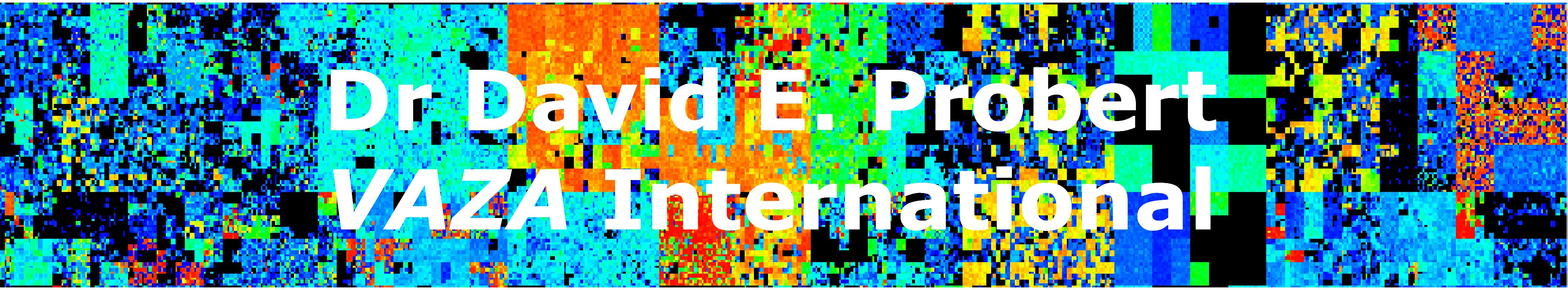
Practical Cyber Defence

-TOP 10 Cyber Threats-

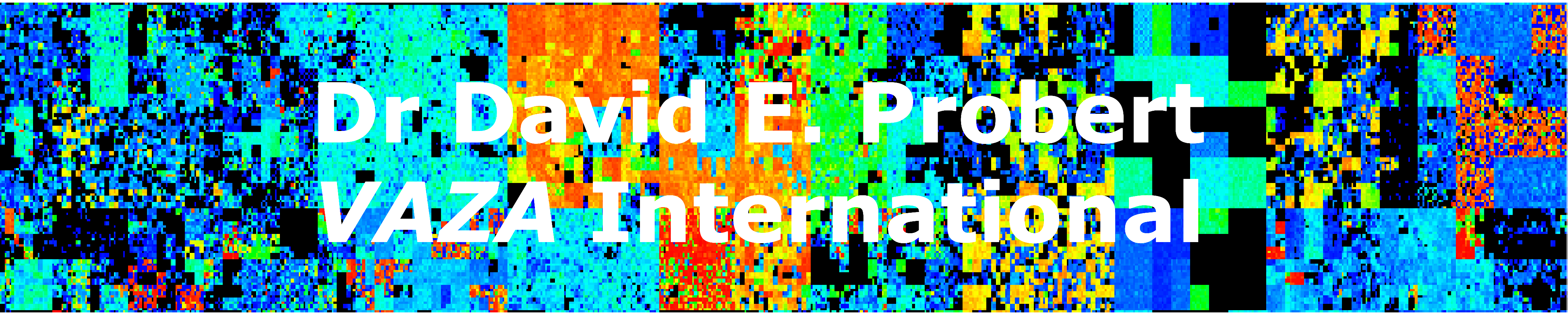


Dr David E. Probert

VAZA International

Практическая кибер Защита

-Топ 10 кибер Угроз-



Dr David E. Probert
VAZA International

"Cybersecurity Trends": *Dual Themes*

Theme (1) – .....Practical Cyber Defence against TOP 10 Cyber Threats.....

Practical Cyber Defence
-TOP 10 Cyber Threats-
Dr David E. Probert
VAZA International

We review Practical CyberDefence against Threats, Hacks & Attacks from Ransomware, BotNets(DDoS), Key Logging, Insider Threats, Legacy IoT Hacks, Social Media Phishing, Data Base Hacks(SQL), Advanced Persistent Attacks (APT), Virus/Trojan & Web/Cookie Hacks.

"Networked" : "Real-Time Cyber Security & Surveillance" 09:45 6th June 2017

Theme (2) – .....Cyber Tools & Trends: The Next 7 years: 2018 – 2025.....

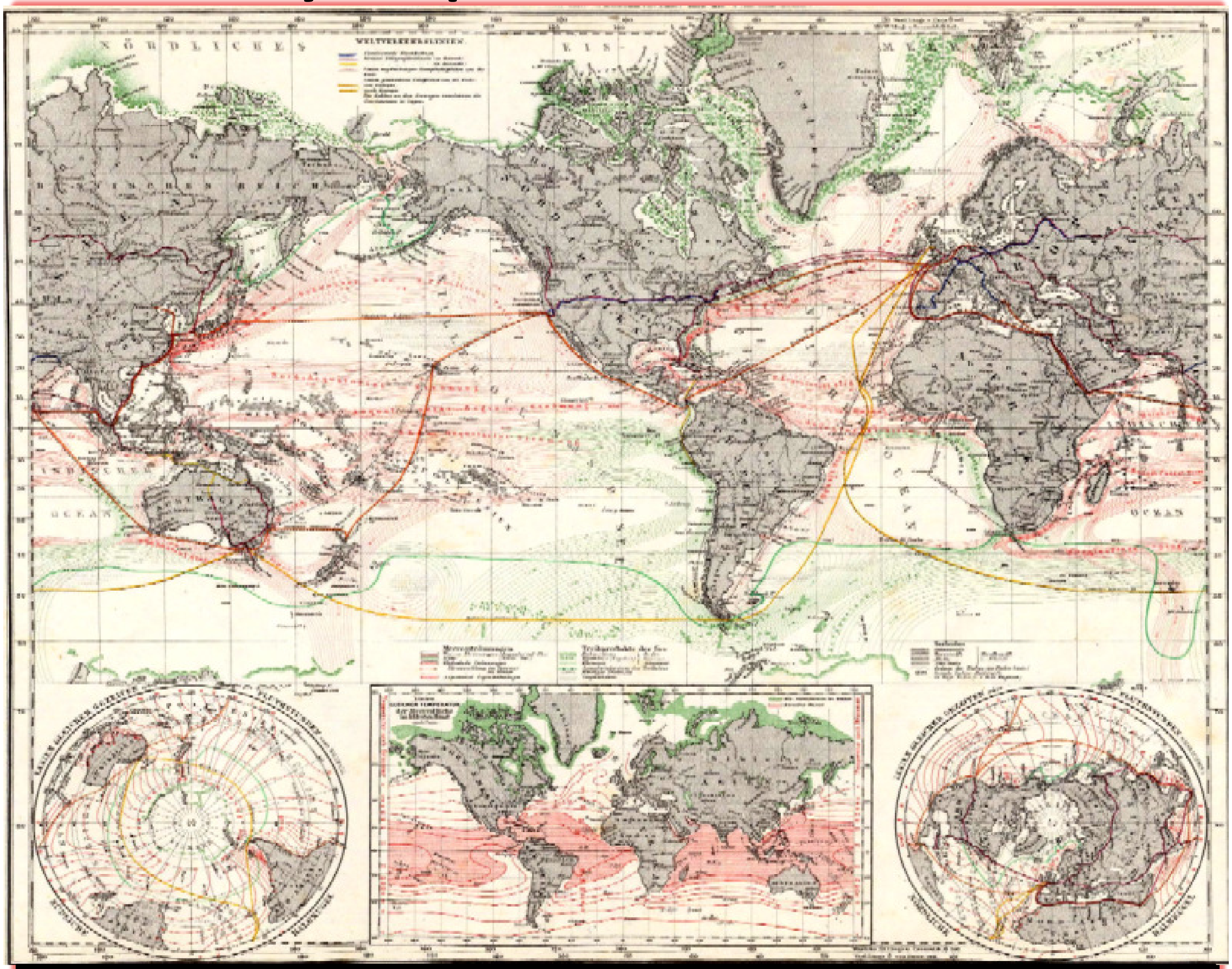
Cyber Tools and Trends
Next 7 Years: 2018 - 2025
Dr David E. Probert
VAZA International

We present Cyber Trends & Scenarios for 2018 (**Cyber Transition**), 2020 (**Intelligent Security**) and 2025 (**Neural Security).** We discuss the Evolution of Advanced AI based Cyber Tools with Applications to Smart Devices (IoT), Smart Transportation & Smart Cities.

