Cyber Threats & Defence!

- "Intelligent CyberSecurity"-

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

Dedicated to Grand-Daughters – Tatiana, Alice & Abigail – *Securing YOUR Life !*

36th International East West Security Conference

- Cyber Threats & Effective Defence! -
"Intelligent Business CyberSecurity"
Seville, Spain, 20th – 21st November2017

Кибер Угрозы и Защита

Умный КиберБезопасность

Dr David E. Probert
VAZA International

Cyber Futures & Defence: *"Dual Themes"*

Theme (1)" - *"Security Futures: 2018-2025+" : Technology, Tools and Trends...*

- *Bringing CyberSecurity to **YOUR** Board Room with Budget & Mission!*
- *Future **Cyber-Scenarios** for Integrated, Adaptive, Intelligent Security!*
- *New CyberSecurity Toolkits to Defend **YOUR** Business Operations!*

" CyberVision: Machine Learning, AI & Neural Security" ***21st Nov: 09:40– 10:20***

Theme (2) – *"Cyber Threats & Defence": Intelligent CyberSecurity for OUR 21st C...*

- ***TOP 10 CyberThreats**: Exploration, Penetration and Attack!*
- *Recent **Case Studies** of Cyber Crime, Terror & Political Attacks!*
- *Developing **YOUR** Action Plans & Cybersecurity Programme!*

"CyberDefence: Real-Time Learning, Detection & Alerts" ***21st Nov: 14:30 – 15:10***

Download Slides: *www.valentina.net/Seville2017/*

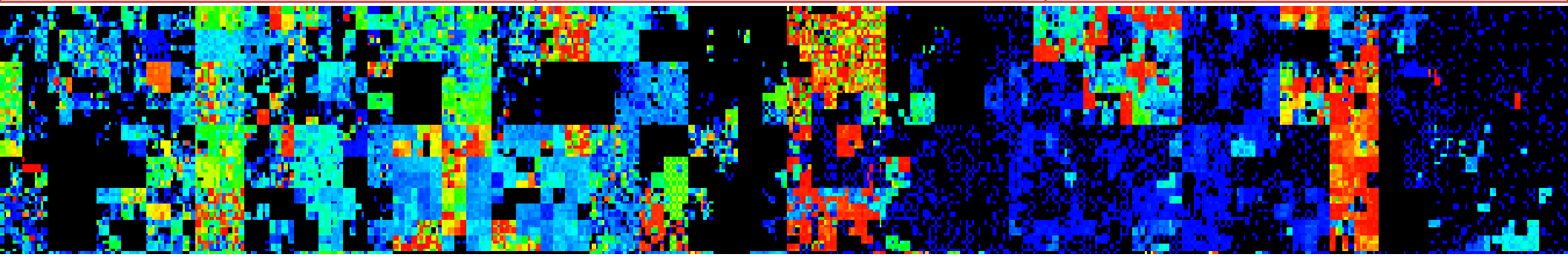
Topics suggested @ Genoa – June 2017

1. CyberCrime & CyberTerror: Who is the Enemy?
2. Effective InfoSec: *Boardroom Responsibility(CSO)*
3. Virus Threat! : *Aware Global - Protect Local !*
4. CyberSecurity in the Financial Services Sector
5. Security Strategies for Corporate Networks
6. Threats to IT Infrastructure & Countermeasures!
7. Effective IT Security: *Prevent & Adapt to Threats*

……We'll respond to ALL these during this talk on "Cyber Threats & Defence": Intelligent Security

Cyber Threats & Defence: Intelligent Security

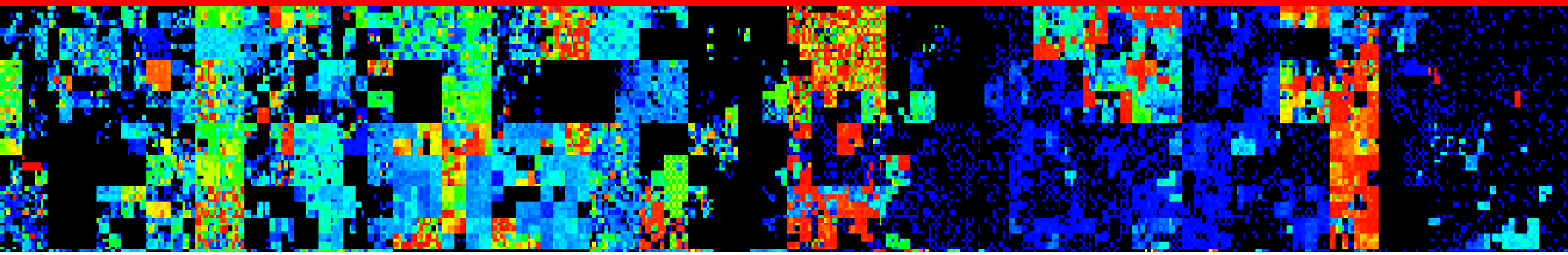
1 –"TOP 10 Cyber Threats & Attacks"	2– Cyber Case Studies: Recent Attacks	3 – Cyber Hack & Attack Campaigns!
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6–Real-Time Cyber Alert and Attack! **"Cyber Attack!"**
7 –In-Depth: Security for Critical Sectors	8– ***YOUR*** Operational Cyber Defence	9 –***YOUR*** Cyber Campaign Action Plan!



Cyber Threats & Defence: Intelligent Security

1 –"TOP 10 Cyber Threats & Attacks!"

CyberCrime – CyberTerror – CyberWar



"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!

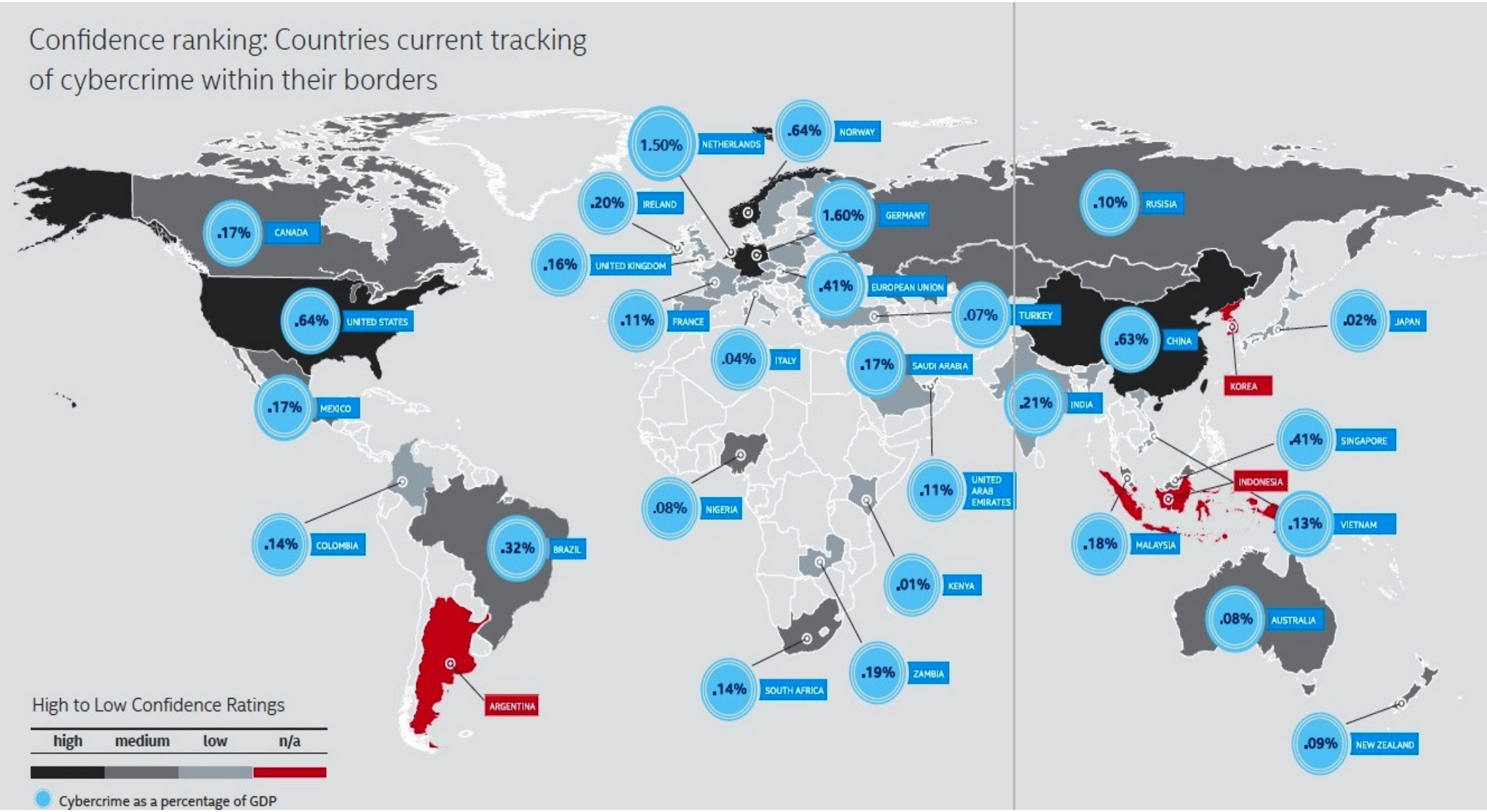
*.....These same **TOP 10 Threats** are used in some combination in **EVERY** Cyber Hack & Attack!....*

World Economic Forum: Global CyberCrime

- $445Billion (Intel Research : June 2014) -

World Economic Forum: Global CyberCrime

- $445Billion (Intel Research : June 2014) -



World Economic Forum: Global CyberCrime

- $445Billion (Intel Research : June 2014) -

World Economic Forum: Global CyberCrime

- $445Billion (Intel Research : June 2014) -

"BAD RABBIT" Ransomware Attack – 24th Oct 2017

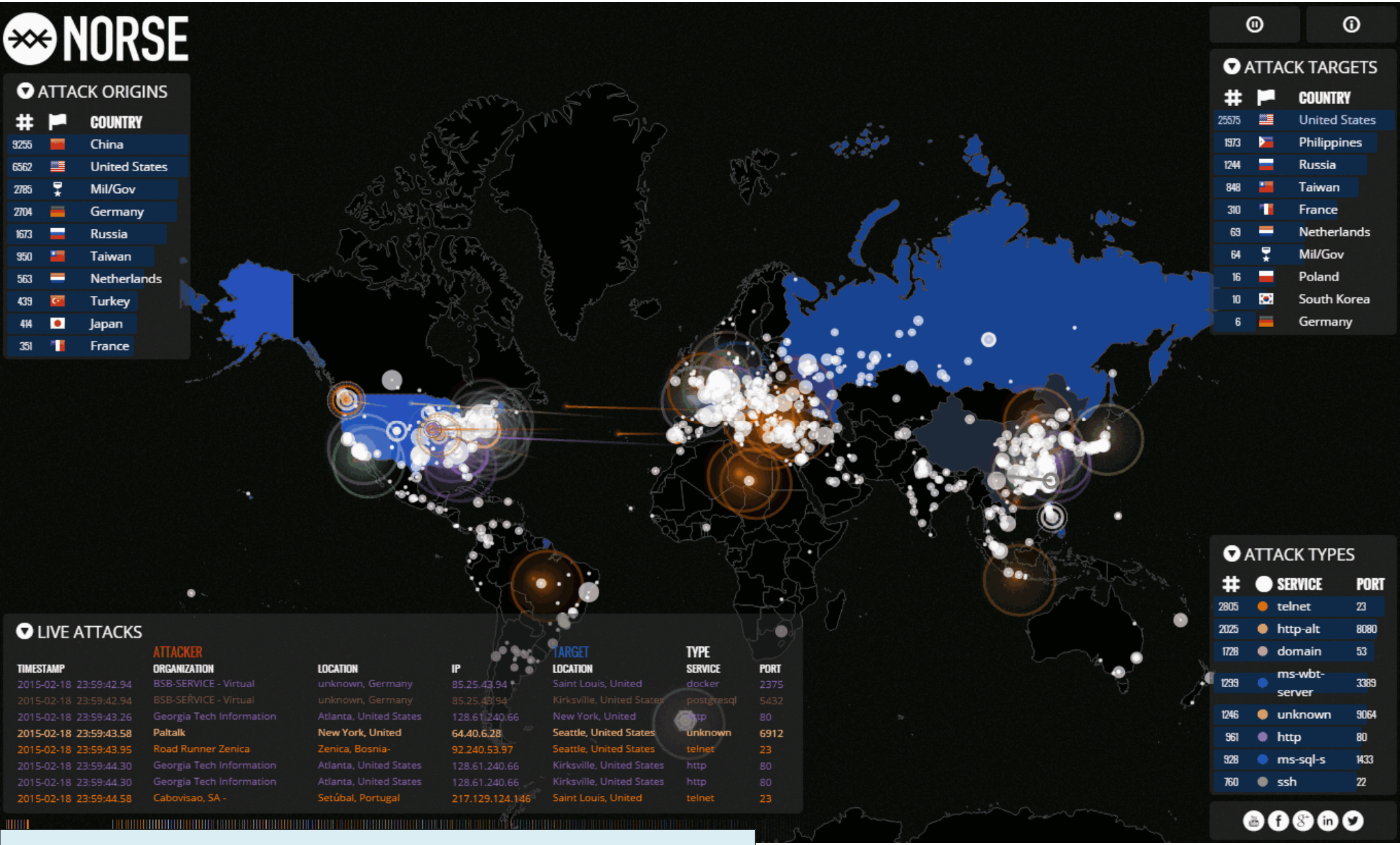
"Countdown to TOP 10 Cyber Threats!"

- **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!...

Real-Time Global DDoS "BotNet" Attack



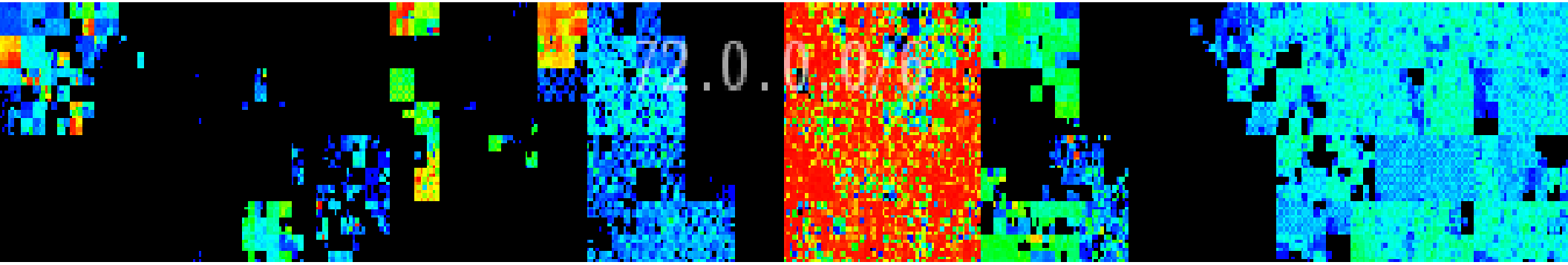
Link: map.norsecorp.com - Norse Corporation

Guide to Cyber Scams: March 2017

https://beta.met.police.uk/globalassets/downloads/fraud/the-little-book-cyber-scams.pdf

Cyber Threats & Defence: Intelligent Security

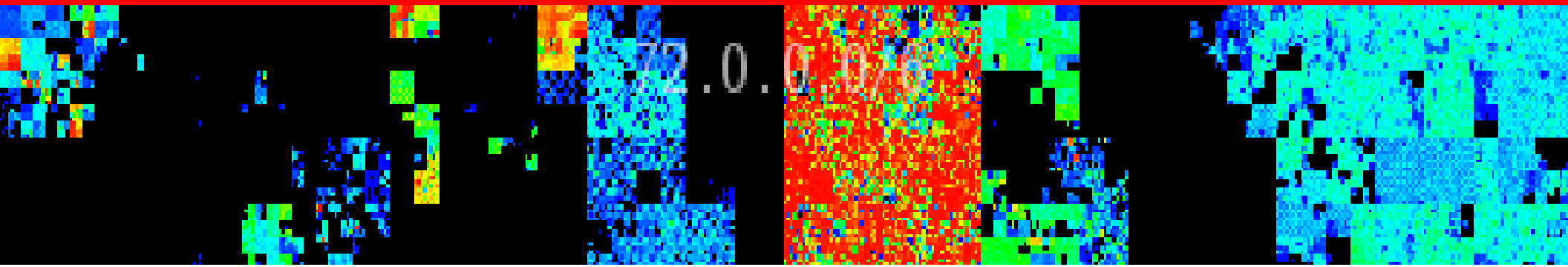
1 –"TOP 10 Cyber Threats & Attacks"	**2 –Cyber Case Studies: Recent Attacks**	3 – Cyber Hack & Attack Campaigns!
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert and Attack! **"Cyber Attack"**
7 –In-Depth: Security for Critical Sectors	8 – ***YOUR*** Operational Cyber Defence!	9 –***YOUR*** Cyber Campaign Action Plan!



Cyber Threats & Defence: Intelligent Security

2 –Cyber Case Studies: Recent Attacks

Ransomware & ID Theft!...



Global RansomWare CyberAttack

"WanaCrypt0r 2.0" - 12th May 2017

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

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

Global RansomWare CyberAttack

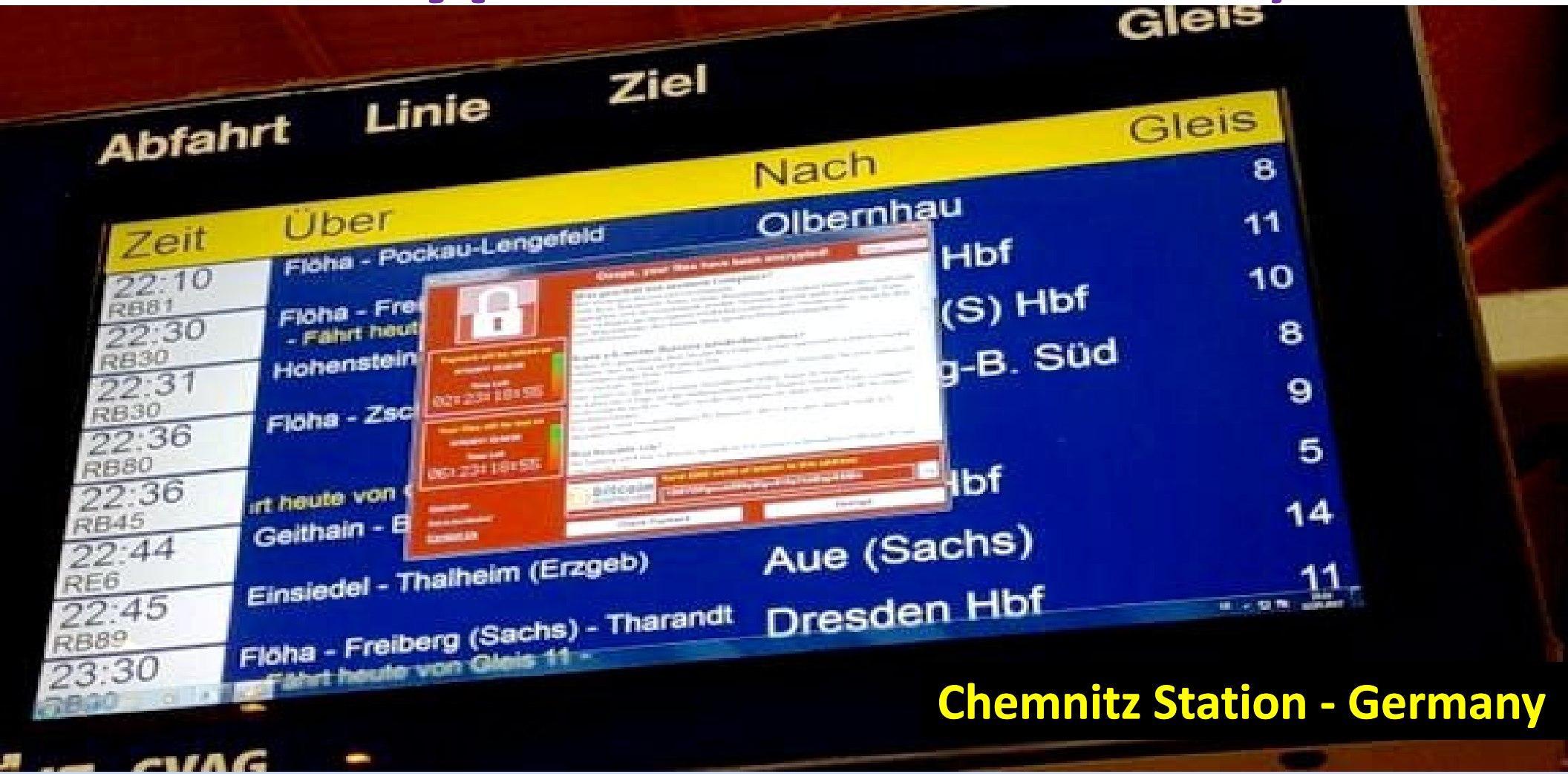
"WanaCrypt0r 2.0" - 12th May 2017

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

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

Global RansomWare CyberAttack

"WanaCrypt0r 2.0" - 12th May 2017



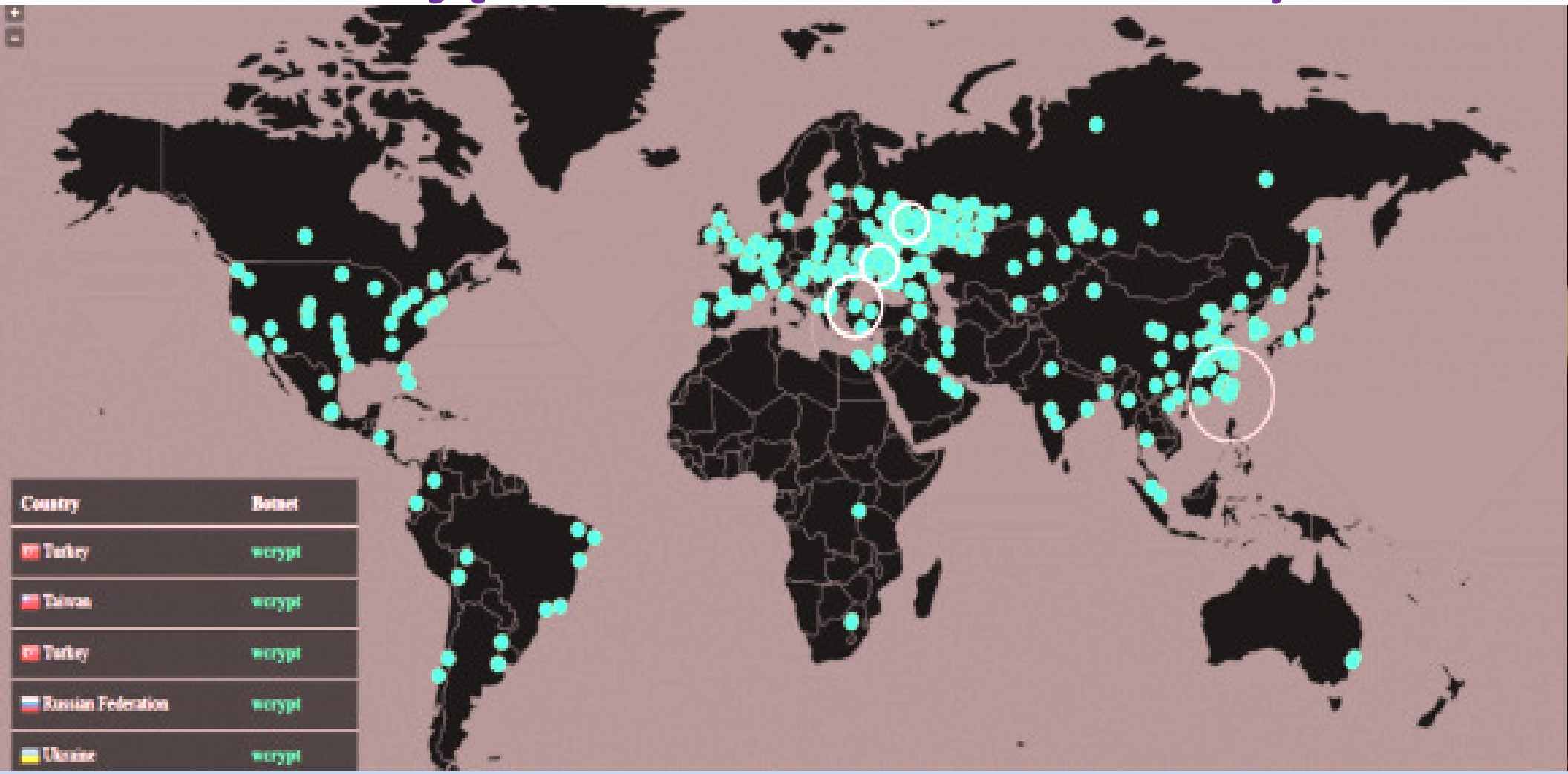
Chemnitz Station - Germany

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

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

Global RansomWare CyberAttack

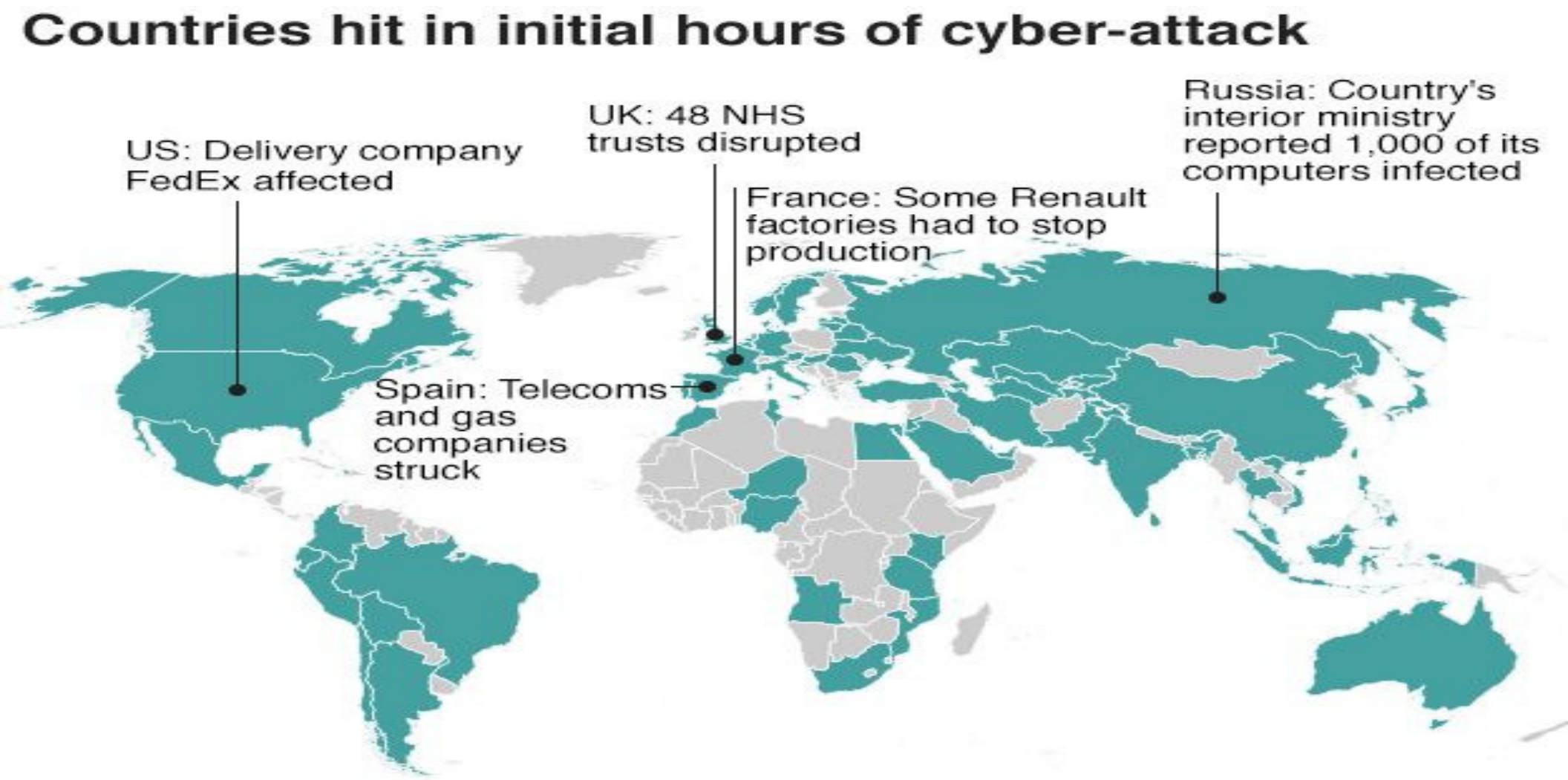
"WanaCrypt0r 2.0" - 12th May 2017



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

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

Global RansomWare CyberAttack

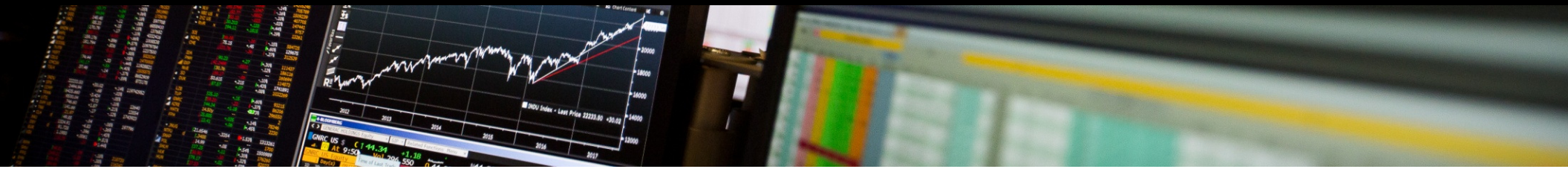


...More than 200k Systems in 150+ Countries!

