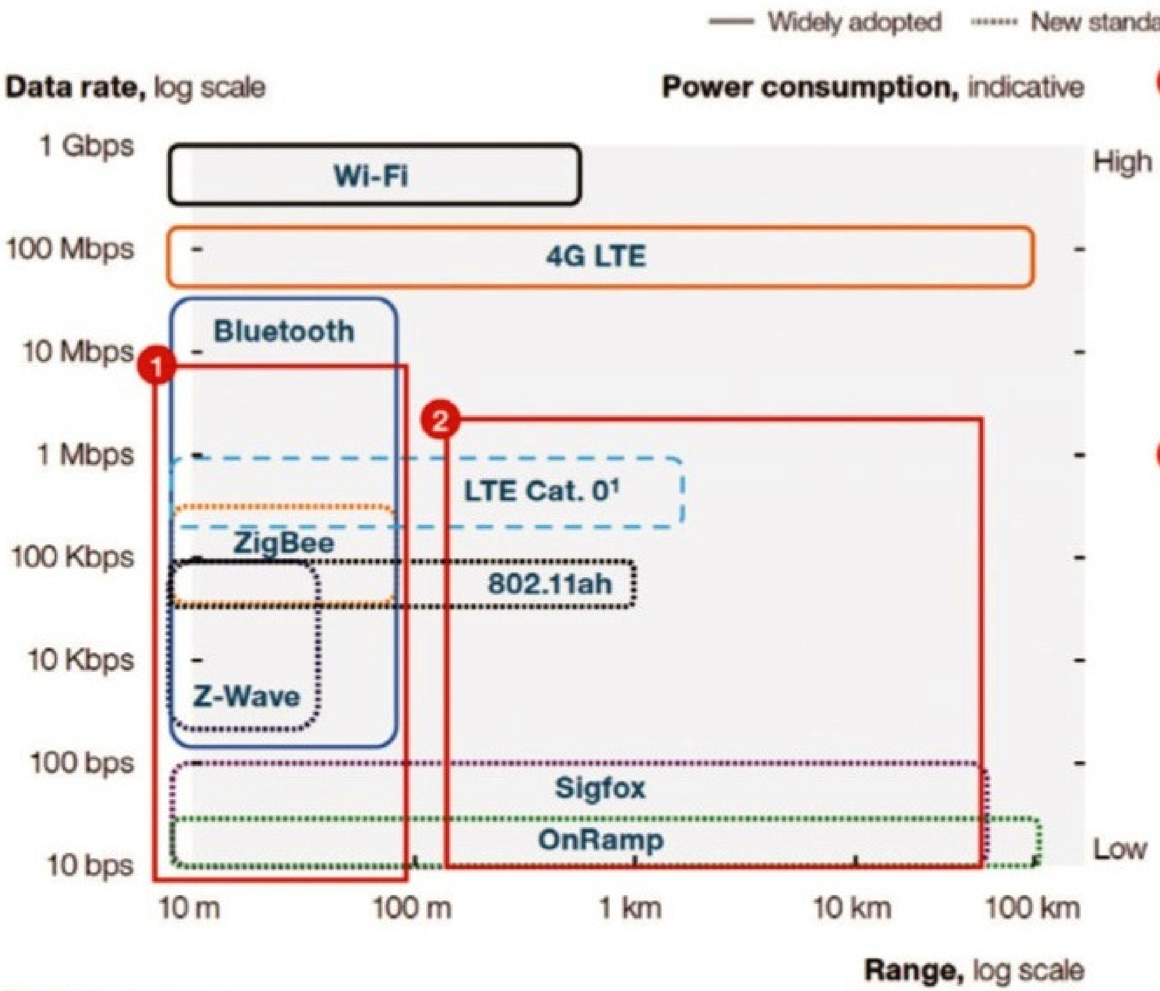
74% of IT Directors & Executives

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

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

Mobile and Wireless Standards for “IoT”

IOT standards are not mature in many categories, including connectivity.