"Neural" : "New Generation Networked Neural Security" 14:15 6th June 2017

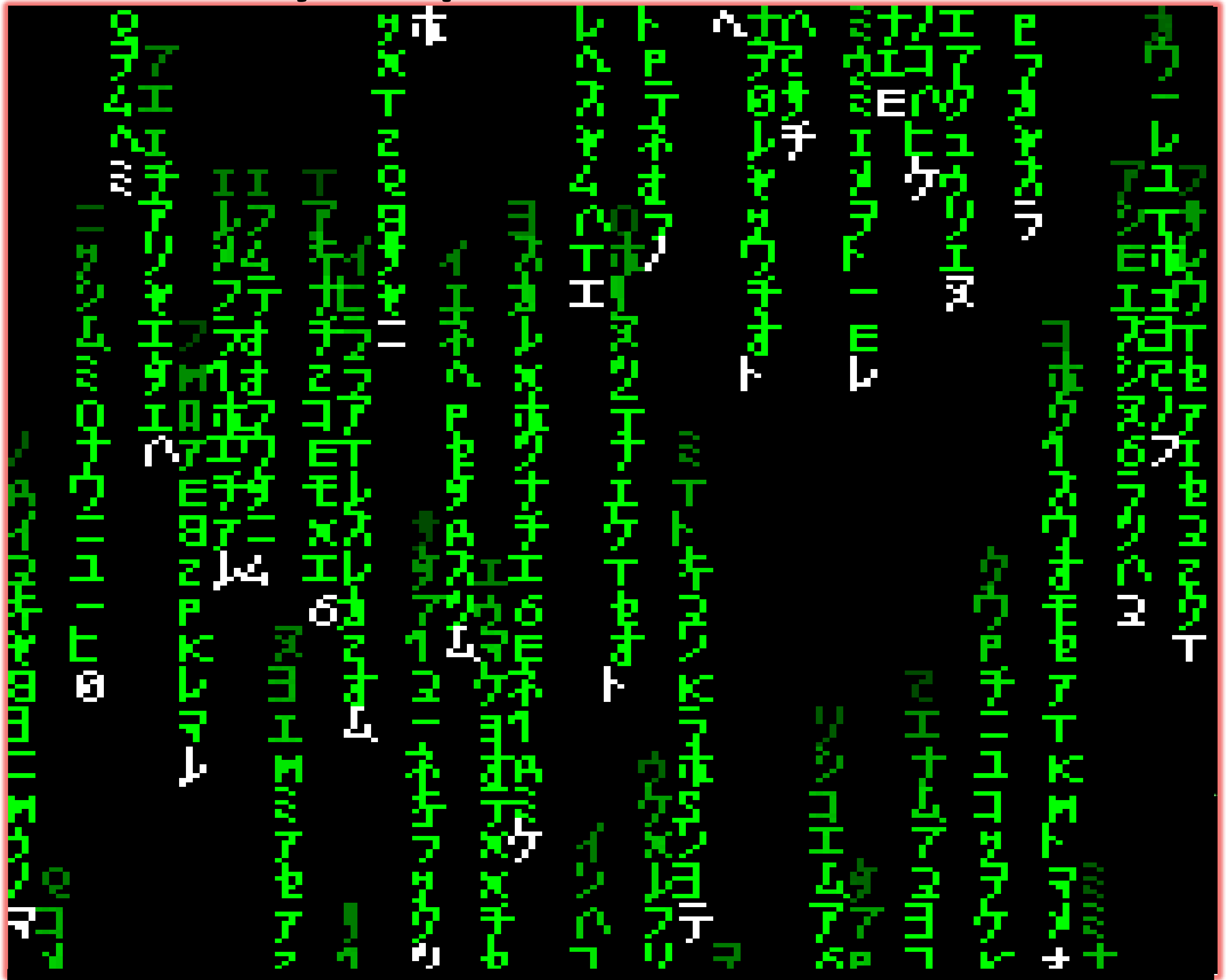
Download Slides: www.valentina.net/Genoa2017/

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



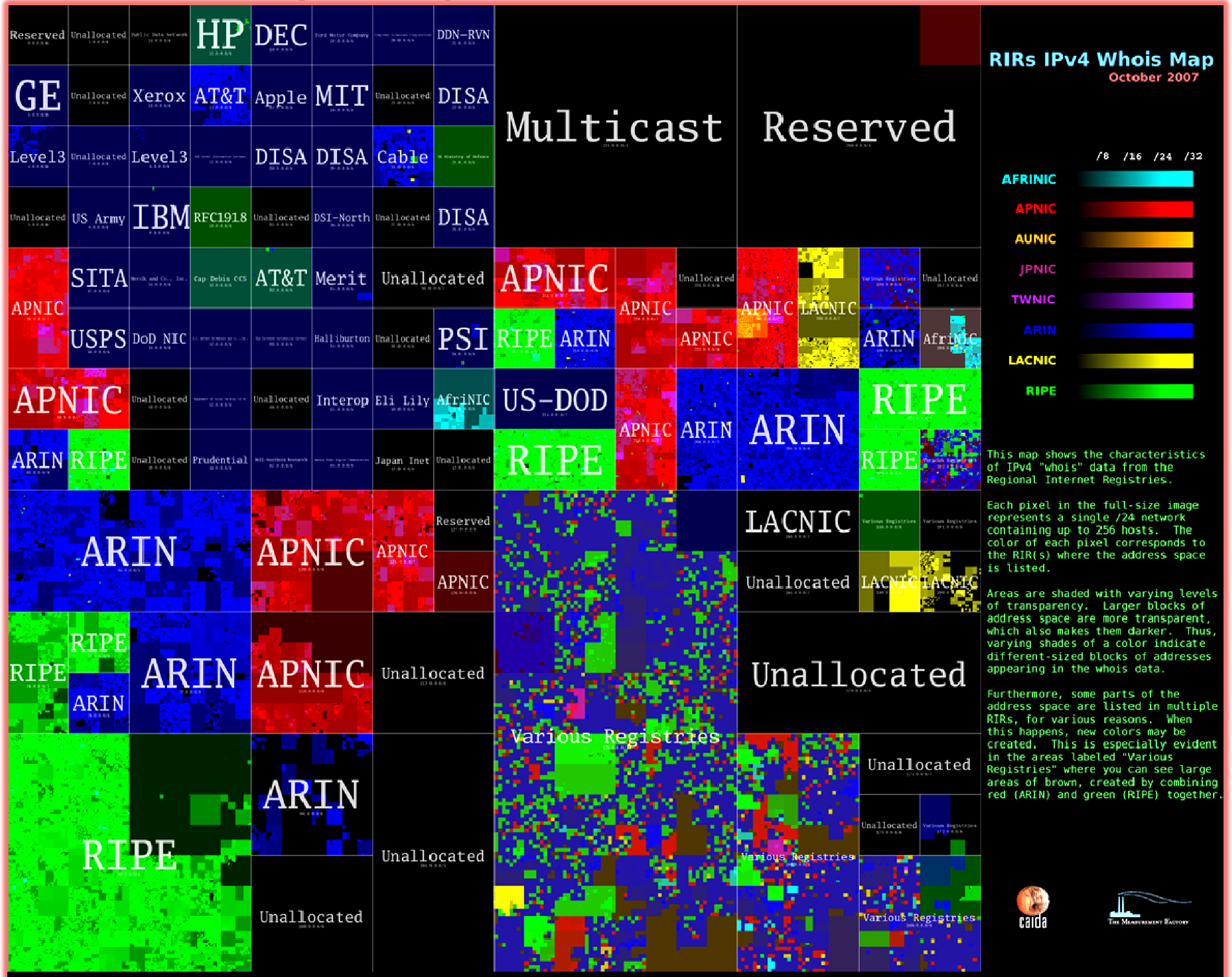
…From 19thC Physical World To 21stC Intelligent World

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



…From 19thC Physical World To 21stC Intelligent World

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



This map shows the characteristics of IPv4 "whois" data from the Regional Internet Registries.

Each pixel in the full-size image represents a single /24 network containing up to 256 hosts. The color of each pixel corresponds to the RIR(s) where the address space is listed.

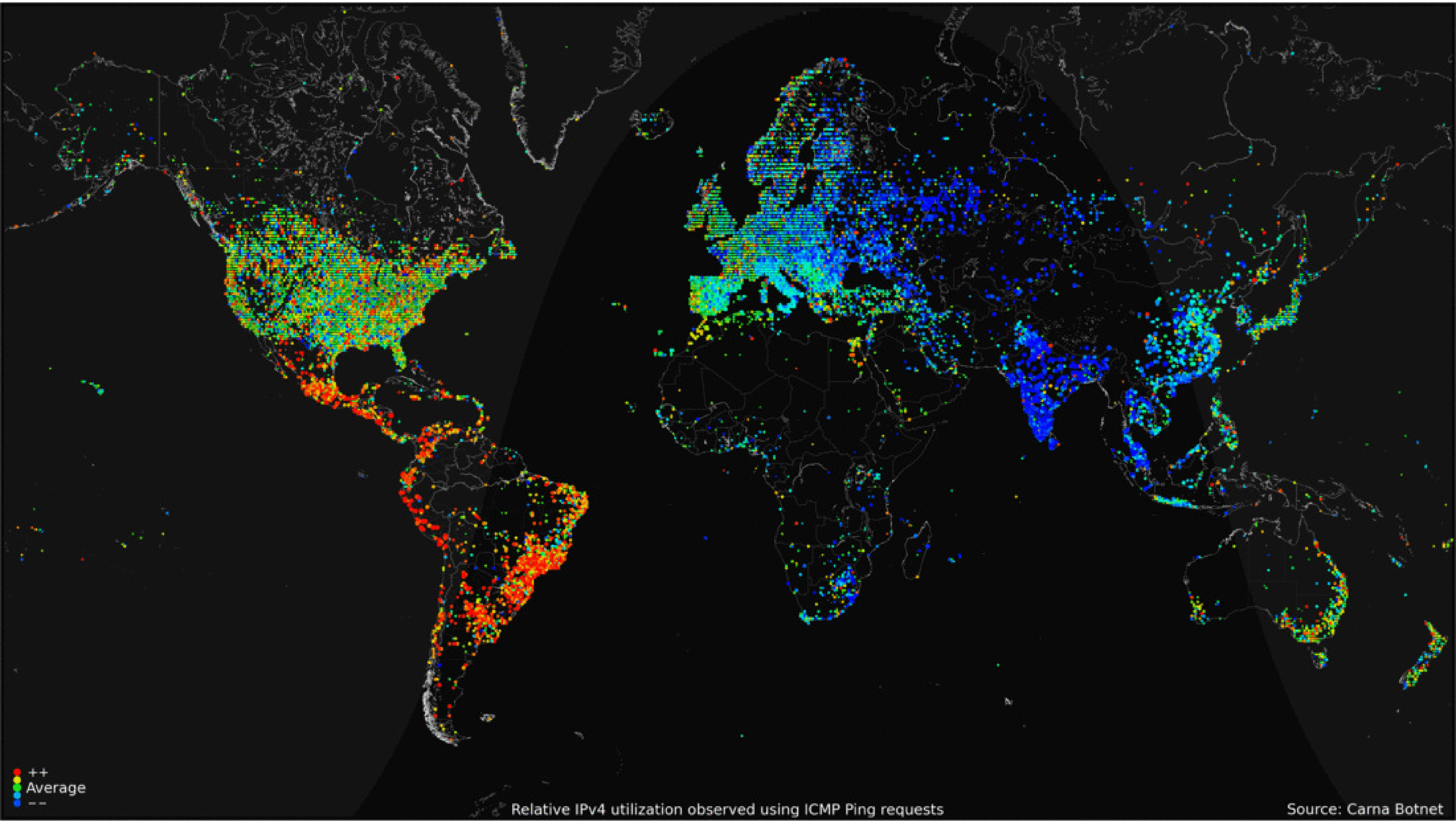
Areas are shaded with varying levels of transparency. Larger blocks of address space are more transparent, which also makes them darker. Thus, varying shades of a color indicate different-sized blocks of addresses appearing in the whois data.