Massive Hack – EQUIFAX - Sept 2017

Personal IDs Stolen from 144Million+ Clients (USA, UK...)

....Credit Cards, Driving Licences, Social Security, eMail....



CyberCrime: Russian Financial Services

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

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

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

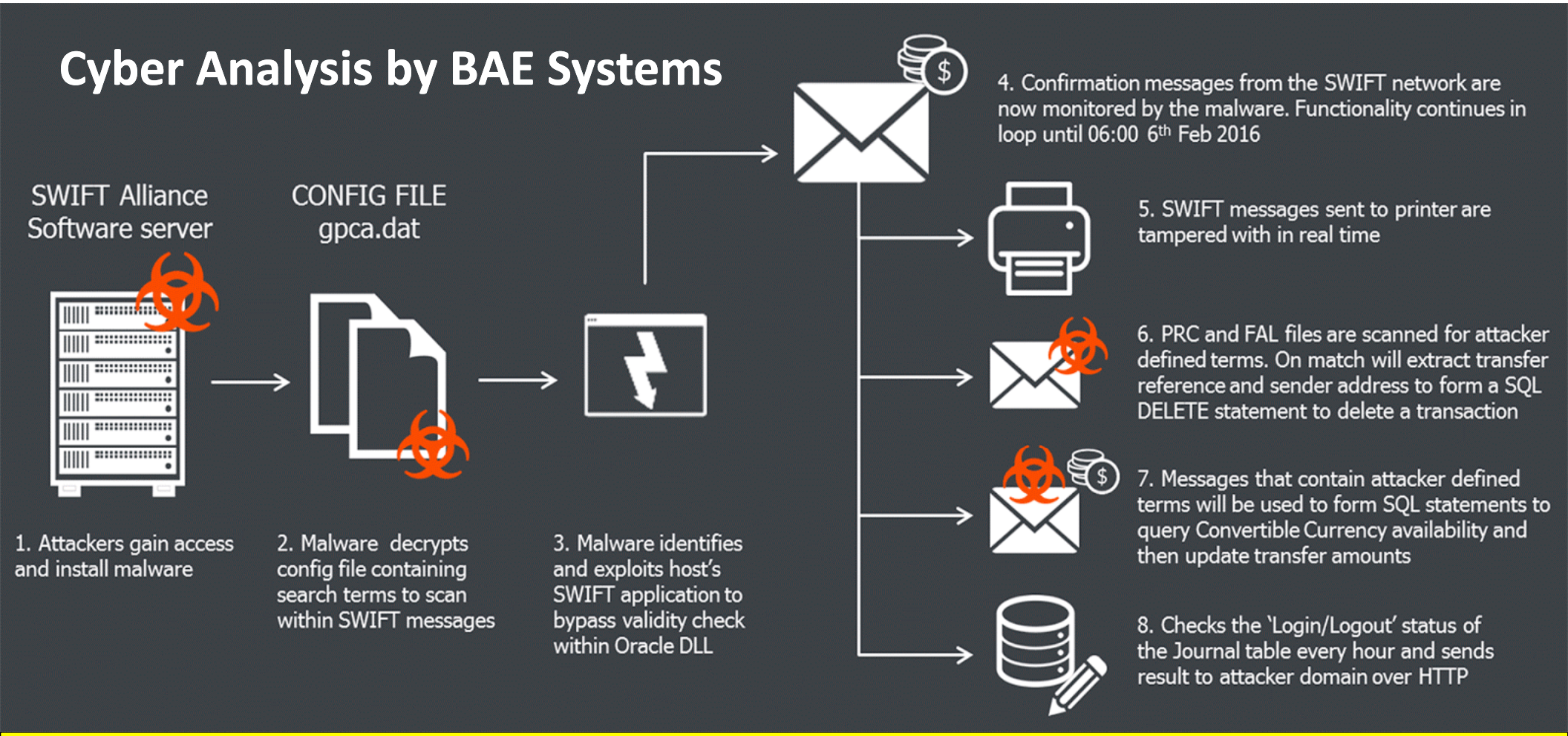
Press Report: TASS News Agency - 1st June 2016 -

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

Malware Attack: SWIFT Bank Net – 2016

Multiple Cyber Attacks including Cyber Heist of $951M from Bangladesh Central Bank of which $81M remains missing!

Malware Attack: SWIFT Bank Net – 2016



Multiple Cyber Attacks including Cyber Heist of $951M from Bangladesh Central Bank of which $81M remains missing!

Project Sauron: CyberEspionage - 2016

Analysed by Symantec and Kaspersky Labs...

- August 2016 -

Known CyberTargets include: Russia, China, Iran, Rwanda, Italy Sweden & Belgium

Other **"State-Designed"** Cyber Malware include:
Stuxnet, Duqu, Flame, Equation and Regin...

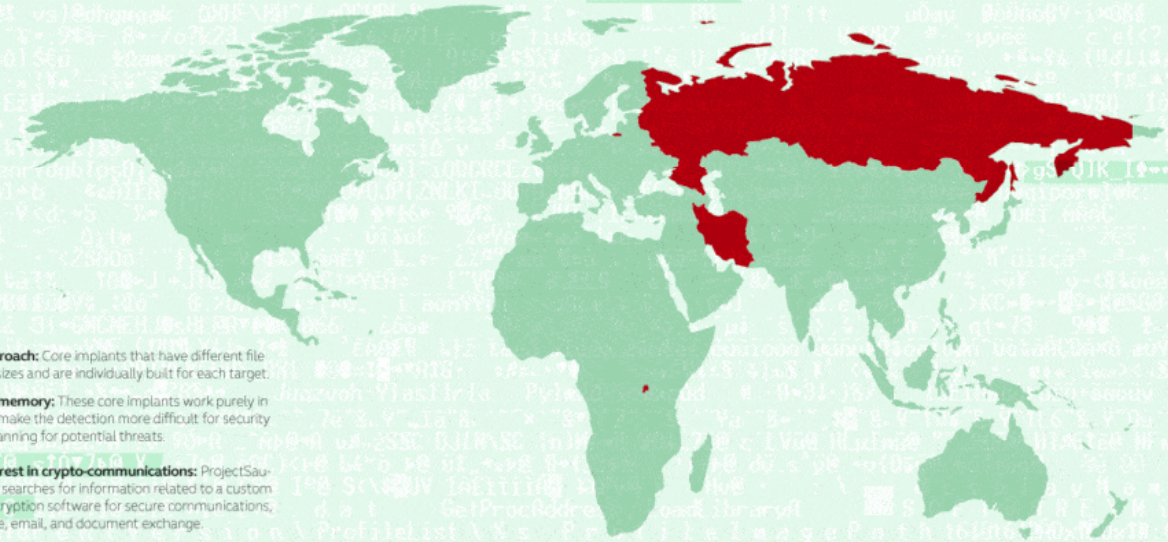
Powerful APT Malware that targeted **Critical National Infrastructure**: **Top Level** Government. Military, Telecoms, Finance and R&D Centres

Project Sauron: CyberEspionage - 2016

ProjectSauron advanced persistent threat

'ProjectSauron' is a unique 'pattern-less' threat actor responsible for highly-targeted, resource-intensive cyber-espionage attacks against government and research organizations as well as communication and financial companies. Victims have been found in the Russian Federation, Iran, and Rwanda but this is likely to represent the tip of the iceberg.

Government | Military organizations | Scientific research centers | Telecoms providers | Financial organizations



Key features:

- **Unique approach:** Core implants that have different file names and sizes and are individually built for each target.
- **Running in memory:** These core implants work purely in memory to make the detection more difficult for security solutions scanning for potential threats.
- **Special interest in crypto-communications:** ProjectSauron actively searches for information related to a custom network encryption software for secure communications, such as voice, email, and document exchange.
- **Bypassing air-gaps:** Remsec uses specially-prepared USB drives to jump across air-gaps, carrying hidden compartments in which stolen data is concealed.

Analysed by Symantec and Kaspersky Labs...

- August 2016 -

```
KBLOG_ROTATE_SECS = 1
tmp_dir = os.getenv("
drive = "C:\\"
SAURON_KBLOG_KEY = "m
create_log = function
  local f = ""
```

Other **"State-Designed"** Cyber Malware include:

Stuxnet, Duqu, Flame, Equation and Regin...

Powerful APT Malware that targeted **Critical National Infrastructure**: **Top Level** Government. Military, Telecoms, Finance and R&D Centres

CyberEspionage in Asia-Pacific Region

APT Victims were in **Malaysia, Philippines Indonesia, India, USA**

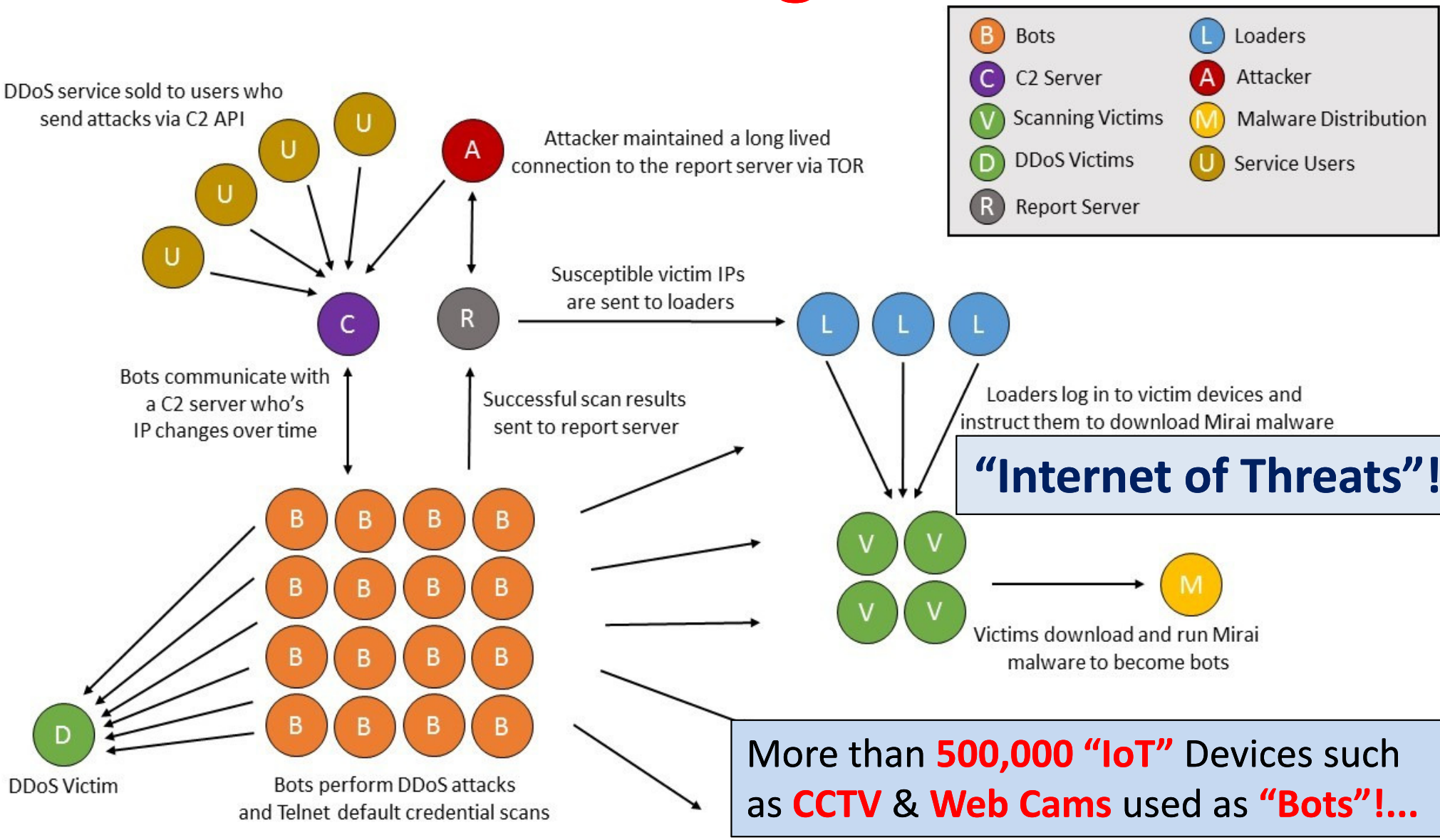
Attacks from **2012** onwards by **Hellsing** and **Naikon** Groups

Targets of **APT** Attacks were **Government** & **Diplomatic Agencies**

Analysed by **Kaspersky Labs**: **April 2015**

36th International East West Security Conference

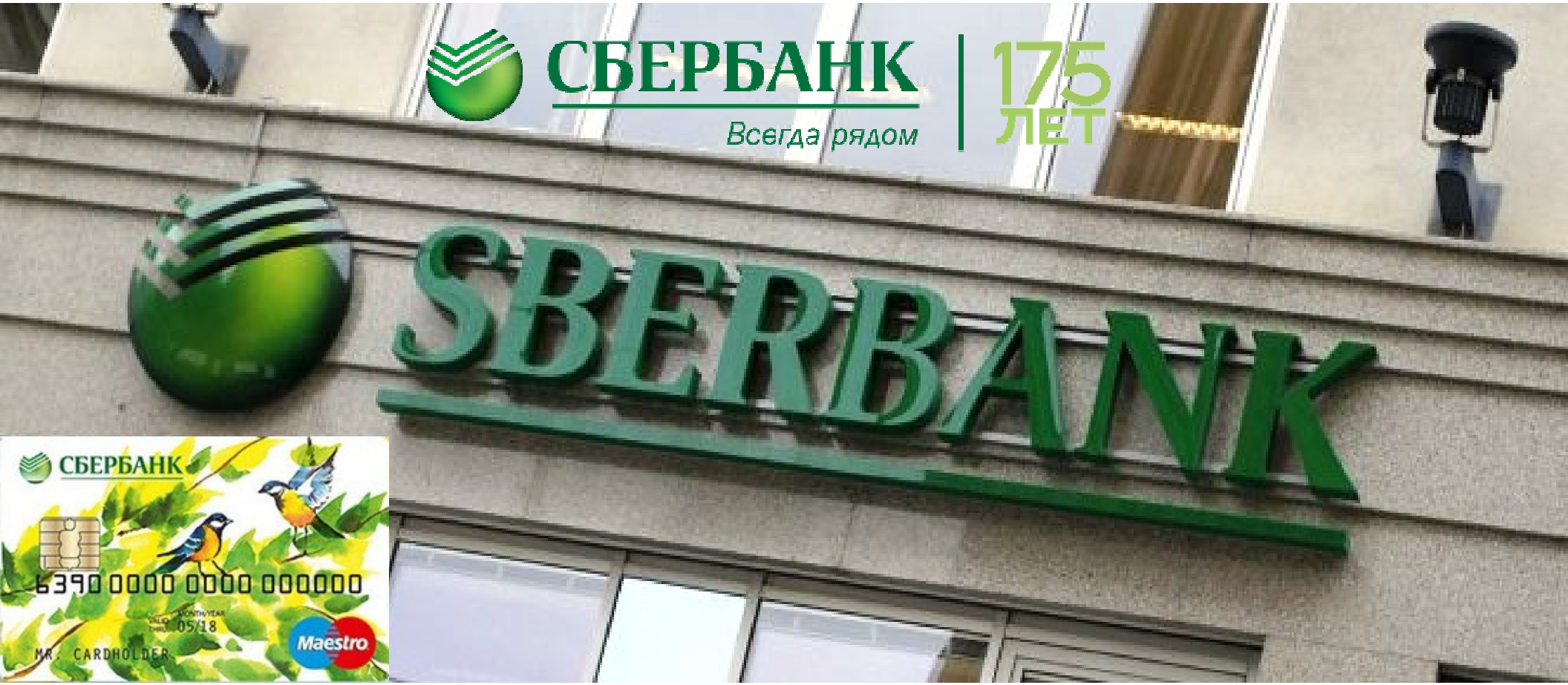
Massive DDoS Attack using Mirai BotNet from "Internet of Things" - 21st Oct 2016



CyberAttack: Tesco Bank – Nov 2016

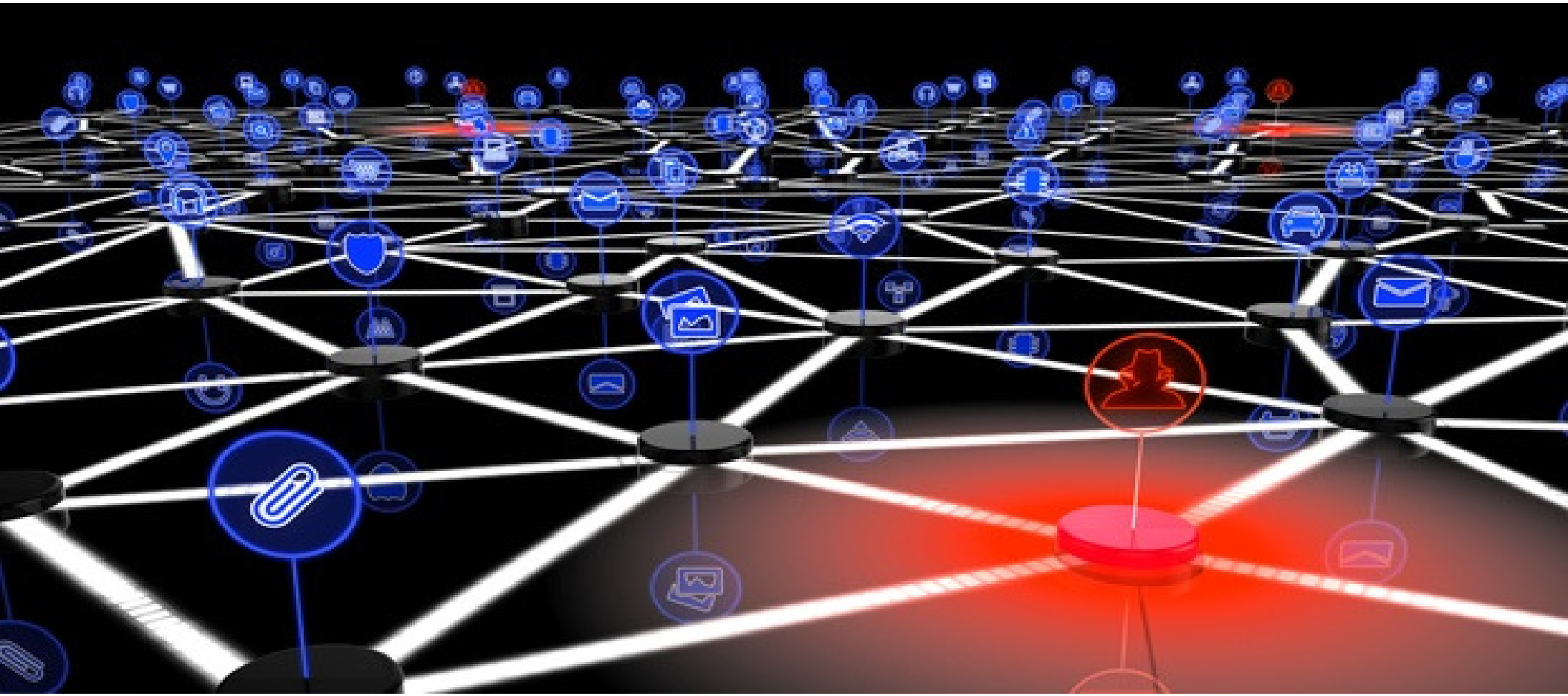
6th Nov 2016: Cyber Criminals from Brazil & Spain hack 40,000 TESCO Bank Accounts with reported Theft of £2.5m from 9,000

CyberAttack: SberBank - Сбербанк: 8th Nov 2016



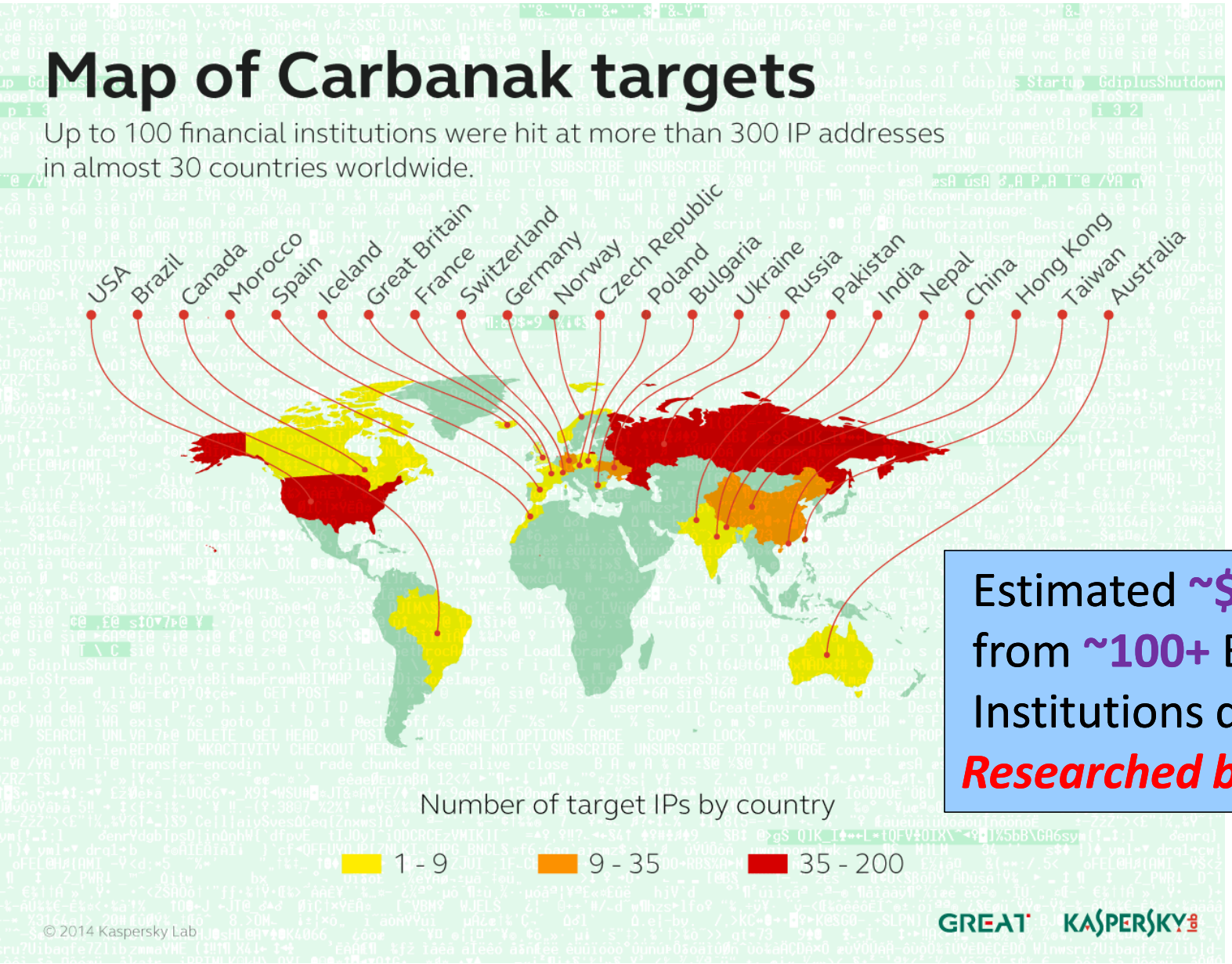
Massive DDoS Attack from **24,000 "Bot" Devices (Internet of Things)**
Hits **SberBank, Alfa Bank, Moscow Bank, RosBank, Moscow Exchange**
- Peak Web **IP Requests** of **660,000/Sec** quoted by **Kaspersky Labs -**

CyberAttack: SberBank - Сбербанк: 8th Nov 2016



Massive DDoS Attack from **24,000 "Bot" Devices (Internet of Things)**
Hits **SberBank, Alfa Bank, Moscow Bank, RosBank, Moscow Exchange**
- Peak Web **IP Requests** of **660,000/Sec** quoted by **Kaspersky Labs -**

Cyber Threat: "Banking Theft"– Carbanak



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

Researched by "Kaspersky Labs"

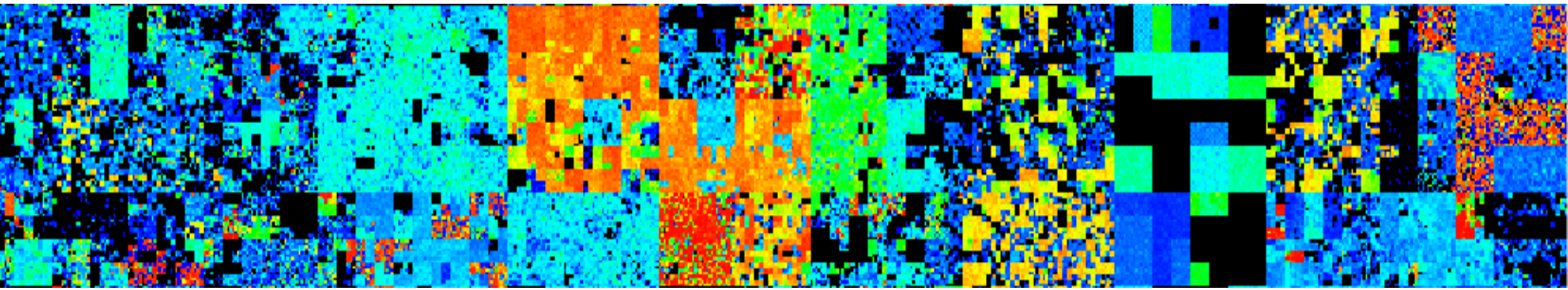
CyberSecurity: Market Sectors

- 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"***!

