- CyberTerrorism (1) -

"Conflict in Cyberspace"

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

Dedicated to Herbert Probert & Percival Probert: *"African Adventures"*

31st International East/West Security Conference

"Cyber-terrorism(1): Conflict in Cyberspace"
Terracina, Italy : 25th-26th May 2015

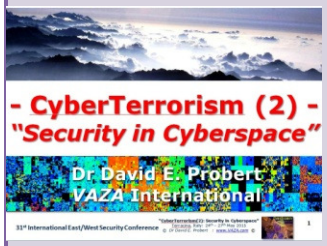
CyberTerrorism – *"Dual Themes"*

Theme (1)" ***"Conflict in Cyberspace" :*** **The Players, Stakeholders & Emerging Trends**

- *The Colonisation of Cyberspace by the "Good Guys" & "Bad Guys"!*
- *Need for Integrated Physical-Cyber Security for 21st C Terrorist Defence*
- *Emergence of the "Internet of Things" as the Future Cyber Conflict Zone*

" Divergence: Chaotic Cyberspace Colonisation " ***26th May: 09:00 – 09:45***

Theme (2) ***– "Security in Cyberspace":*** ***Operational Security Models for 21st Century***



- *Survey of Cybersecurity Strategies, Models & Frameworks*
- *Protection of Banking & Corporate Enterprises from Cyber Threats*
- *Developing YOUR Action Plans & Practical Cybersecurity Programme*

"Convergence: Integrated Real-Time Defence" ***26th May: 14:15 – 14:55***

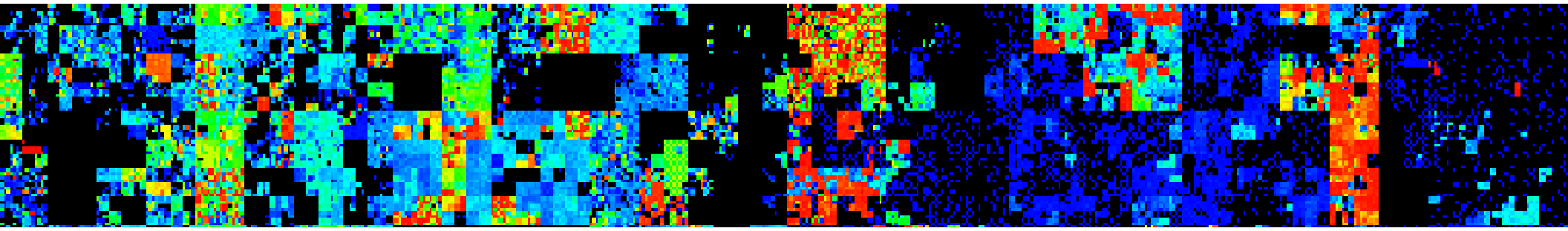
Download Slides: www.valentina.net/East-West2015/

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

…From 19thC Physical World To 21stC Intelligent World

- CyberTerrorism (1) – "Conflict in Cyberspace"

1 – Background: *"Cyber Terror Landscape"*	**2 – Cyber Players & Targets**	**3 –Typical Cyber Threat Scenarios**
4 – Recent Cyber Terror Case Studies	**5 – Advanced Hybrid 4D Terrorism**	**6 – Industrial to Intelligent Cyber Society**
7 – Cyber Models, Strategies & Tactics	**8 –New Conflict Zone: *Internet of Things***	**9 – Top 10 - CSO Cyber Action Themes**



Personal *"Cyber Experiences":* 1991 – 2015

- Armenia
- Belarus
- Bulgaria
- Czech Republic
- Georgia
- Hungary
- Kazakhstan
- Poland
- Romania
- Russia
- Slovakia
- Ukraine
- Bahrain
- Eqypt
- Israel
- Jordan
- Qatar
- South Africa

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"

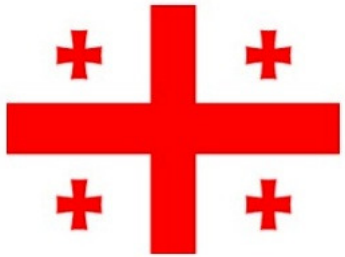
*** Report Prepared by: Dr David E Probert – VAZA International ***

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/

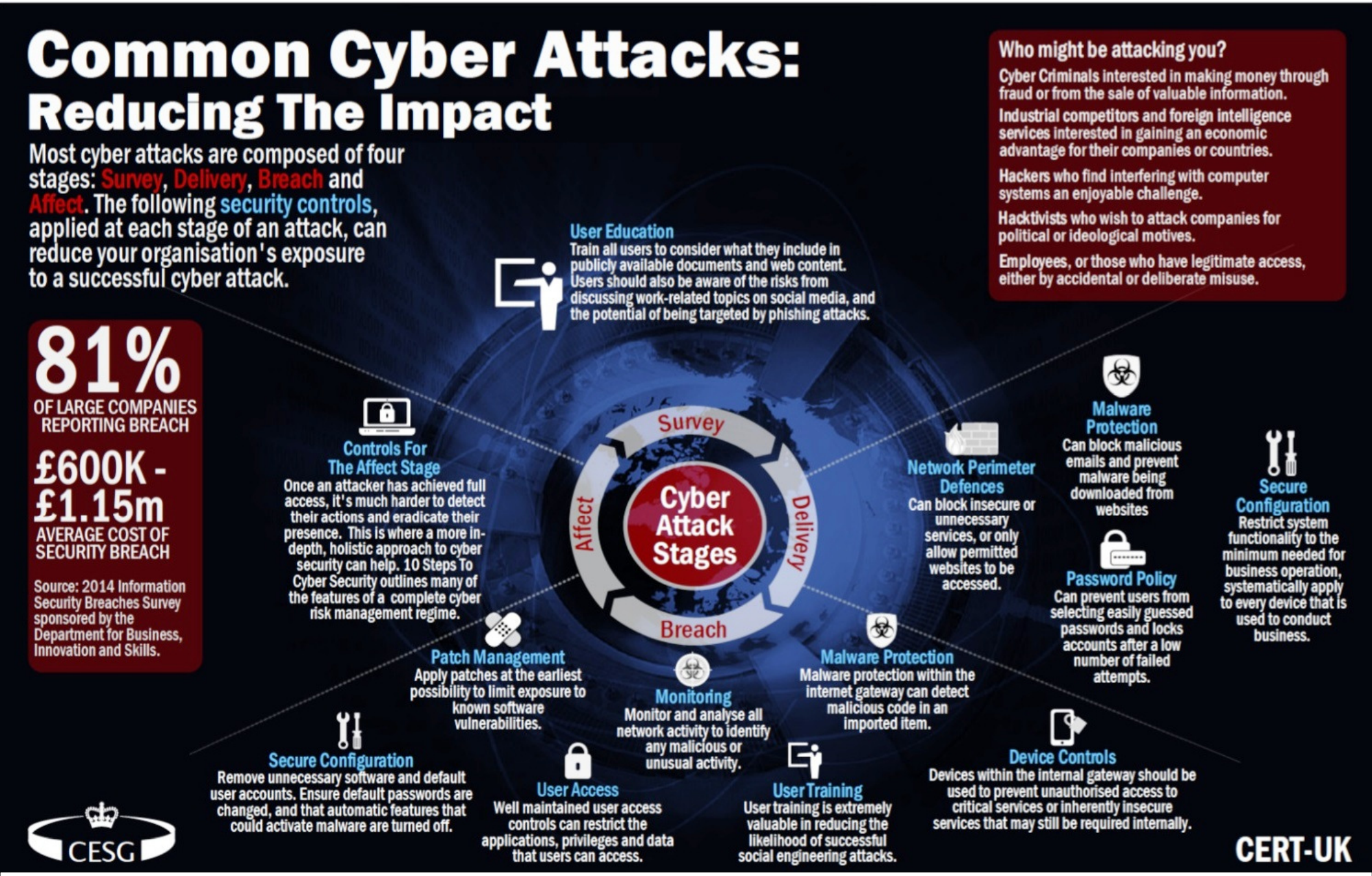
Background: *"CyberTerror Landscape"*

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

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

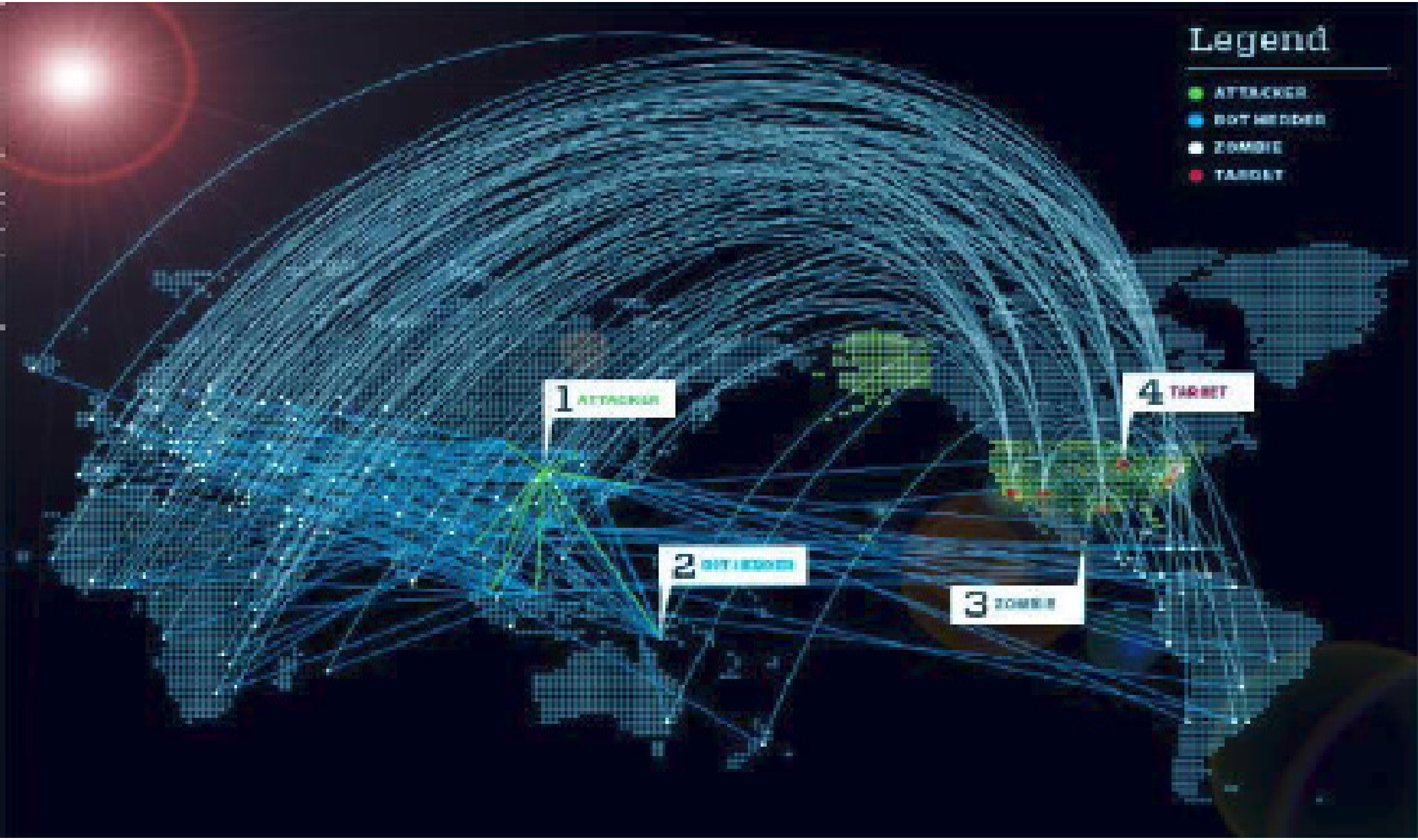
CyberTerrorism @ World Counter Terror Congress – Olympia, London – April 2015

Welcome to the 20th Infosecurity Europe Conference & Exhibition



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

Typical Global *"Botnet"* Cyber Attack



Command & Control (C2) ***Malware*** Servers

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

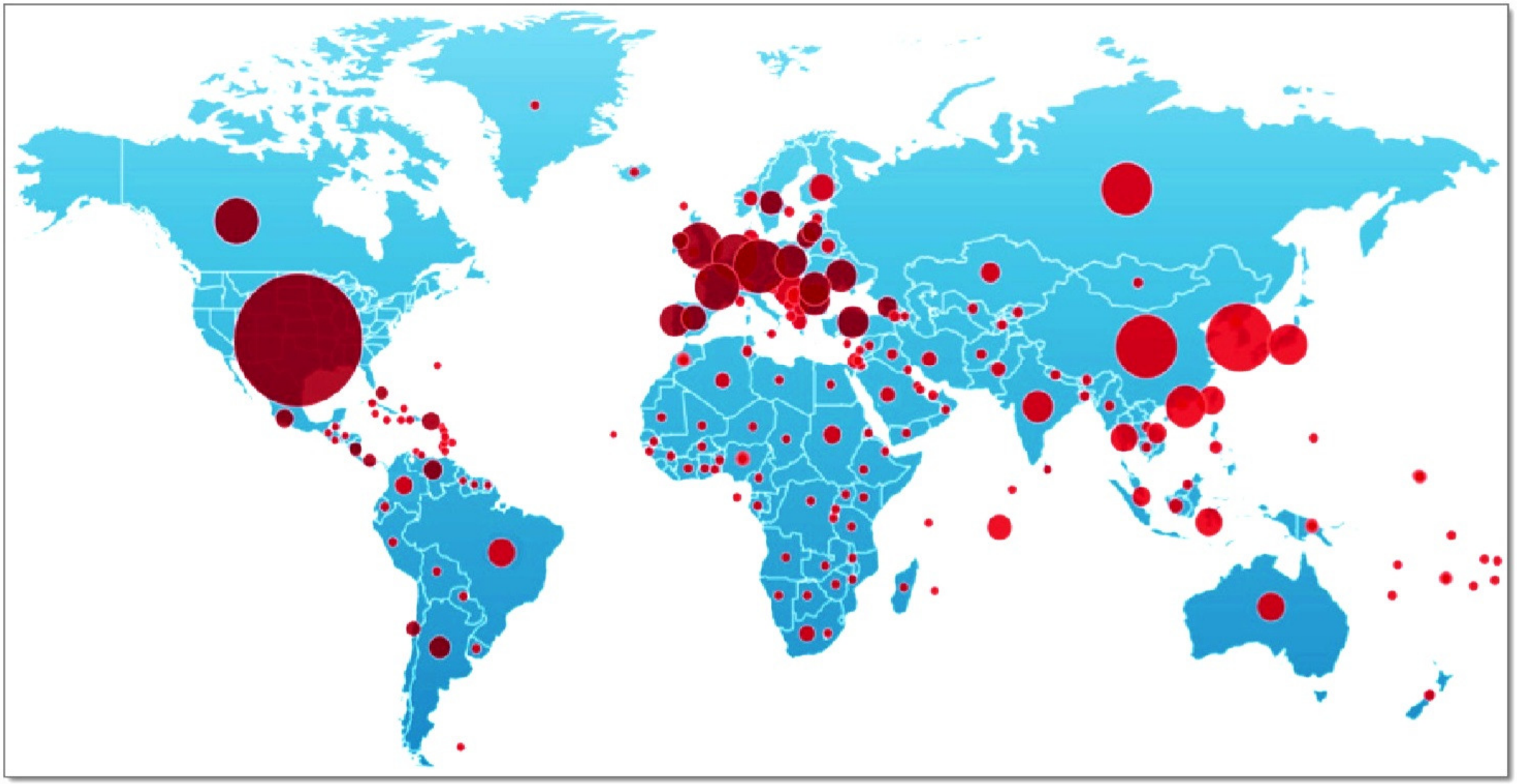
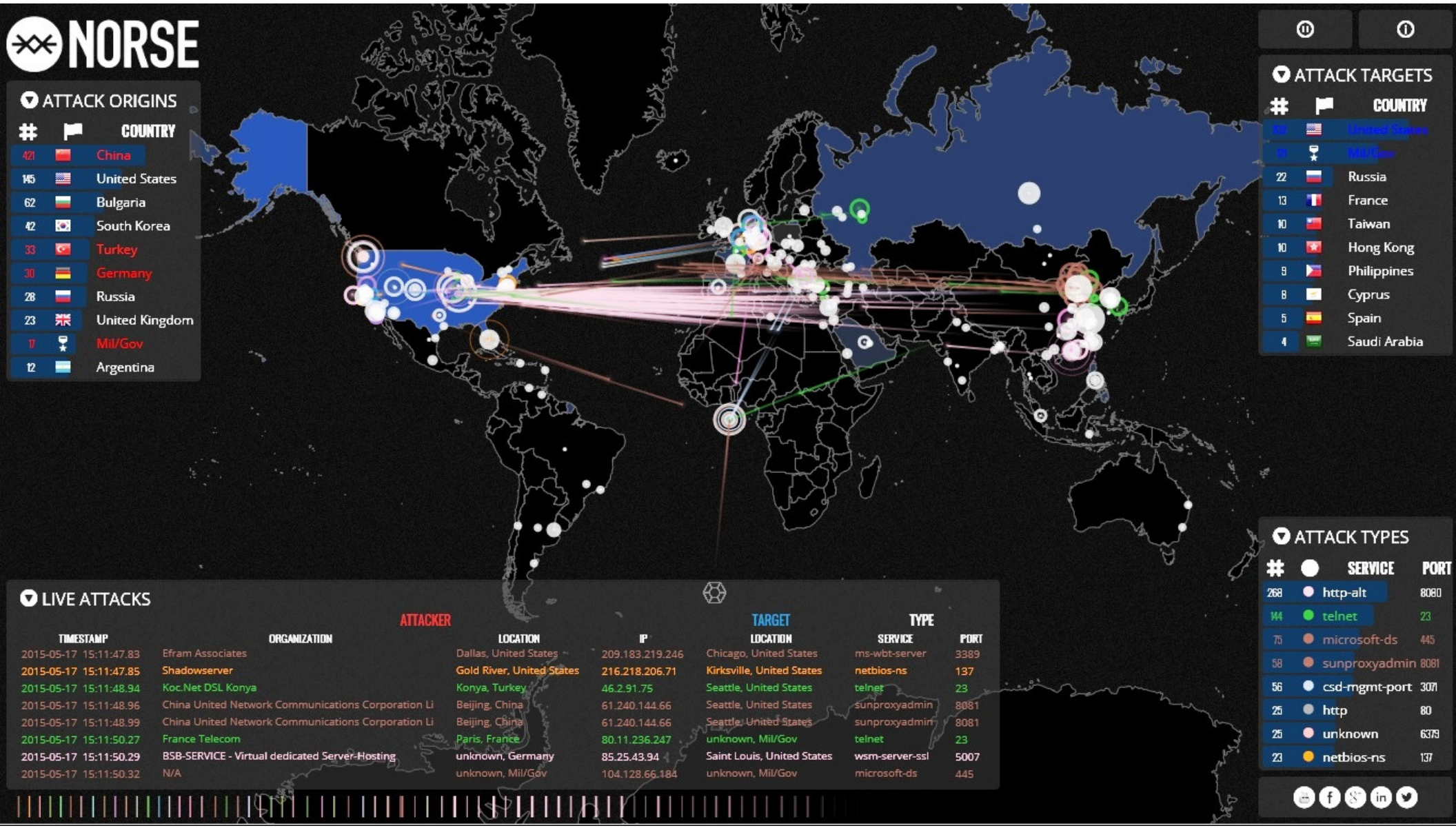