Furthermore, some parts of the address space are listed in multiple RIRs, for various reasons. When this happens, new colors may be created. This is especially evident in the areas labeled "Various Registries" where you can see large areas of brown, created by combining red (ARIN) and green (RIPE) together.

…From 19thC Physical World To 21stC Intelligent World

GeoVision 24/7 Internet Connectivity

- “Carna Botnet Internet Census 2012” -



Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet

"Cybernetics & Security": 1943 - 2018!

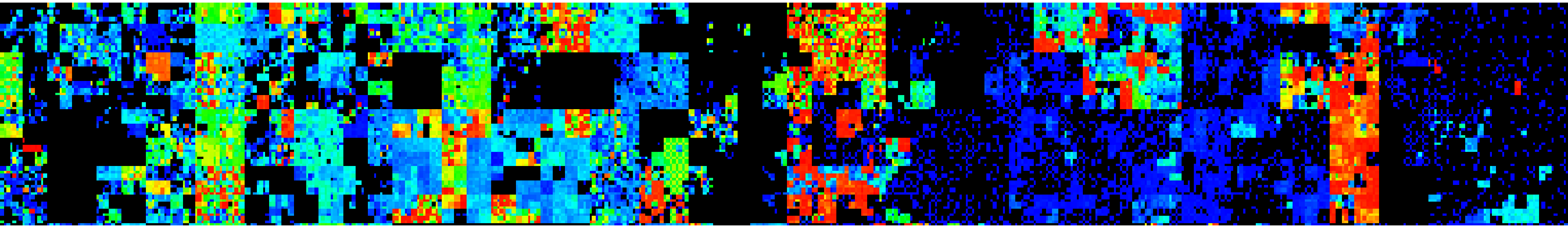
- Back to the Future: The Last 75 Years! -

- 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 - 1st "Apple Computer Virus
- 1986 – "Brain" – 1st Microsoft MS-DOS Virus
- 1988 – 1st "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!*

“Practical Cyber Defence”: TOP 10 Cyber Threats!

1 –“*Cyber Crime, Cyber Terror & Cyber War*”	2 – Countdown to TOP 10 Cyber Threats!	3 – 21stC Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools “Exploration”	5 – Cyber Entry & Exit Routes & Tools “Penetration”	6 – Real-Time Cyber Alert: Hack & Attack! “Cyber Attack!”
7 – In-Depth: 21stC Technical Cyber Defence	8– ***YOUR*** Operational Cyber Defence	9 –***YOUR*** Cyber Defence Campaign Plan!



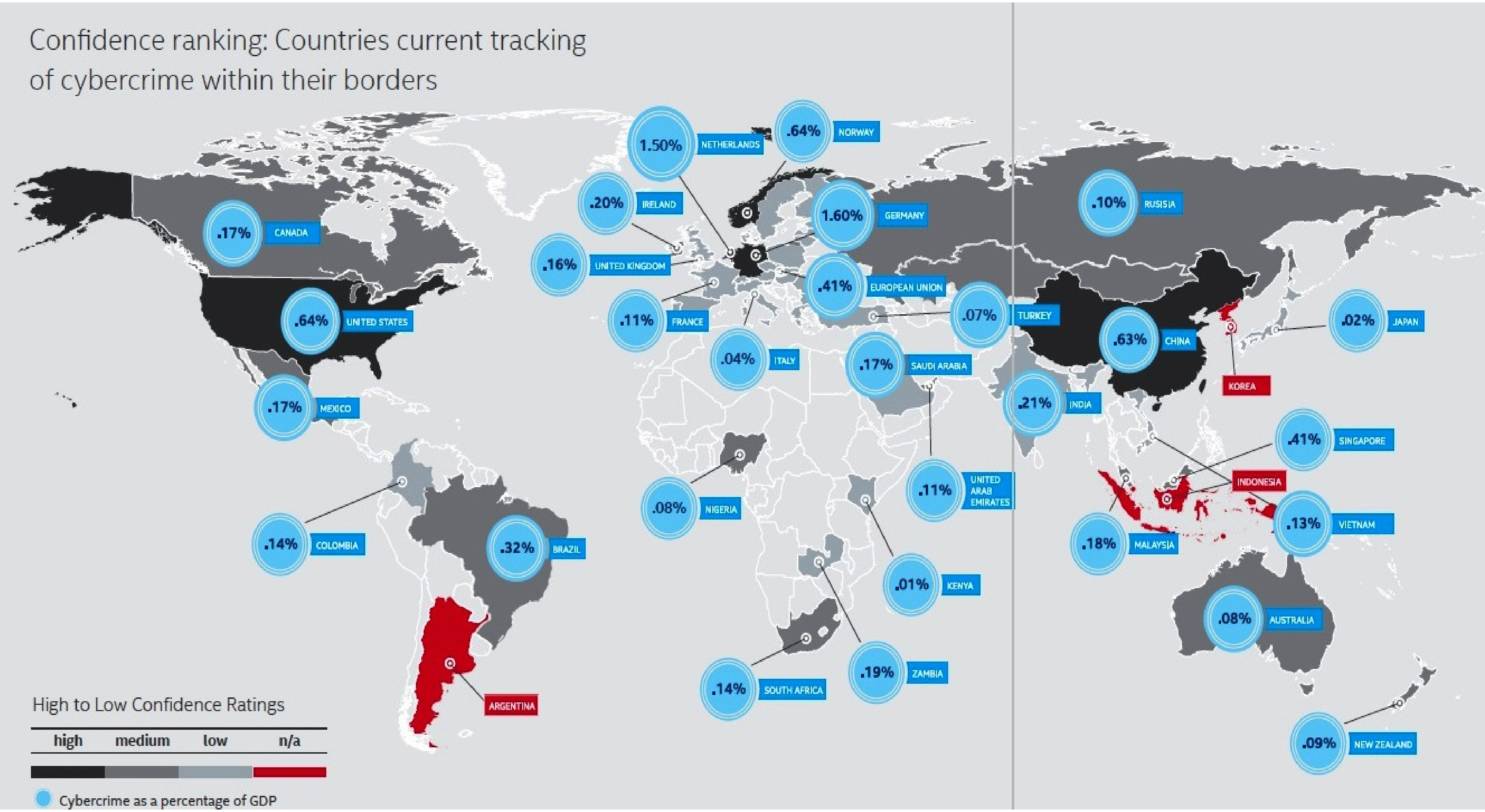
"CyberCrime, CyberTerror & CyberWar"

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) -



Confidence ranking: Countries current tracking of cybercrime within their borders

World Economic Forum: Global CyberCrime

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

Net Losses: Estimating the Global Cost of Cybercrime

Economic impact of cybercrime II

Center for Strategic and International Studies
June 2014

Confidence ranking: C
of cybercrime within t
.17%
CA
.17
.14
High to Low Confidence Ratings
high
medium
low
n
Cybercrime as a percentage of GDP
SISIA
CHINA
.02%
JAPAN
KOREA
.41%
SINGAPORE
INDONESIA
.13%
VIETNAM
YSIA
.08%
AUSTRALIA
.09%
NEW ZEALAND