Cyber Threats & Defence: Intelligent Security

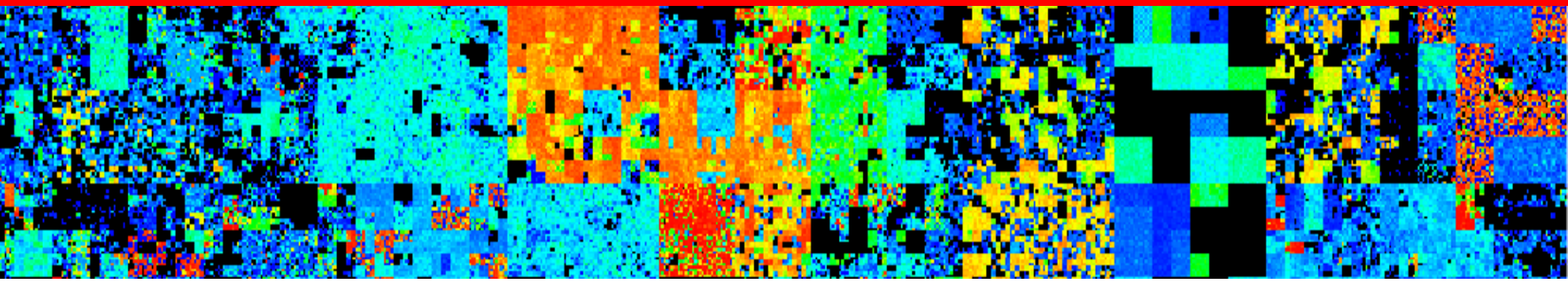
1 –"TOP 10 Cyber Threats & Attacks"	2– Cyber Case Studies: Recent Attacks	**3 – Cyber Hack & Attack Campaigns!**
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert and Attack! **"Cyber Attack"**
7 –In-Depth: Security for Critical Sectors	8 – ***YOUR*** Operational Cyber Defence!	9 –***YOUR*** Cyber Campaign Action Plan!



Cyber Threats & Defence: Intelligent Security

3 – Cyber Hack & Attack Campaigns!

Professional "Bad Guys"!...



"21stC Cyber Hack & Attack Campaigns"

- **CyberCrime & Terrorism** are now organised on an "Industrial Scale" with Toolkits & BotNets for "Hire by the Hour" on the "DarkWeb"...
- **Major Cyber Attacks** demand the Professional Skills of a well managed Criminal Enterprise...
- **The Cyber Enterprise** may be a small CyberCell of 3 or 4 "Staff" and scale up to teams of hundreds in some Cyber Banking "Heists"...

.....Next we explore some Cyber Criminal Skills...

Main *Cyber* Players and their Motives

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

"Cyber" Tracking & Profiling: *"Bad Guys"*

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

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

"Cyber" Tracking & Profiling: *"Bad Guys"*

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

  - 3D Video Analytics from CCTV Facial Profiles
  - Track On-Line Social Media, eMail & "Cell" Comms
  - Scan "DarkNet" for "Business Deals", Plans & Messages
  - Check, Track & Locate Mobile Communications
  - Track "Bad Guys" in National Transport Hubs
  - Deploy RFID Devices to Track High-Value & Strategic "Assets"
  - Use Real-Time ANPR for Target Vehicle Tracking

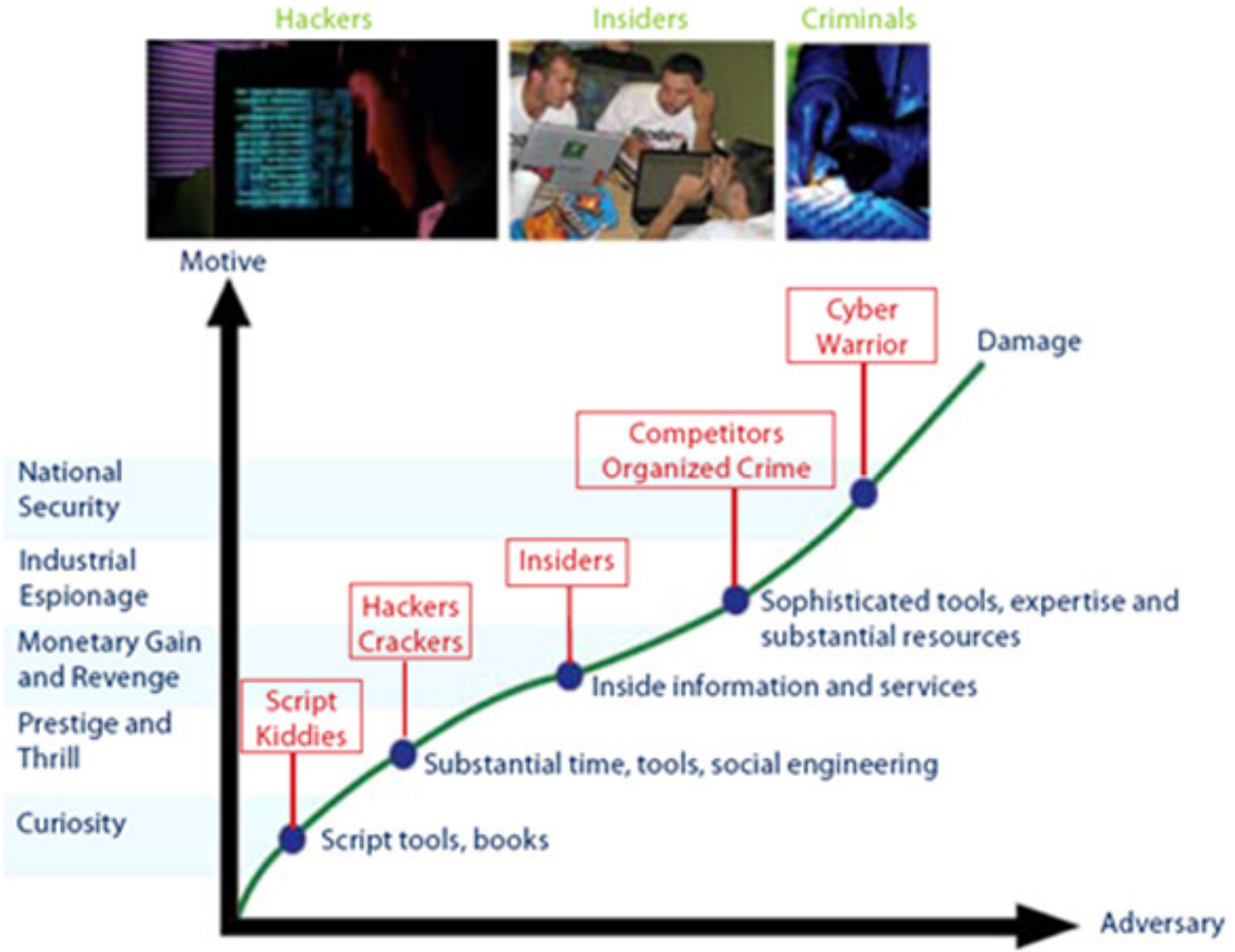
...***Cyber Computing Smart Apps*** can now Track Massive Databases of Target "Bad Guy" Profiles ***@ Light Speed!...***

Cyber Criminal Team Skillset!...

- Skills required by the **"Bad Guys"** to launch and manage major Cyber Crime Campaigns:
  - **ICT:** Cyber Technical Specialist (Hacking Tools)
  - **Finance:** Money Laundering & Campaign Budget
  - **HR-Human Resources:** Headhunting Cyber Talent!
  - **Intelligence:** Recruit "Insiders" in Business/Govt
  - **Project Management:** Co-ordinate Campaign!
  - **Security:** Detect "BackDoors" both in the Physical and Cyber Defences of the Target Business/Govt

...In summary, the **"Bad Guys"** will often organise themselves as an *Criminal Cell or Illegal Business*!

Hierarchy of **Cyber Hacking Skills!**



"Dark Web" *Criminal Cyber Economy*

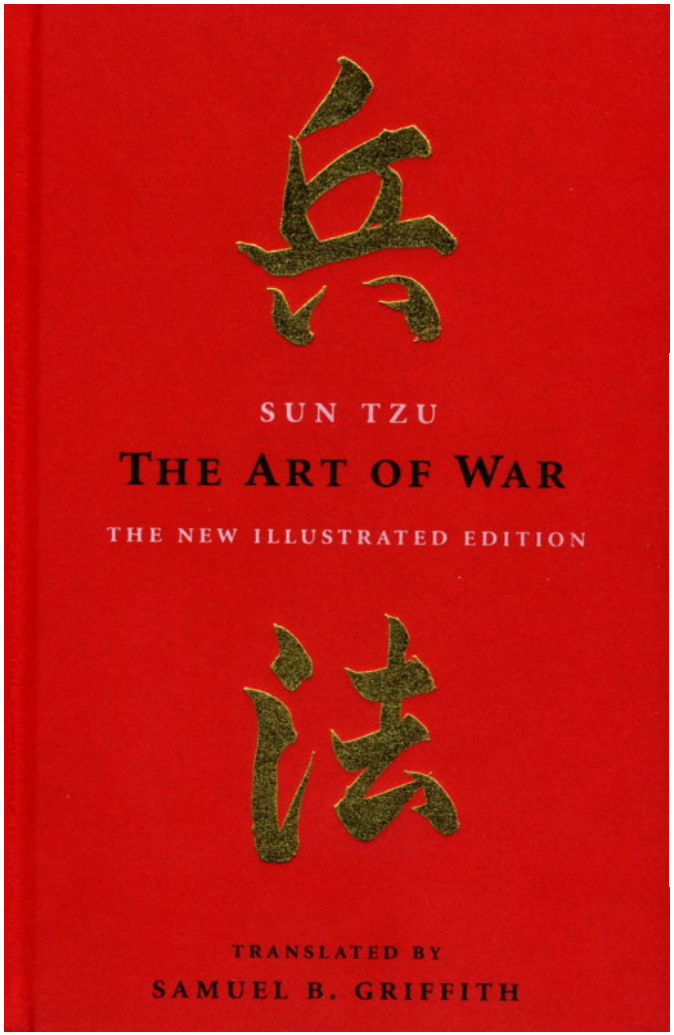
-*"Bad Guys"* Rent/Buy *Tools & Resources!* -

Figure 1. Underground Cyber Economy			
Rank	Item	Percentage	Price Range
1	Credit Cards	22%	$0.50–$5
2	Bank Accounts	21%	$30–$400
3	E-mail Passwords	8%	$1–$390
4	Mailers	8%	$8–$10
5	E-mail Addresses	6%	$2 per megabyte–$4 per megabyte
6	Proxies	6%	$0.50–$3
7	Full Identity	6%	$10–$150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5–$7
10	Compromised Unix Shells	2%	$2–$10

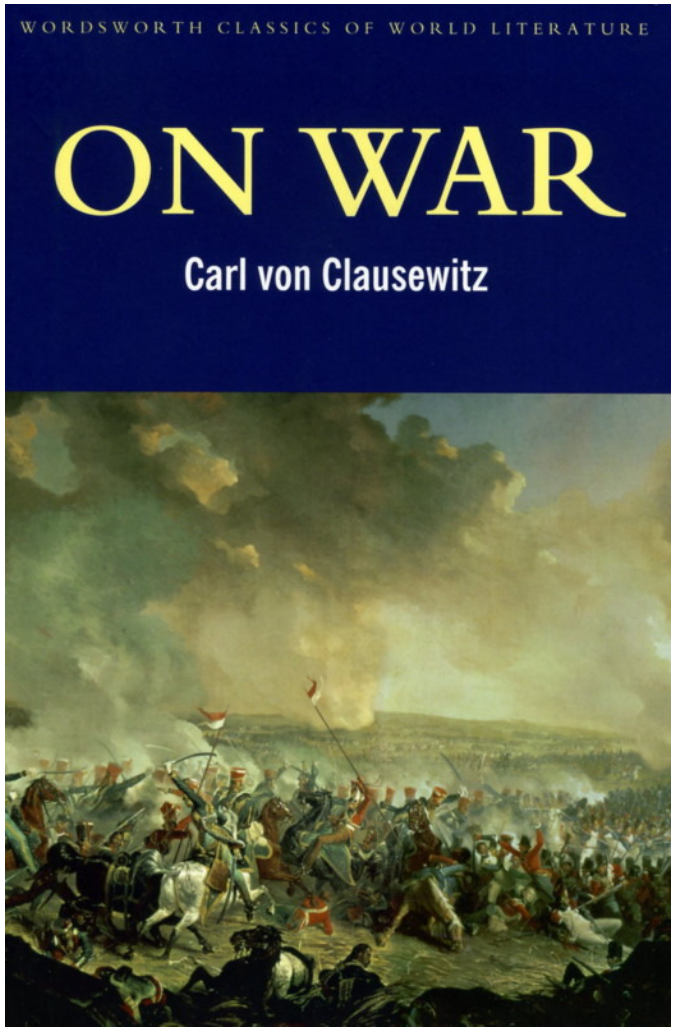
– Symantec Corp. - September 2007

...Already Criminalised & Commercialised more than 10 Years ago!

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



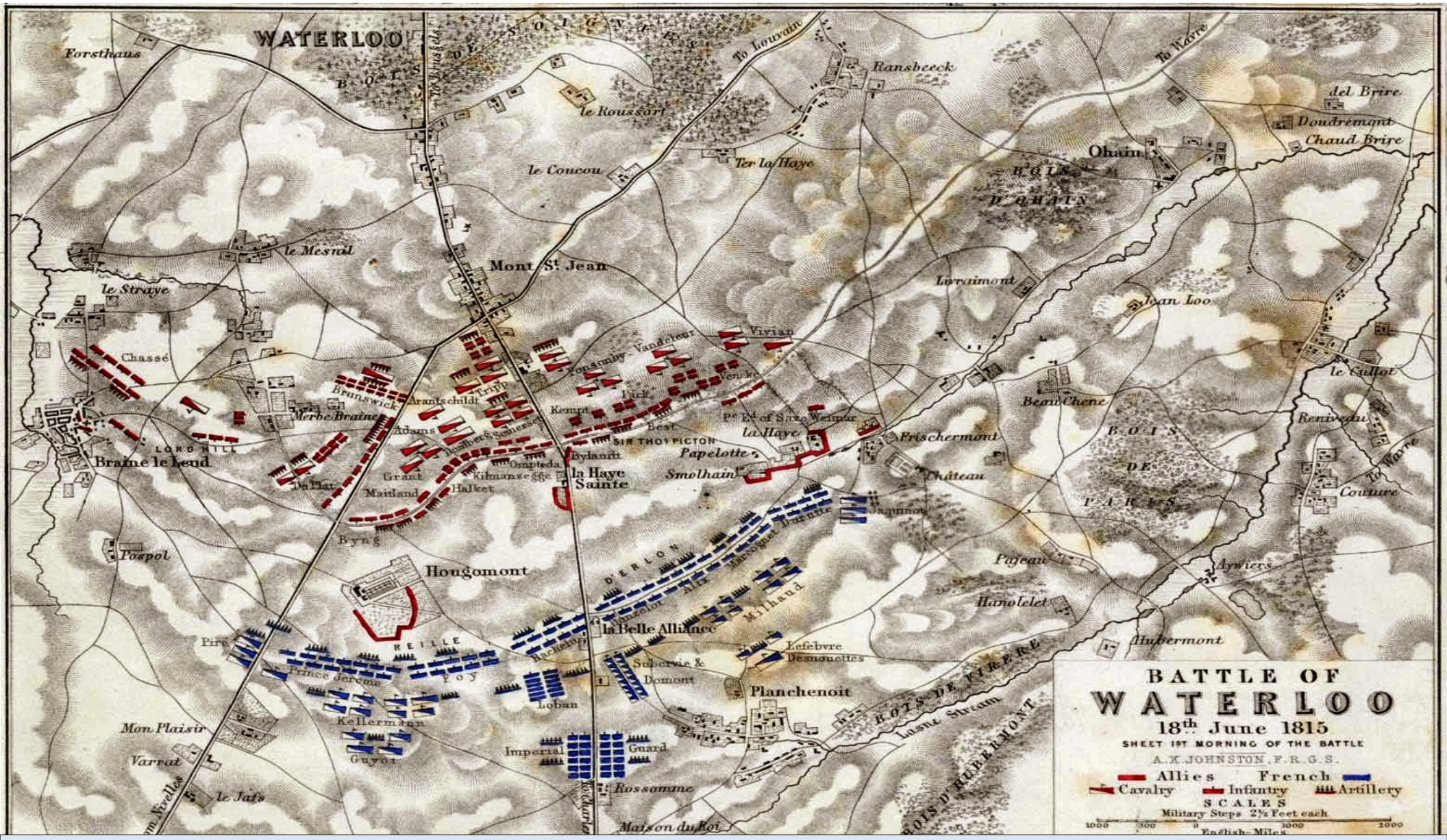
Recommended "Bedtime Reading" *for* Cybersecurity Specialists!



Classic Works on "War" are still relevant today for 21stC Cybersecurity!

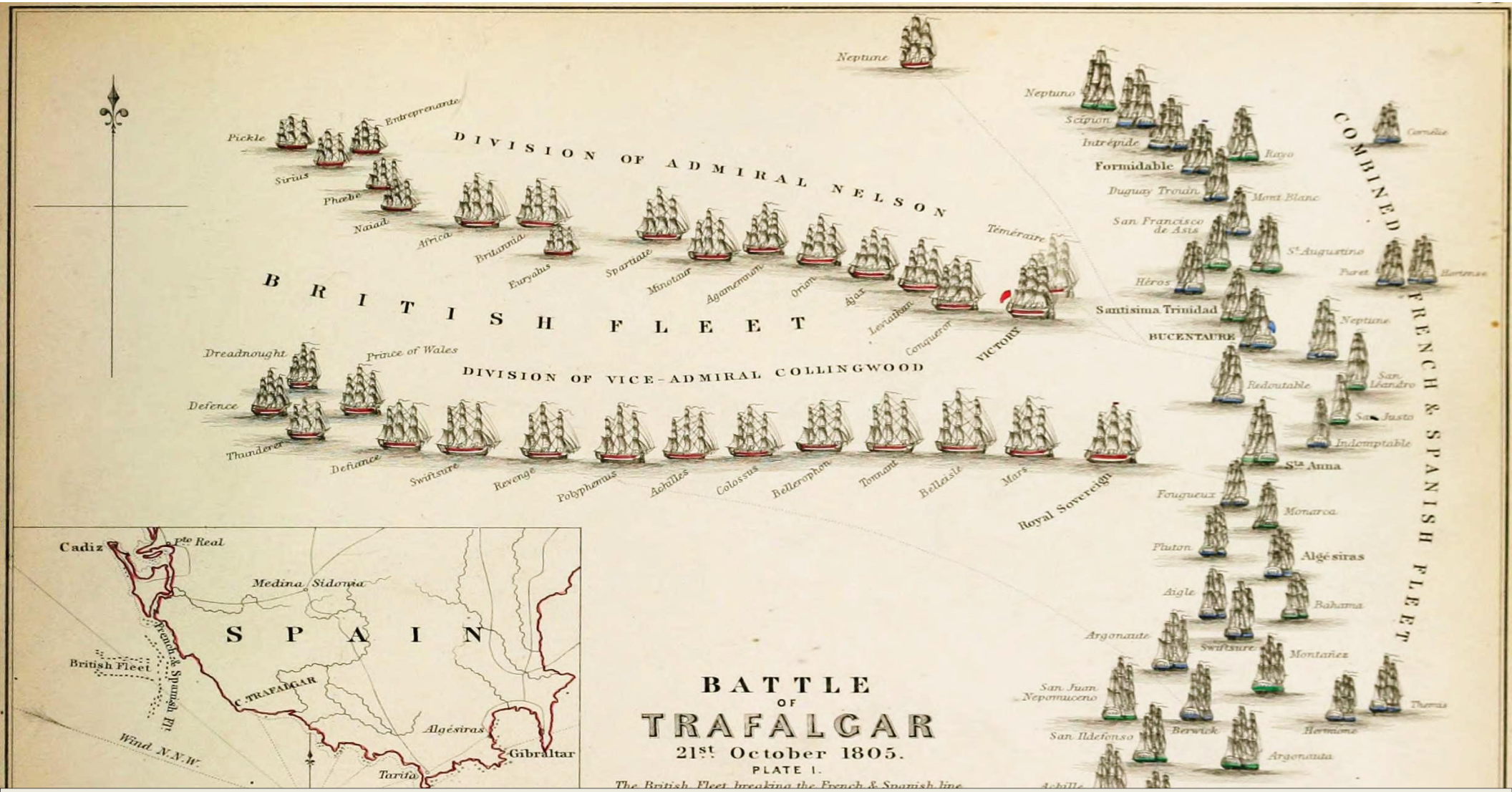
Cyber Criminals now plan Cyber Campaigns & Attacks with In-Depth Research & 21st Weapons!

Classic Campaigns: Battle of Waterloo-1815



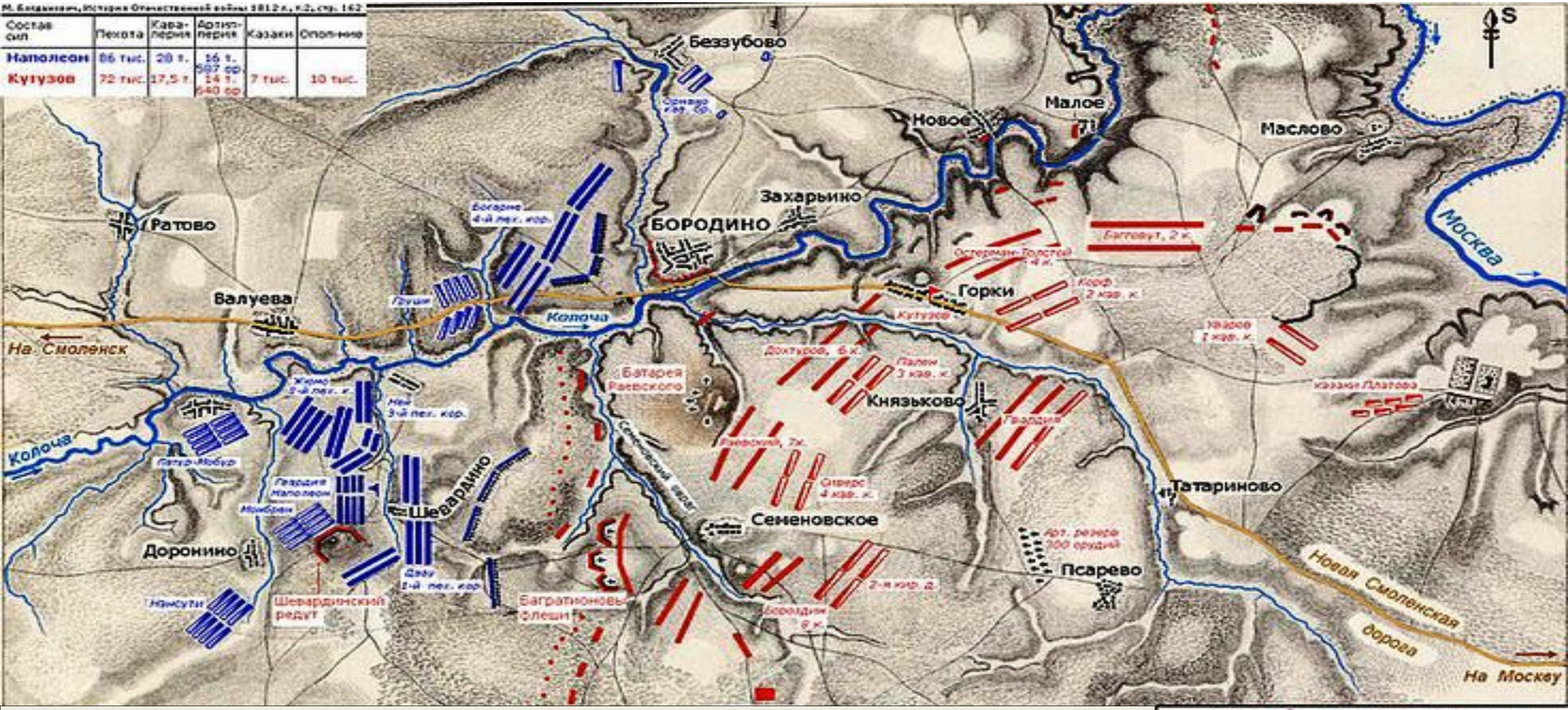
"Clausewitz" 19thC *Physical Strategies* remain relevant for 21stC *Cyber Campaigns !*

"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"!