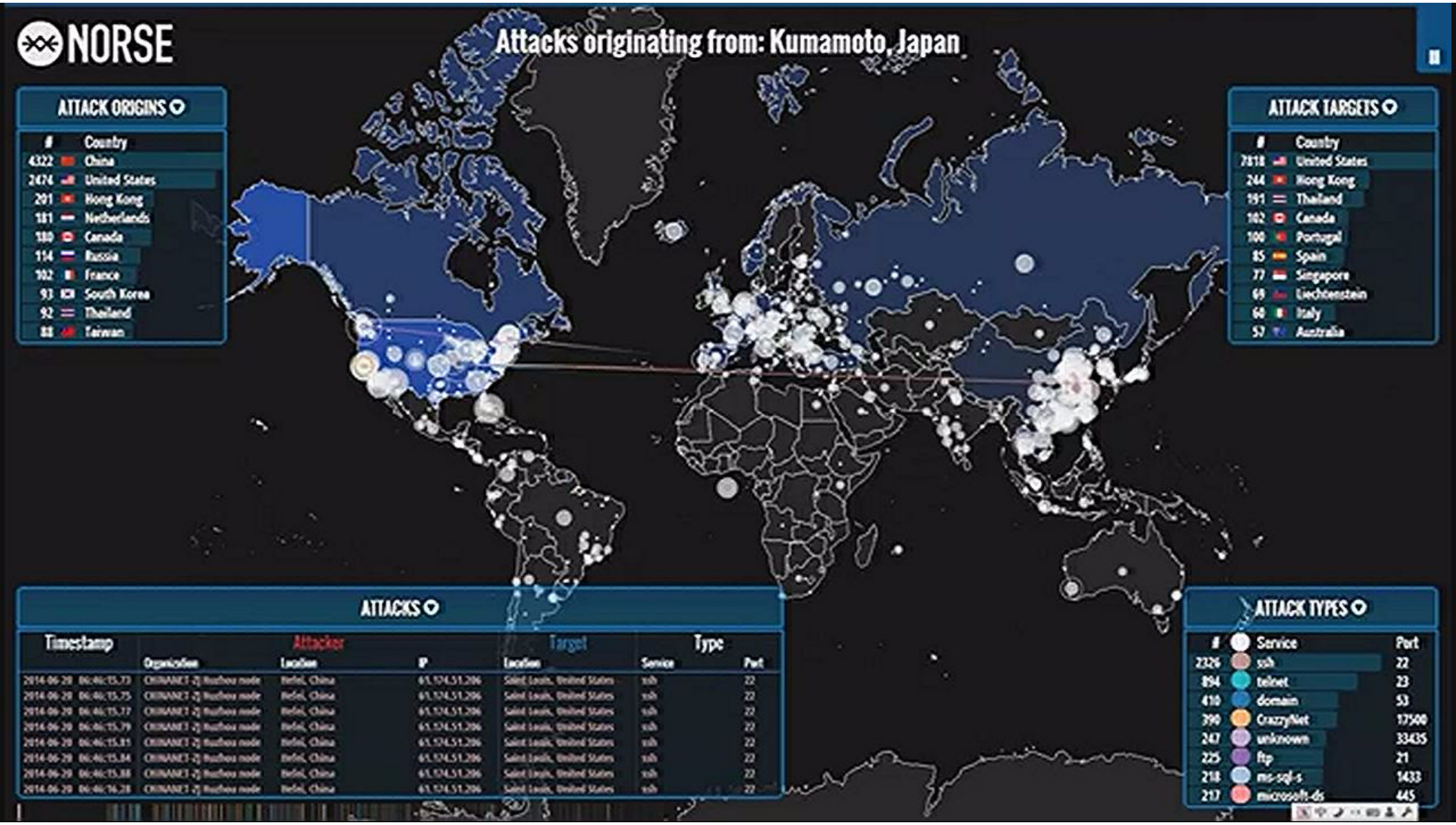
Image: www.fireeye.com – FireEye Inc (c)

Monitoring *"Real-Time"* Cyber Attacks



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

Global "Real-Time" DarkNet CyberAttacks



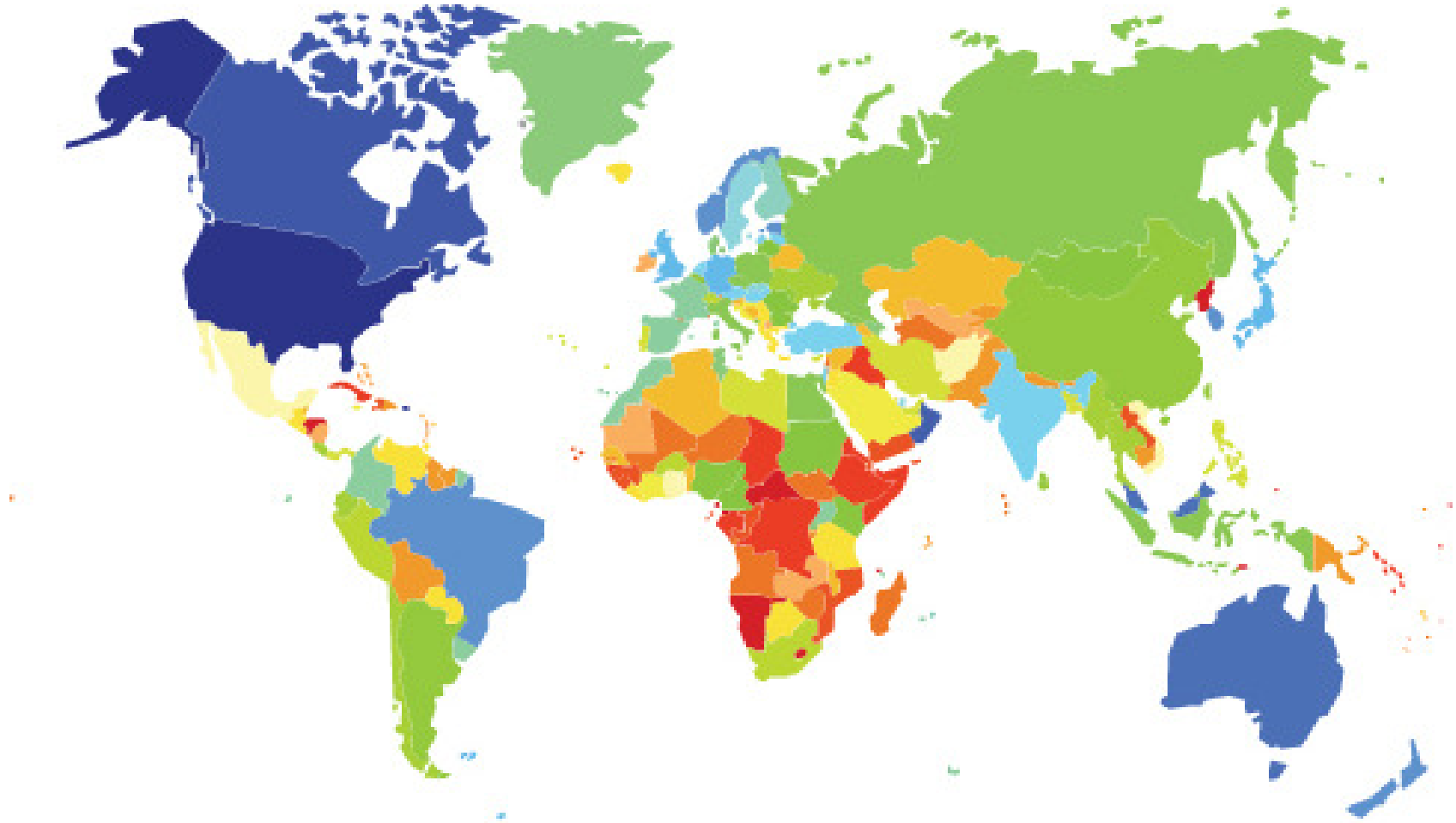
Link: **map.ipviking.com** - Norse Corporation

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

31st International East/West Security Conference

"Cyber-terrorism(1): Conflict in Cyberspace"
Terracina, Italy : 25th-26th May 2015

UN/ITU – *Global Cybersecurity Index* (Dec 2014)



ABIresearch | Global Cybersecurity Index

ITU

National Cybersecurity Commitment HIGHEST LOWEST

Criminal & Political ***Cyber-Colonisation***

- ***21st C "Pirates":*** eCriminals, Hacktivists and CyberTerrorist Groups are now colonising both the Public Internet & "Global IP Darknet" as 21stC *"Pirates"!*

- ***"Slaved IT Botnets":*** Computer Networks, Servers & PCs are "slaved" through Computer Malware to work in massive networks of "IT Botnets" using PCs & Smart Devices

- ***Global Response:*** National Governments and Corporations are now implementing Cyber Defences against Multiple Classes of CyberAttack, CyberCrime and CyberTerrorism!.....

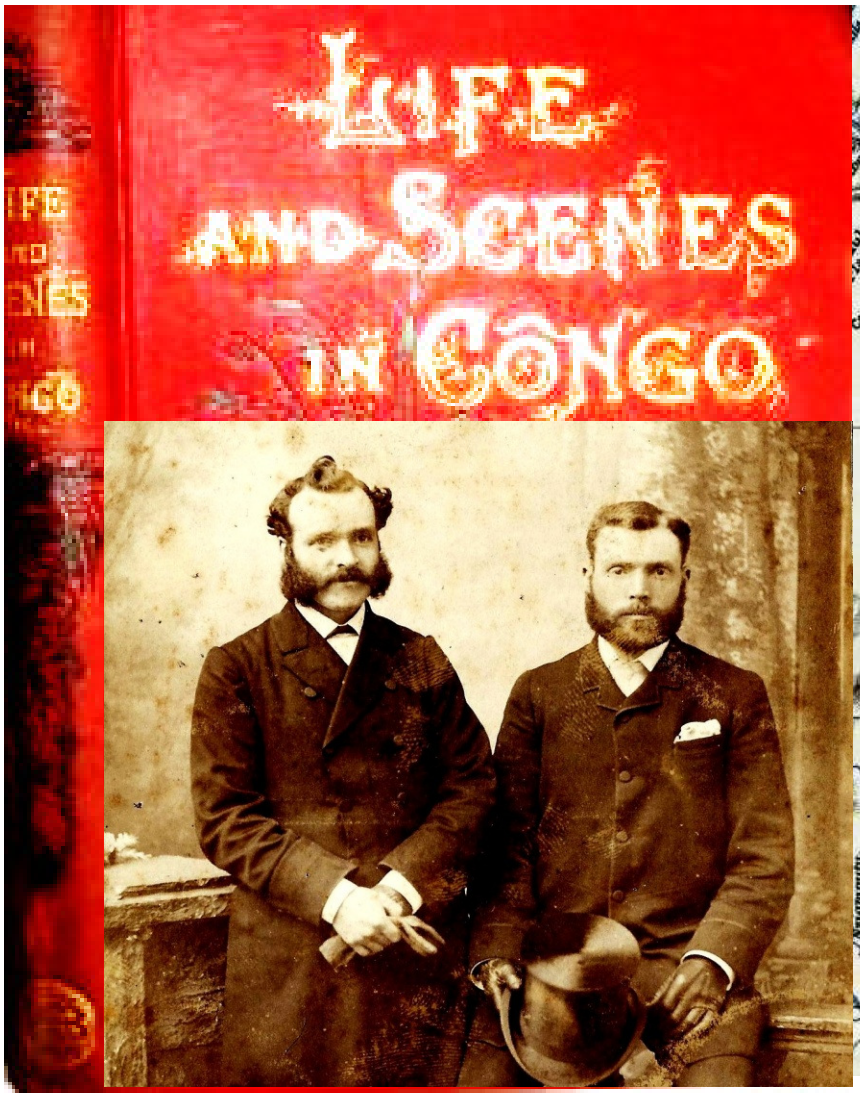
..."Physical Space" - 20thCentury *Exploration & Colonisation* was ***"Geographical"***

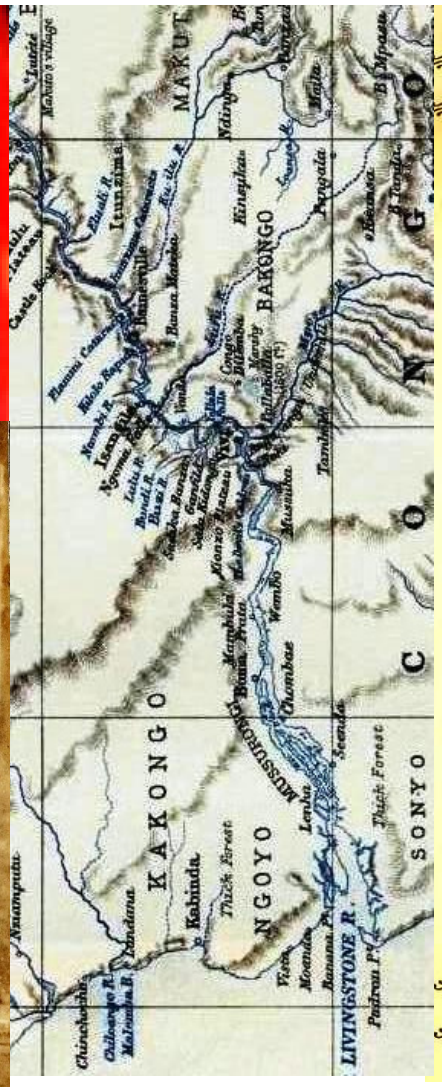
... "Cyber Time" - 21stCentury *Cyber-Colonisation* is at the ***"Speed of Light"***

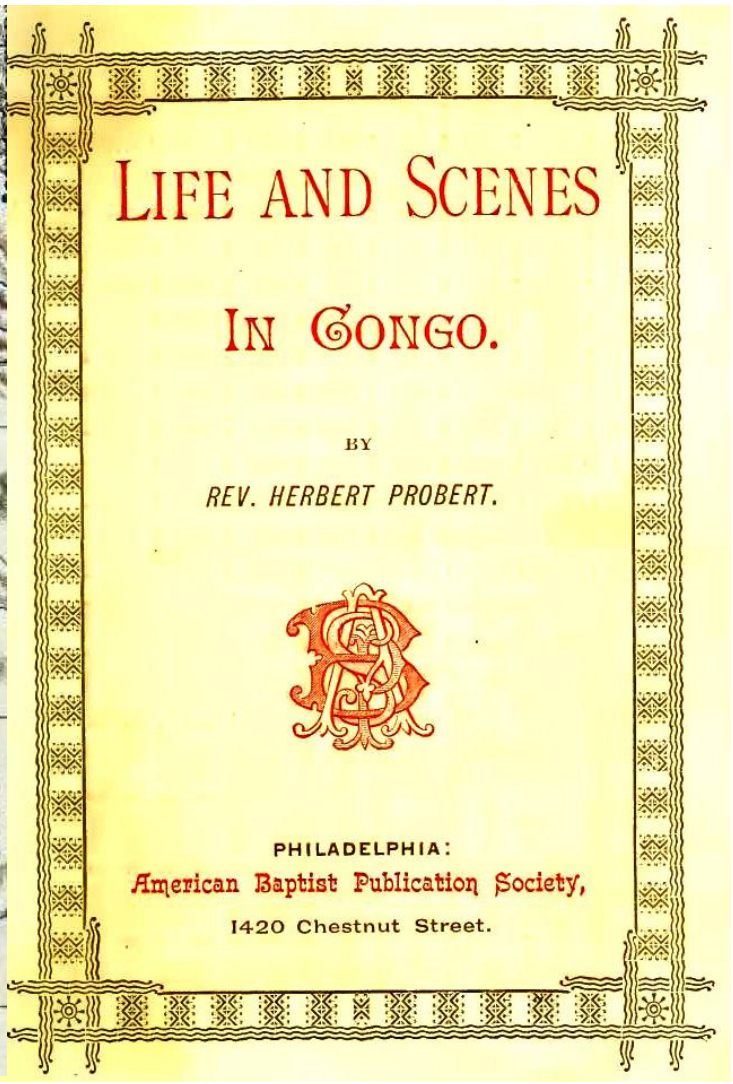
Physical Terrorism *and* ***Cyber Terrorism*** *have different dynamics but can be much more effective when combined within Integrated* ***Physical-Cyber Operations***

Physical Exploration - 1885 – 1887 : *Rev Herbert E. Probert*

- *Travelling from Big Horn, Wyoming, USA to Equatorville, Congo, Central AFRICA* -






LIFE AND SCENES

IN CONGO.