World Economic Forum: Global CyberCrime

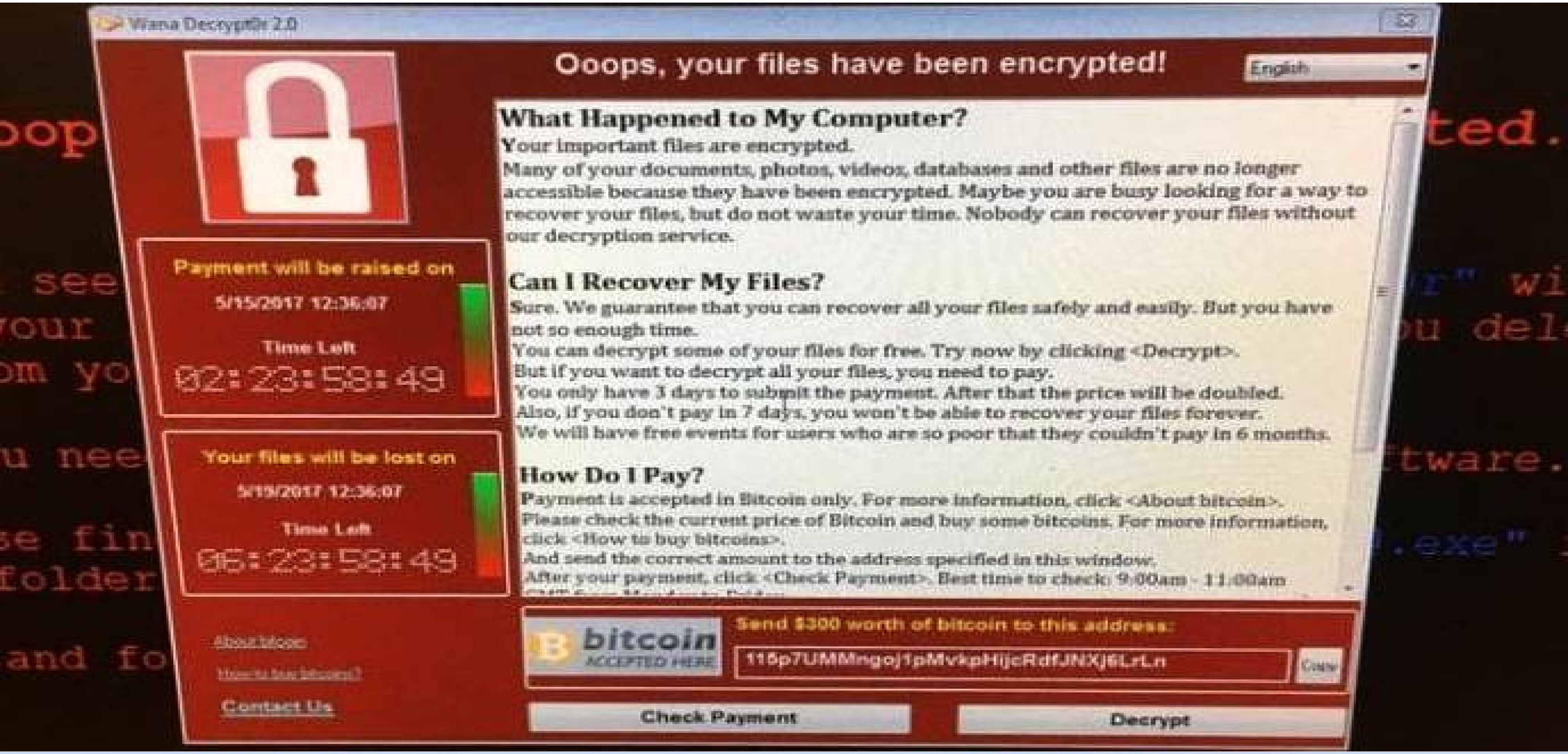
- $445Billion (Intel Research : June 2014) -

Red Alert!

– In-Coming Cyber Attack! –

Global RansomWare CyberAttack

"WanaCrypt0r 2.0" - 12th May 2017



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49

Your files will be lost on
5/19/2017 12:36:07
Time Left
05:23:58:49

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

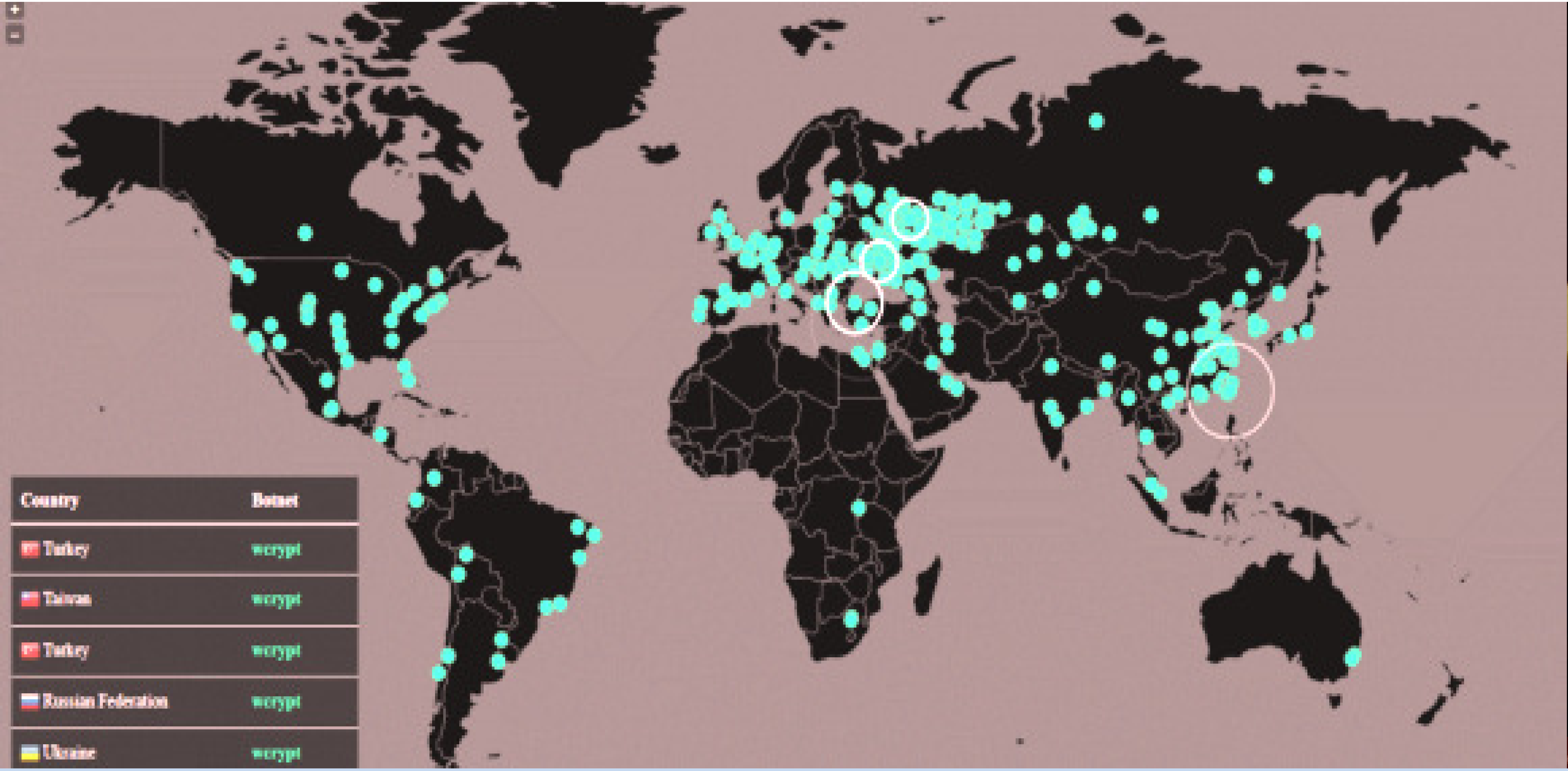
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