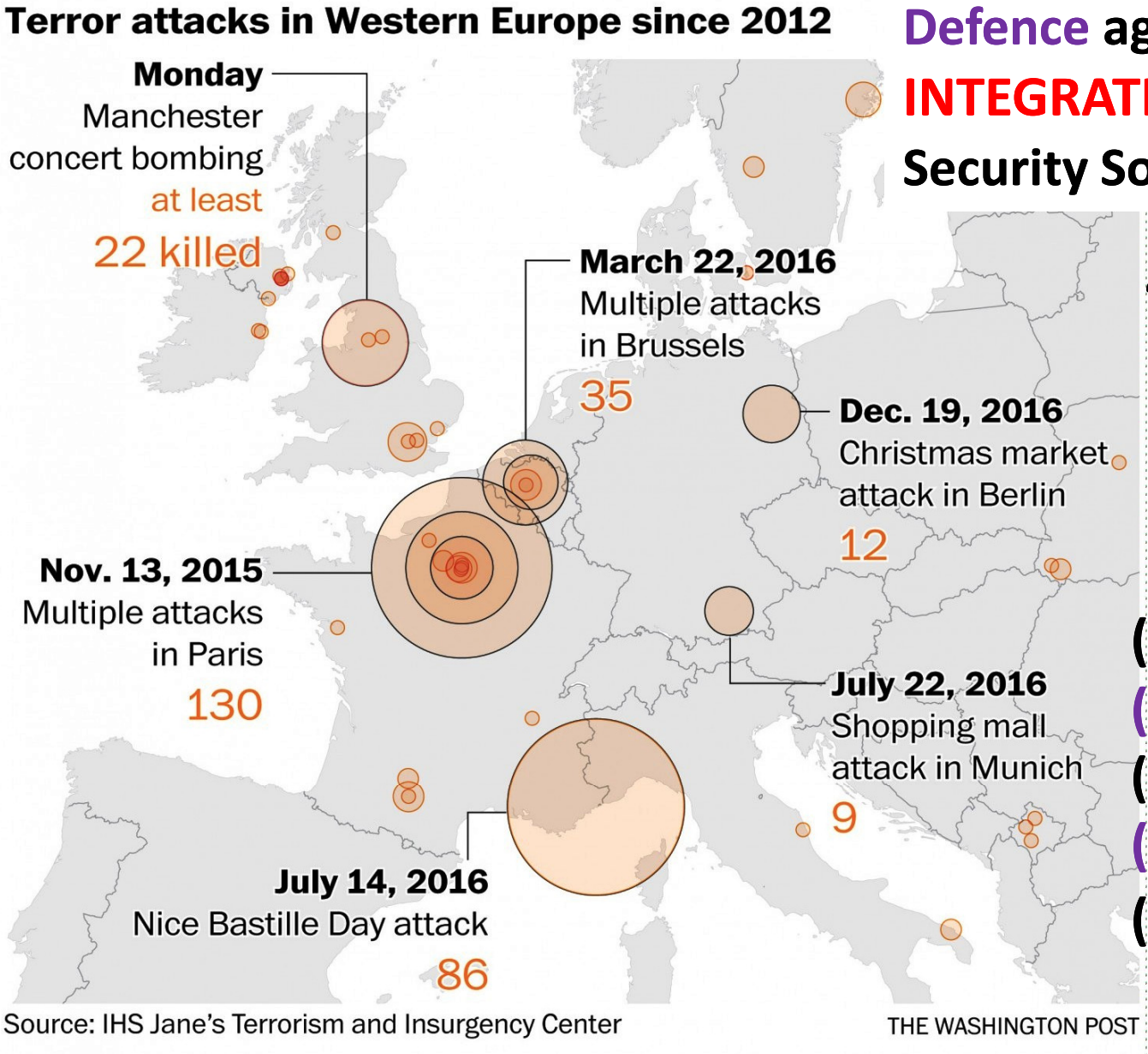
Classical Warfare: Battle of Borodino-1812



21stC Cyber War & Peace!

"Classic Works" are relevant to Cyber War Campaigns!

21stC Warfare: "Urban Terrorism"



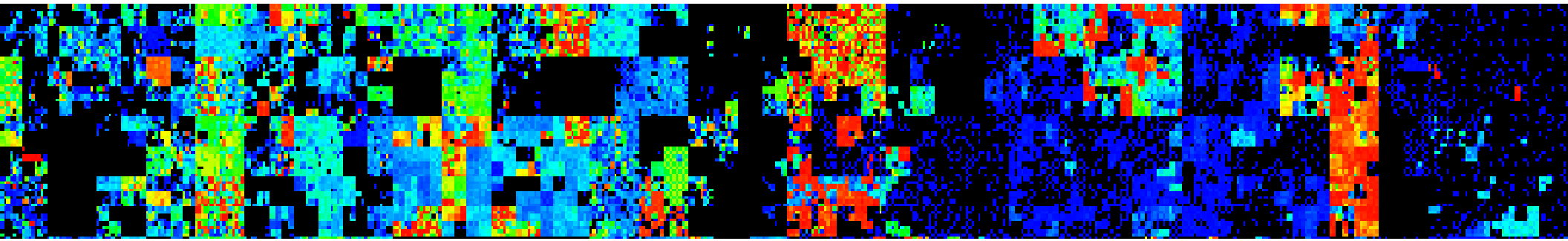
Defence against "Urban Terror" needs INTEGRATION of PHYSICAL & CYBER Security Solutions = SMART SECURITY

"Bad Guys" use **Cyber Tools** & Resources to extensively **Research** & **Launch** Major **Physical Terror Attacks!**

(1) DarkWeb for **Weapons!**
(2) Research Urban Targets
(3) Social Media for Comms
(4) Recruitment & Training
(5) Ransomware for CA$H..

Cyber Threats & Defence: Intelligent Security

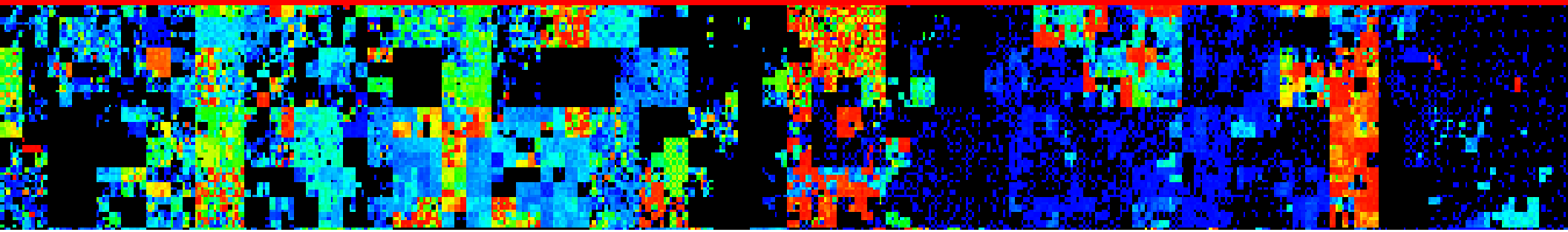
1 – "TOP 10 Cyber Threats & Attacks"	2 –Cyber Case Studies: Recent Attacks	3 – Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert and Attack! **"Cyber Attack"**
7 –In-Depth: Security for Critical Sectors	8 – ***YOUR*** Operational Cyber Defence!	9 – ***YOUR*** Cyber Campaign Action Plan!



Cyber Threats & Defence: Intelligent Security

4 – Cyber Intelligence Gathering Tools

"Exploration"



"Cyber Intelligence Gathering Tools

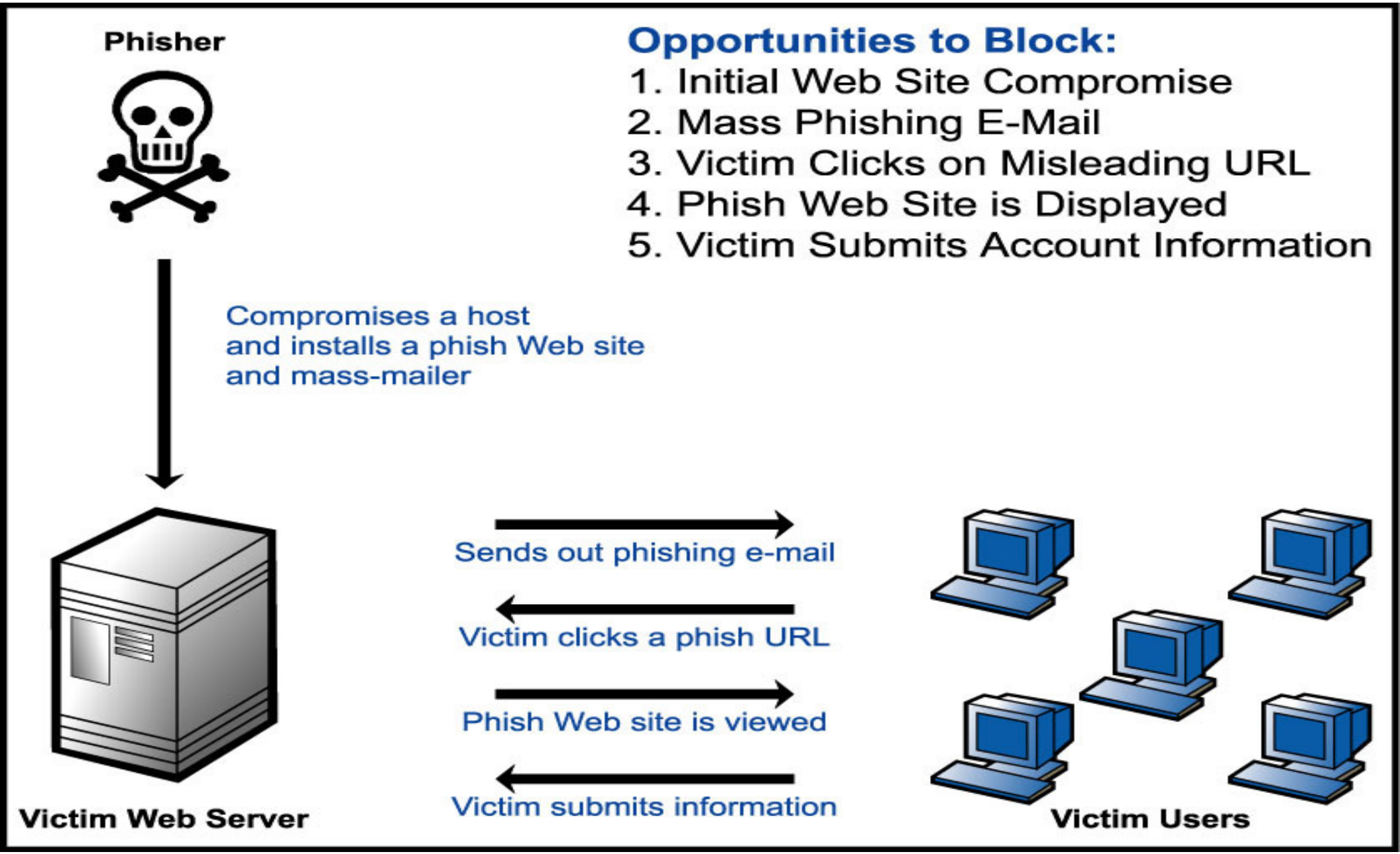
*** EXPLORATION ***

- 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!....

Phishing Attack: Typical "Cyber Hacking" Process



Cyber Threats: "Fake" Profiles & Toxic eMail

SAFETY ON INTERNET CHAT

- Use nicknames as ID instead of real names, e.g. TopRookie instead of Abdul Hamid
- Never provide personal information that is sensitive
- Do not meet a stranger that you met on Internet chat
- Only open or download files from people you know
- When using a public computer, key in your ID and password manually

Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

An agency under MOSTI

CyberSecurity Malaysia
Level 7, Sapura @ Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan
Tel: +6 03 89926888 Fax: +6 03 89453205 | www.cybersecurity.my |

SPAM EMAILS

SPAM is an unwanted email that you receive from someone that you don't know on the Internet.
(virus, getrich, chain, phishing, spyware, bots)

WHAT YOU SHOULD DO?

- Delete spam emails without opening them
- Do not reply or forward spam emails
- Do not give personal information on emails
- Do not open unknown email attachments
- Do not click any web links from SPAM emails
- Do not forward any chain letters
- Use anti-spam filters

Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

An agency under MOSTI

CyberSecurity Malaysia
Level 7, Sapura @ Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan
Tel: +6 03 89926888 Fax: +6 03 89453205 | www.cybersecurity.my |

Cyber Threats: Spyware & Password Hacks

BEWARE OF SPYWARE

SPYWARE refers to software that performs certain tasks on your computer without your consent. This may include giving you advertisements or collecting personal information about you.

(Pop-ups, slow system, system crashes, changes in your system, new toolbar on your browser, unwanted software)

HOW TO PREVENT FROM SPYWARE?

- Use a firewall
- Adjust your security setting on your browser for the Internet zone to "Medium"
- Install and update your anti-spyware software
- Download software from website that you trust only

Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

An agency under MOSTI

CyberSecurity Malaysia
Level 7, Sapura @ Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan
Tel: +6 03 89926888 Fax: +6 03 89453205 | www.cybersecurity.my |

PROTECT YOUR PASSWORD

- Never reveal your password to anyone
- Never provide your password over phone or email
- Change your password regularly
- Create difficult to guess password
- Mix uppercase and lowercase letters, symbols and numbers (e.g. aLc9?xtop)
- It should be more than 8 characters long

Let's Make The Internet A Safer Place
www.esecurity.org.my

CyberSecurity MALAYSIA

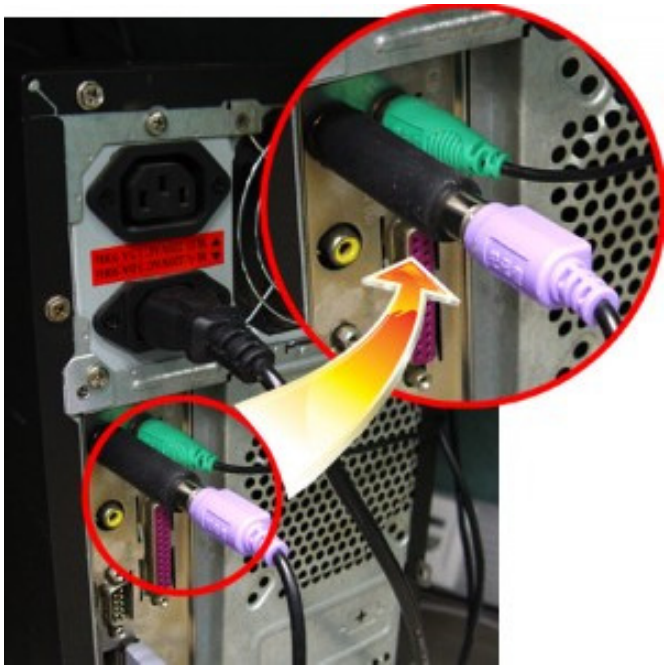
An agency under MOSTI

CyberSecurity Malaysia
Level 7, Sapura @ Mines, No 7, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan
Tel: +6 03 89926888 Fax: +6 03 89453205 | www.cybersecurity.my |

Cyber Threats: Keyloggers - Hardware & Software

- Easily inserted by CyberCriminal “Insiders”!

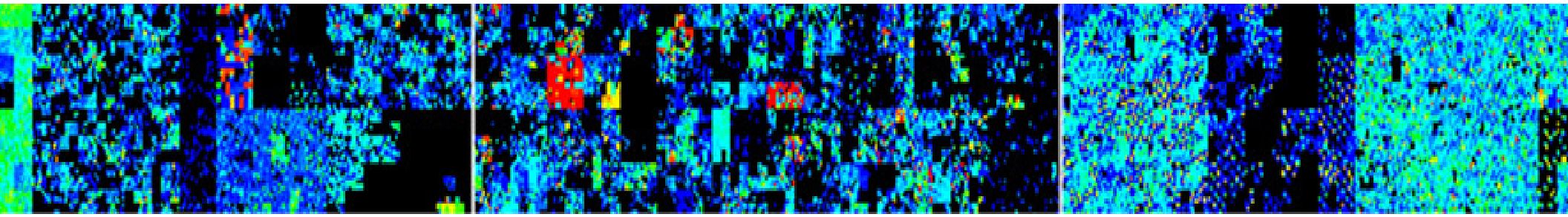
- Wi-Fi Scanners & Loggers also Easily Acquired
- Alternative Software Keyloggers can be illegally downloaded into compromised servers & PCs



- Logged files can be uploaded to CyberCriminals through eMail or by FTP through Open Ports
- Examples have also been found inside credit card terminals, pre-installed by criminals in production plants with SIM Cards and Phone.

Cyber Threats & Defence: Intelligent Security

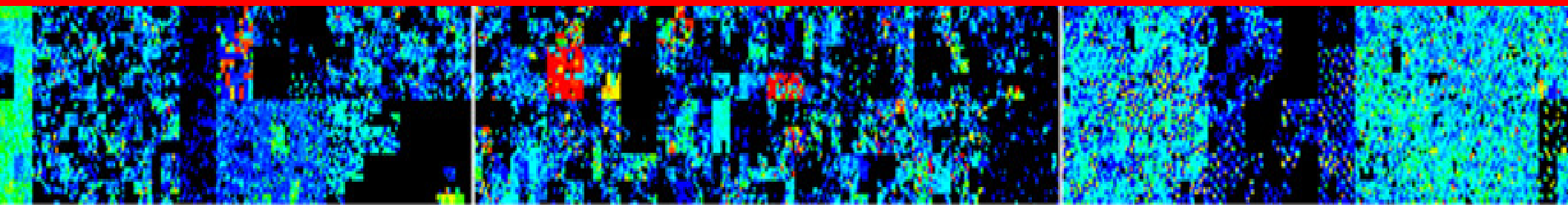
1 -"TOP 10 Cyber Threats & Attacks"	2 –Cyber Case Studies: Recent Attacks	3 – Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 –Cyber Entry & Exit Routes &Tools **"Penetration"**	6 – Real-Time Cyber Alert and Attack! **"Cyber Attack"**
7 - In-Depth: Security for Critical Sectors	8 – *YOUR* Operational Cyber Defence!	9 – *YOUR* Cyber Campaign Action Plan!



Cyber Threats & Defence: Intelligent Security

5 – Cyber Entry & Exit Routes &Tools

"Penetration"



"Cyber Entry & Exit Routes & Tools"

*** PENETRATION ***

- The "Bad Guys" will **Penetrate** the "Target" Business 0or 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!

Typical C2 *Malware* Signatures

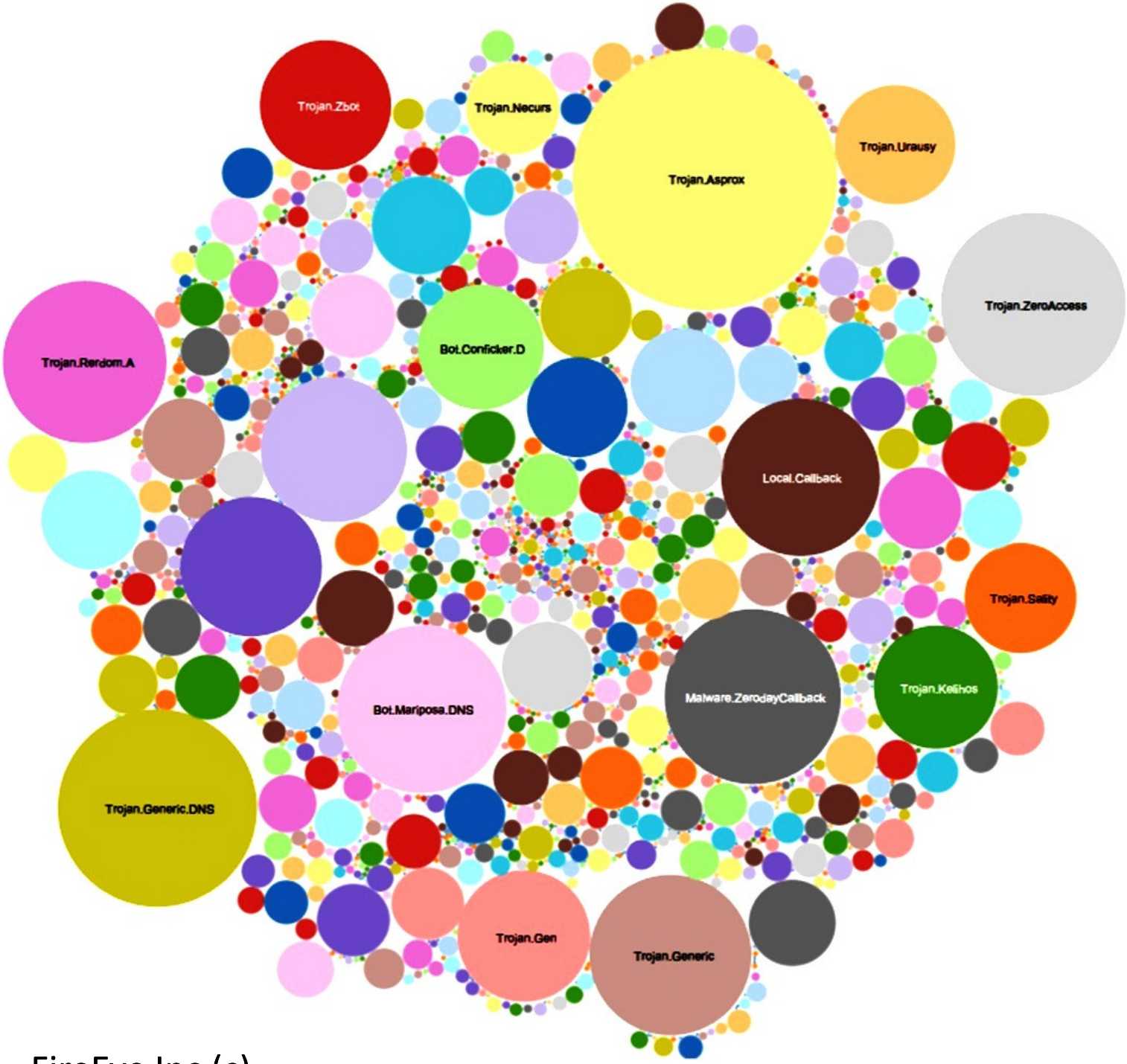
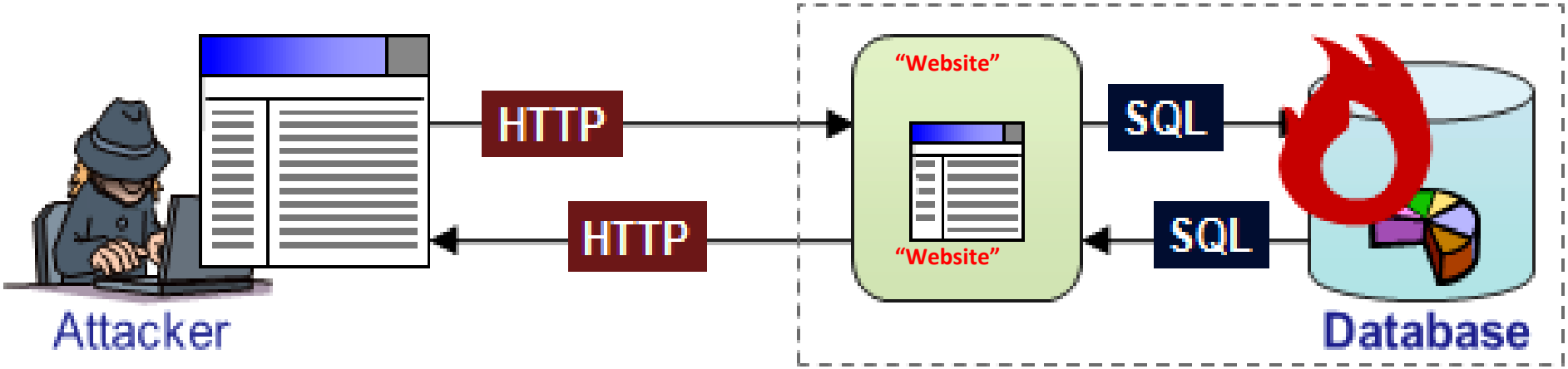


Image: www.fireeye.com – FireEye Inc (c)

"Cyber Threat": SQL Injection Vulnerability

Problem	"Website" has an SQL injection vulnerability that could allow a remote attacker to gain administrator privilege.

1. A remote attacker sends a specially crafted HTTP request that turns into an SQL statement to be executed on the database.



2. The SQL statement, as the result of its execution, allows the attacker to escalate his privilege to administrator privilege.

Solution: Ensure all SQL Inputs are **"Non-EXECUTABLE"** Parameterised Statements!...