BY

REV. HERBERT PROBERT.

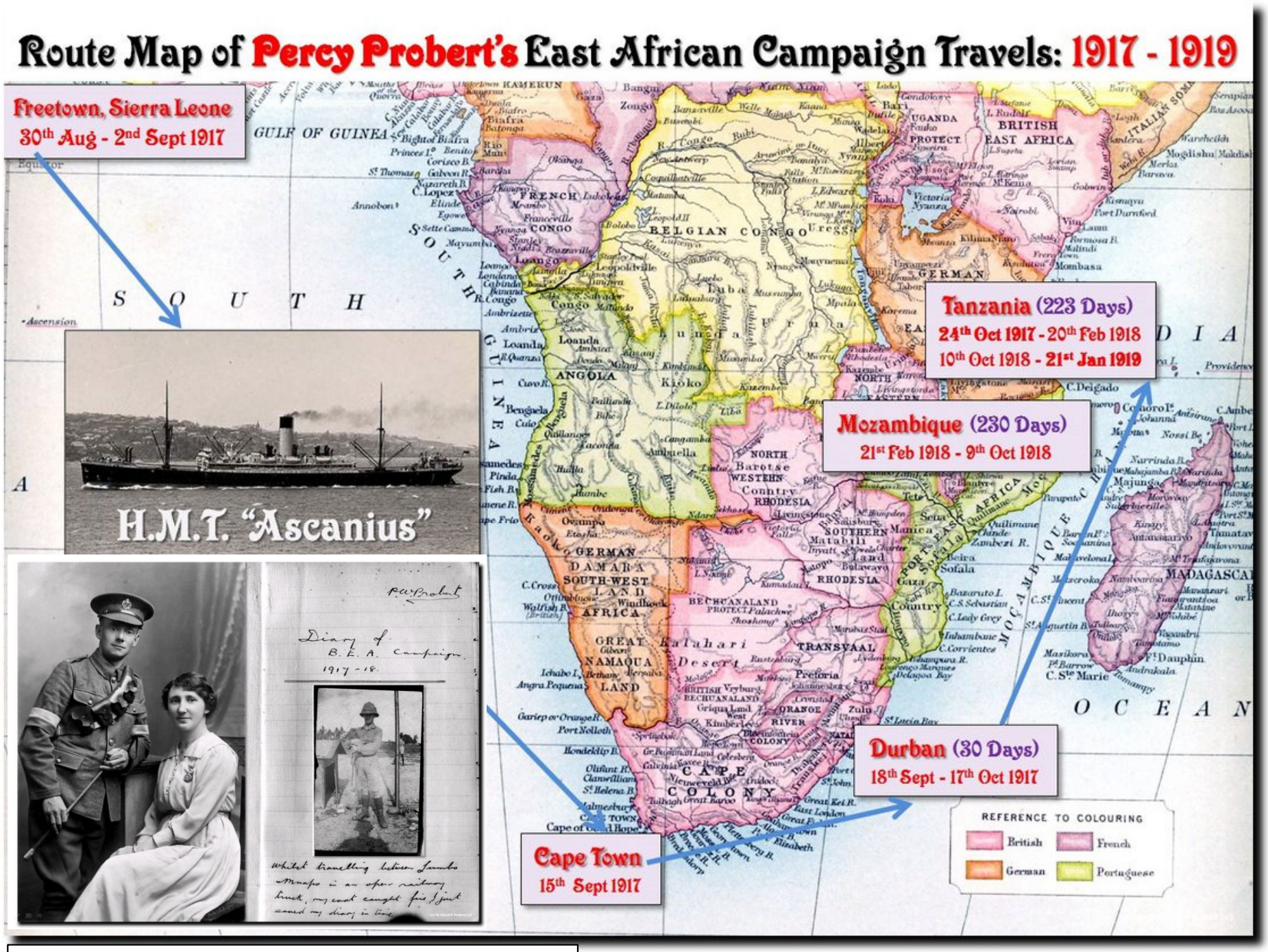
PHILADELPHIA:

American Baptist Publication Society,

1420 Chestnut Street.

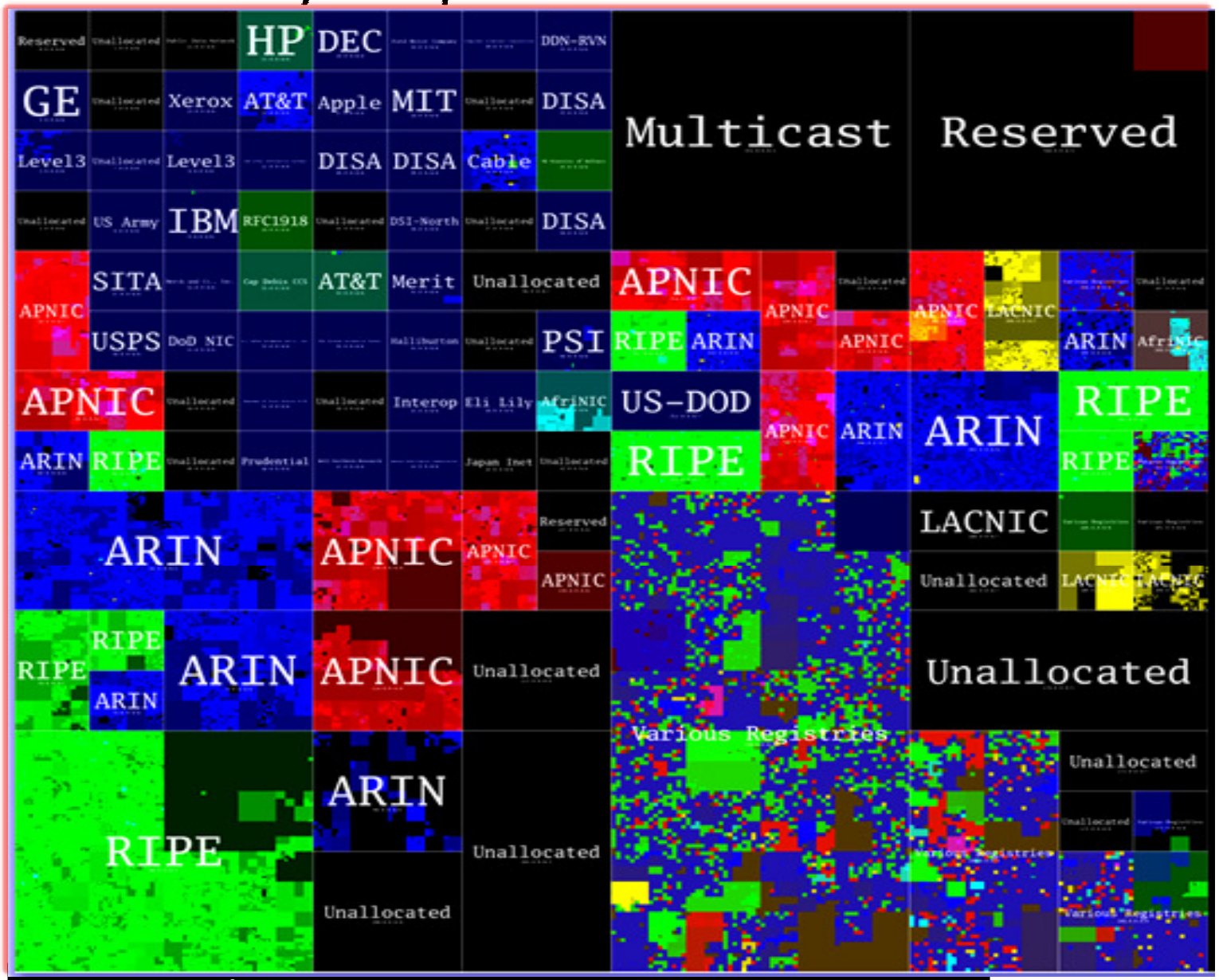
"Life and Scenes in Congo" – Published 1889 – Free *eBook* download from: www.archive.org

Route Map of Percy Probert's East African Campaign Travels: 1917 - 1919



Diary Link : www.valentina.net/PWP/

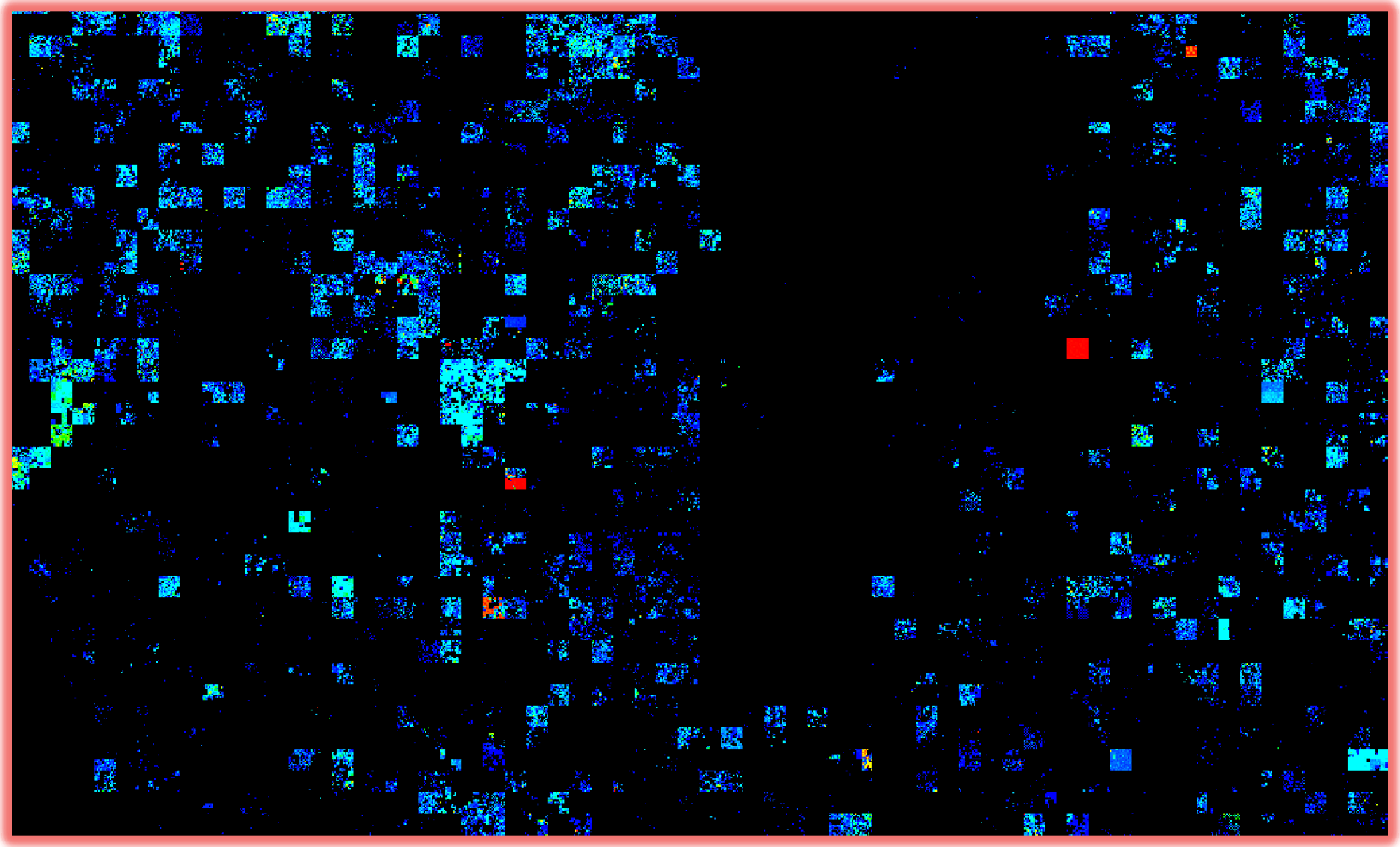
"Visualisation of Cyberspace": *Global IP "WHOIS" Addresses*



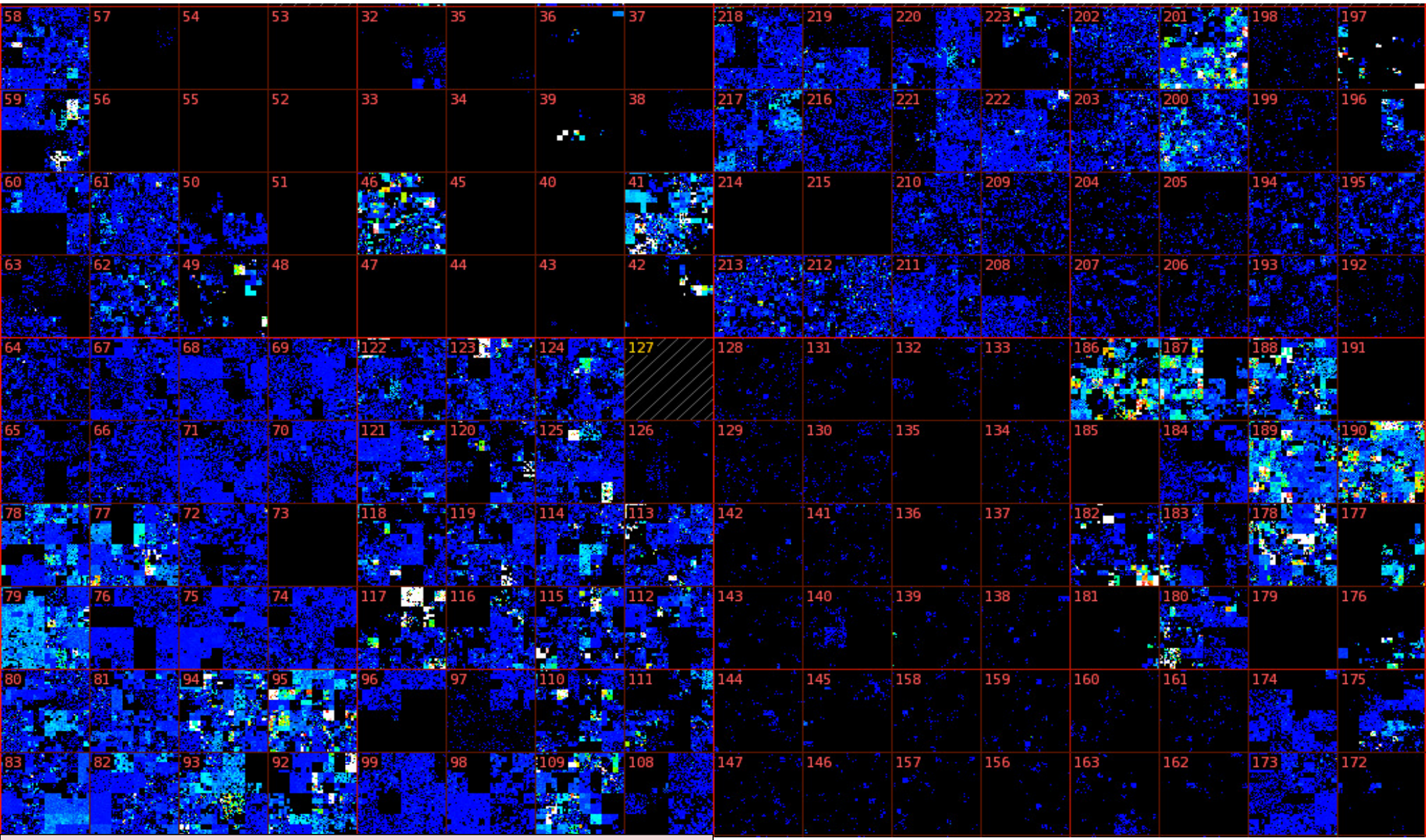
…From 20thC Physical World To 21stC Cyberspace! …