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



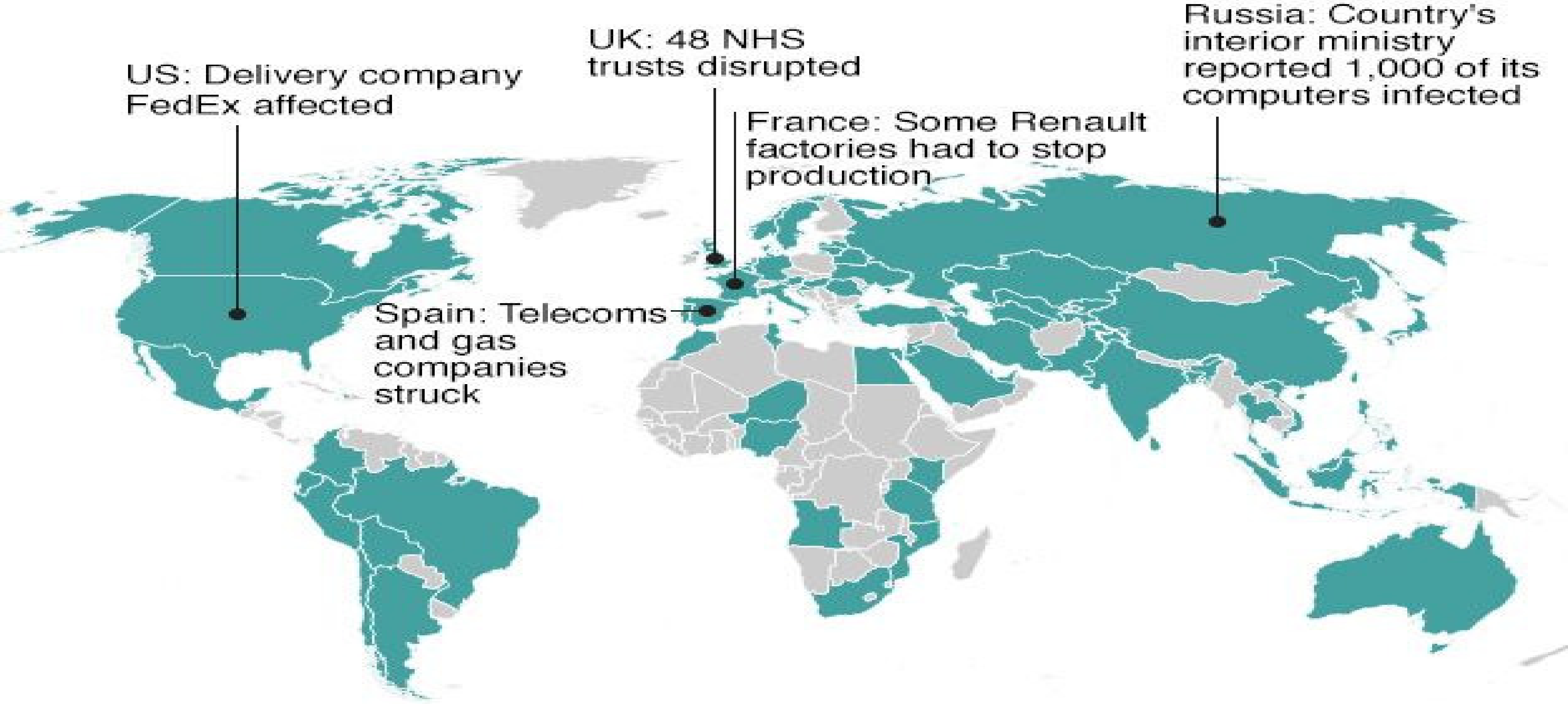
Country	Botnet
Turkey	wcrypt
Taiwan	wcrypt
Turkey	wcrypt
Russian Federation	wcrypt
Ukraine	wcrypt

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

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

Global RansomWare CyberAttack

Countries hit in initial hours of cyber-attack



US: Delivery company FedEx affected

UK: 48 NHS trusts disrupted

France: Some Renault factories had to stop production

Russia: Country's interior ministry reported 1,000 of its computers infected

Spain: Telecoms and gas companies struck

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

Source: Kaspersky Lab's Global Research & Analysis Team

BBC

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

Guide to Cyber Scams: March 2017

Recommended!

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

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

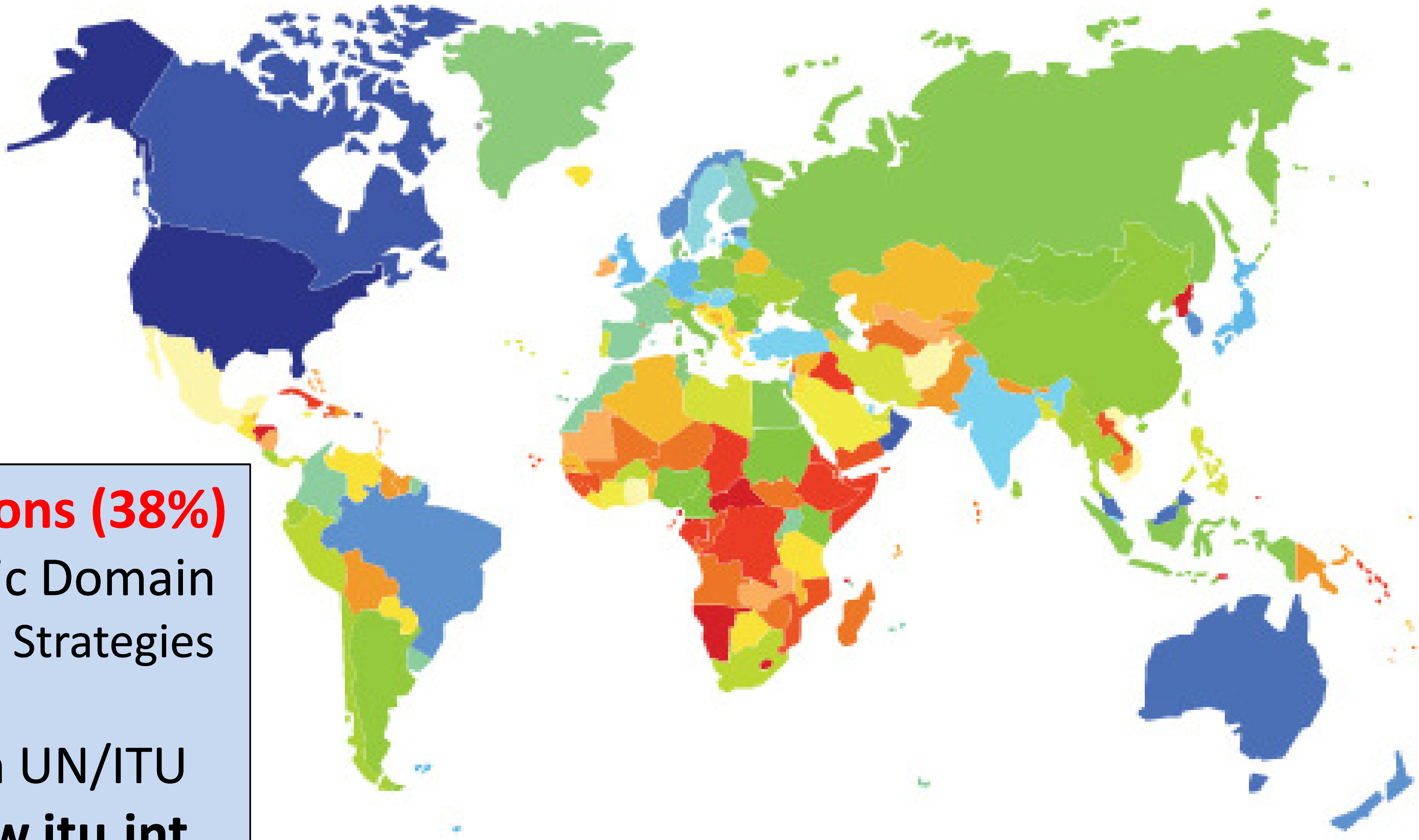
Practical Guide on Development and Execution

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

UN/ITU – Global Cybersecurity Index



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

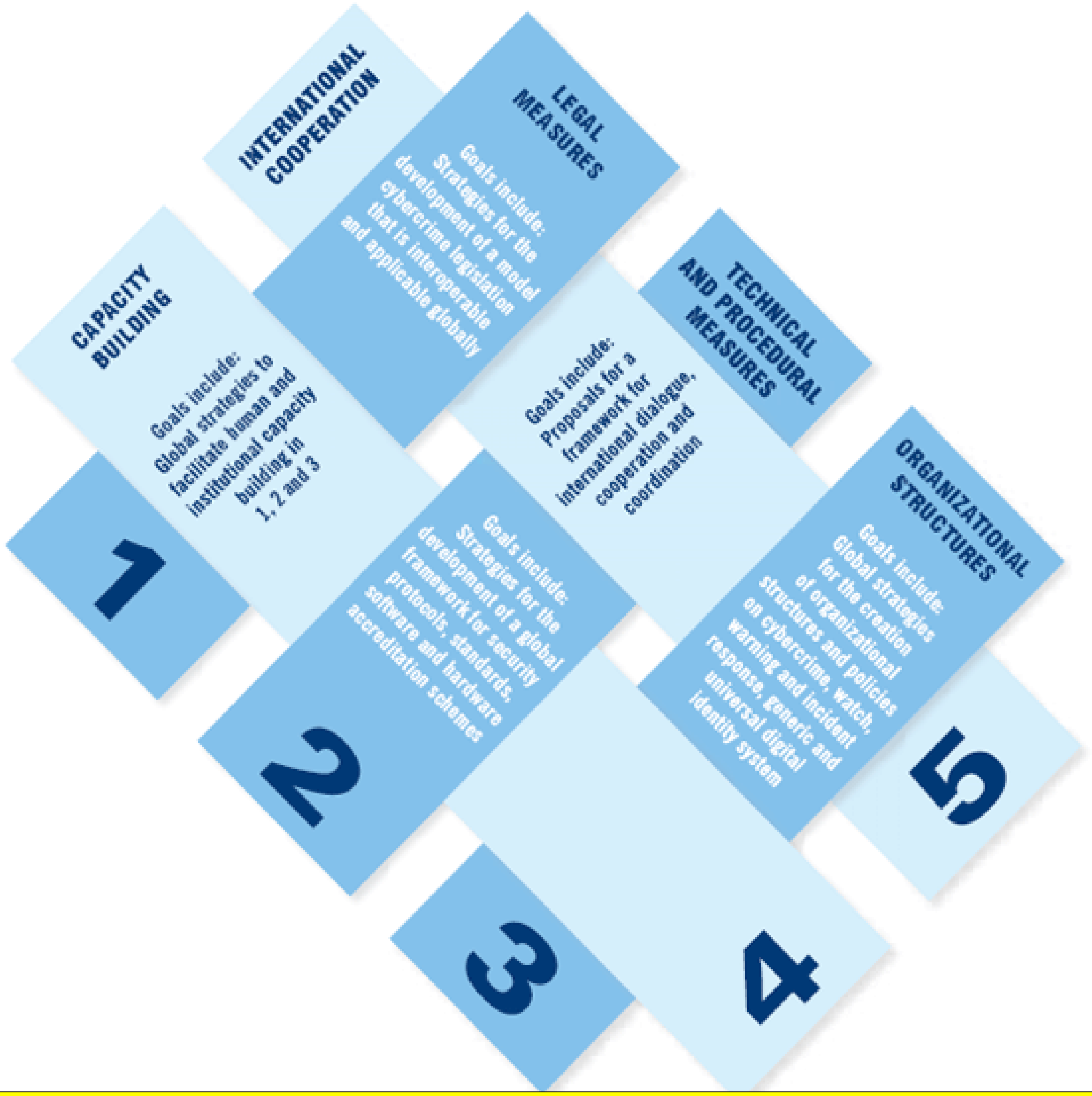
Available on UN/ITU
Website: **ww.itu.int**