Cyber Threats: "Twitter" Cross-Site Scripting Vulnerability

Twitter fixes cross-site scripting vulnerability that was used to distribute compromised links

Dan Raywood September 07, 2010

PRINT EMAIL REPRINT FONT SIZE: A | A | A BOOKMARK

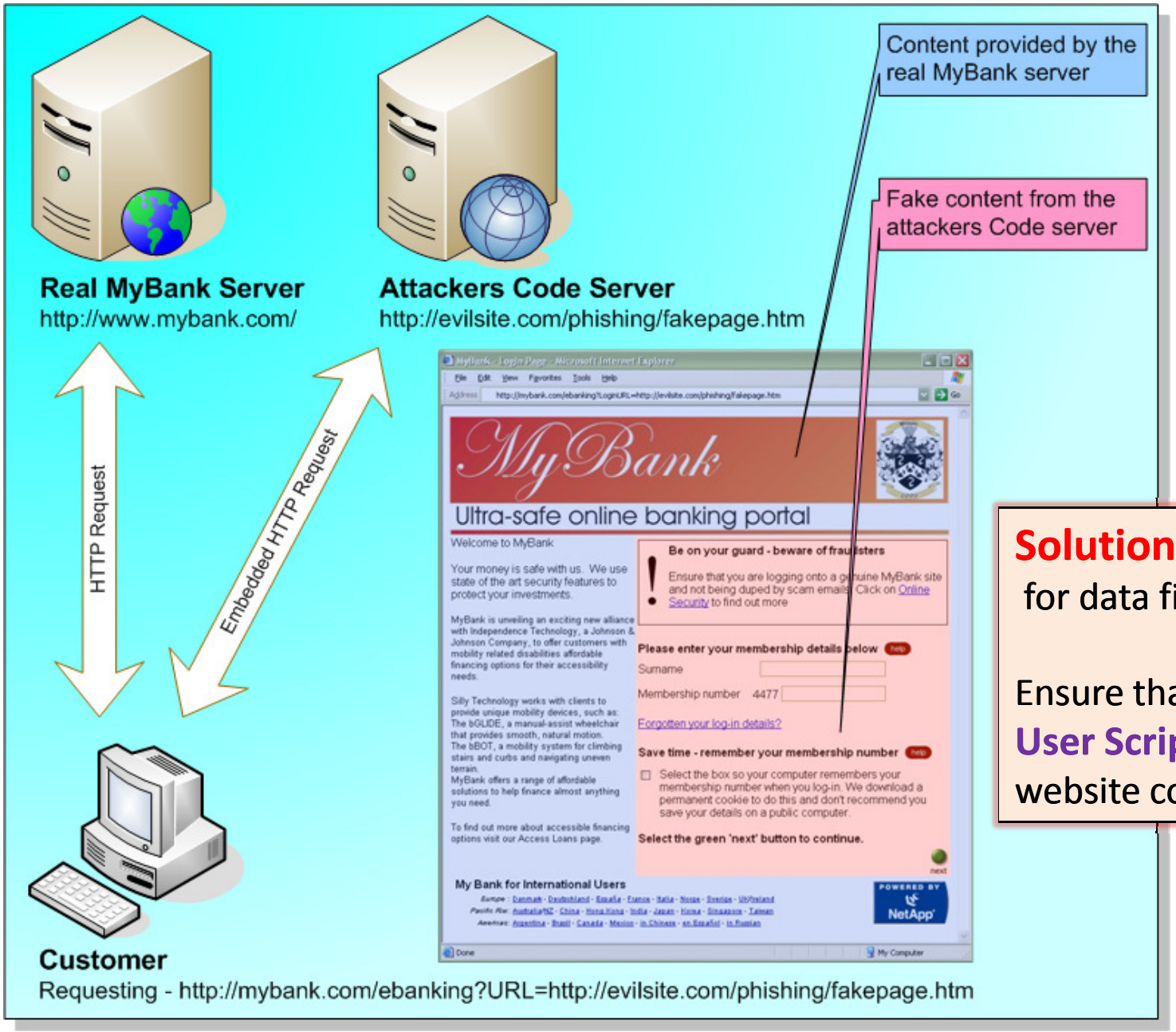
Twitter has fixed a cross-site scripting (XSS) vulnerability that stole a user's cookie to distribute compromised links.

It was detected by Stefan Tanase, senior security researcher at Kaspersky Lab. He said that the exploit steals the cookie of the Twitter user, which is transferred to two specific servers and essentially, any account that clicked on the malicious links is compromised.

He said that the bit.ly statistics for one of the malicious links show that more than 100,000 users clicked on the link.

SC MAGAZINE
SECURE BUSINESS INTELLIGENCE

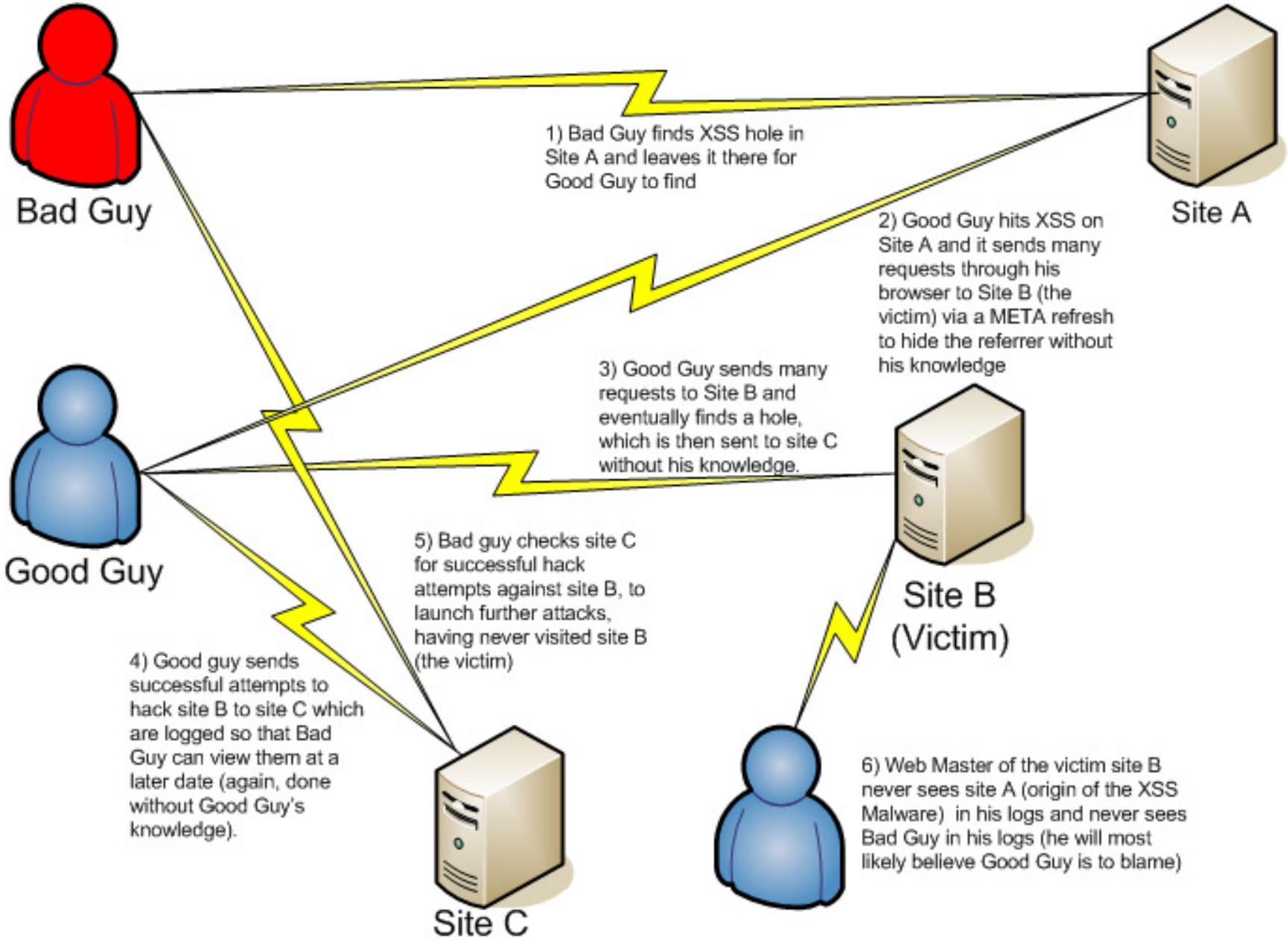
Impact of XSS Cross-Site Scripting "Cyber Threat"



Solution: Always check rigorously for data fields that allow user-input.

Ensure that there is no possibility for **User Script** input to be executed in website coded **"php"** or **"asp"** pages

Cross-Site Scripting Threat by Proxy : XSS



Designer "StuxNet" Worm - Industrial "SCADA" Systems

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

Stuxnet Worm : 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

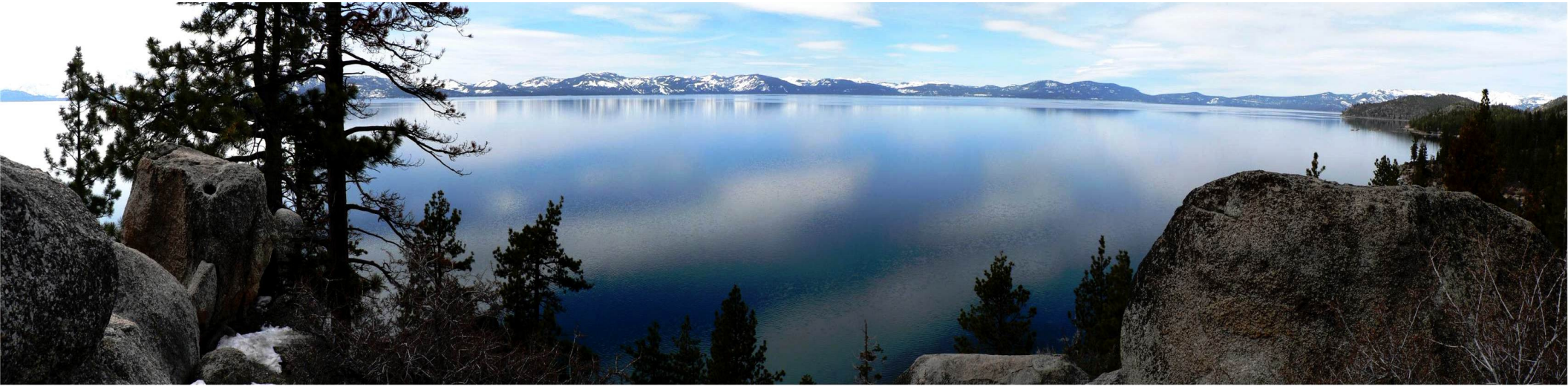
WORM_STUXNET.A targets SCADA WinCC systems, which are used to manage industrial operations such as power plants and energy refineries.

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.

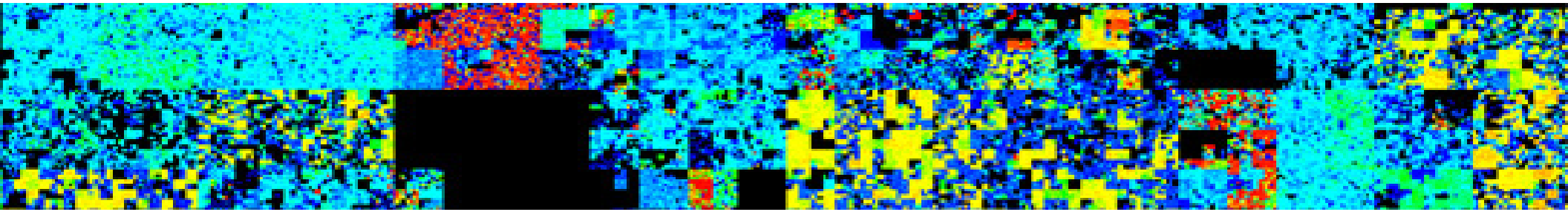
SCADA = Supervisory Control & Data Acquisition
- Mainly for Power Stations & Industrial Plants

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

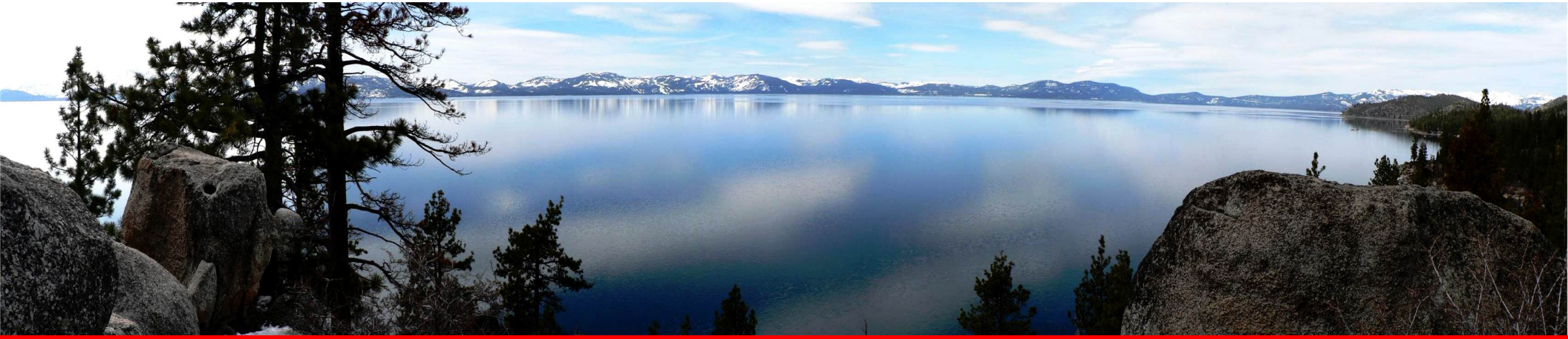
Cyber Threats & Defence: Intelligent Security



1 – "TOP 10 Cyber Threats & Attacks"	2 –Cyber Case Studies: Recent Attacks	3 – Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert and Attack! **"Cyber Attack"**
7 –In-Depth: Security for Critical Sectors	8 – ***YOUR*** Operational Cyber Defence!	9 – ***YOUR*** Cyber Campaign Action Plan!

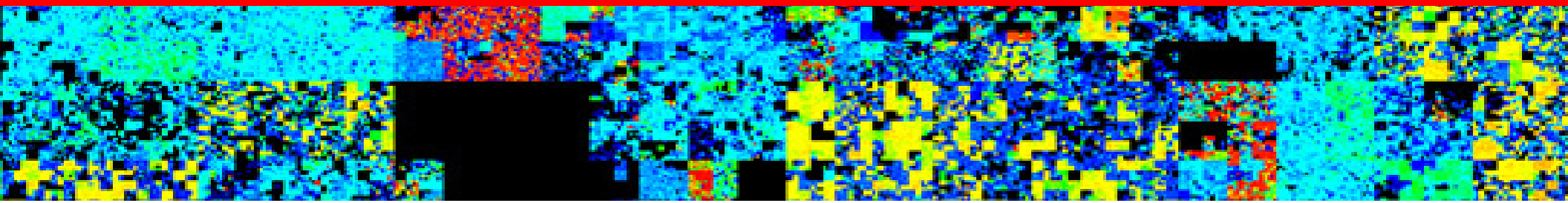


Cyber Threats & Defence: Intelligent Security



6 – Real-Time Cyber Alert and Attack!

"Cyber Attack"

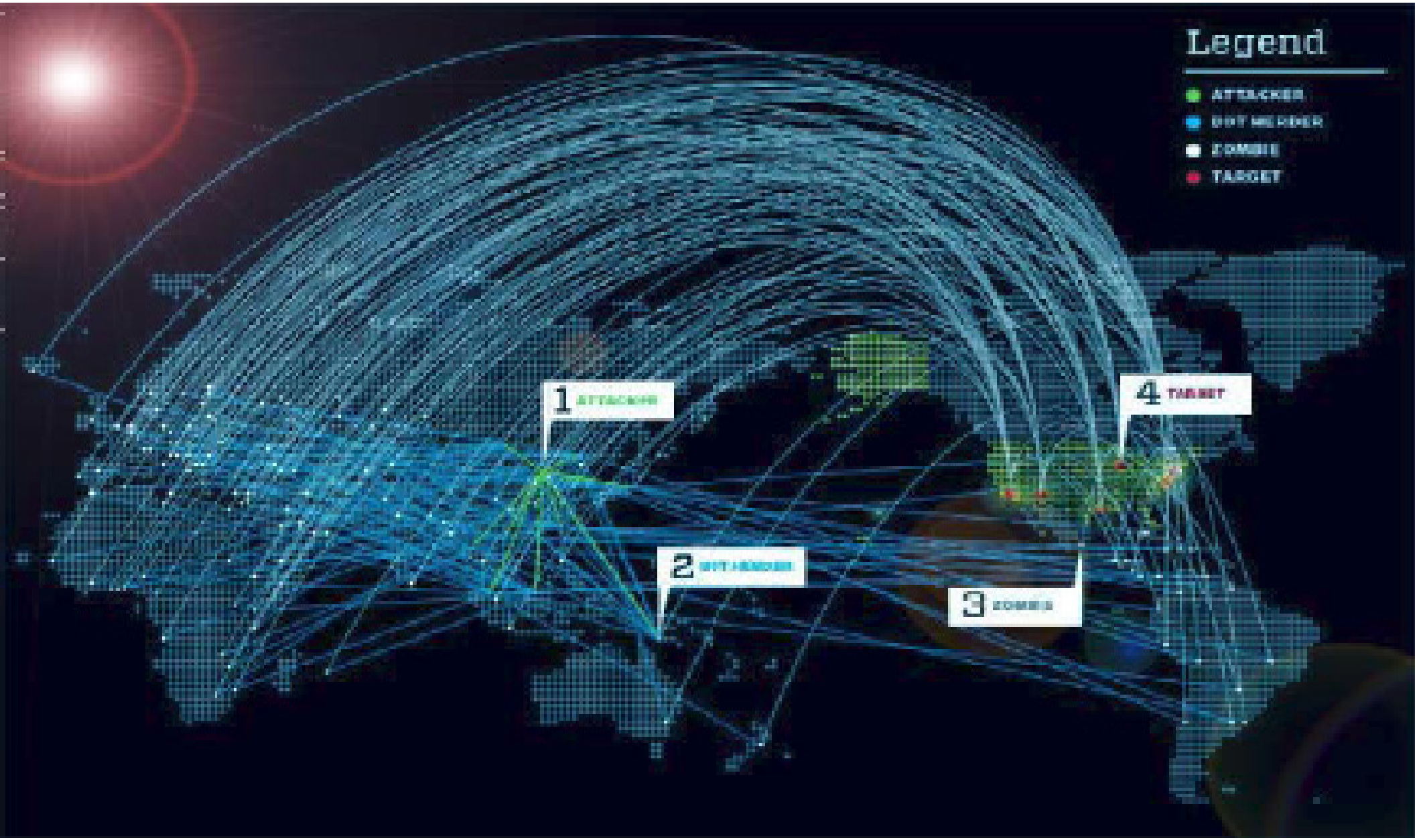


"Real-Time Cyber Alert: *Hack & Attack*"

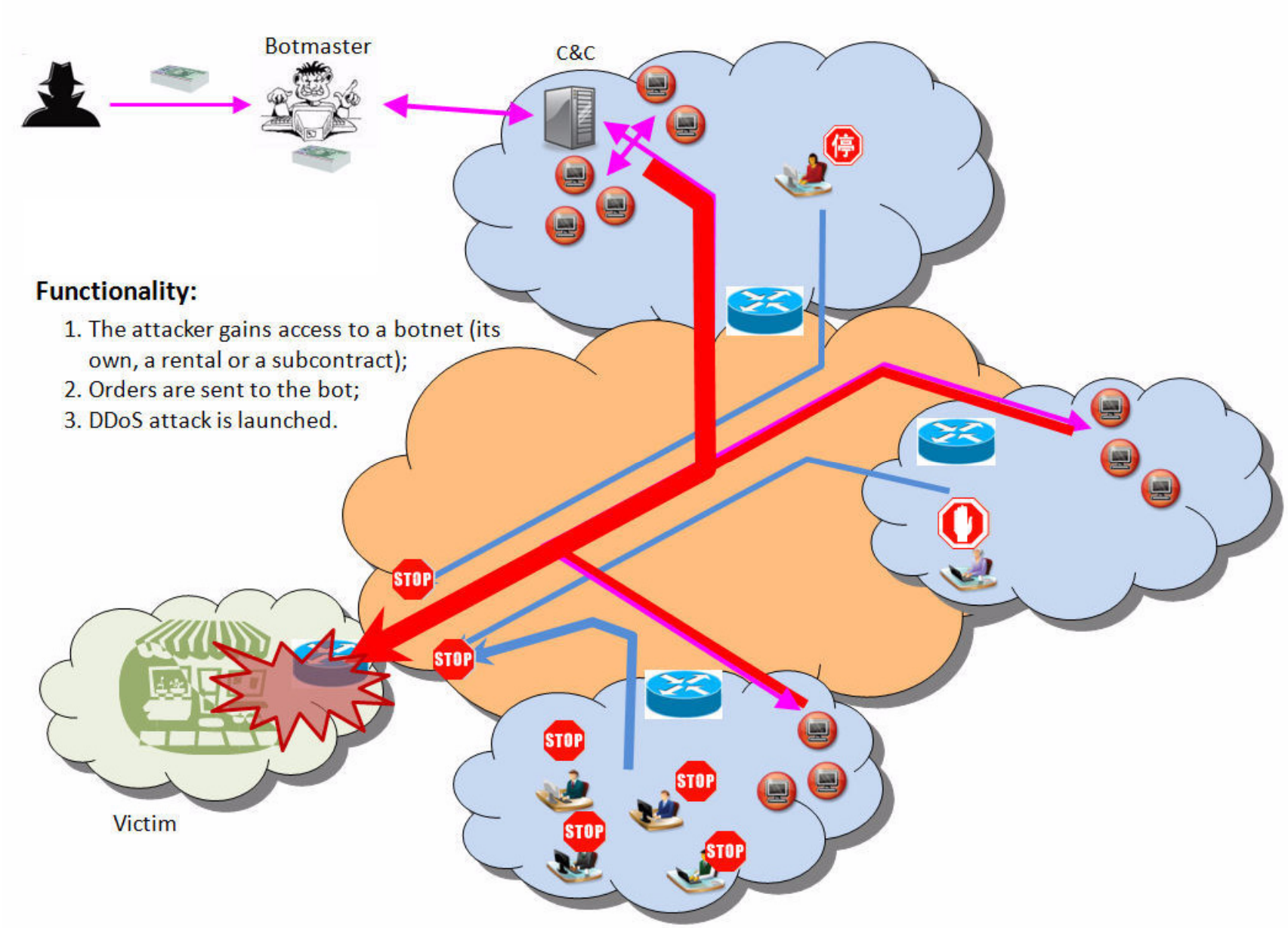
*** CYBER ATTACK ***

- 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"!

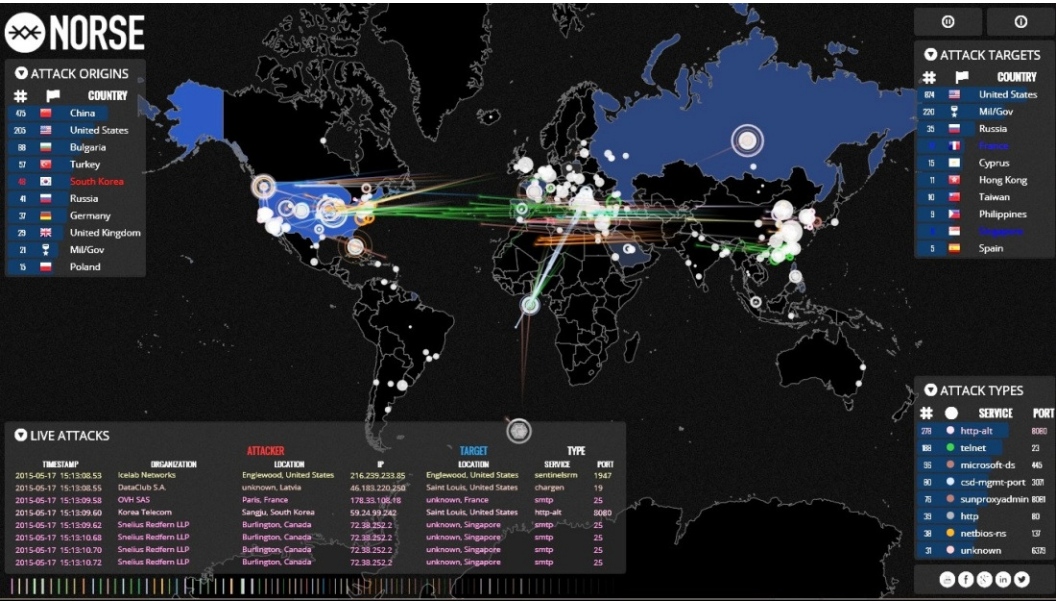
Typical Global "Botnet" CyberAttack!