Active Internet Domains: *"American IP Registry"*

"Outer Galaxies of Cyberspace" – *Other IP Registries*



Map of *Recent* Malicious Activity in *"Cyberspace"*



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

Contrast between Physical & Cyber Worlds

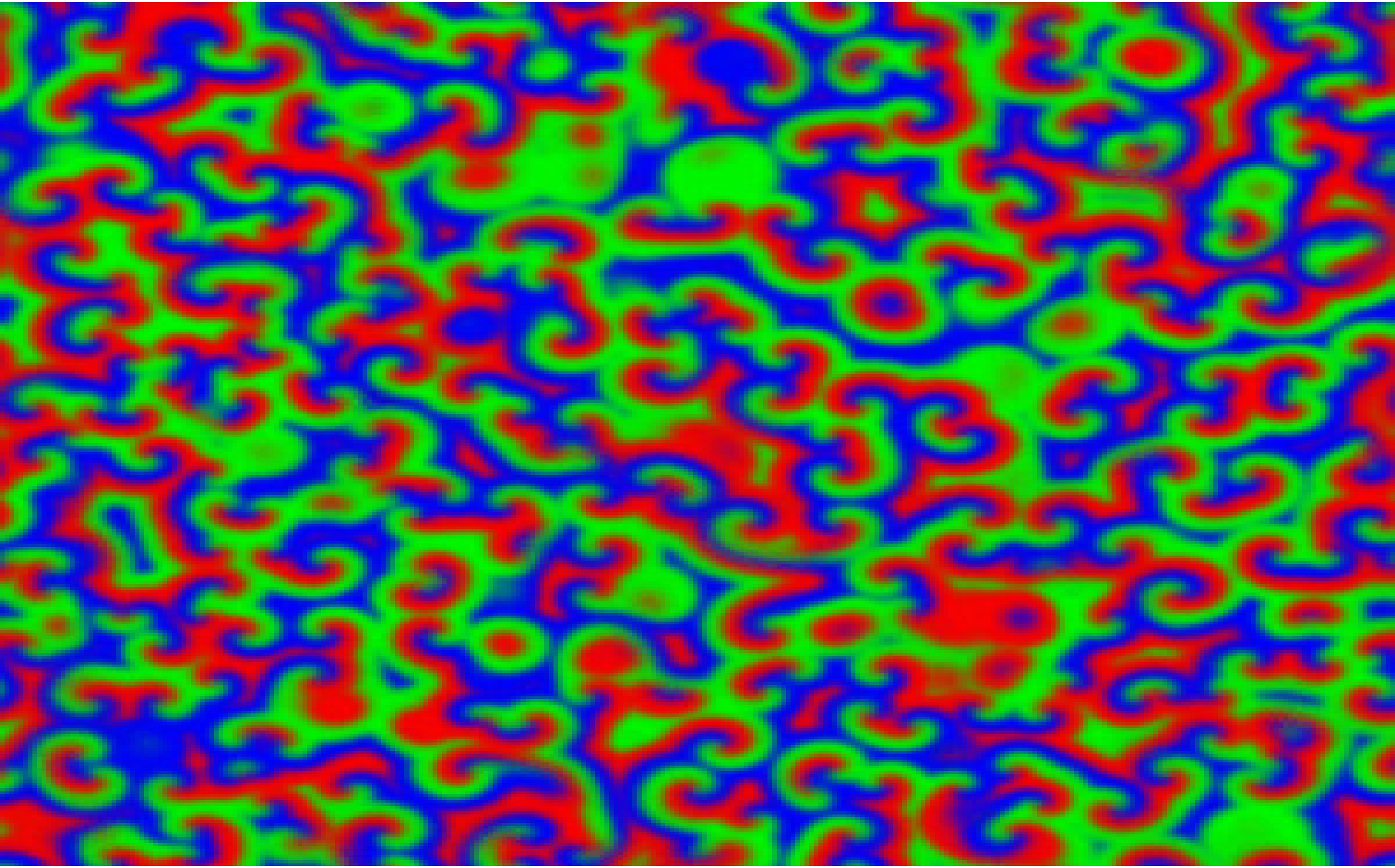
Convergence to 21stC "Intelligent Worlds" will take time!

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
• Supersonic	• Speed of Light
• Convergent	• Divergent
• Hierarchical	• Organic
• Carbon Life	• Silicon Life
• Tanks & Missiles	• Cyber Weapons & "Botnets"
• Mass Media	• Social Media

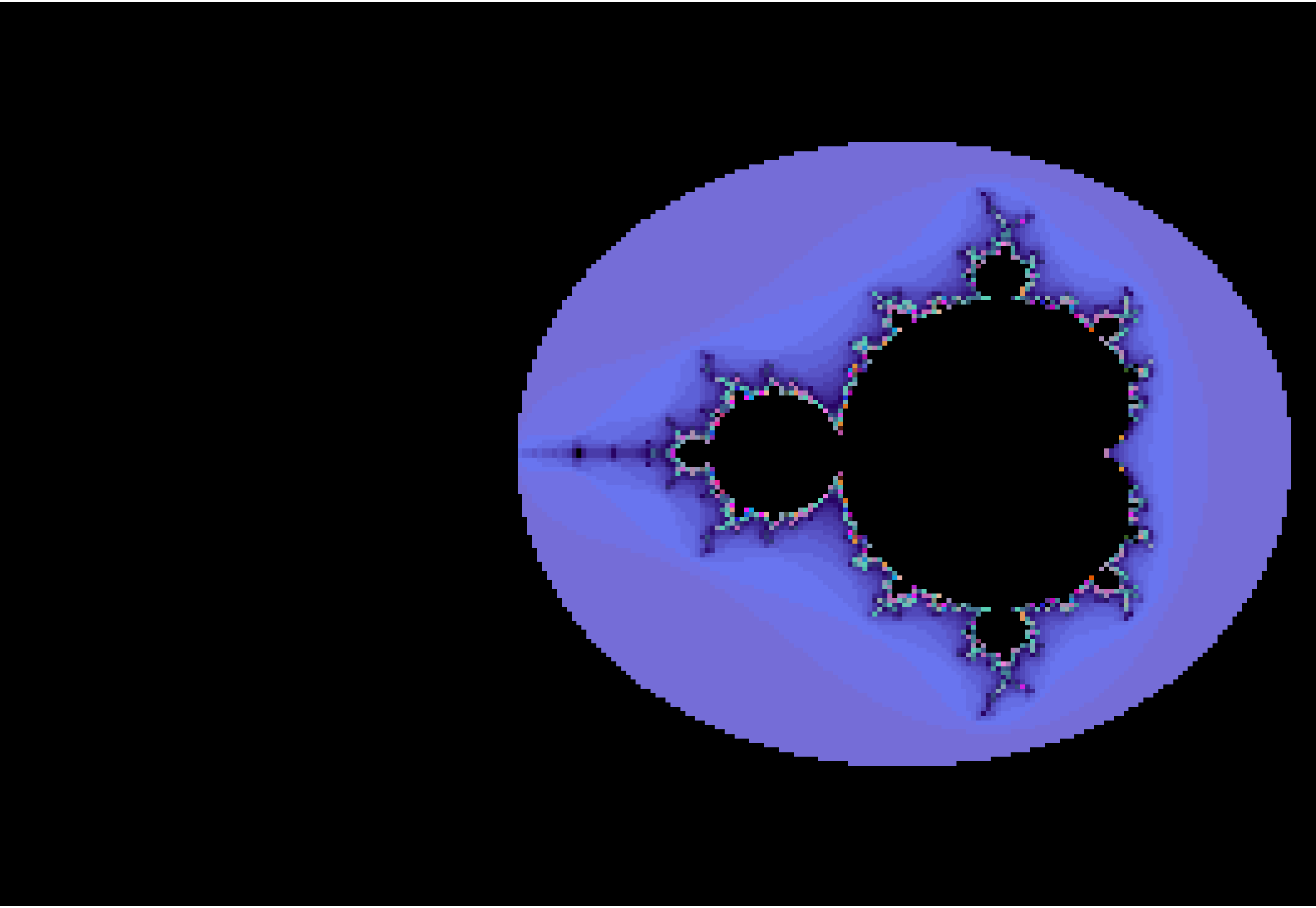
"Smart Security" will require Embedded Networked Intelligence in ALL future devices

"Smart" Autonomous Chemical Oscillator:

- Belousov–Zhabotinsky Reaction (BZ) -



“Smart Scaling”: Fractal Mandelbrot Set



CyberCrime, CyberTerrorism & Espionage

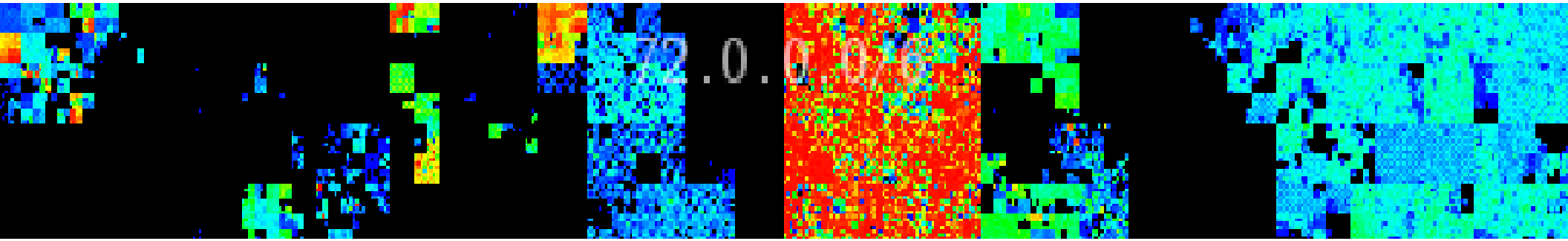
- ***Profit:*** Cybercrime is generally for commercial gain and profit with focus on Financial Service Sector. It is now carried out on an *"Industrial Scale"* by IT Technically skilled criminal specialists as Global eCrime Business!

- ***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.

- CyberTerrorism (1) – "Conflict in Cyberspace"

1 – Background: "*Cyber Terror Landscape*"	**2 – Cyber Players and Targets**	3 – Typical Cyber Threat Scenarios
4 – Recent Cyber Terror Case Studies	5 – Advanced Hybrid 4D Terrorism	6 – Industrial to Intelligent Cyber Society
7 – Cyber Models, Strategies & Tactics	8 – New Conflict Zone: *Internet of Things*	9 – Top 10 - CSO Cyber Action Themes

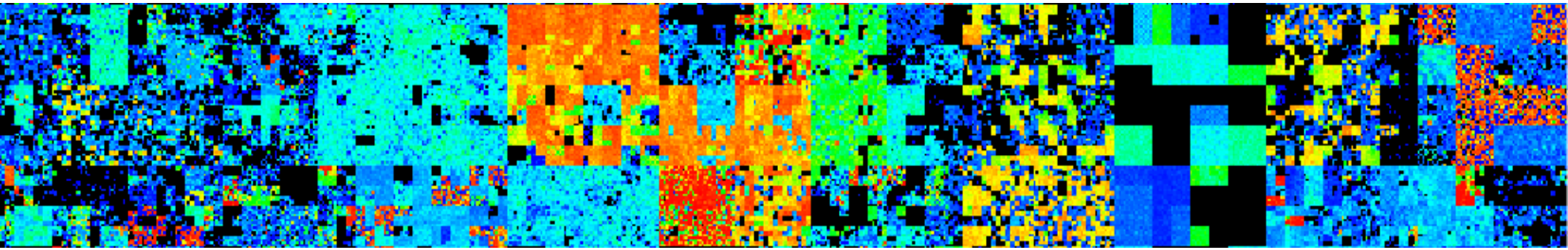


Main Cyber Players and their Motives

- *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

- CyberTerrorism (1) – "Conflict in Cyberspace"

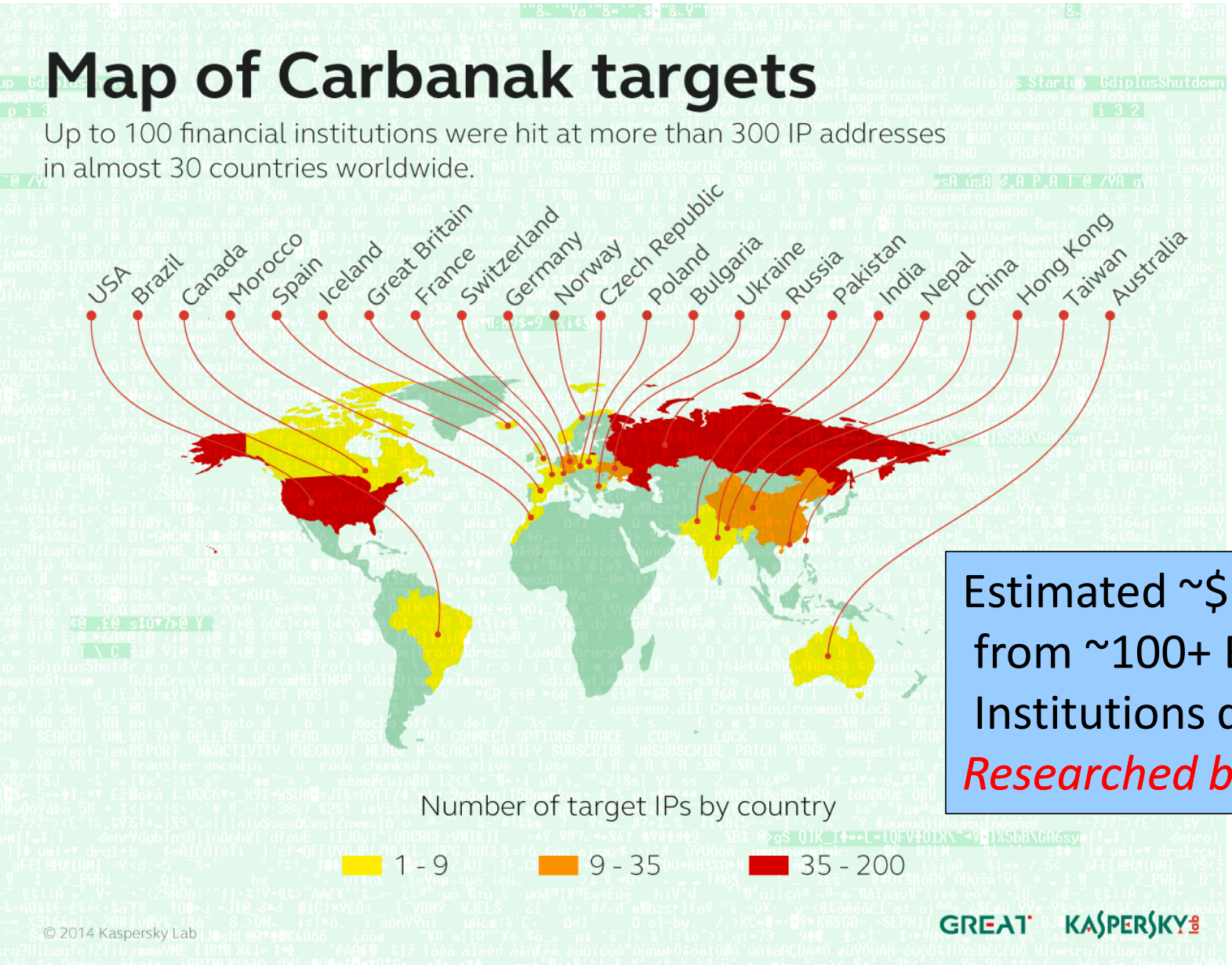
1 – Background: "*Cyber Terror Landscape*"	2 – Cyber Players & Targets	**3 – Typical Cyber Threat Scenarios**
4 – Recent Cyber Terror Case Studies	5 – Advanced Hybrid 4D Terrorism	6 – Industrial to Intelligent Cyber Society
7 – Cyber Models, Strategies & Tactics	8 –New Conflict Zone: *Internet of Things*	9 – Top 10 - CSO Cyber Action Themes



Typical Physical & CyberTerror Targets

- *Physical Terror:* Attacks focus on Business & Social "Hubs" such as Shopping Mall, Stadiums, Campus, Airports & Train Stations
- *Cyber Terror:* Attacks focus on Hi-Value WebSites, Servers & Data Centres such as Banks, Government, On-Line Shopping & Social Media – Facebook, Twitter & Yahoo
- *Hybrid Terror:* Synchronised Physical & Cyber Terror Attacks on Critical National Infrastructure such as Banking, Energy, Transportation & Military Assets

Cyber “Banking Theft”– Carbanak

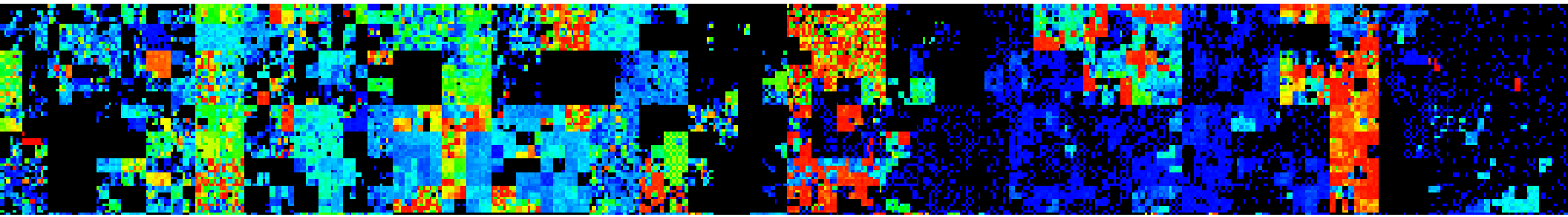


Estimated ~$1Billion stolen from ~100+ Banks & Financial Institutions during 2013/2014

Researched by “Kaspersky Labs”

- CyberTerrorism (1) – "Conflict in Cyberspace"

1 – Background: "*Cyber Terror Landscape*"	2 – Cyber Players & Targets	3 – Typical Cyber Threat Scenarios
4 – Recent Cyber Terror Case Studies	5 – Advanced Hybrid 4D Terrorism	6 – Industrial to Intelligent Cyber Society
7 – Cyber Models, Strategies & Tactics	8 – New Conflict Zone: *Internet of Things*	9 – **Top 10** - CSO Cyber Action Themes



Pre-2012 - Cyber Terror 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)

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

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

Case Study: StuxNet Worm - Industrial *SCADA* Systems - 2010

User accesses an infected removable drive; his/her system is then infected by **WORM_STUXNET.A**

Stuxnet Worm : 1st Discovered June 2010

WORM_STUXNET.A drops files onto the *Windows* folder, creates registry entries, and injects codes into processes to stay memory-resident; it also drops **RTKT_STUXNET.A** to hide its malicious routines

WORM_STUXNET.A targets SCADA WinCC systems, which are used to manage industrial operations such as power plants and energy refineries.