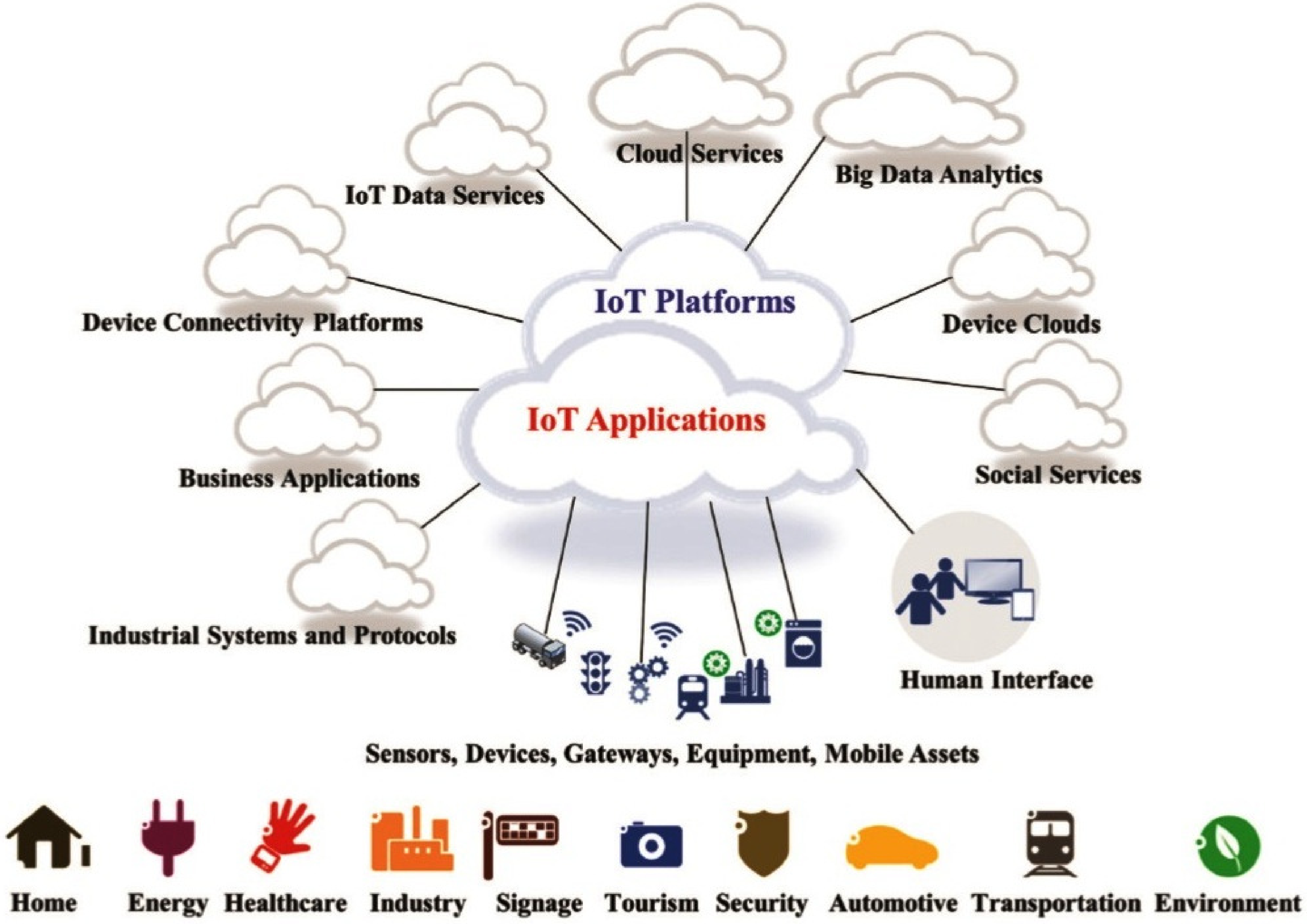
1 Many competing standards for low-range, medium-low data rate hinder growth for many IOT applications
- Interoperability missing
- Consortia wars might be emerging
- Additional incompatibilities in higher communication layers, eg, 6LoWPAN vs ZigBee

2 Standard white space for low-data-rate, low-power, high-range applications such as smart grid
- Wi-Fi and LTE have high power consumption
- Alternatives with low power and wide range (eg, LTE Cat. 0, 802.11ah, Sigfox, and OnRamp) are in very early stages and compete against each other

¹Preliminary specs.

Source: Company websites; expert interviews; GSA and McKinsey IOT collaboration; press research

Internet of Things: *Integrated Services*



ITU: Cybersecurity Training – UTECH, Kingston, JAMAICA

Government, Central Bank, Energy & Telecoms Sectors

University of Technology, Jamaica
University of Technology, Jamaica
FACULTY OF
ENGINEERING AND COMPUTING