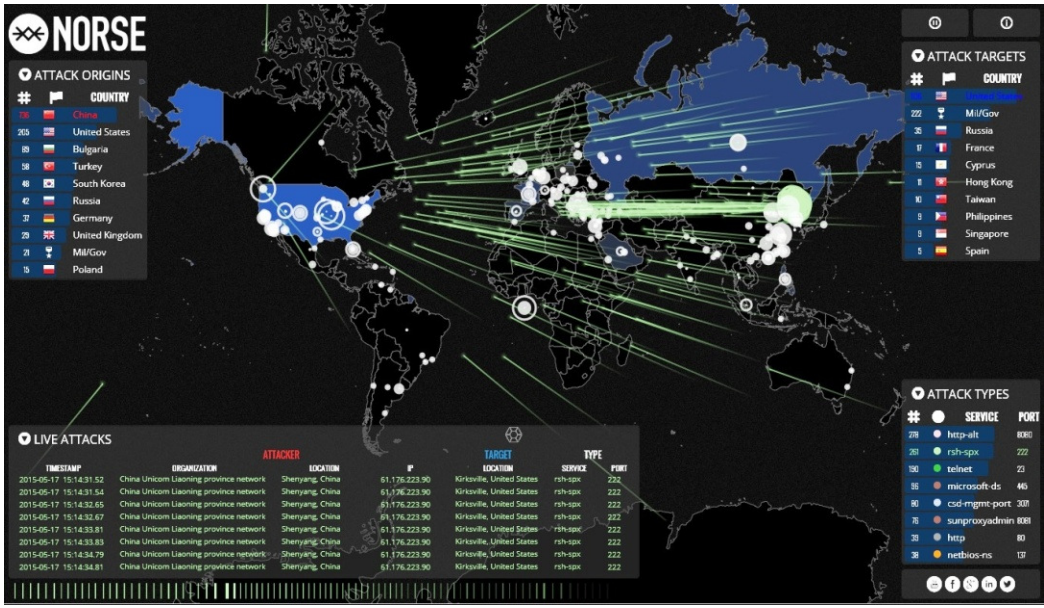


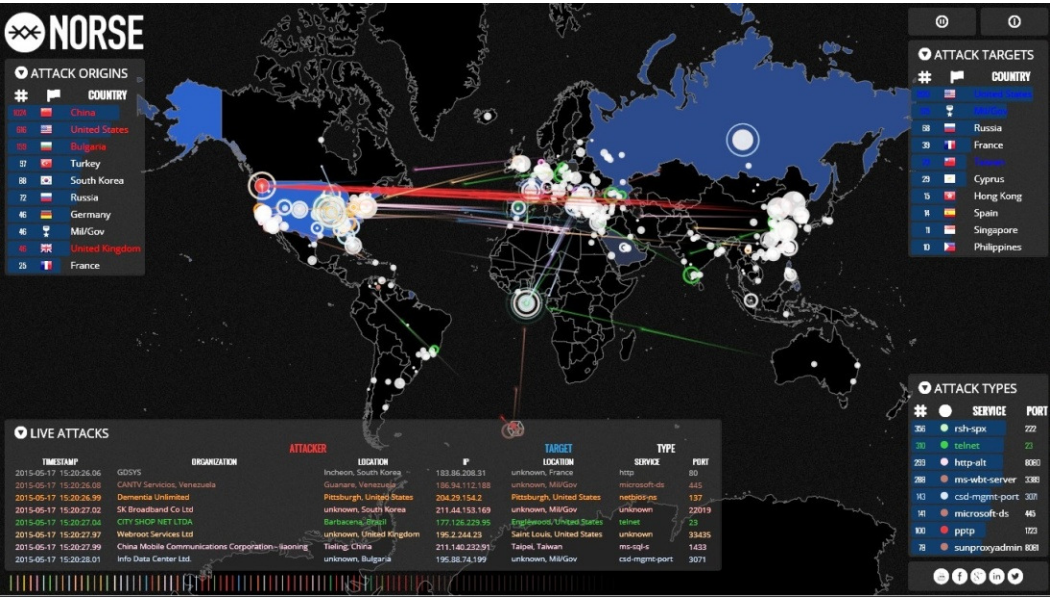
Typical DDOS "BotNet" Attack

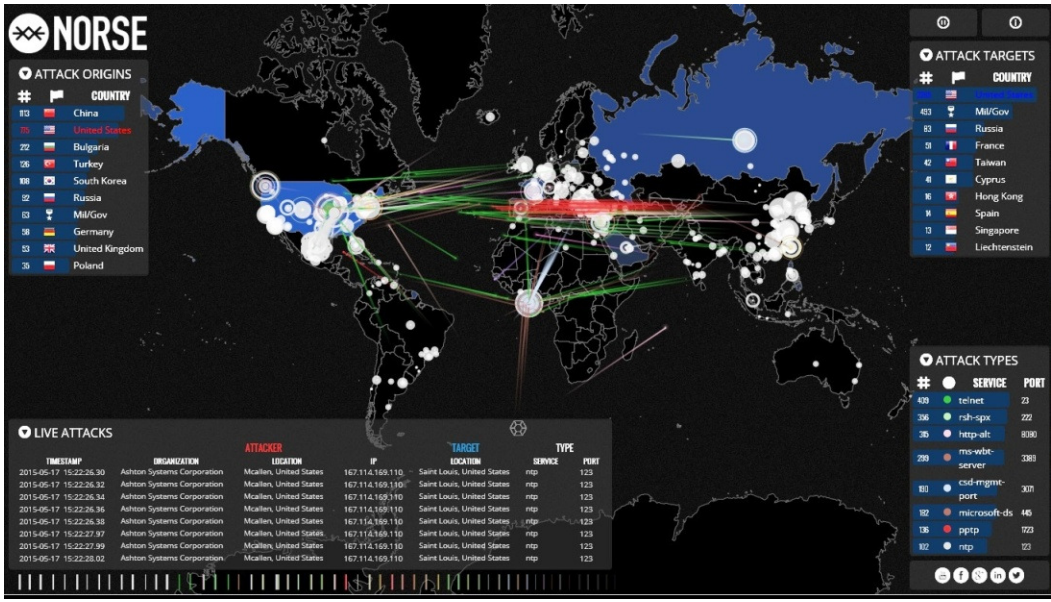


Successive "Real-Time" *DarkNet* CyberAttacks



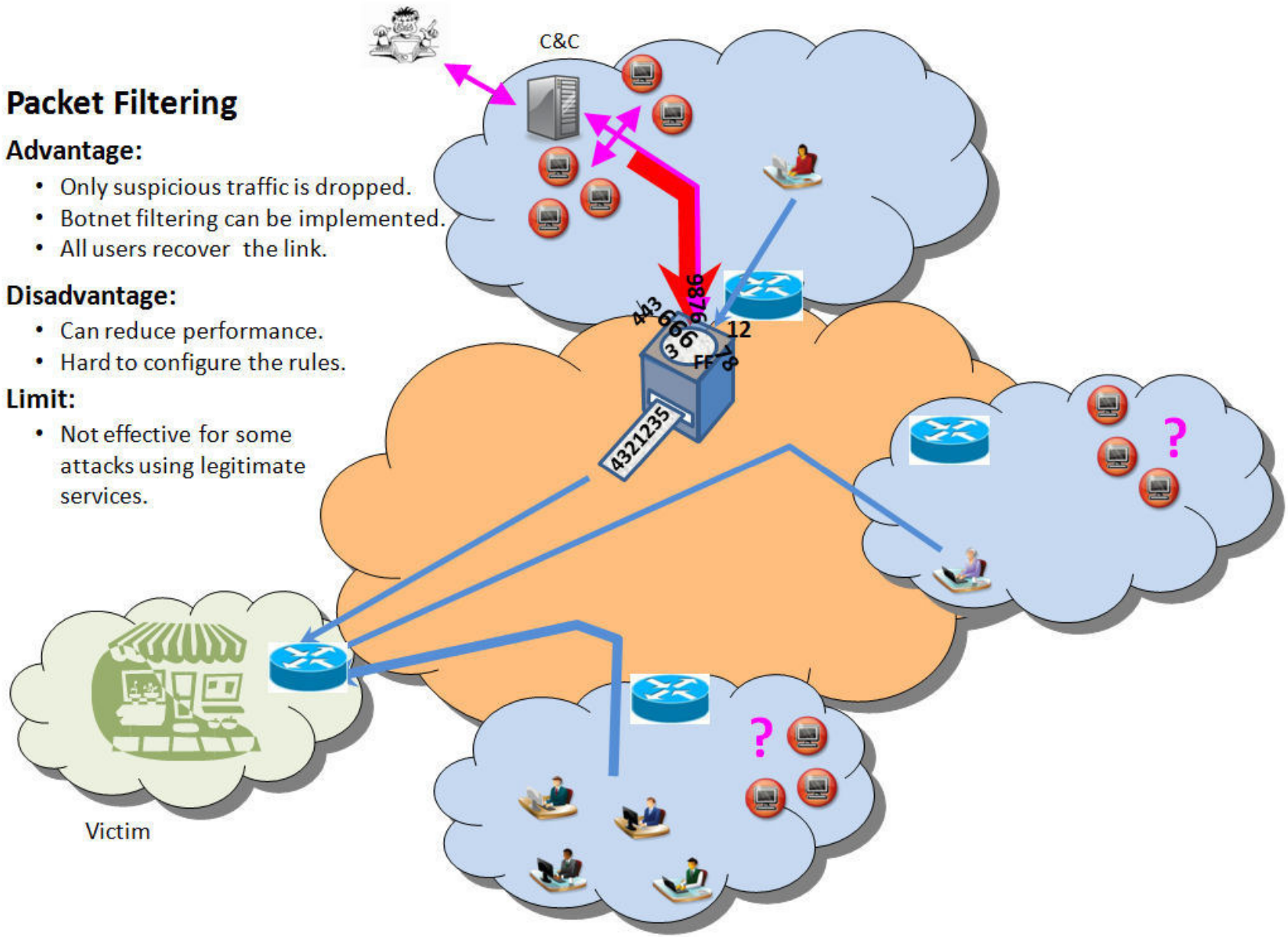




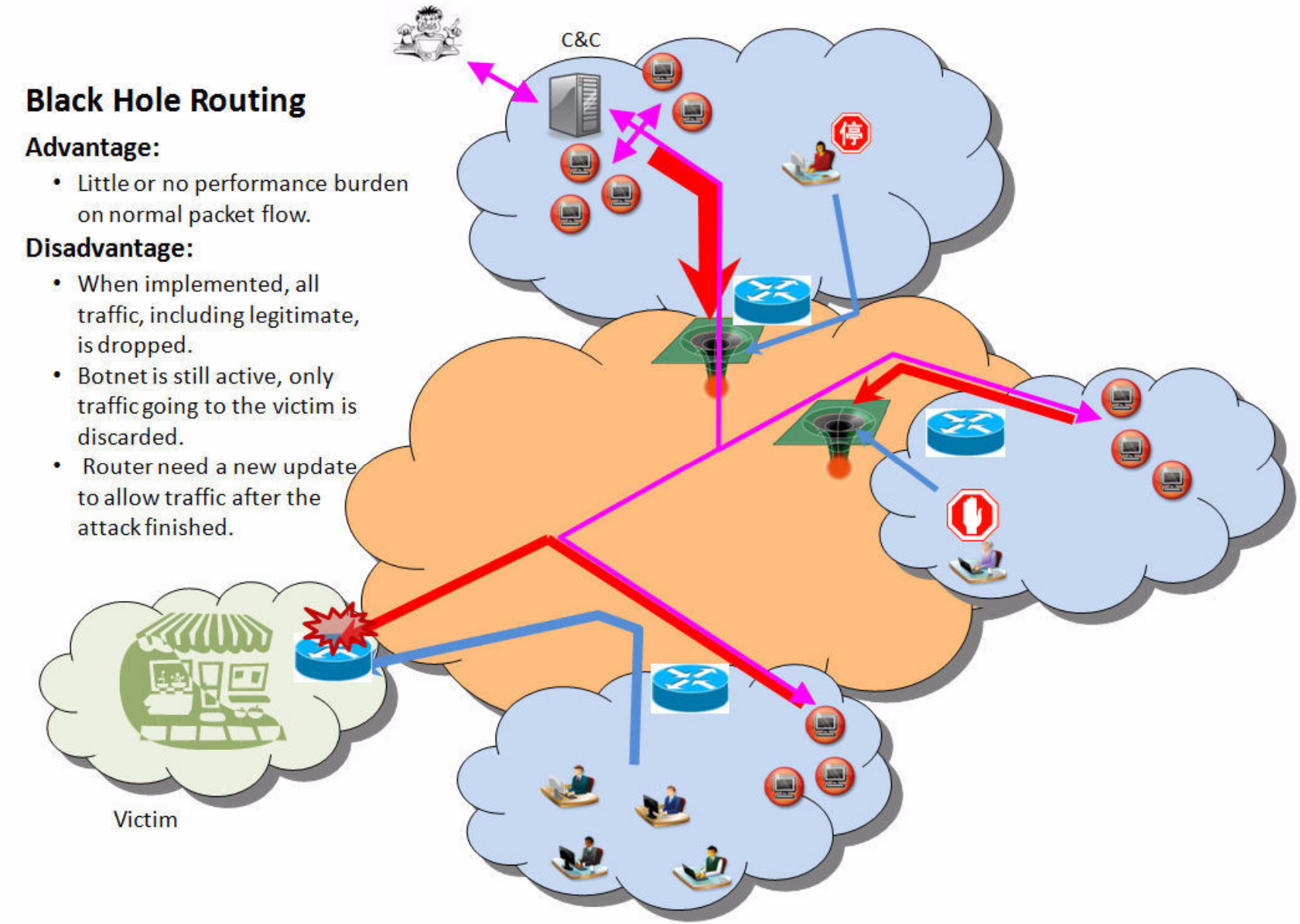


Link: map.norsecorp.com - Norse Corporation

DDoS Mitigation : "Packet Filter"

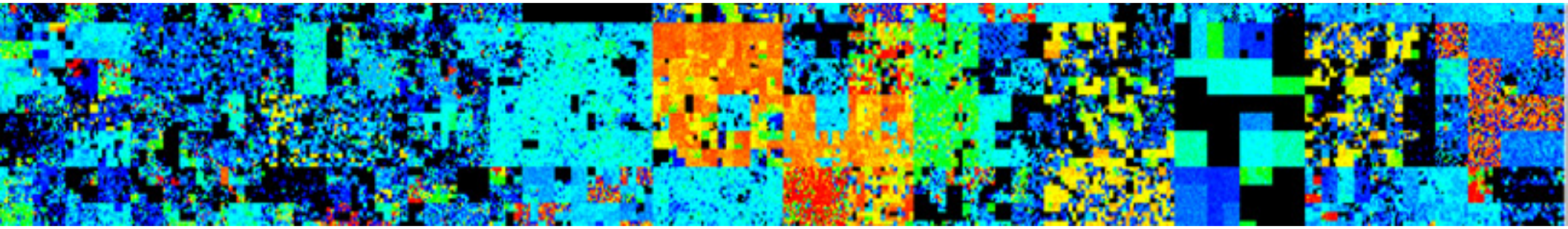


Mitigate DDoS Attack: "Black-Holing"



Cyber Threats & Defence: Intelligent Security

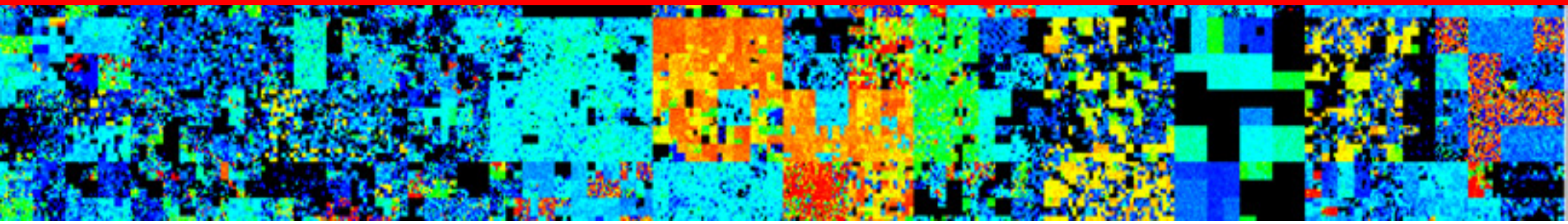
1 – "TOP 10 Cyber Threats & Attacks"	2–Cyber Case Studies: Recent Attacks	3 – Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert and Attack! **"Cyber Attack"**
7 –In-Depth: Security for Critical Sectors	8 – *YOUR* Operational Cyber Defence!	9 – *YOUR* Cyber Campaign Action Plan!



Cyber Threats & Defence: Intelligent Security

7 – In-Depth: Security for Critical Sectors

Defending *YOUR* Nation!...



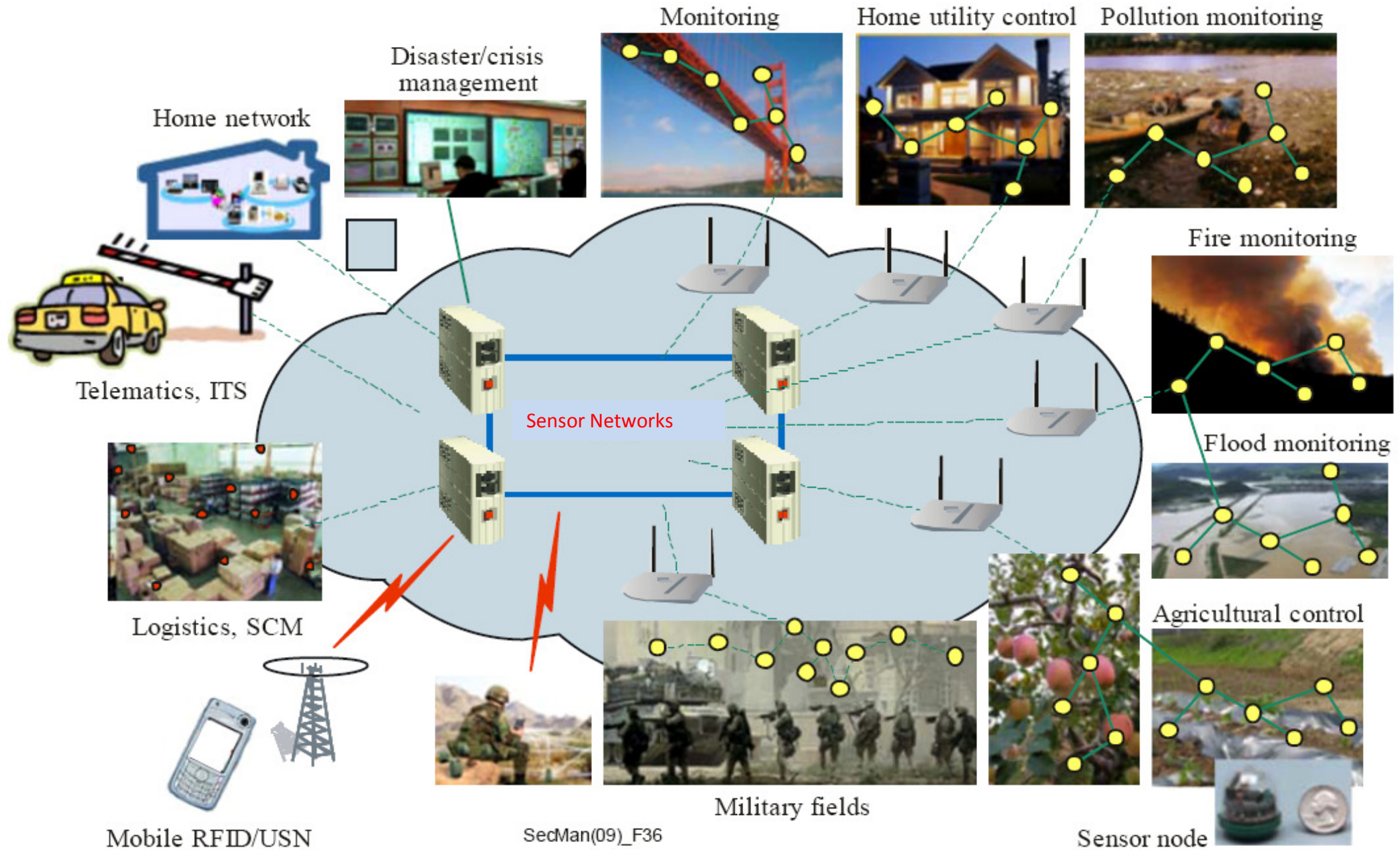
Critical Sectors: *Cyber Threat Scenarios*

- Hybrid Cyber-Physical Security Threats **will** target ALL of *YOUR* Critical Business and Government Sectors!....

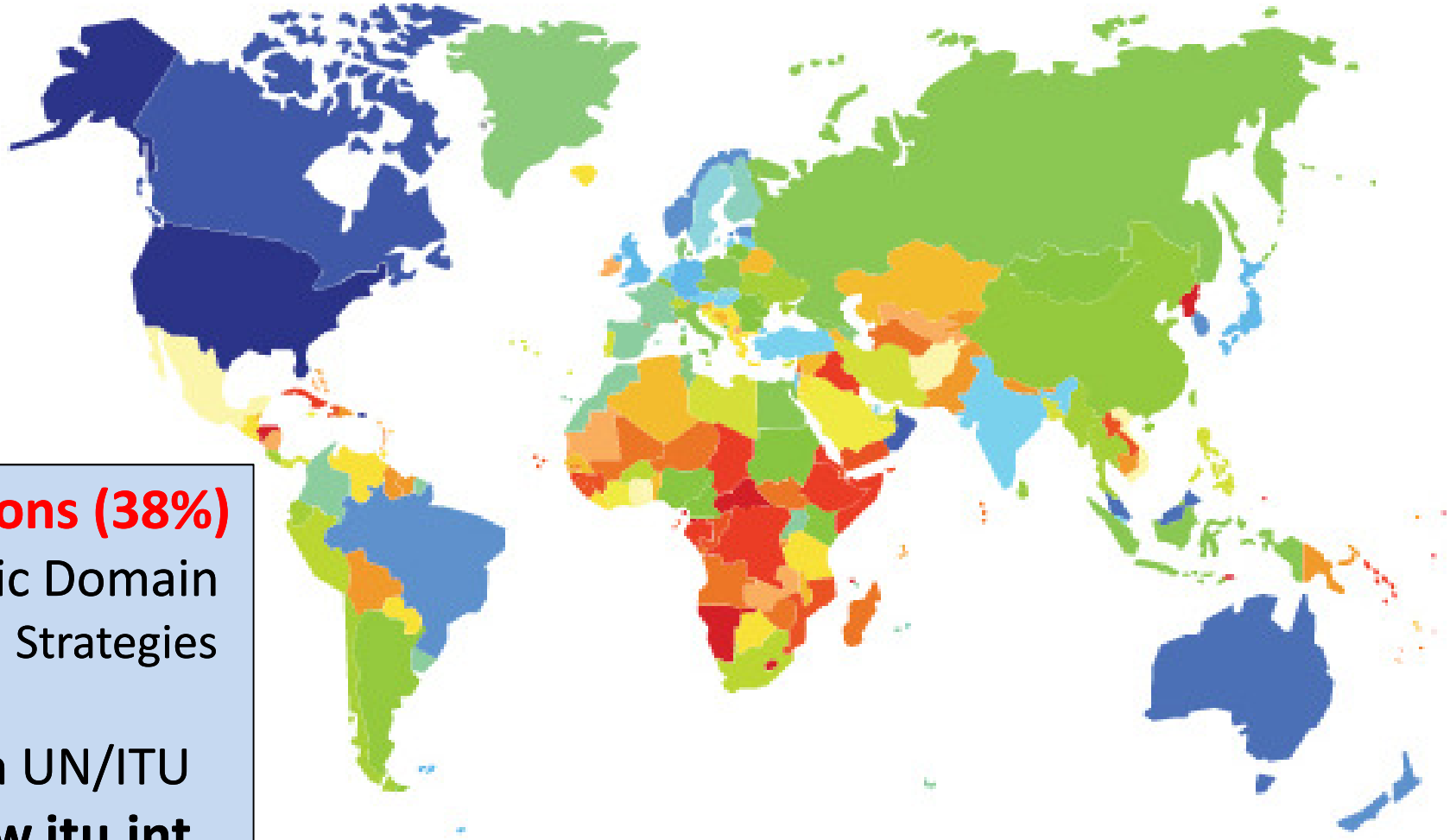
a) **Finance & Banking** – ATMs, Fraud, Money Laundering
b) **Transport & Tourism** – Airports, Metro, Tourist Sights
c) **Energy & Utilities** – Nuclear, Chemical & Water Resources
d) **Government & Defence** – Intel Theft, Hacking, Military
e) **Education & Research** – Campus-Wide Armed Attacks
f) **Industry & Manufacturing** – Competitive Espionage
g) **Retail, Sports & Culture** – Malls, Concerts, Olympics.....

....**CSOs** are advised to *URGENTLY* define practical & effective action plans to mitigate such attacks!...