It is also interesting to note that it attempts to access sites related to an online football-betting site. Though this does not pose threats, it may be a diversion tactic to confuse security analysts, causing them to fail to immediately realize the worm's main functionalities.

WORM_STUXNET.A drops copies of itself, a .LNK file detected as **LNK_STUXNET.A,** onto all removable drives connected to an affected system, allowing it to propagate

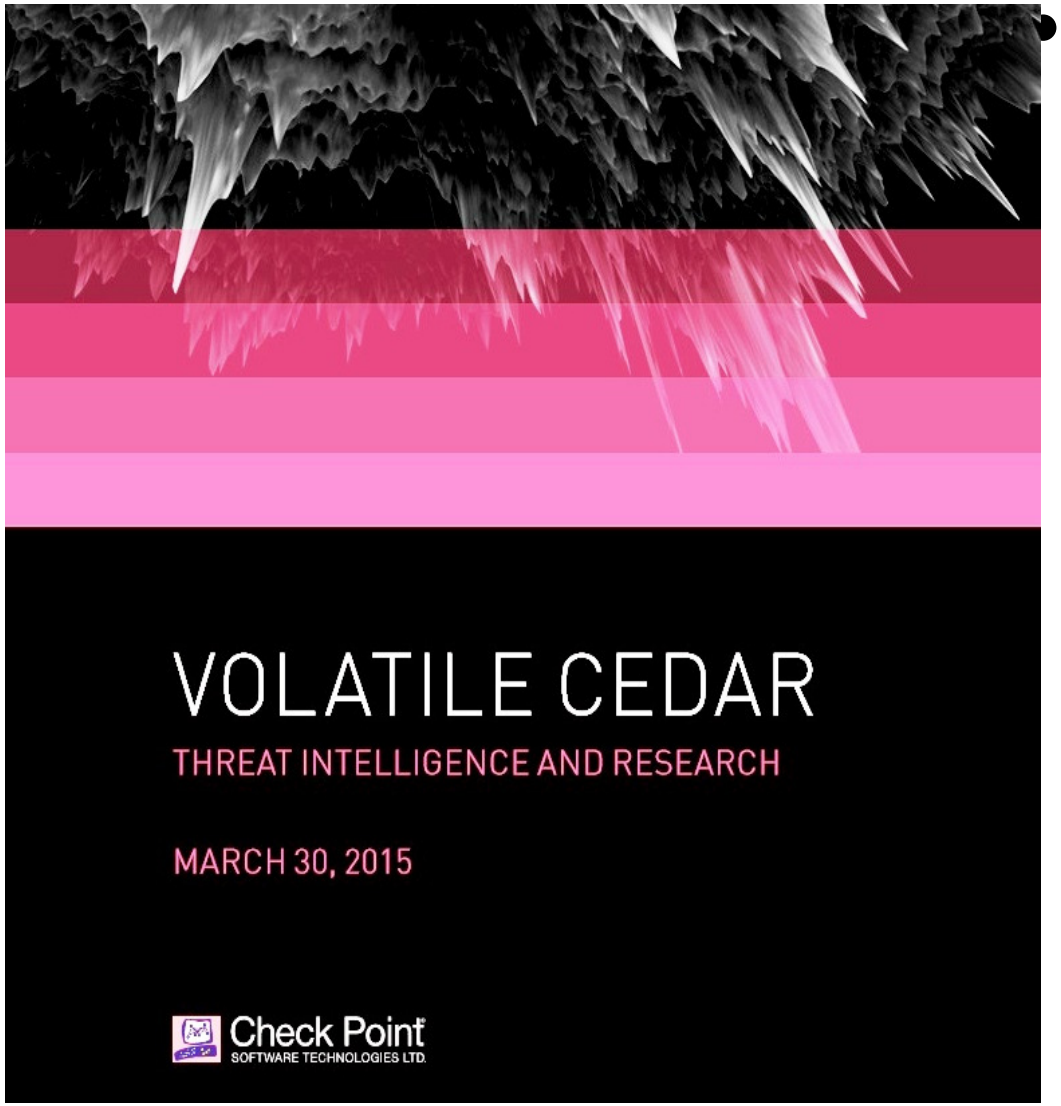
SCADA = **Supervisory Control & Data Acquisition**
- Mainly for Power Stations & Industrial Plants -

CyberCaliphate: *Middle East and Africa(1)*

Multiple CyberAttacks of US Central Command and French TV5Monde (April 2015)

CyberEspionage: Middle East and Africa (2)

CyberEspionage Group: Volatile Cedars



- *"Volatile Cedars"* : Cyber Espionage Group operating from Lebanon since 2012 with in-depth research and full report by Checkpoint Software Technologies Ltd (2015)

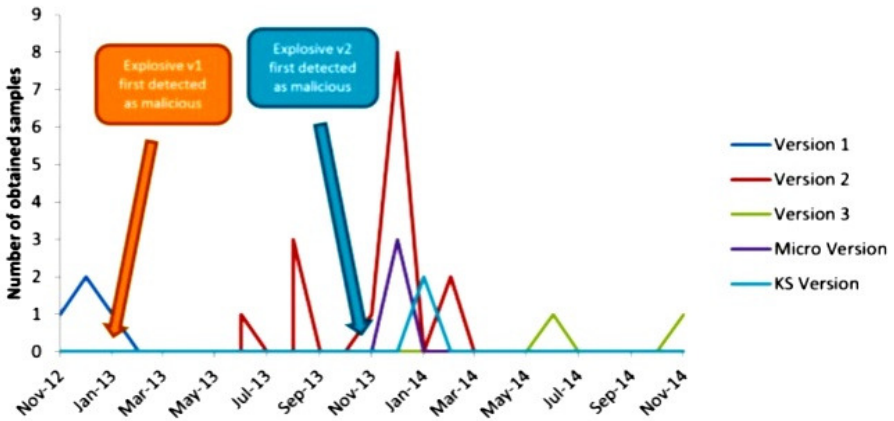
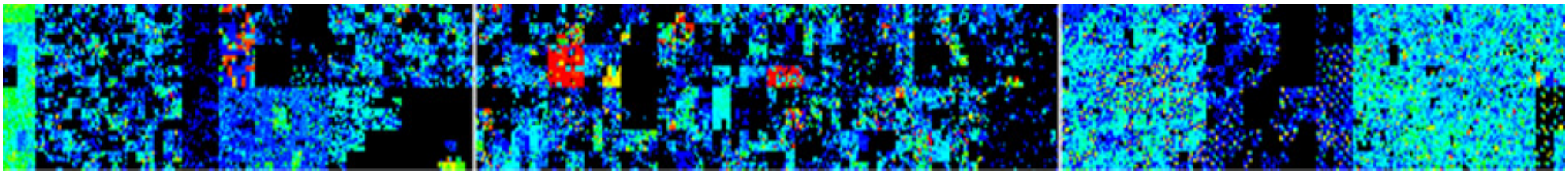


Figure 1 - Explosive version timeline

- CyberTerrorism (1) – "Conflict in Cyberspace"

1 – Background: "*Cyber Terror Landscape*"	2 – Cyber Players & Targets	3 – Typical Cyber Threat Scenarios
4 – Recent Cyber Terror Case Studies	**5 – Advanced Hybrid 4D Terrorism**	6 – Industrial to Intelligent Cyber Society
7 – Cyber Models, Strategies & Tactics	8 – New Conflict Zone: *Internet of Things*	9 – **Top 10** - CSO Cyber Action Themes



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

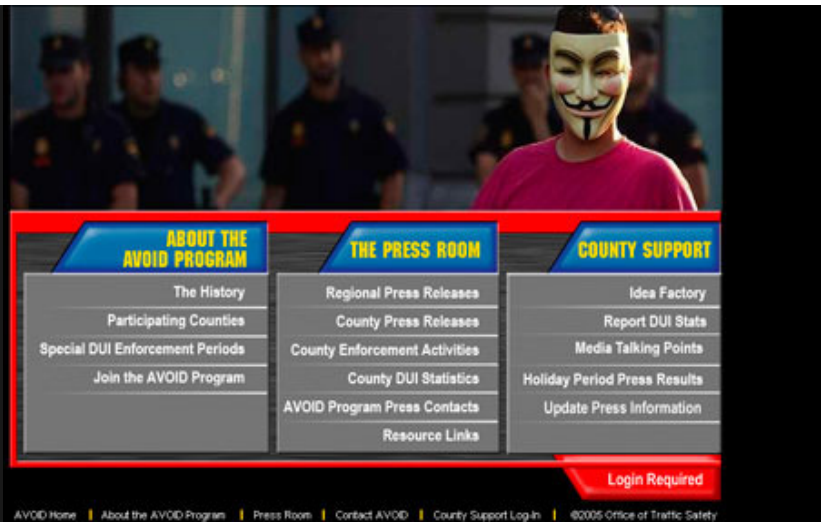
- The Emergence of *"Hybrid" Terror Attacks* will demand that we re-design & engineer Security for Government, Business & Society in 21st C!

...21stC Warfare & Terrorism will evolve as *Hybrid Power Play* integrating Territorial Control with Global Cyber-Info Terrorism!

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*



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

"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!

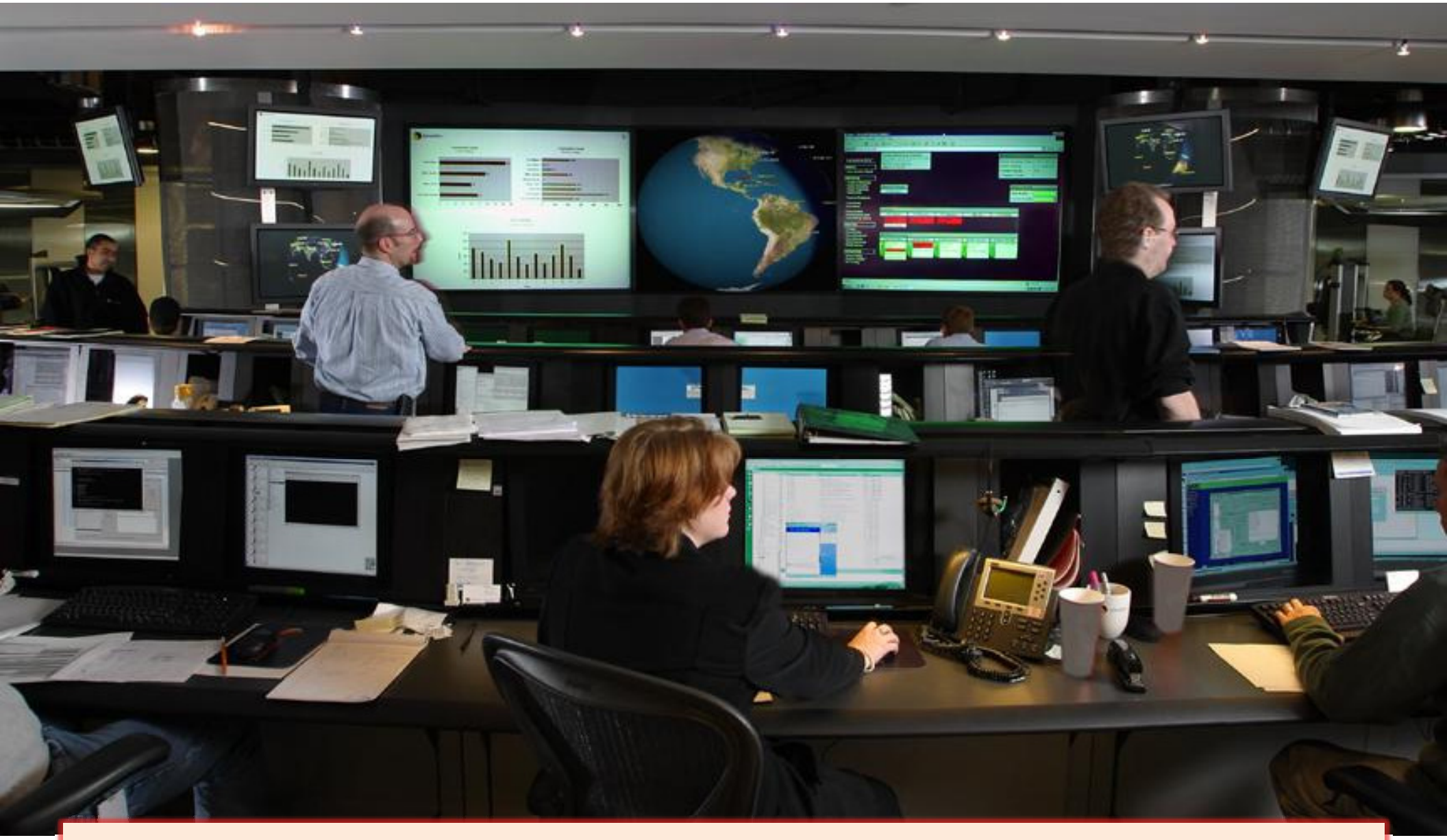
Cyber Integration with *Physical Security Operations*

- *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"

Cyber: Integrated Command & Control



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

Physical: Integrated CCTV Surveillance

- ***CCTV Command and Control Operations Centre for Large UK City***

Emerging Physical & Cyber: National Operations Room:
- US Transportation Security Administration (TSA) -

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

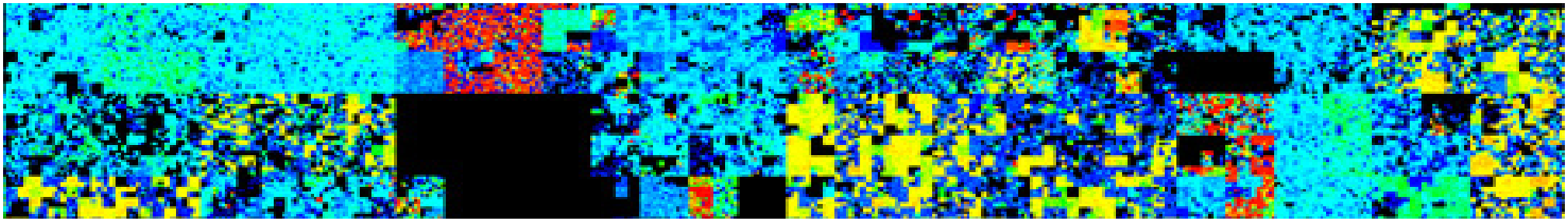
...Smart Security for Business & Government is a Multi-Year Programme!

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!

- CyberTerrorism (1) – "Conflict in Cyberspace"

1 – Background: "*Cyber Terror Landscape*"	2 – Cyber Players & Targets	3 – Typical Cyber Threat Scenarios
4 – Recent Cyber Terror Case Studies	5 – Advanced Hybrid 4D Terrorism	**6 – Industrial to Intelligent Cyber Society**
7 – Cyber Models, Strategies & Tactics	8 – New Conflict Zone: *Internet of Things*	9 – **Top 10** - CSO Cyber Action Themes



Transition from 20thC to 21stC Smart Security

- **Cybersecurity 2015-2025:**
  - Every country in the world will need to transition from the traditional 20thC culture & policy of massive physical defence to the connected "neural" 21stC world of in-depth intelligent & integrated cyber defence solutions
- **National Boundaries:**
  - Traditional physical defence and geographical boundaries are still strategic national assets , but they need to be augmented through integrated cyber defence organisations & assets.
- **Critical National Information Infrastructure:**
  - 21stC national economies function electronically, & yet they are poorly defended in cyberspace, and very often open to criminal & political attacks
- **Multi-Dimensional Cyber Defence:**
  - Nations need to audit their critical infrastructure – government, banks, telecommunications, energy, & transport – and to upgrade to international cybersecurity standards based upon accepted "best practice" (ISO/IEC)

From Industrial to Cyber Defence

- **Industrial Age Security:** Throughout the Industrial Age of the 19th & 20th Centuries our governments & business focused upon Physical Security & Defence

- **Information Age Security:** ALL Business Sectors in the 21st C now need to invest significant resources for BOTH Physical and Cyber Security within an Integrated Team

- **"Real-Time" Response:** Cyber Attacks travel at the "Speed of Light" so our CyberSecurity Apps must operate in "Real-Time" with instant response to Threat Alerts.

Enhancing *"CBRNe"* Capabilities

- *Updating CBRNe:* Within traditional *"Terror"* training the focus is often on Physical CBRNe = Chemical, Biological, Radiological, Nuclear & Explosives

- *Extend Security Models:* We now need to extend such threats to include the parallel CyberTerror Attacks

- *Hybrid Terror Risks:* In potential terror scenarios, the potential CBRNe options can be manipulated & extended through Cyber Penetration of Government and Business IT Information Networks & Servers

..In summary we need to rethink traditional Physical & CBRNe Security & Terror Scenarios to include the multi-dimensional risk of stealthy Cyber Penetration and potential destruction of Critical System Controls & Data.