ABIresearch

ITU

Global
Cybersecurity
Index

UN/ITU: Global Cybersecurity Agenda


INTERNATIONAL COOPERATION
LEGAL MEASURES
Goals include: Strategies for the development of a model cybercrime legislation that is interoperable and applicable globally
CAPACITY BUILDING
Goals include: Global strategies to facilitate human and institutional capacity building in 1, 2 and 3
TECHNICAL AND PROCEDURAL MEASURES
Goals include: Proposals for a framework for international dialogue, cooperation and coordination
ORGANIZATIONAL STRUCTURES
Goals include: Strategies for the development of a global framework for security protocols, standards, software and hardware accreditation schemes
Goals include: Global strategies for the creation of organizational structures and policies on cybercrime, watch, warning and incident response, generic and universal digital identity system
1
2
3
4
5

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

EGTI
Estratégia Geral de Tecnologia da Informação
2013 / 2015
SISP
Versão 1.0

Islamic Republic of Afghanistan
Ministry of Communications and IT
National Cyber Security Strategy of Afghanistan (NCSA)
Prevention - Protection - Safety - Resiliency

Ministry of Defence
THE DEFENCE CYBER STRATEGY

NORWEGIAN MINISTRIES
Strategy
Cyber Security Strategy for Norway

SINGAPORE'S CYBERSECURITY STRATEGY

Federal Ministry of the Interior
Cyber Security Strategy for Germany

NATIONAL CYBER SECURITY STRATEGY
GOVERNMENT OF JAMAICA

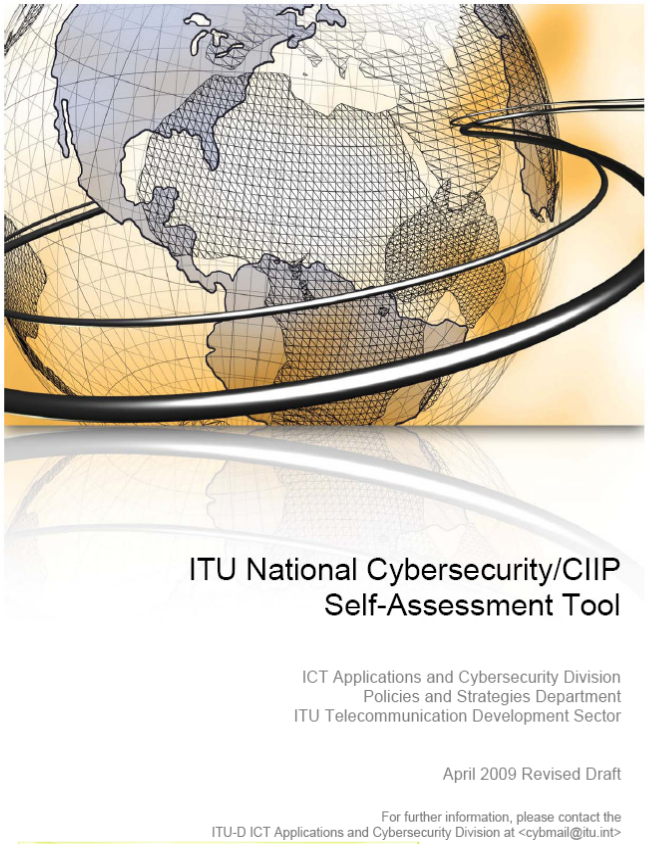
وزارة الاتصالات وتقنية المعلومات
Ministry of Communications and Information Technology
Developing National Information Security Strategy for the Kingdom of Saudi Arabia
NISS, Draft 7
National Information Security Strategy

Gov
NATIONAL ICT STRATEGY AND PLAN
NICI - 2015

THE DOD CYBER STRATEGY
THE DEPARTMENT OF DEFENSE

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

United Nations/ITU Cybersecurity Guides

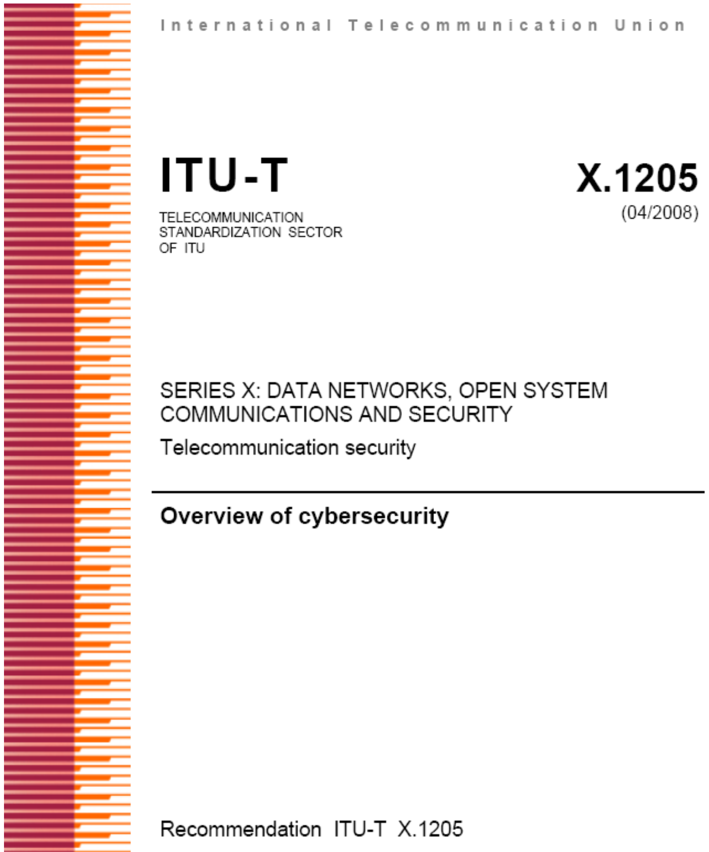


ITU National Cybersecurity/CIIP Self-Assessment Tool

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

April 2009 Revised Draft

For further information, please contact the
ITU-D ICT Applications and Cybersecurity Division at <cybmail@itu.int>



International Telecommunication Union

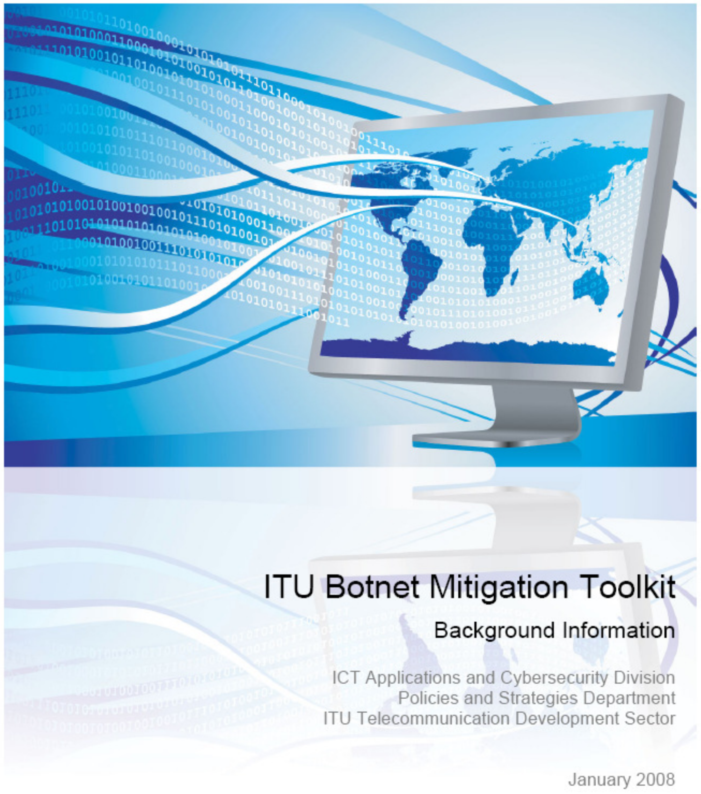
ITU-T
TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1205
(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY
Telecommunication security