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



UN/ITU – Global Cybersecurity Index



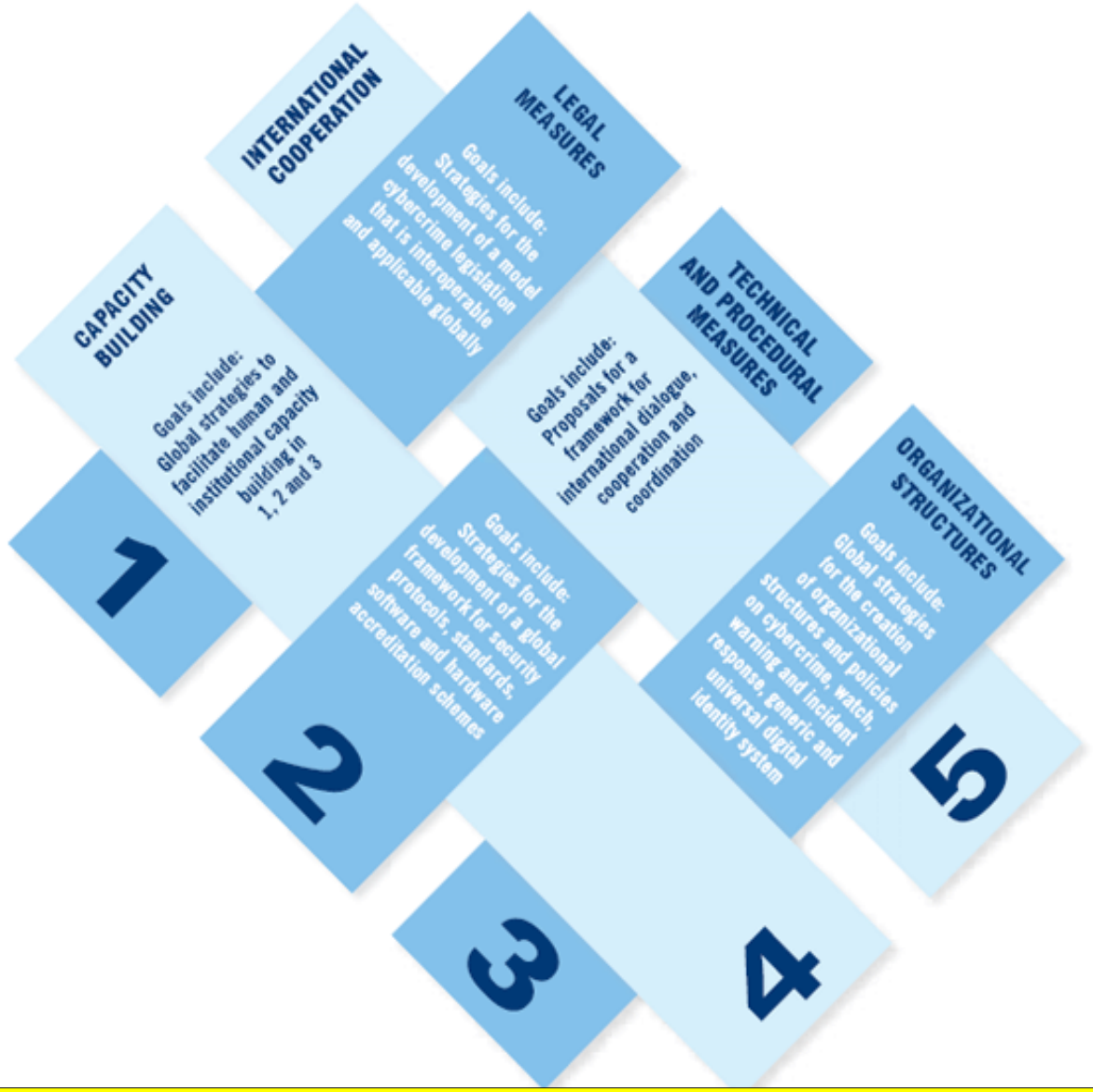
Only 73 Nations (38%)
Publish Public Domain
CyberSecurity Strategies

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

ABIresearch | Global Cybersecurity Index

National Cybersecurity Commitment HIGHEST LOWEST

UN/ITU: Global Cybersecurity Agenda



UN/ITU GCA - Global Cybersecurity Agenda:

---

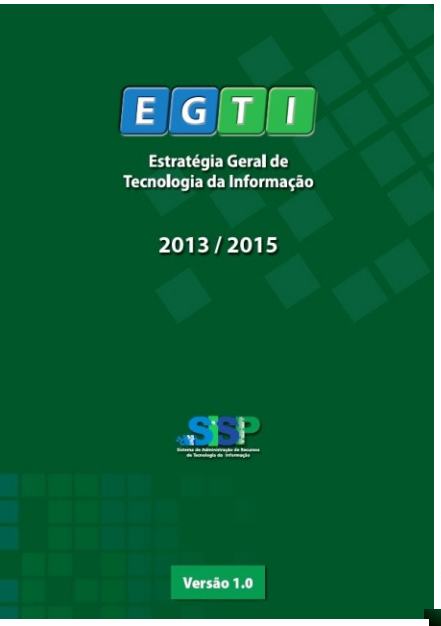
1 – Legal Measures
2 – Technical Measures
3 – Organisational Measures
4 – Capacity Building
5 – International Cooperation

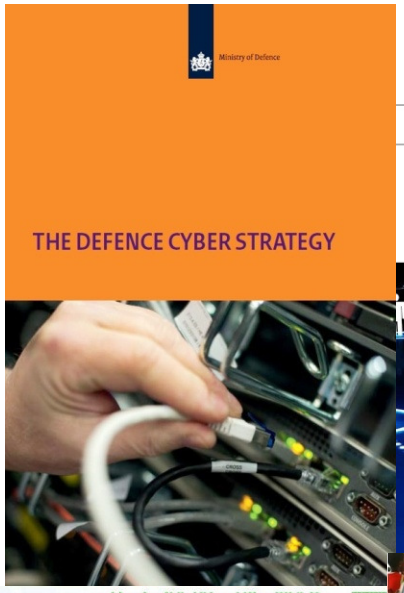
...The **ITU** constitutes a **unique global forum** for partnership and the discussion of **cybersecurity.**

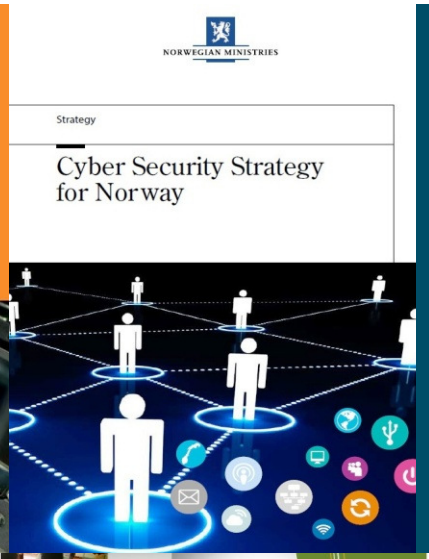
---

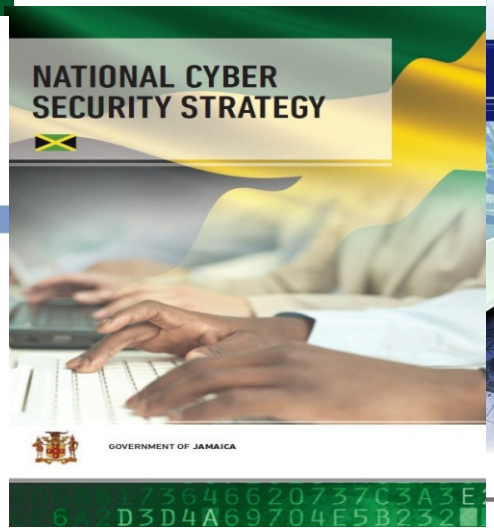
www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

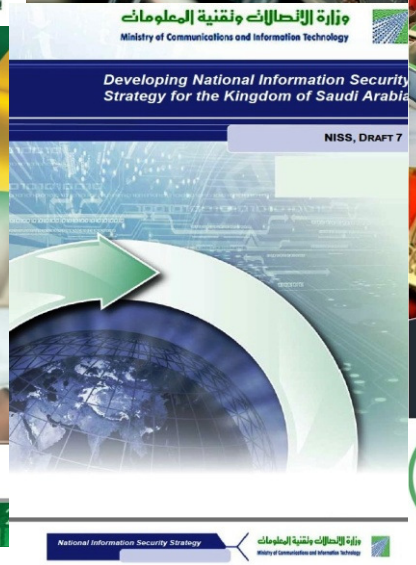
UN/ITU: National Cybersecurity Strategies

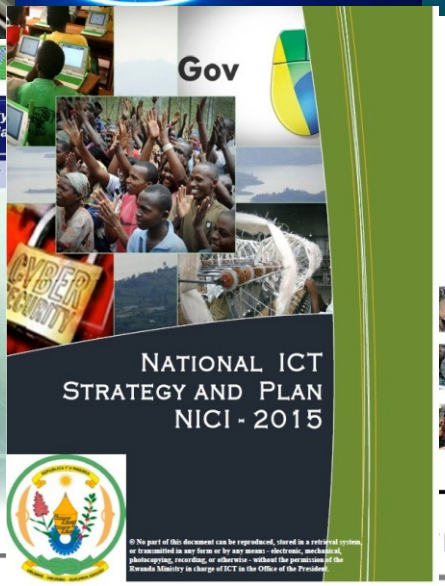


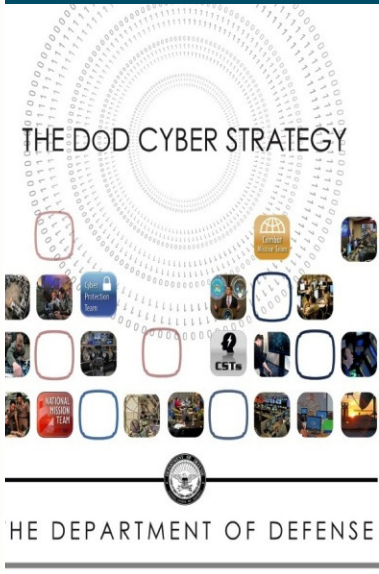






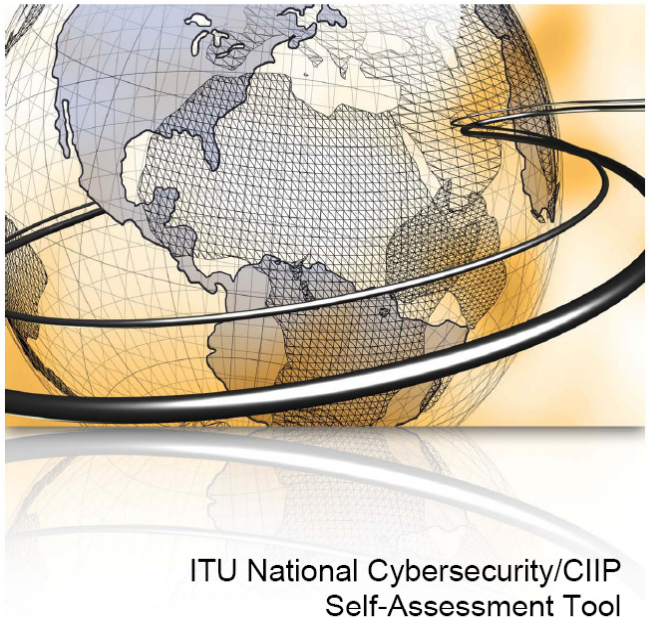


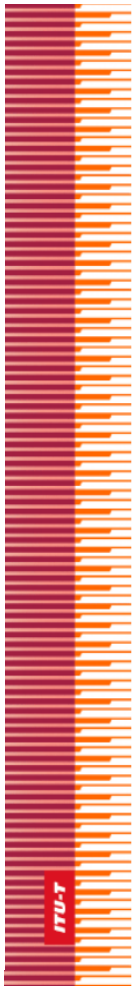




www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

United Nations/ITU Cybersecurity Guides





- UN/ITU *CyberSecurity* Agenda -

Quest for CyberConfidence (Eng/Rus)

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

36th International East West Security Conference

- Cyber Threats & Effective Defence! -
"Intelligent Business CyberSecurity"
Seville, Spain, 20th – 21st November2017

EU Agency for Info Security: ENISA

enisa
European Network and Information Security Agency

ENISA Strategic Security Framework Provides effective "Cyber" model for National Governments & Ministries

National Cyber Security Strategies

Practical Guide on Development and Execution

An evaluation Framework for National Cyber Security Strategies

- ALL EU Countries now have approved **National Cybersecurity Strategies -**

www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

BET365: Gambling Sector adopts ISO/IEC 27001 Security Standards

- **London 5 April 2017**- **BET365'S** commitment to standards recognised with **ISO/IEC 27001:2013** Certification for Info Security Management (ISMS).
- **UTECH Jamaica PhD - CyberSecurity & Gambling:** *"Cybercrime in Online Gaming & Gambling": An Implementation Framework for Developing Countries - A Case Study for the Jamaica Jurisdiction: George Brown...*

*.....Research Programme initiated following **UN/ITU** CyberSecurity Training @ **UTECH – September 2010....***

Cyber Tool: Web-Site Security - Acunetix

Cyber Tool: Web-Site Security - Acunetix

Cyber Tool: Web-Site Security - Acunetix

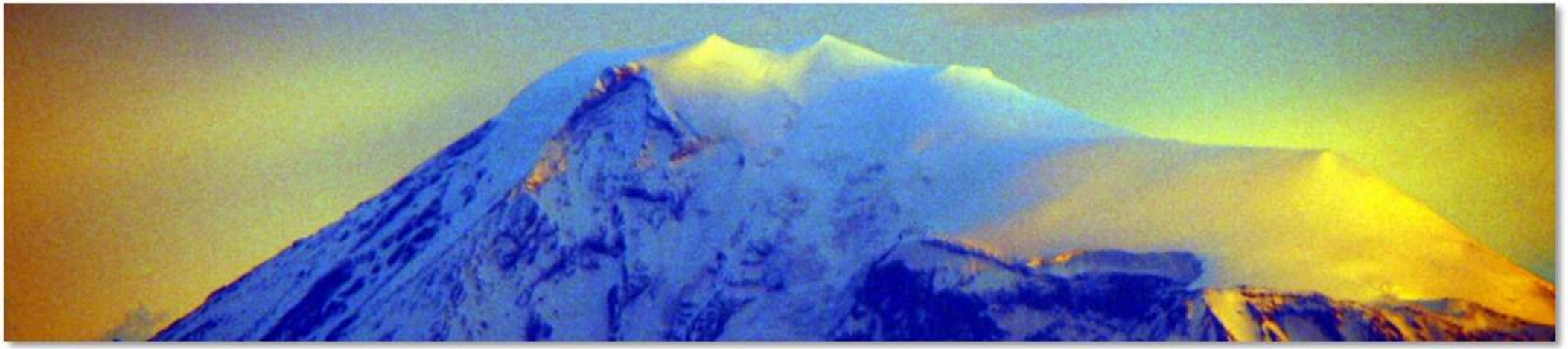
"Smart Security" for Critical Sectors:

YOUR Shopping and To Do List!

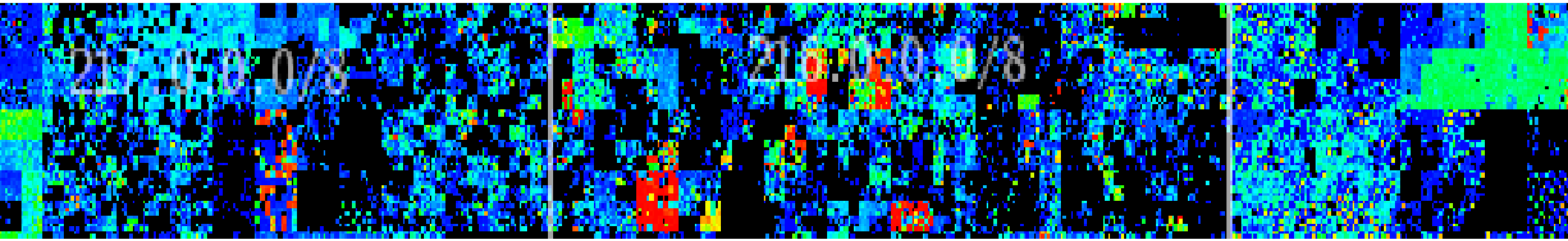
- ***Security Audit:*** In-Depth Security Audit and Action Report - Spanning BOTH Physical and Cybersecurity Operations, Assets and Technologies
- ***International Standards:*** Understand and Implement Security Policies and Programmes to International Standards – ISO/IEC, UN/ITU, IEEE, NIST, ASIS, ISF
- ***Training:*** Professional Training: Form strategic partnerships with leading educational & research institutions to develop pipeline of professional graduations in cybersecurity & integrated security technologies
- ***CERT/CSIRTs:*** Understand the critical role of Cybersecurity CERTs and link their alerts and operational processes within your overall security policies
- ***Security Associations*:** Join Security Associations and follow developments in Cybersecurity for ***"Intelligent Real-Time Systems"*** & ***"Internet of Things"***

*....**YOUR** Top Priority is Professional **Cybersecurity Training & Certification** with regular course **"Top-Ups"** since the field is moving at **Supersonic Speed**!*

Cyber Threats & Defence: Intelligent Security



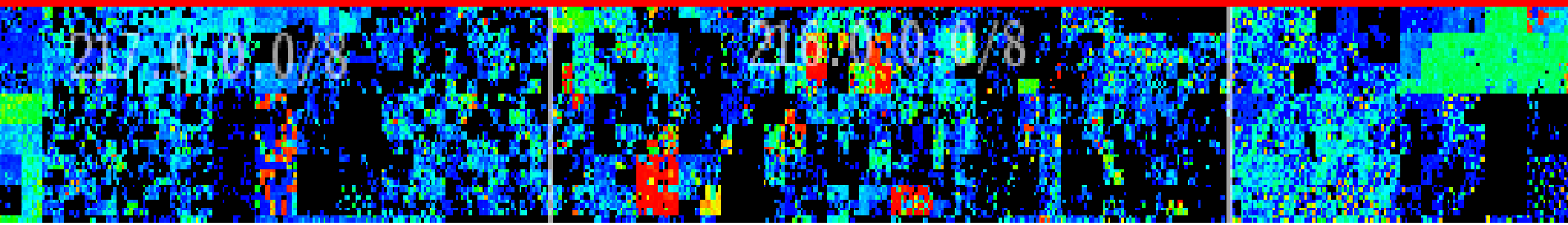
1 – "TOP 10 Cyber Threats & Attacks"	2–Cyber Case Studies: Recent Attacks	3 – Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 –Real-Time Cyber Alert and Attack! **"Cyber Attack"**
7 –In-Depth: Security for Critical Sectors	8 – ***YOUR*** **Operational Cyber Defence!**	9 – ***YOUR*** Cyber Campaign Action Plan!



Cyber Threats & Defence: Intelligent Security

8 – *YOUR* Operational Cyber Defence!

"Budget, Training & Plan!"



"YOUR Cyber Campaign *Action Plan*"

- Defeating the **"Bad Guys"** requires YOU to Launch a Campaign Action Plan for Active Cyber Defence!
- Fighting the **TOP 10 Cyber Threats** requires:
  - **C$O:** Board Level Security Plan and $ Investment
  - **Technical:** Professional Team, Tools & Training
  - **Operational:** Security, Standards & Compliance

....**CyberSecurity** is Continuously Evolving so keep up with **Conferences & Professional Memberships**!....

"In-Depth 21stC Technical Cyber Defence"

- Effective **Cyber Defence** to **TOP 10 Threats** requires BOTH **Technical** & **Operational** Plans:
- Technical Actions, Plans & Policies include:
  - **DataBase:** Secure Physical & Cloud DataBase Scripts
  - **Back-Ups:** Continuous Real-Time DB/Web Back-Ups
  - **BYOD:** Strict Policy for "Bring Your Own Device"
  - **eMail:** Script Locks on eMail Attachments & Web Links
  - **DDoS:** Switch DNS/IP Settings in case of DDoS Attack
  - **CERT:** Set-Up Computer Emergency Response Team

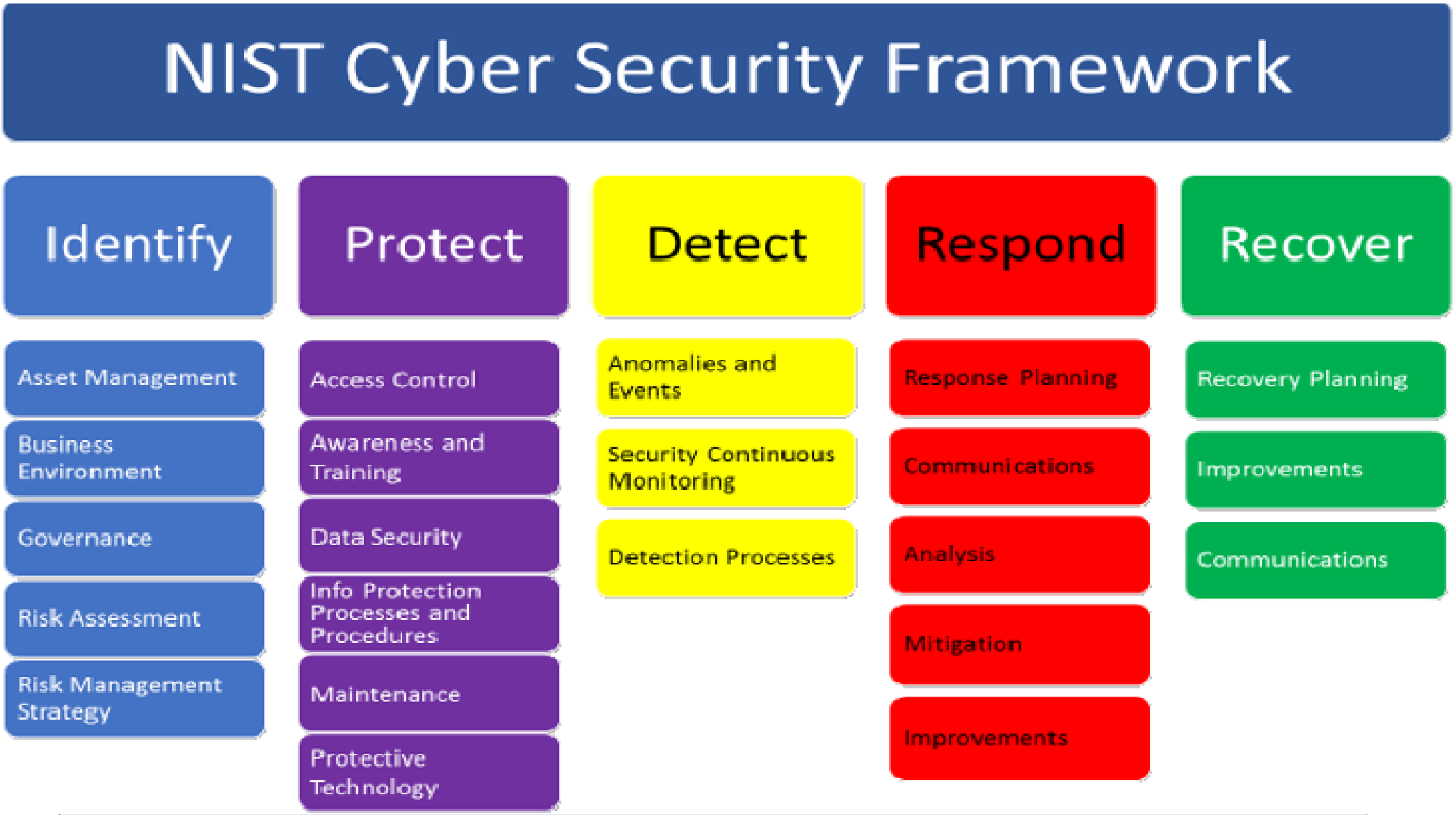
.....**CERTs** work together **Globally** to provide **Cyber Alerts & Intelligence** to Govt & Business

"YOUR Operational Cyber Defence"

- **C$O:** Board Level Role – Chief $ecurity Officer - with Security Investment Plan and **$$$** Budget!..
- **Cyber Standards:** Migrate to International Security Standards such as ISO2700x Series
- **Compliance:** Implement regular IT Asset & Process Audits to ensure Full Compliance
- **Training:** Ensure Key Staff are Professionally Certified (CISSP) with Bi-Annual Updates.
- **Culture:** Launch Business/Agency Security Policy so **ALL** Staff understand their Responsibilities!

*....A Major Targeted **Cyber Attack** can easily destroy **YOUR Business** as effectively as Bankruptcy so **Plan & Invest**!*

Guide to CyberSecurity Event Recovery:NIST

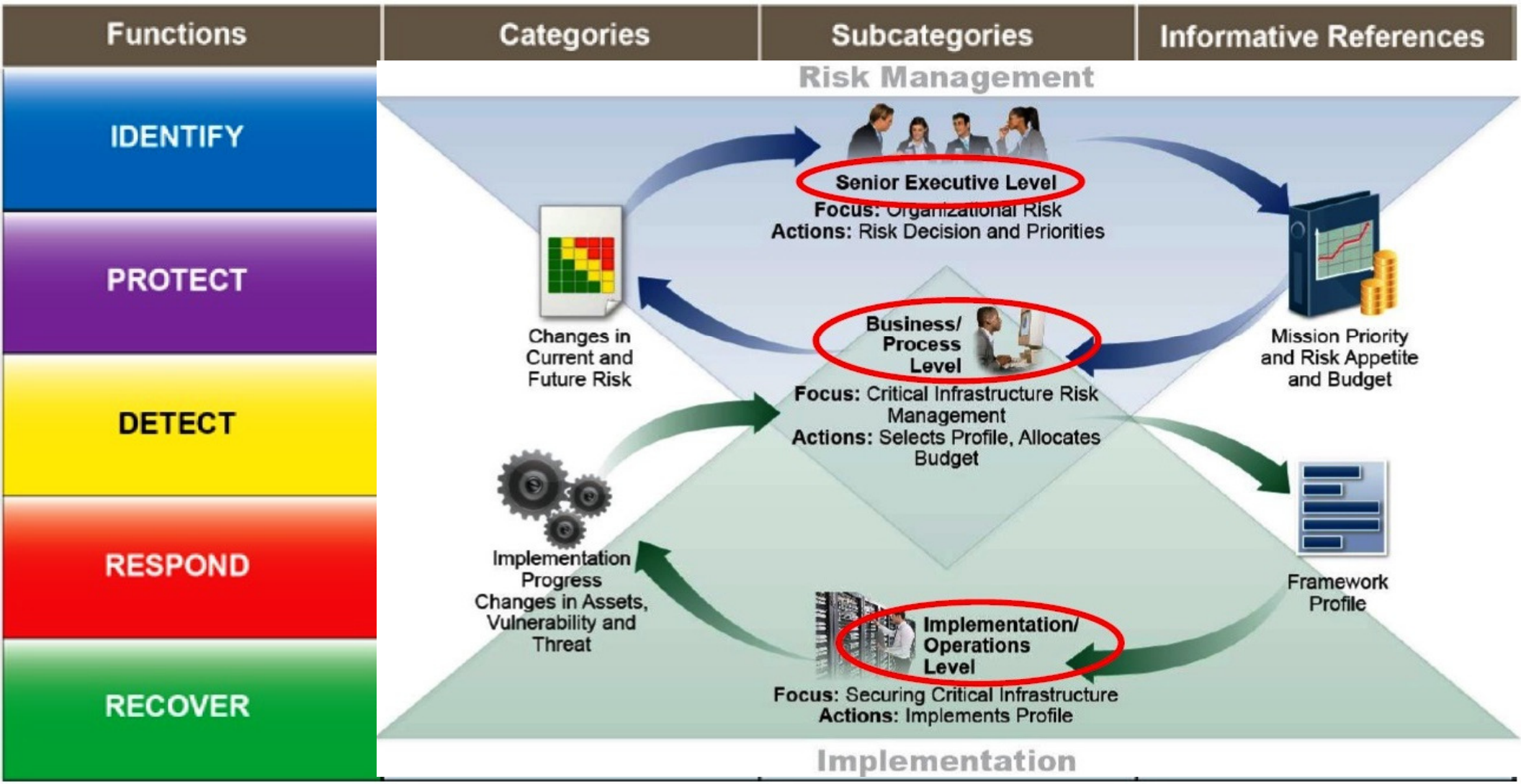


Free Download: **https://doi.org/10.6028/NIST.SP.800-184**

NIST *Cybersecurity* Framework

National Institute of Standards & Technology

Functions	Categories	Subcategories	Informative References



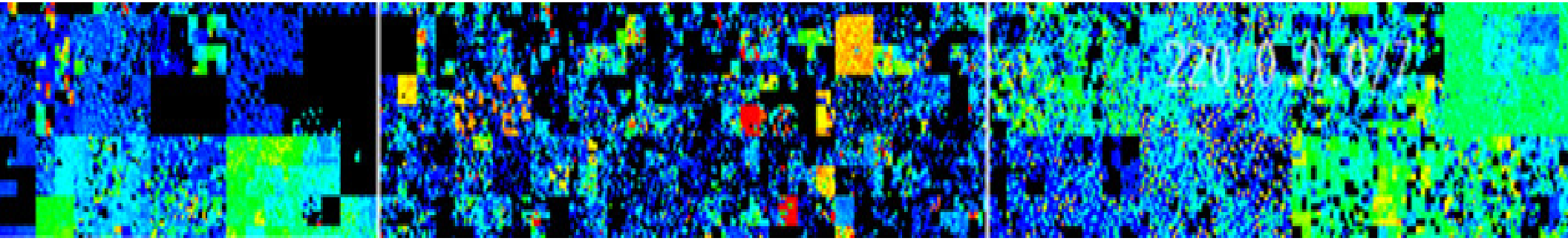
Web: www.nist.gov/cyberframework/

36th International East West Security Conference

- Cyber Threats & Effective Defence! -
"Intelligent Business CyberSecurity"
Seville, Spain, 20th – 21st November2017

Cyber Threats & Defence: Intelligent Security

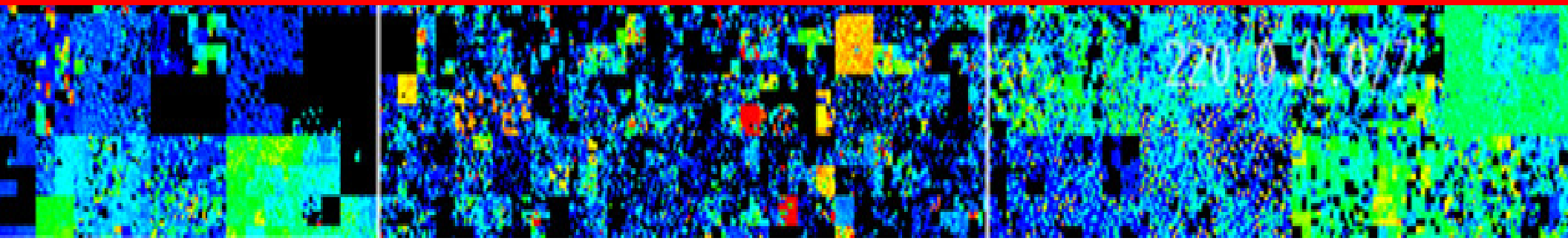
1 – "TOP 10 Cyber Threats & Attacks"	2– Cyber Case Studies: Recent Attacks	3 – Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert and Attack! **"Cyber Attack"**
7–In-Depth: Security for Critical Sectors	8 – *YOUR* Operational Cyber Defence!	9 – *YOUR* Cyber Campaign Action Plan!