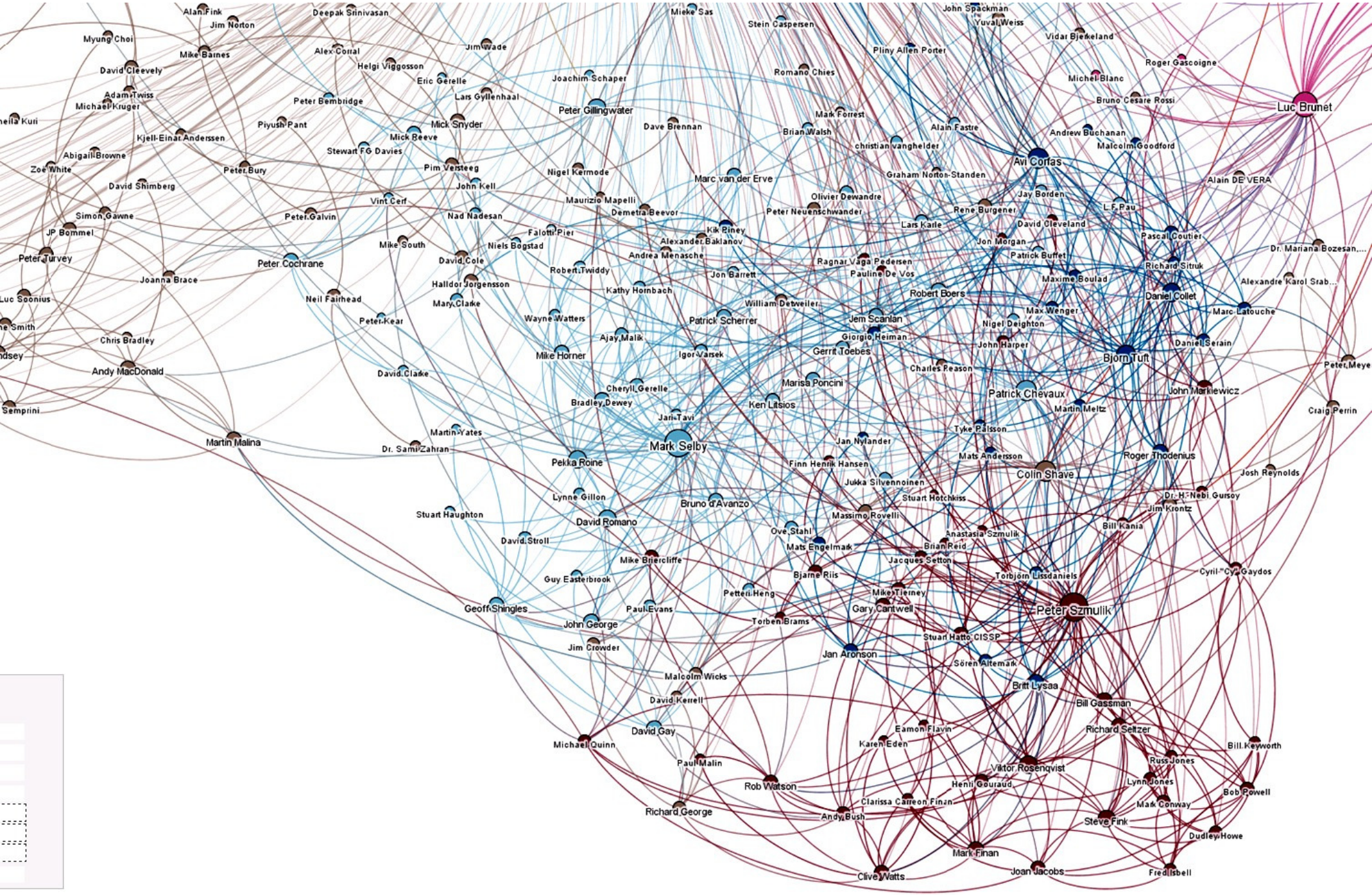
Monitoring and Securing Social Media

- CyberTerrorists are experienced in "Bottom-Up" attacks plans that begin with *"Spear Phishing Attacks"* using email & social media

- ALL Businesses & Government Agencies are at risk through "social hacking" of staff accounts and *Advanced Persistent Attacks* (APT)

- Business *must* monitor & protect staff against eMail Phishing Attacks & Malware Injection through *Social Media* – Facebook & Twitter...

Mapping Social Media Networks: *LinkedIn (Probert)*



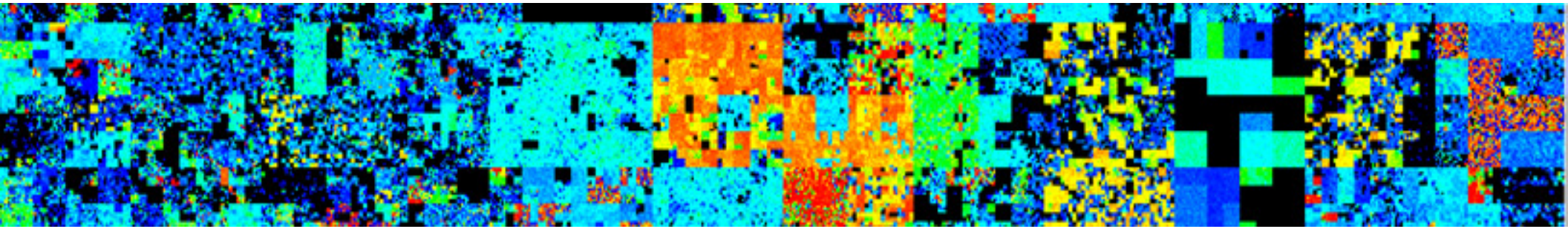
Cybersecurity for Social Networks

- *Social Sites:* During recent years, social & professional networking sites such as Facebook and Linkedin have become the latest commercial targets for cybercriminals
- *Cyber Scams* include Identify Theft and requests for instant money transfers from parents to support the "release" of children & friends overseas
- *Cybercriminals* also sign-up as "friends" in order to infiltrate student & family networks, and then to secure personal information & account details
- *Paedophiles* also use these social networks in order to cultivate relationships with children and teenagers below the "age of consent"
- *Businesses* may be at risk if employees publish confidential company information on their social network accounts that may easily go public
- *Facebook* now works with child protection authorities in countries such as a the UK so that those at risk can quickly contact "help lines"

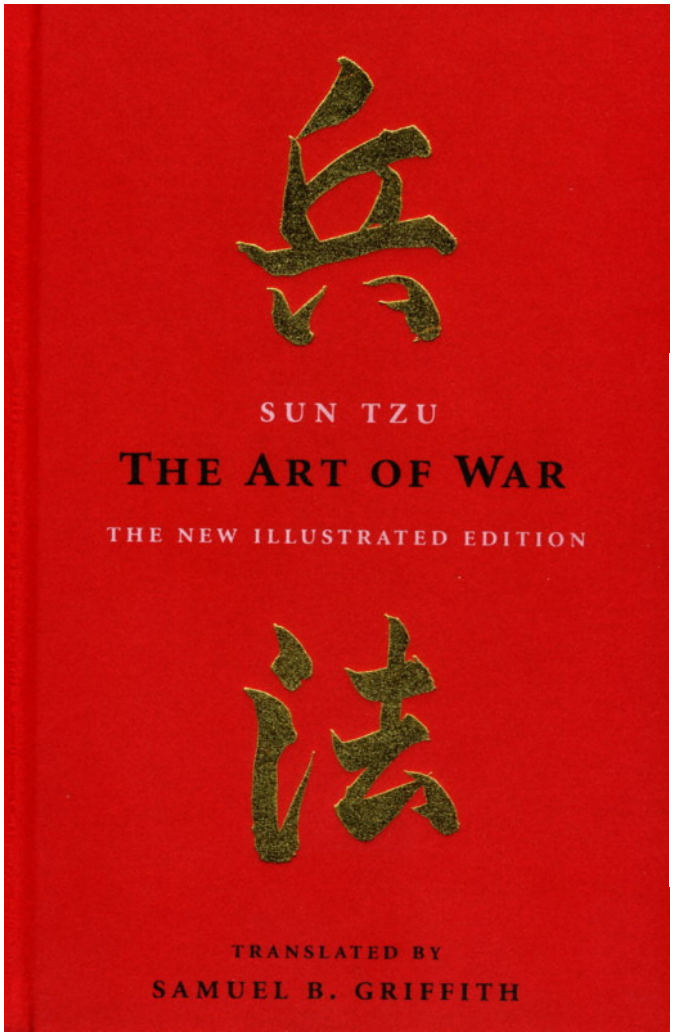
……Business and Government should consider ways to exploit the power of social networking whilst protecting their own networks against attack.

- CyberTerrorism (1) – "Conflict in Cyberspace"

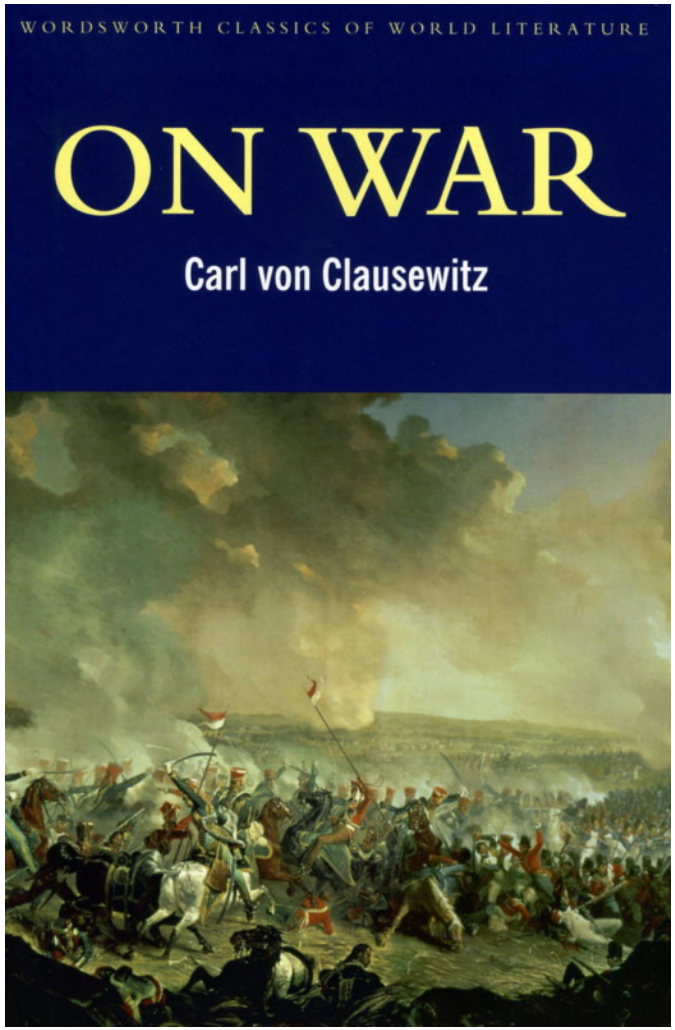
1 – Background: "*Cyber Terror Landscape*"	2 – Cyber Players & Targets	3 – Typical Cyber Threat Scenarios
4 – Recent Cyber Terror Case Studies	5 – Advanced Hybrid 4D Terrorism	6 – Industrial to Intelligent Cyber Society
7 – Cyber Models, Strategies & Tactics	8 – New Conflict Zone: *Internet of Things*	9 – Top 10 - CSO Cyber Action Themes



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



Recommended "Bedtime Reading" *for* Cybersecurity Specialists!



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

Cybersecurity Models, Strategies & Tactics

- *UN/ITU:* Global CyberSecurity Agenda (GCA)
- *UK Contest:* Counter Terror Strategy: -
  ...Pursue, Prevent, Protect & Prepare
- *NATO/CCDDOE:* National Cybersecurity Framework
- *EU/ENISA:* Info Security Agency – Cyber Good Practice Guide
- *OAS/CICTE:* Inter-American Committee against Terrorism
- *SANS Institute:* Critical Security Controls
- *ISF:* Information Security Forum: "Good Practice Standard"
- *ISO/IEC 27000 Series:* Information Security Standards
- *NIST* : Institute of Standards – Cybersecurity Framework

....We'll review these in "Security in Cyberspace" after lunch!

SANS: Critical Security Controls (CSC)

Mapping the Controls Across the Cyber Defense Lifecycle

The Critical Controls provide high value across different stages of the typical "Prevent/Detect/Respond" cyber-security lifecycle. SANS has created a mapping allocating the Controls across four phases:

CYBER DEFENSE LIFECYCLE

CRITICAL SECURITY CONTROLS

Resource Hardening	Privilege and Access Management	Attack Detection/Mitigation	Compromise Detection, Response, Recovery, and Reporting
Hardware and Software Inventory **CSC1 & CSC2**	Admin Privileges **CSC12**	Malware Defenses **CSC5**	Data Recovery **CSC8**
Secure Configurations **CSC3, CSC7, CSC10 & CSC11**	Controlled Access **CSC15**	Boundary Defense **CSC13**	Audit **CSC14**
Vulnerability Assessment & Application Security **CSC4 & CSC6**	Account Managing **CSC16**		Data Protection **CSC17**
			Incident Response **CSC18**

People and Processes

The Critical Security Controls includes a number of security areas which focus on people and processes and are applicable across the entire lifecycle:

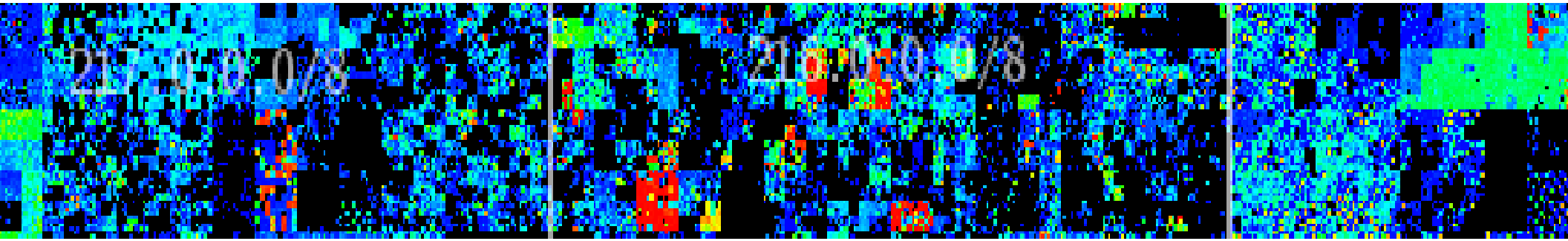
CSC9 – Security Skills Assessment and Training
CSC19 – Secure Network Engineering
CSC20 – Penetration Testing and Red Team Exercises

SANS = SysAdmin, Audit, Networking and Security

Link: www.sans.org/critical-security-controls/

- CyberTerrorism (1) – "Conflict in Cyberspace"

1 – Background: "*Cyber Terror Landscape*"	2 – Cyber Players & Targets	3 – Typical Cyber Threat Scenarios
4 – Recent Cyber Terror Case Studies	5 – Advanced Hybrid 4D Terrorism	6 – Industrial to Intelligent Cyber Society
7 – Cyber Models, Strategies & Tactics	**8 –New Conflict Zone: *Internet of Things***	9 – **Top 10** - CSO Cyber Action Themes



New Conflict Zone: *"Internet of Things"*

- *CyberEvolution:* During the next 25 year phase of Cyber Evolution the Internet will extend to most IT enabled devices within cars, homes, offices, power stations & retail products! This is the "Internet of Things" – IoT

- *CyberSecurity:* ALL IoT connected devices, nodes & servers will need to be secured against *cyber attack*!

- *Next Conflict Zone:* The IoT is destined to become the next major Cyber Conflict Zone during *2015 – 2040*....

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.

Home | News | Events | Documents | Newsletters | About IERC | Partners | Links | Contact

IERC OBJECTIVES

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

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.