Overview of cybersecurity

Recommendation ITU-T X.1205

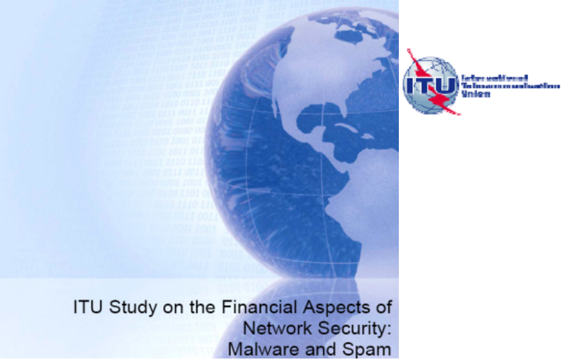


ITU Botnet Mitigation Toolkit
Background Information

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

January 2008

ICTs for e-Environment
Guidelines for Developing Countries,
with a Focus on Climate Change



ITU Study on the Financial Aspects of Network Security:
Malware and Spam

Cybersecurity Guide
for Developing Countries

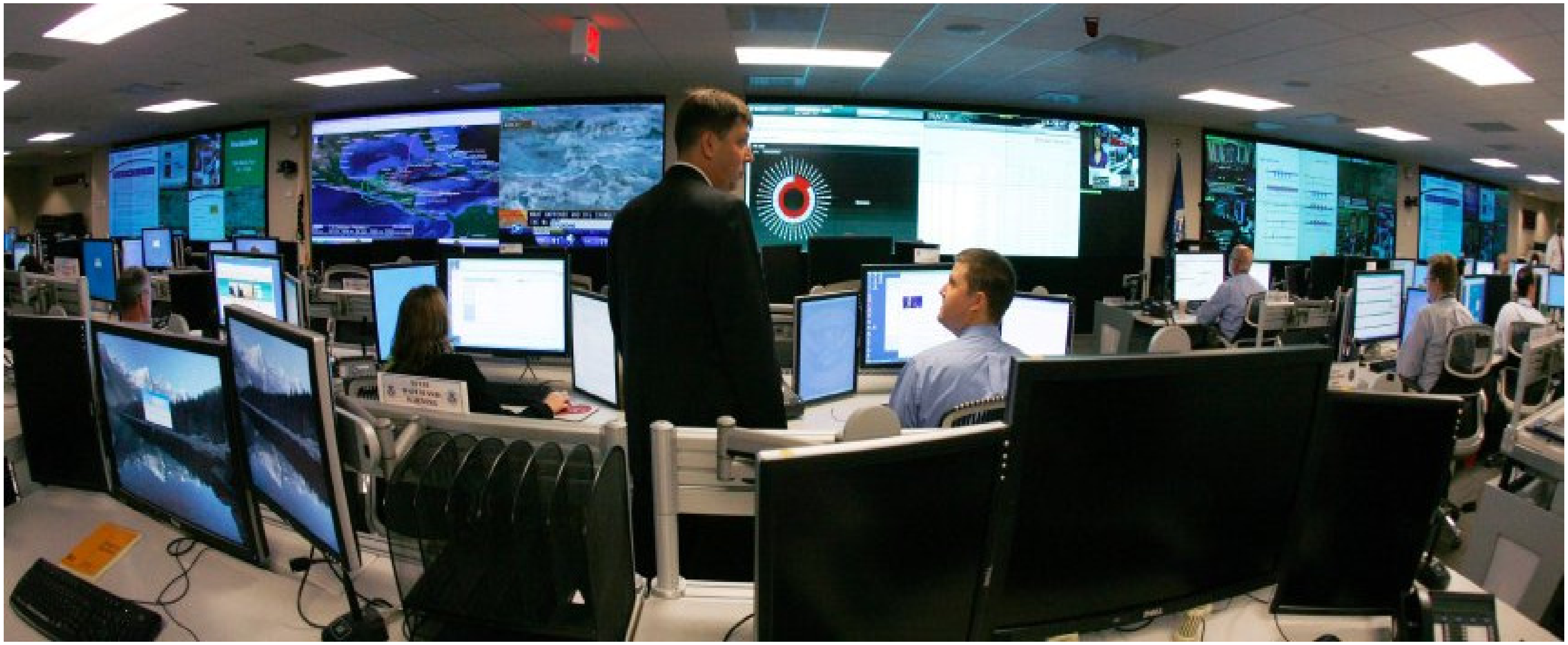
- UN/ITU *CyberSecurity* Agenda -

Quest for CyberConfidence (Eng/Rus)

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

"CyberSecurity USA": Critical Infrastructure

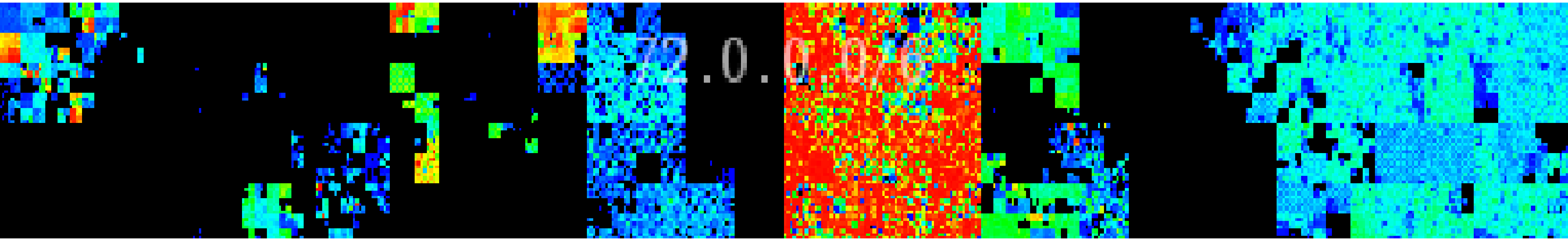
- **11th May 2017**: Presidential Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"



- **NIST Mandated: "**Framework for Improving Critical Infrastructure Cybersecurity"– **2017**

"Practical Cyber Defence": TOP 10 Cyber Threats!

1 – Cyber Crime, Cyber Terror & Cyber War!	**2 – Countdown to TOP 10 Cyber Threats!**	3 – 21stC Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert: Hack & Attack! **"Cyber Attack"**
7 – In-Depth: 21stC Technical Cyber Defence	8 – ***YOUR*** Operational Cyber Defence	9 –***YOUR*** Cyber Defence Campaign Plan!



“Countdown to TOP 10 Cyber Threats!”

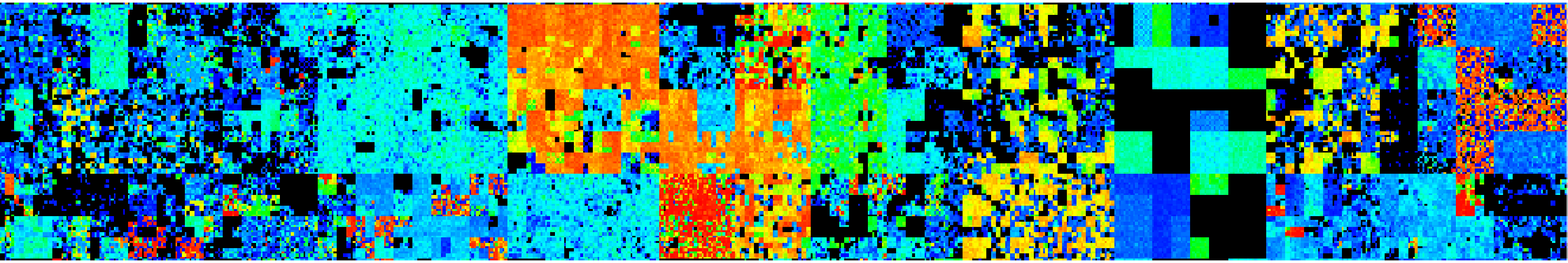
- **TOP Cyber Threats** may be roughly classified by Role during Criminal/Political Cyber Campaign:

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!...

"Practical Cyber Defence": TOP 10 Cyber Threats!

1 – Cyber Crime, Cyber Terror & Cyber War	2 – Countdown to TOP 10 Cyber Threats!	3 – 21stC Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools "Exploration"	5 – Cyber Entry & Exit Routes & Tools "Penetration"	6 – Real-Time Cyber Alert: Hack & Attack! "Cyber Attack"
7 – In-Depth: 21stC Technical Cyber Defence	8 – *YOUR* Operational Cyber Defence	9 – *YOUR* Cyber Defence Campaign Plan!