Cyber Threats & Defence: Intelligent Security

9 – *YOUR* Cyber Campaign Action Plan!

CSO - Cyber Leadership!



Wrap-Up: CyberSecurity Landscape

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

Now Design & Implement YOUR Business Plan for 21stC "Cyber"!...

YOUR Action Plan for 21stC Cyber!...

- Every CSO needs Board-Level Approval for Annual Security Business Plan that includes CyberSecurity
- **YOUR CyberSecurity Plan Actions** will include:
  - Investment Budget for Integrated Security Solutions
  - Job Specifications for Professional "Cyber" Team
  - Security Staff Training & Professional Development
  - Technical & Operational Plans & Upgrades
  - Actions for Compliance, Security Audit & ISO Standards

.....Invest & Equip **YOUR** Business with **21stC CyberDefence**

Download Presentation @ www.valentina.net/Seville2017/

"Cyber Defence" against "Alien Invaders"

Cyber Threats & Defence!

- "Intelligent CyberSecurity"-

A.I. & Machine Learning CyberSecurity Tools will Provide ***"Speed of Light"*** Real-Time Defence against ***TOP 10*** Threats & Attacks!

"Steam Powered Birds arrive over our Cities! - 1981

Pen & Ink Drawing by **Dr Alexander Rimski-Korsakov**

Cyber Threats & Defence: Intelligent Security

36th East/West Security Conference: Seville, Spain

Cyber Threats & Defence: Intelligent Security

36th East/West Security Conference: Seville, Spain

East-West Security Conference: Seville 2017

- "Cyber Futures & Defence" : On-Line!

Security Futures: 2018-2025+

Technology, Tools & Trends

Cyber Threats & Defence!

- "Intelligent CyberSecurity"-

Theme (1): Security Futures:2018-2025 **Theme (2): Cyber Threats & Defence**

Download Link: www.valentina.net/Seville2017/

Download Presentation Slides:
www.Valentina.net/Seville2017/

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, and then by UN/ITU to review Cybersecurity for the Government Ministries.

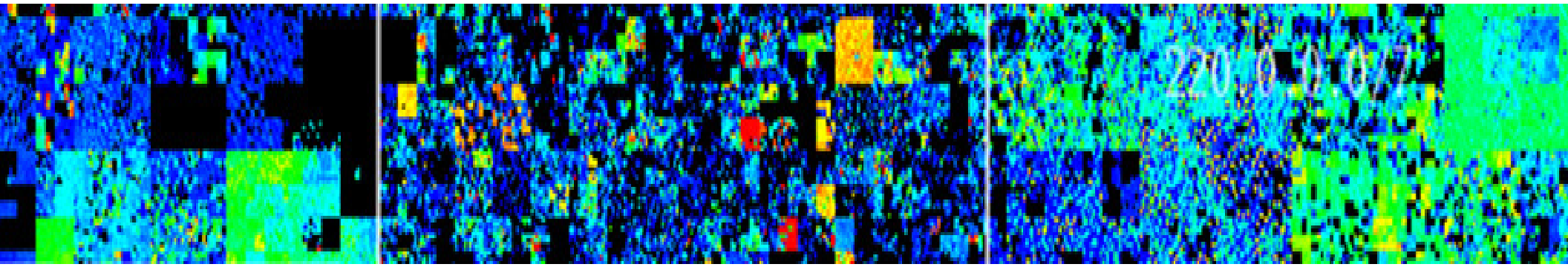
- ***UN/ITU*** – Senior Adviser – Development of Cybersecurity Infrastructure, Standards, Policies, & Organisations in countries within both Europe & Americas

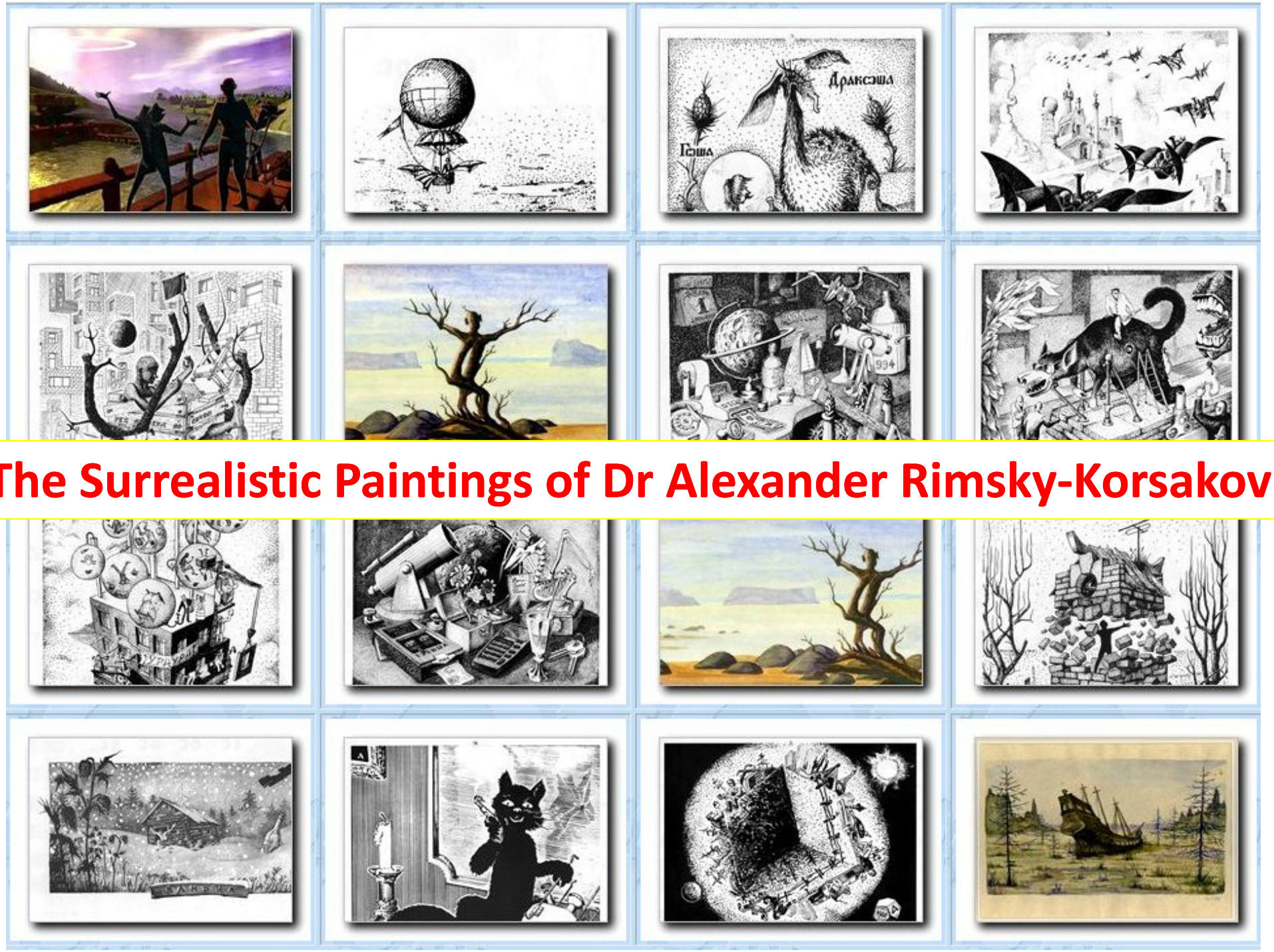
Dr David E. Probert is a Fellow of the Royal Statistical Society, IEEE Life Member and 1st Class Honours Maths Degree (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata) , and his full professional biography is featured in the Marquis Directory of Who's Who in the World: 2007-2018 Editions.

Cyber Threats & Defence: Intelligent Security

36th East/West Security Conference: Seville, Spain

BACK-UP SLIDES



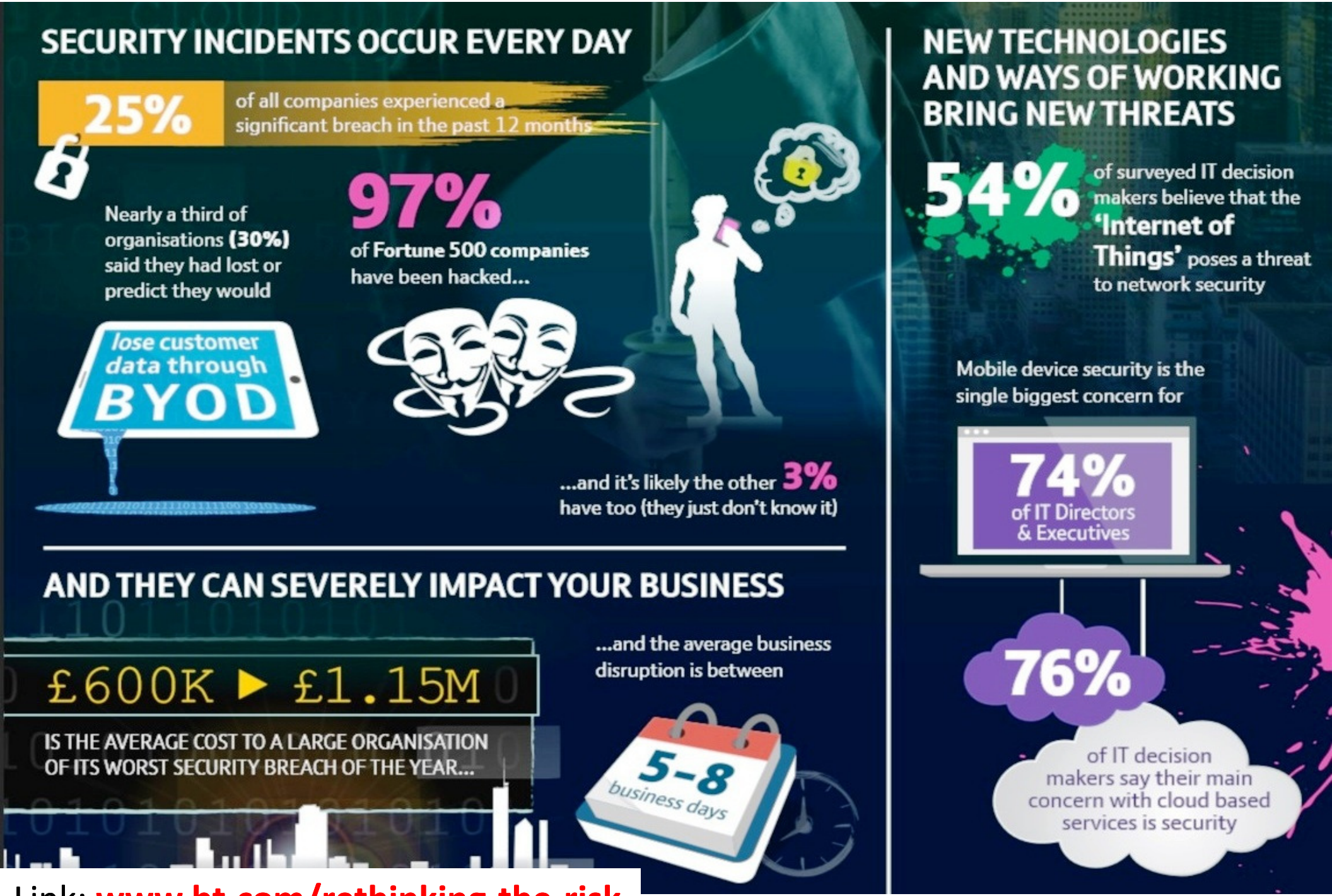


The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov

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

36th International East West Security Conference

- Cyber Threats & Effective Defence! -
"Intelligent Business CyberSecurity"
Seville, Spain, 20th – 21st November2017



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

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.

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.

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.

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.

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.

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.

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.

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

*** Security Equipment for Alpine Climbing ***

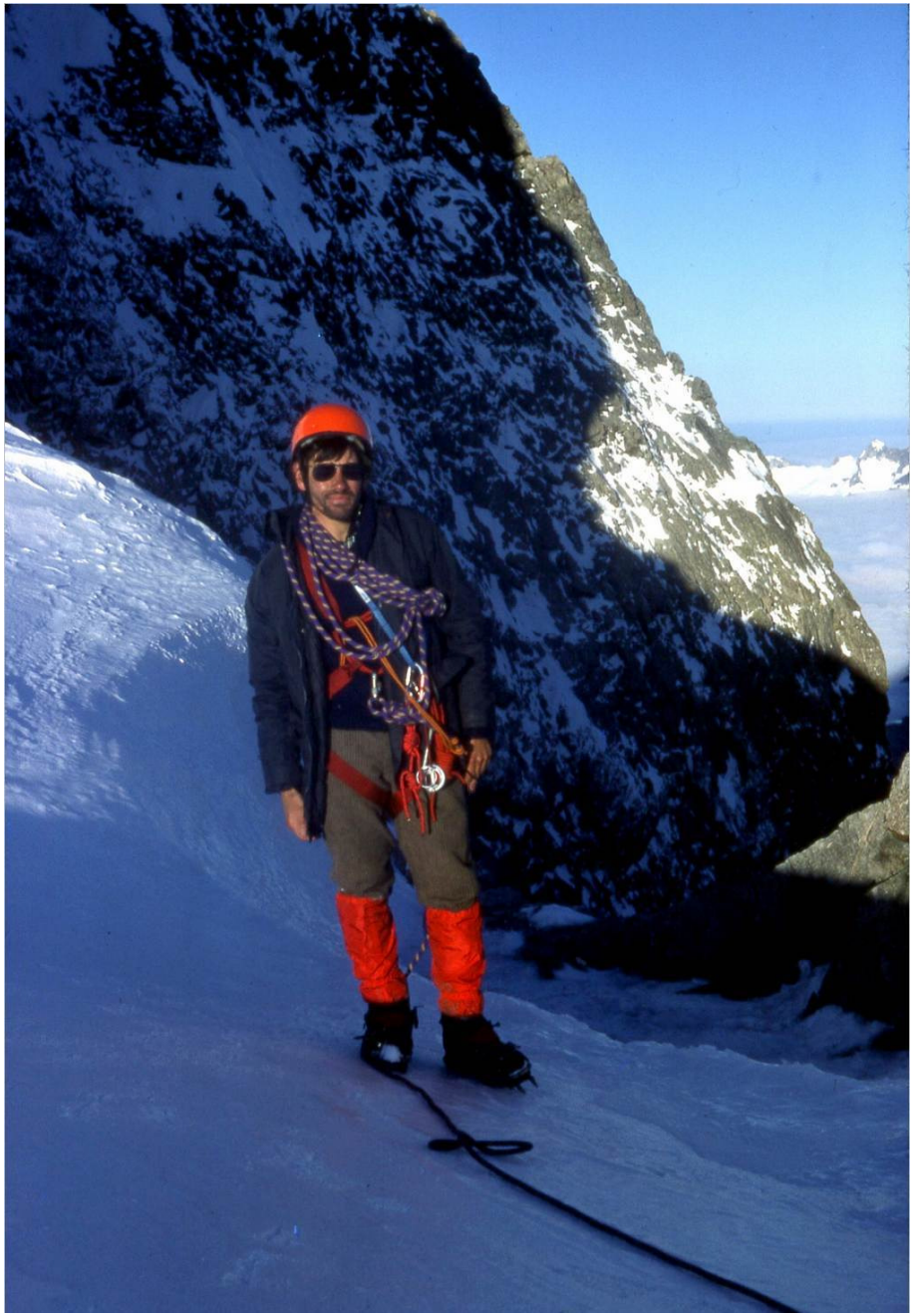
Sunrise on « Barre des Écrins » – 4102metres

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

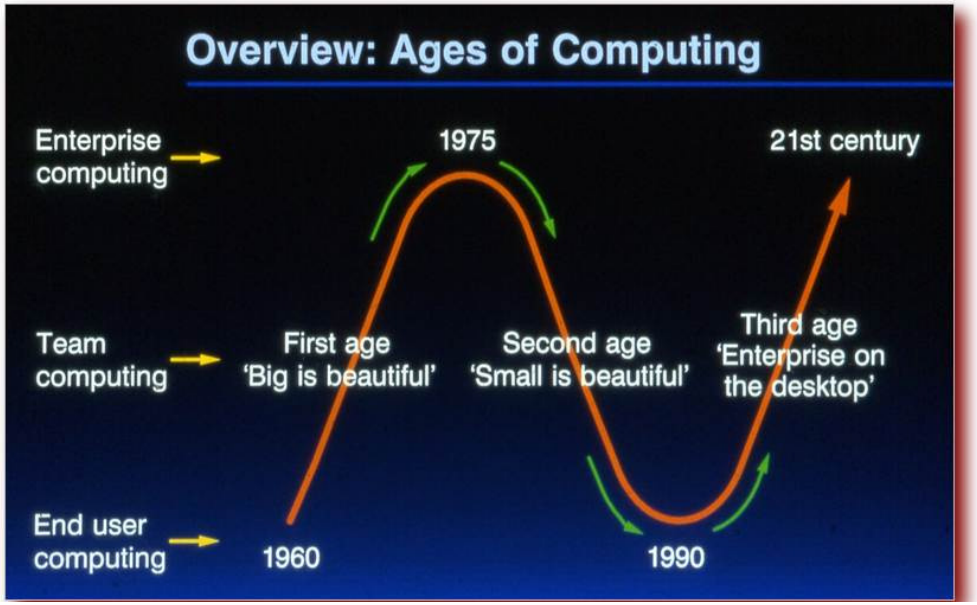
15th Sept 2015: « 7 Alpinistes died in Avalanche »

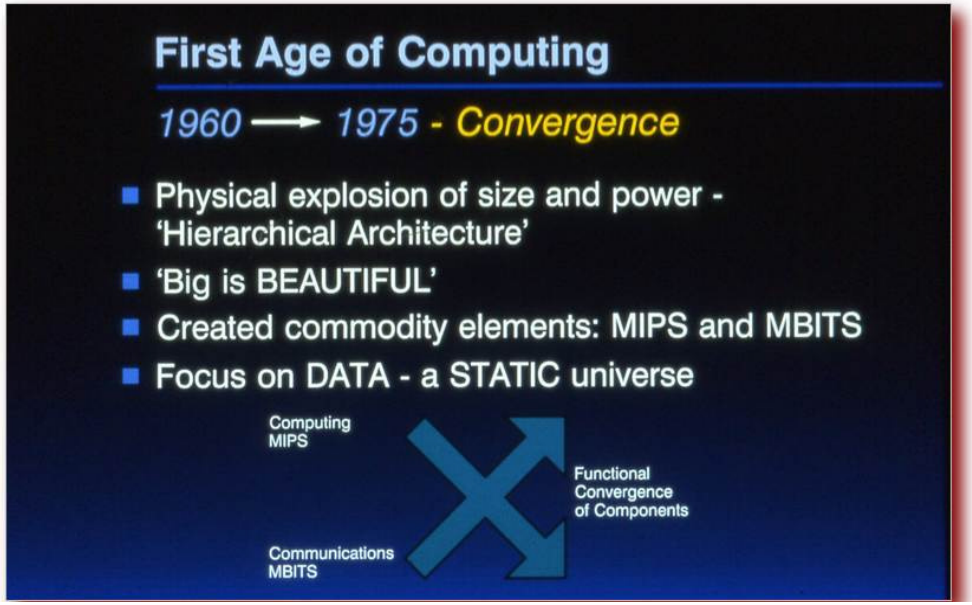
36th International East West Security Conference

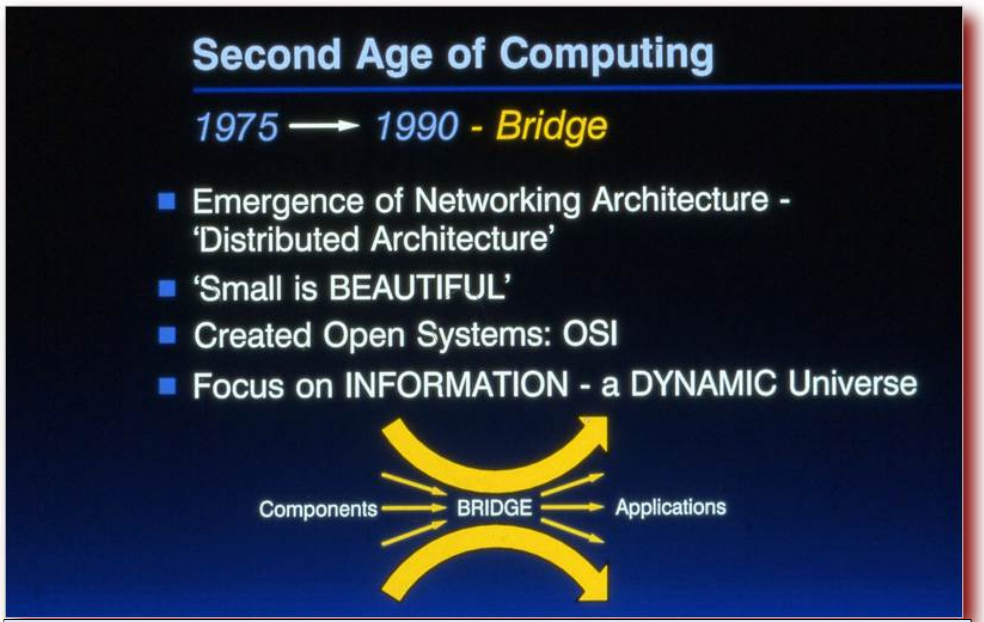
Security Equipment for *Alpine Ascents*

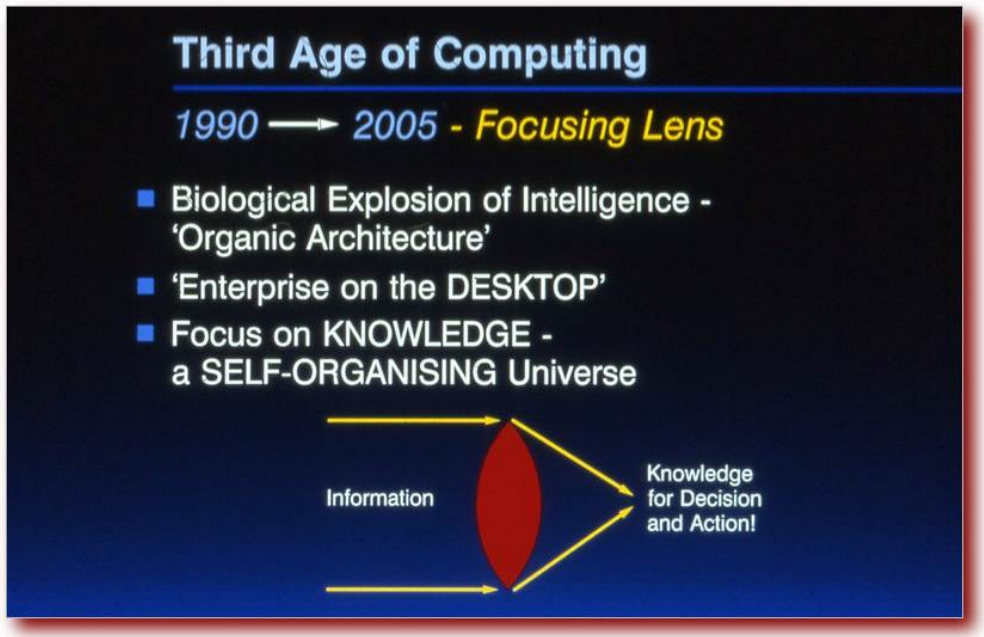


Ages of Computing, Networking & Intelligence: *1960 - 21stC*









From: "Business Blueprint": Probert – July 1989