Internet of Things

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

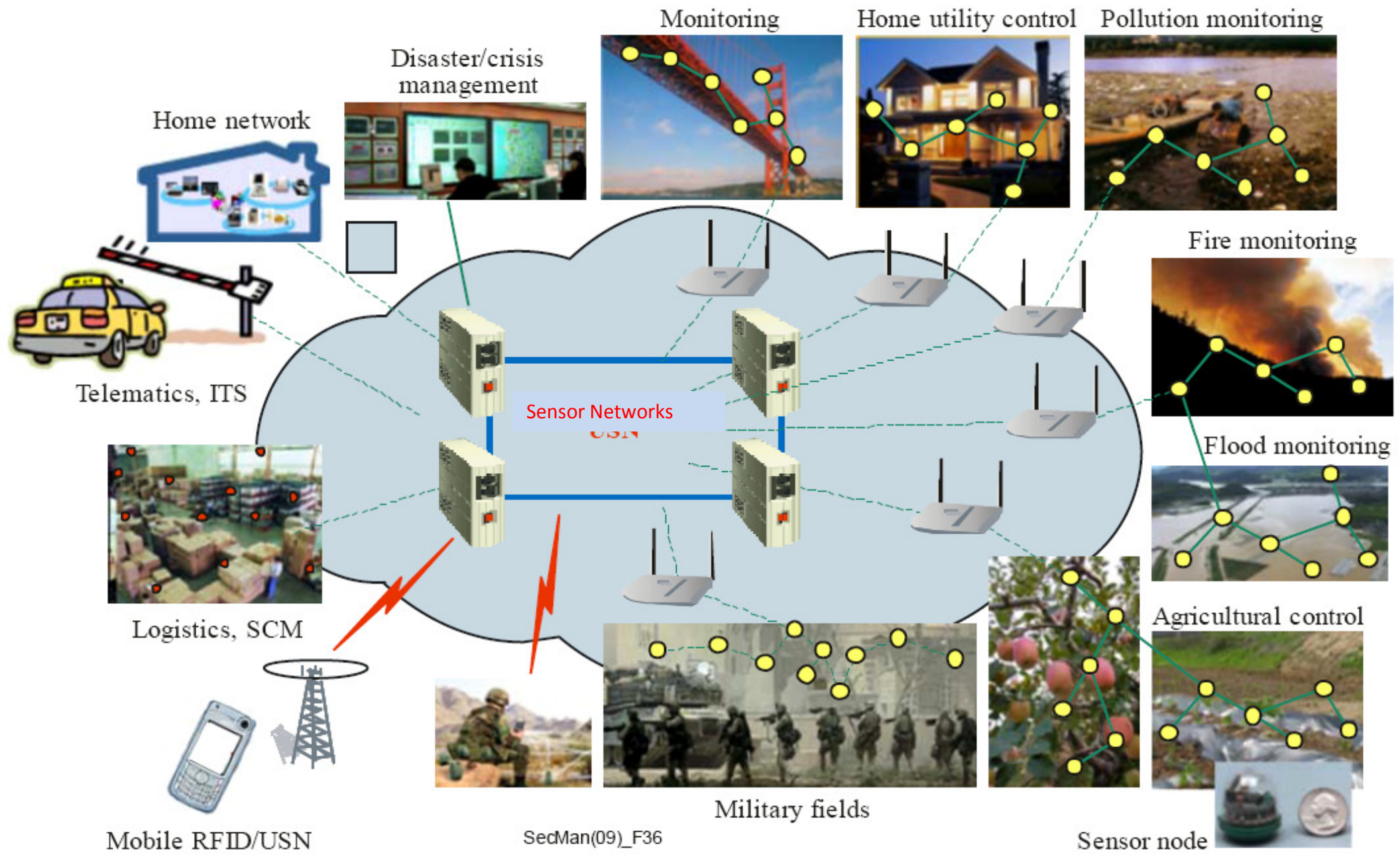
NEWS

- 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

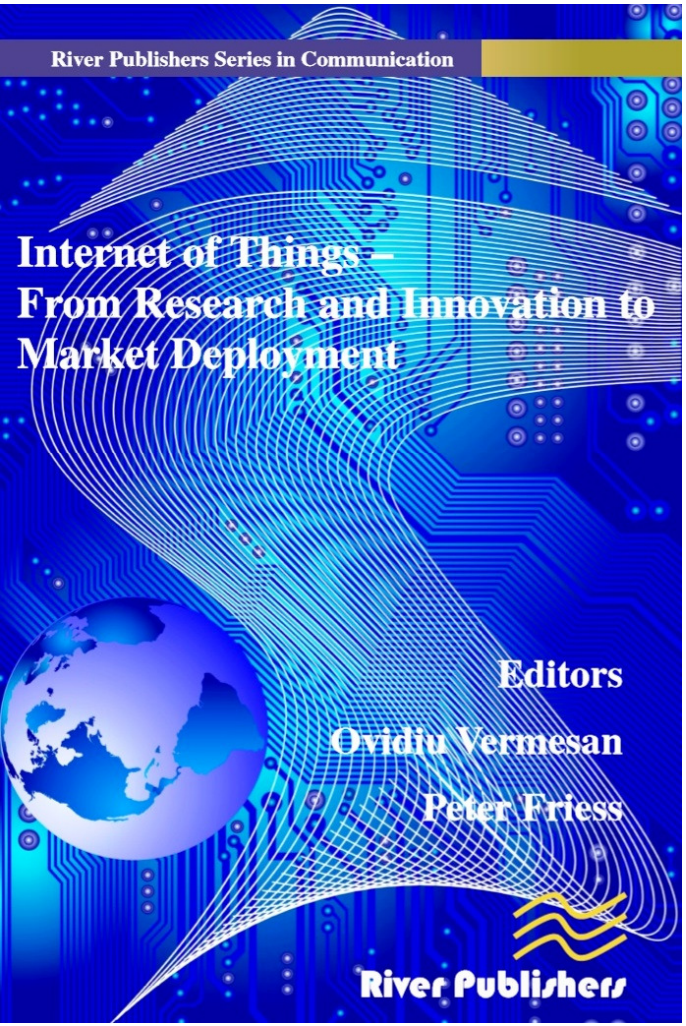
DOCUMENTS

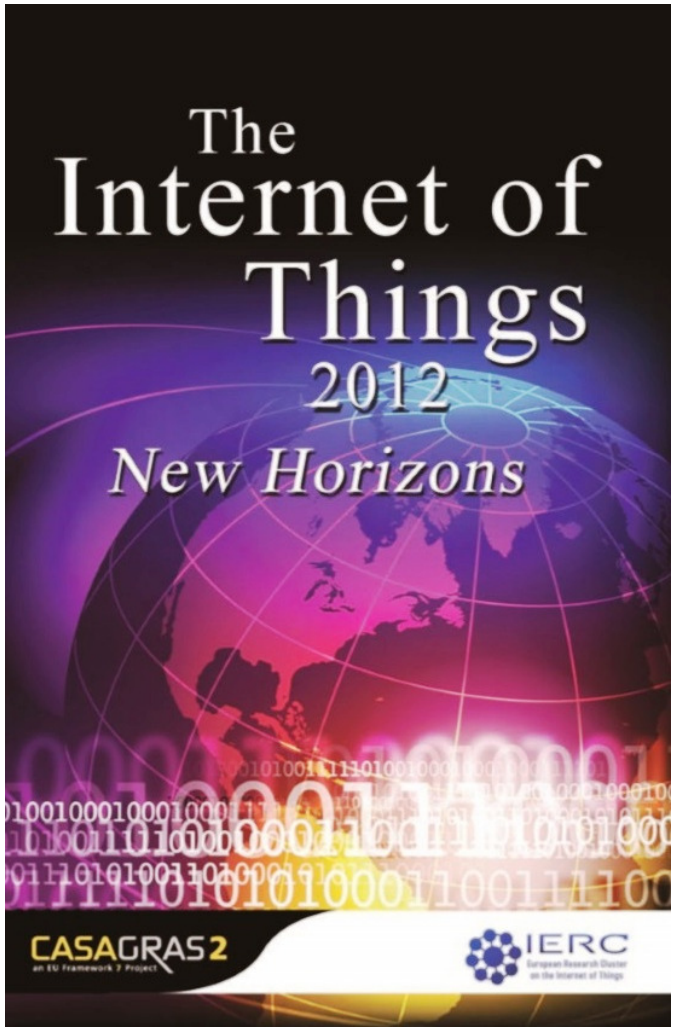
- Internet of Things: From Research and Innovation to Market Deployment
  -IERC Cluster Book 2014
- Internet of Things: Strategic Research and Innovation Agenda
  -IERC Cluster SRIA 2014
- IoT: Converging Technologies for Smart Environments and Integrated Ecosystems
  -IERC Cluster Book 2013
- The Internet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

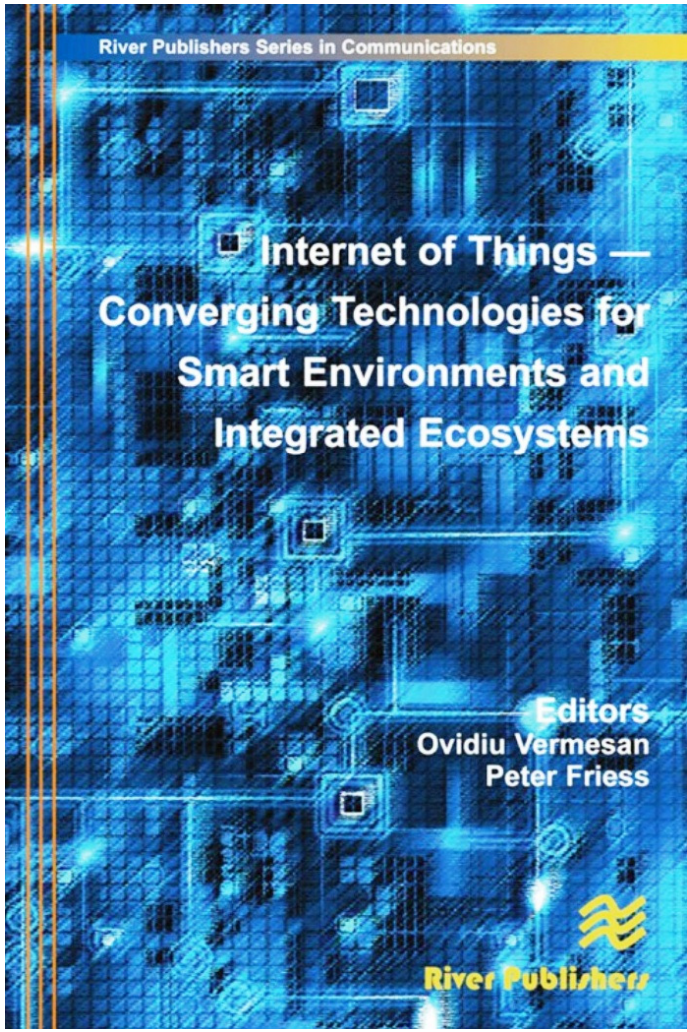
Cybersecurity for Critical Sector Networks: *"Internet of Things"*



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

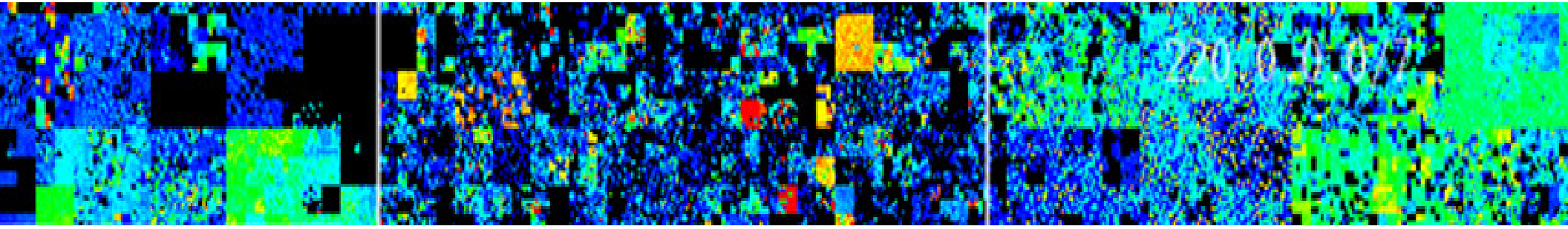






- CyberTerrorism (1) – "Conflict in Cyberspace"

1 – Background: "*Cyber Terror Landscape*"	2 – Cyber Players & Targets	3 – Typical Cyber Threat Scenarios
4 – Recent Cyber Terror Case Studies	5 – Advanced Hybrid 4D Terrorism	6 – Industrial to Intelligent Cyber Society
7 – Cyber Models, Strategies & Tactics	8 – New Conflict Zone: *Internet of Things*	**9 – Top 10 – CSO Security Action Themes**



- Smart Sustainable Security in the Wild! -

The Sociable Weaver Bird

"World's largest Bird Nests"

*** Southern Africa ***

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

...all the features of a 21st C-"Cyber Defence Centre"–including Disaster Recovery & Business Continuity!

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***

"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!

Case Study: White Paper: 21st C Georgia – *"Cyber-Vardzia"*

…"21stC Georgia"…

…"Cyber-Vardzia"…

"Integrated Cyber & Physical Security"

*** for ***

… e-Government, e-Society & e-Georgia.

Author: *Dr David E Probert – VAZA International*

*** Integrated Cyber & Physical Security Systems for 21stC Georgia ***

Author: *Dr David E Probert – VAZA International*

(0) Executive Summary

In this White Paper I argue that for Georgia to secure its national borders and to protect its critical national infrastructure in the 21stC, that it should develop its cybersecurity & physical security within the framework of an integrated security organisation with charter from highest levels of Government.

The paper briefly reviews the major cybersecurity and physical security technologies and solutions, and then discusses the more complex security threats that can only be detected through the operational integration of the cyber and physical security organisations.

I then consider examples of ways in which cyber and physical security solutions can be operationally & technologically integrated to provide a more effective response to evolving cybercriminal threats. Following this generic review of integrated security, I move to a more detailed discussion of the security requirements on a sector-by-sector basis, focusing on those sectors that are critical to the national economic & political infrastructure including: government, telecommunications, banking, energy, transportation, education, police and defence.

My personal vision for this project is based upon the Georgian Historical Cave City of Vardzia!...

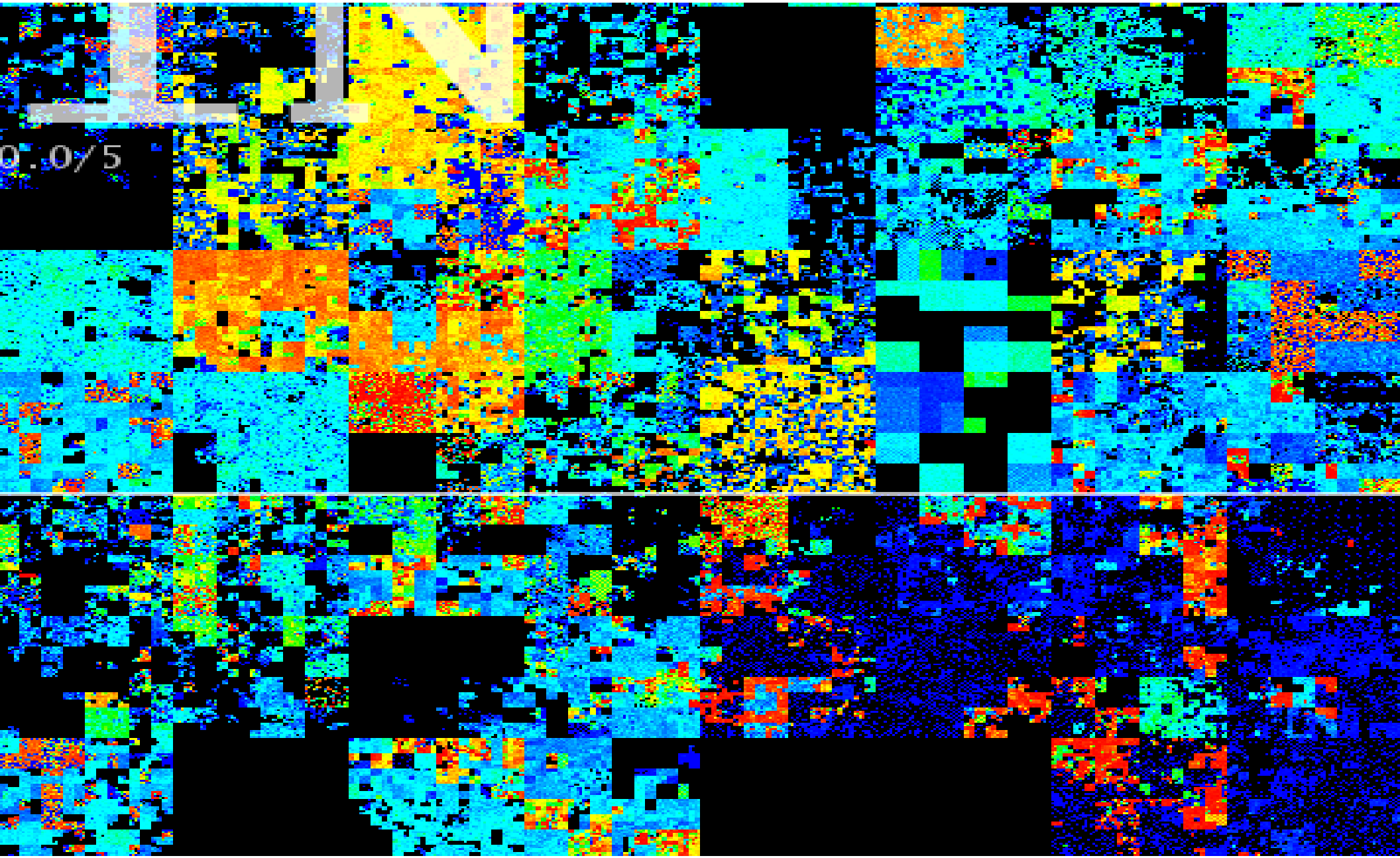
.....Significant investment is being made by international agencies and countries into the Georgian Economy, and already much progress has been achieved during the last 3 to 5 years. However in parallel there needs to be incremental investment to upgrade both Georgian physical and cyber security for its critical national infrastructure. There remains an international perception that Georgia's borders & cyber-networks are still not fully secured....

..... So just as the 12thC **Vardzia** Cave Complex protected the country for several hundred years during the medieval period, so this new integrated security programme will dramatically increase Georgia's protection against cyber-attacks and potential invasions during our 21stCentury!

Finally I summarise some of the major benefits for Georgia to consider cybersecurity and physical security within the same organisational and operational framework, and suggestions for next steps.

Web Link : *www.Valentina.net/vardzia/Georgia2010.pdf*

The Challenging Complexity of *Securing IP Cyberspace*



TOP 10 ***CSO*** *Cybersecurity* Action Themes

1) CSO – Chief Security Officer's Team – Roles & Responsibilities
2) Professional Training – Suggest Top-Level CISSP Certification
3) Implement International Security Standards (ISO/IEC- 27000)
4) Develop CERT/CSIRT Team
5) Profile Security Staff and Contractors for Possible Risks
6) ICT: Hire Qualified Cyber Systems Technology, Software & Operations Team
7) Cyber Asset Monitoring including Memory Chips & Smart Phones
8) Bring Your Own Device Policy – Communicate Rules to Staff
9) Professional Association Membership for Team Networking & Skill Building
10) Cyber Legal Protection – Check *Your* Contracts for Cyber Trading Risks

This afternoon we'll further review and discuss these ***Top 10 CSO Action Themes!***

CyberTerrorism (1): *Wrap-Up Summary*

1) *Cyber Epidemic:* Most Business & ALL Governments now experience regular Cyber Penetration Threats & Occasional Attacks
2) *Cyber Terror:* Emerging as a new Disruptive Threat to Critical Businesses (Banks, Energy, Industry) as well as National Governments
3) *Hybrid Security:* Business now need to Plan, Design and Implement Integrated Physical-Cyber Security to Defend against CyberAttacks. CyberCrime & CyberTerrorism

.....In my next talk– **CyberTerrorism:** *"Security in Cyberspace"* we discuss practical options for Securing *YOUR* Business against Cyber Penetration, Cyber Attacks & possible CyberTerrorism

CyberTerrorism (1): "Conflict in Cyberspace"

International East-West Security Conference: Terracina, Italy

Thank-You!...

Download Presentation Slides:

www.Valentina.net/East-West2015/

East-West Security Conference – Italy 2015

- CyberTerrorism Presentation Slides (PDF) -

- CyberTerrorism (1) -
"Conflict in Cyberspace"

31st International East/West Security Conference "Cyber-terrorism(1): Conflict in Cyberspace" Terracina, Italy : 25th-26th May 2015 © Dr David E. Probert : www.VAZA.com © 1

Theme (1) – "Conflict in Cyberspace"

- CyberTerrorism (2) -
"Security in Cyberspace"

31st International East/West Security Conference "CyberTerrorism(2): Security in Cyberspace" Terracina, Italy: 24th – 27th May 2015 © Dr David E. Probert : www.VAZA.com © 1

Theme (2) – "Security in Cyberspace"

Download Link: *www.valentina.net/East-West2015/*

Download Presentation Slides:
www.Valentina.net/East-West2015/

Thank you for your time!

Additional *Cybersecurity* Resources

Link: www.valentina.net/vaza/CyberDocs

Professional Profile - *Dr David E. Probert*

- ***Computer Integrated Telephony (CIT)*** – Established and led British Telecom's £25M EIGER Project during the mid-1980s' to integrate computers with telephone switches (PABX's). This resulted in the successful development and launch of CIT software applications for telesales & telemarketing

- ***Blueprint for Business Communities*** – Visionary Programme for Digital Equipment Corporation during late-1980's that included the creation of the "knowledge lens" and "community networks". The Blueprint provided the strategic framework for Digital's Value-Added Networks Business

- ***European Internet Business Group (EIBG***) – Established and led Digital Equipment Corporation's European Internet Group for 5 years. Projects included support for the national Internet infrastructure for countries across EMEA as well as major enterprise, government & educational Intranet deployments. Dr David Probert was a sponsoring member of the European Board for Academic & Research Networking (EARN/TERENA) for 7 years (1991 ➔1998)

- ***Supersonic Car (ThrustSSC)*** – Worked with Richard Noble OBE, and the Mach One Club to set up and manage the 1st Multi-Media and e-Commerce Web-Site for the World's 1st Supersonic Car – ThrustSSC – for the World Speed Record.

- ***Secure Wireless Networking*** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.

- ***Networked Enterprise Security*** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional engineers & a diverse portfolio of hi-tech security products.

- ***Republic of Georgia*** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament.

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

Dr David E. Probert is a Fellow of the Royal Statistical Society. He has a 1st Class Honours Degree in Mathematics (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata) , and his full professional biography is featured in the Marquis Directory of Who's Who in the World: 2007-2015 Editions.

"Master Class": Armenia - *DigiTec2012*

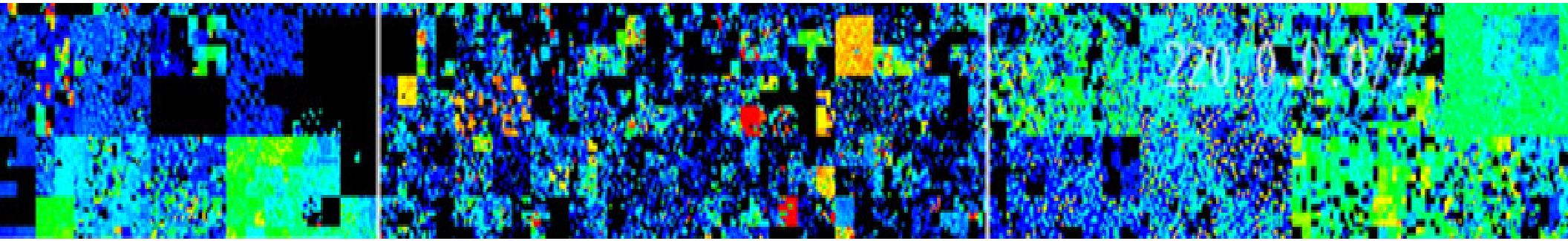
- Smart Security, Economy & Governance -

Download: www.valentina.net/DigiTec2012/

CyberTerrorism (1) : "Conflict in Cyberspace"

International East-West Security Conference: Terracina, Italy

BACK-UP SLIDES



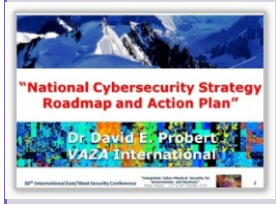
Smart Sustainable Security – *"Theme Trilogy"*

Theme (1) – *Smart Security :* *Integrated Cybersecurity and Physical Security*

- *Understanding and Mapping the Worldwide Cyber Threats*
- *Transition to Smart Systems : Embedded Networked Intelligence*
- *Emergence of Smart Security: Hybrid Cyber-Physical Applications*

"Operational Convergence " ***13th Oct: 09:10 – 09:50***

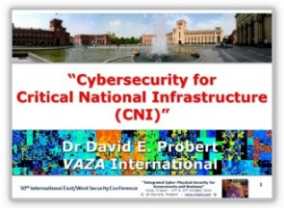
Theme (2) – *National Security :* *Strategy, Models, and Road Maps*



- *UN/ITU – Global Cybersecurity Agenda and Guide*
- *Operations, Technology, Legal, Training, Partnerships*
- *Case Studies of "National Cybersecurity Agencies"*

"Architecture & Standards" ***13th Oct: 14:30 – 15:10***

Theme (3) - *Critical Security :* *Sector Threats and Smart Solutions*



- *Smart Security for Critical National Infrastructure (CNI):*
- *Finance, Transportation, ITC, Energy, Defence and more!...*
- *Engineering Smart Technical and Operational Solutions*

"Intelligent Applications" ***14th Oct: 11:15 – 11:55***

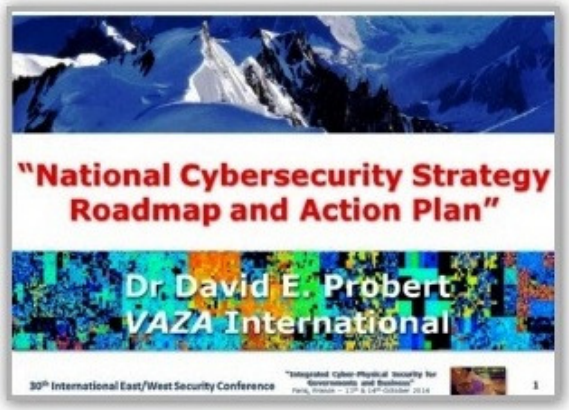
Download Slides: www.valentina.net/East-West2014/

East-West Security Conference – Paris 2014

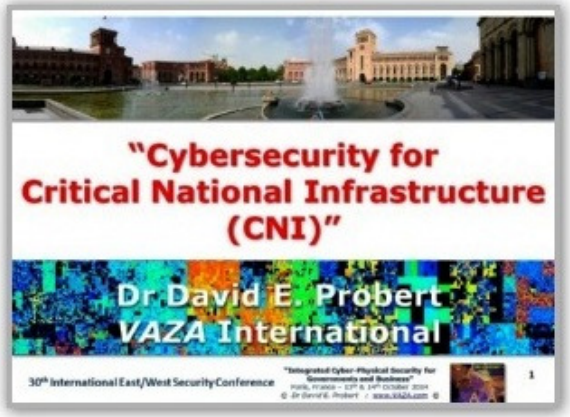
- Cybersecurity Presentation Slides (PDF) -

Smart Sustainable Security - "Theme Trilogy"

(1) Smart Security



(2) National Security



(3) Critical Security

Download Link: *www.valentina.net/East-West2014/*

Computer Telephony Integration (CTI):

Virtual Integration of Voice-Data via Command Protocol Link

PABX – Telephone Switch

Computer Server

CTI - Command Protocol
Using ITU - ISDN – Q.831

Low Bandwidth Command Link

CTI Solutions – Used in most Large **Call Centre** Operations now for more than 25 years

Hi-Speed Data

Hi-Quality Voice

10 Steps To Cyber Security

CESG

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

User Education and Awareness

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

Home and Mobile Working

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

Network Security

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

Establish an effective governance structure and determine your risk appetite.

Information Risk Management Regime

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

Secure Configuration

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

Malware Protection

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

Removable Media Controls

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

Monitoring

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

Managing User Privileges

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

Incident Management

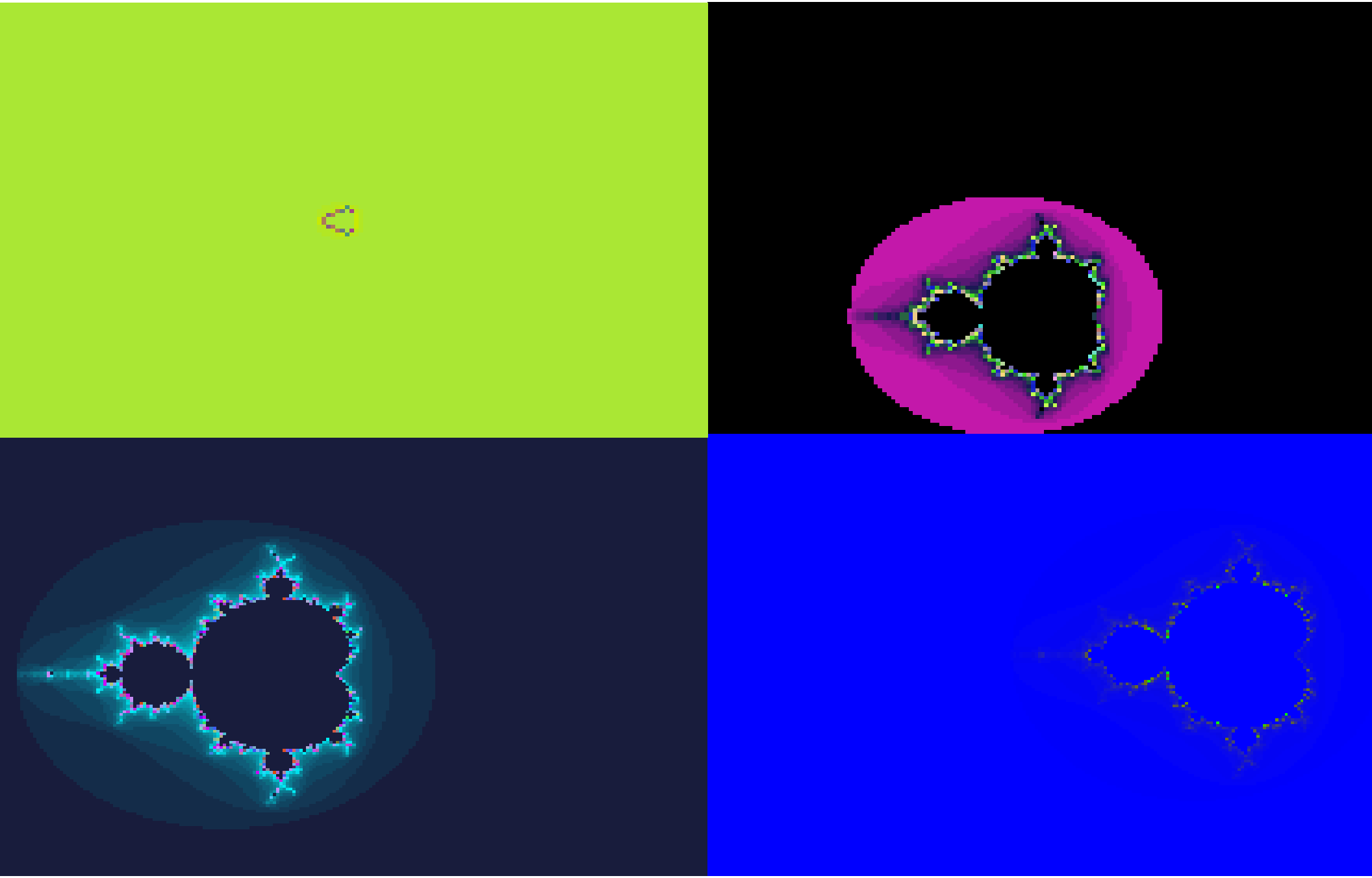
Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

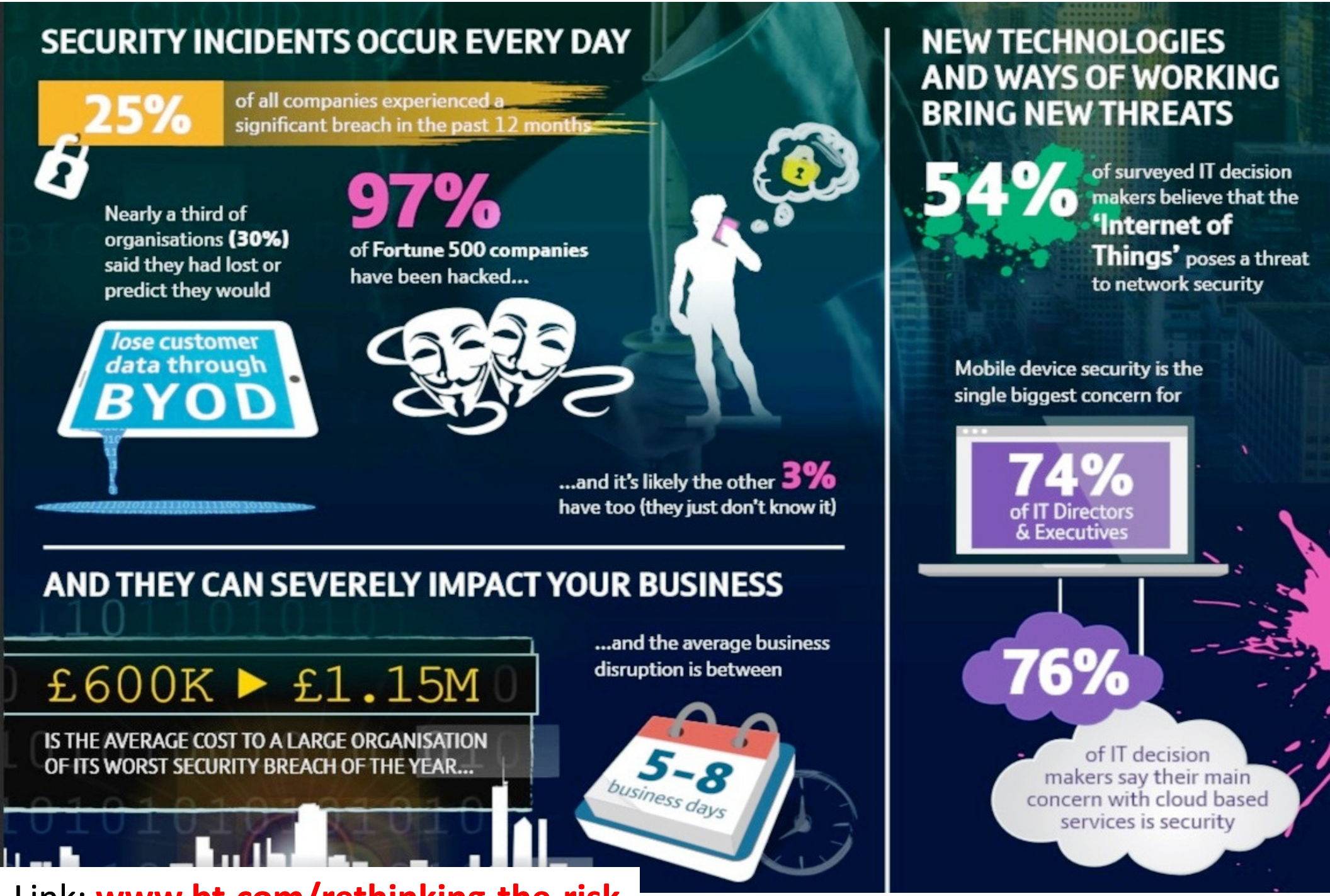
Department for Business Innovation & Skills | CPNI Centre for the Protection of National Infrastructure | Cabinet Office

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

"Smart Scaling": Fractal Mandelbrot Set

.....Fractal Scaling is frequently found in Natural Systems.....





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