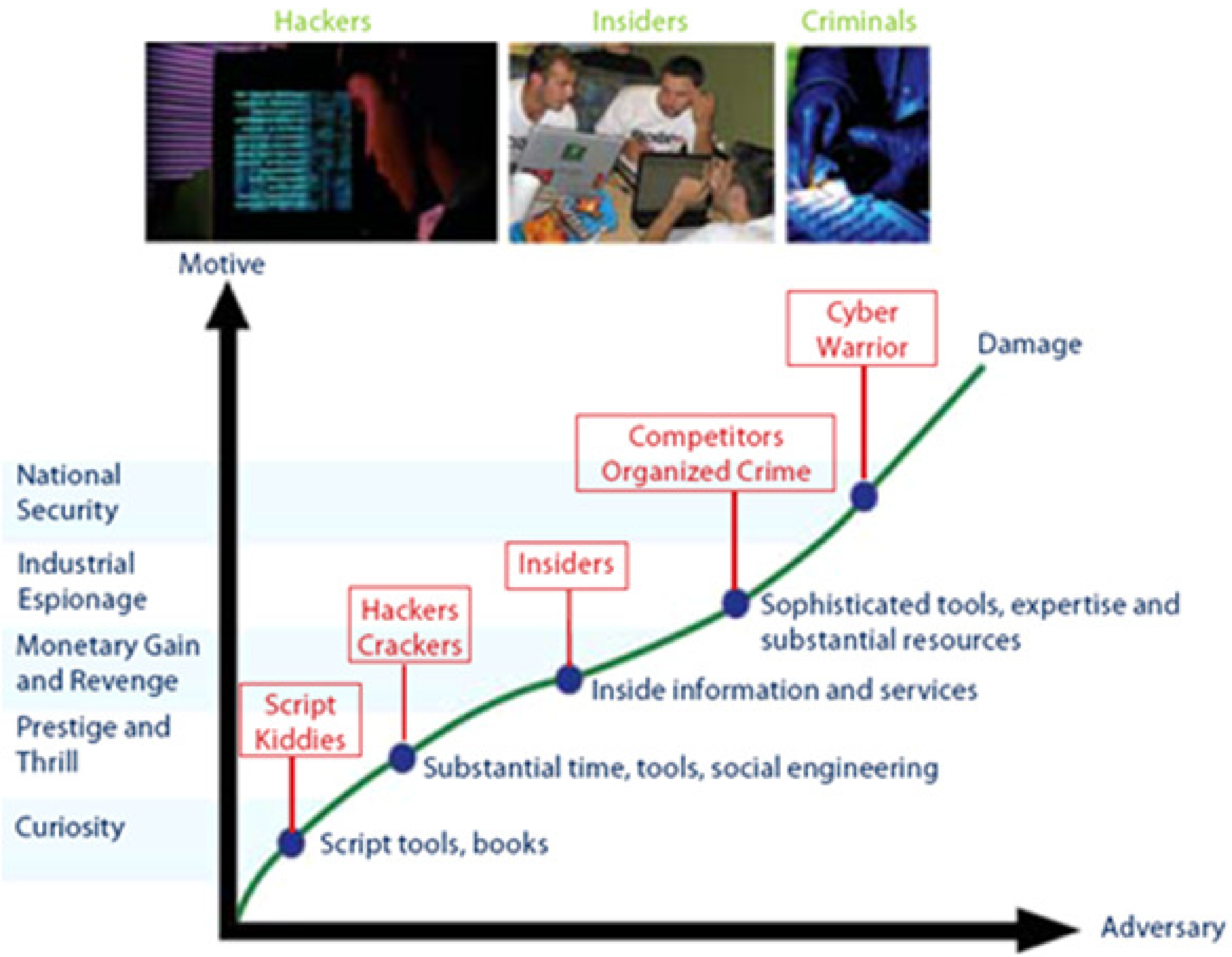


“21stC Cyber Hack & Attack Campaigns”

- **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...

Hierarchy of **Cyber Hacking Skills!**


Hackers
Insiders
Criminals
Motive
Cyber Warrior
Damage
Competitors Organized Crime
National Security
Industrial Espionage
Insiders
Sophisticated tools, expertise and substantial resources
Hackers Crackers
Monetary Gain and Revenge
Inside information and services
Script Kiddies
Prestige and Thrill
Substantial time, tools, social engineering
Curiosity
Script tools, books
Adversary

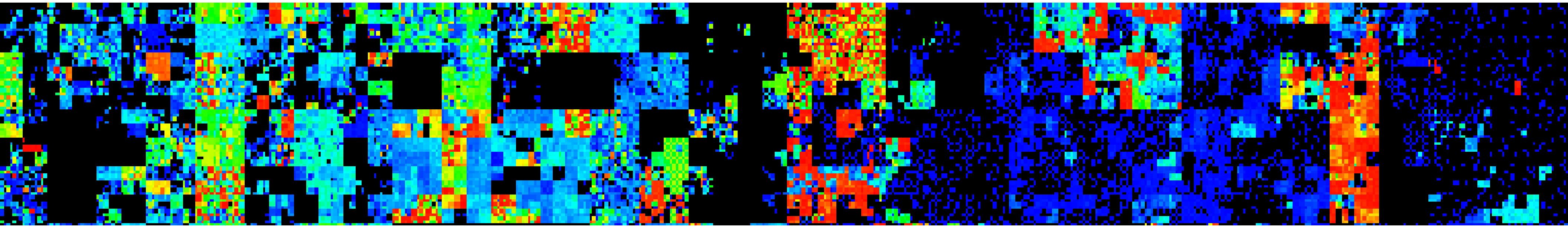
Cyber Criminal Team **Skillset**!...

- 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*!

"Practical Cyber Defence": TOP 10 Cyber Threats!

1 – Cyber Crime, Cyber Terror & Cyber War	2 – Countdown to TOP 10 Cyber Threats!	3 – 21stC Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert: Hack & Attack! **"Cyber Attack"**
7 –In-Depth: 21stC Technical Cyber Defence	8 – ***YOUR*** Operational Cyber Defence	9 – ***YOUR*** Cyber Defence Campaign Plan!



“Cyber Intelligence Gathering Tools

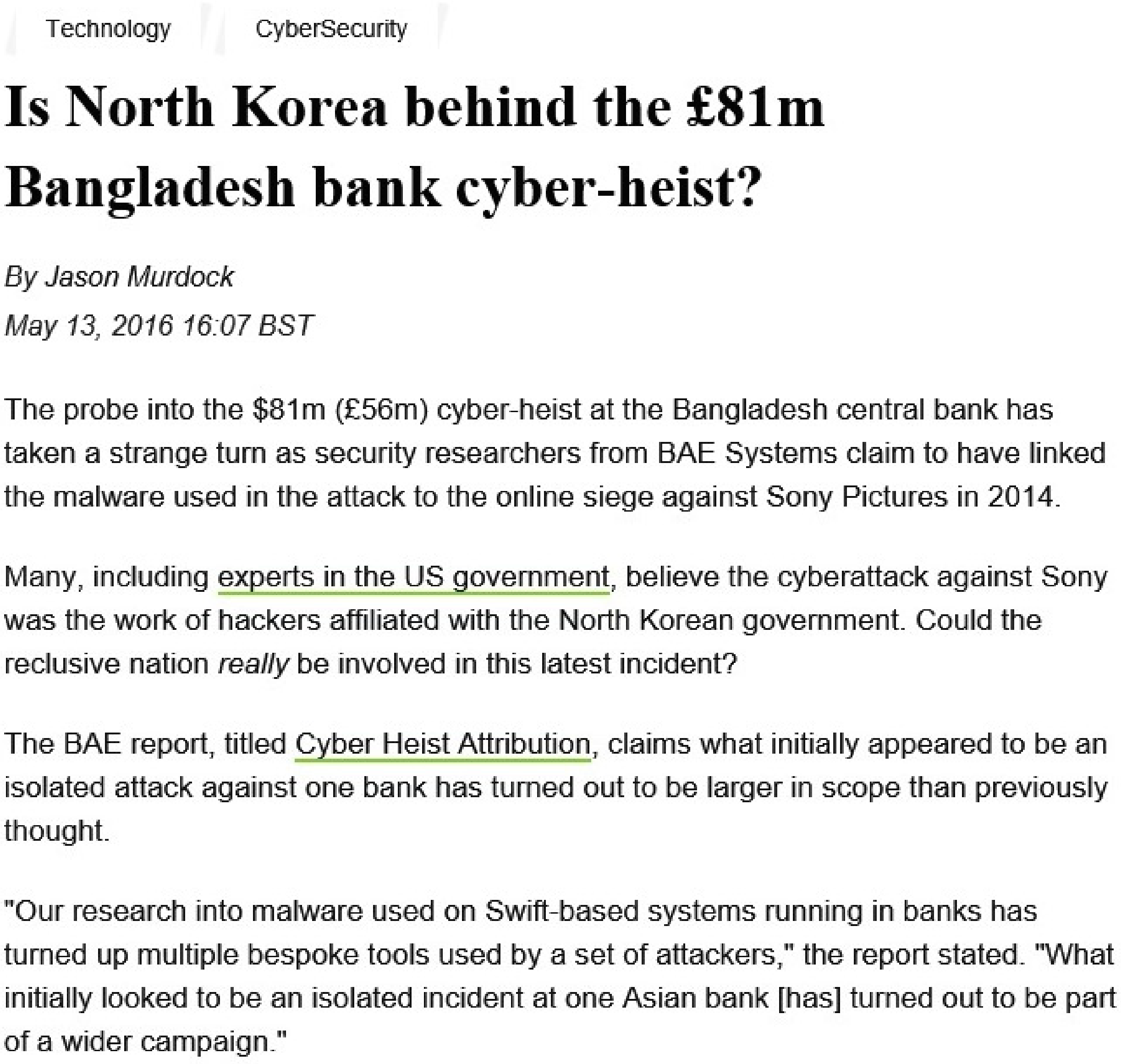
*** EXPLORATION ***

- 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!....

May 2016 : $81m Bank Cyber-Heist



Technology | CyberSecurity

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

By Jason Murdock

May 13, 2016 16:07 BST

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

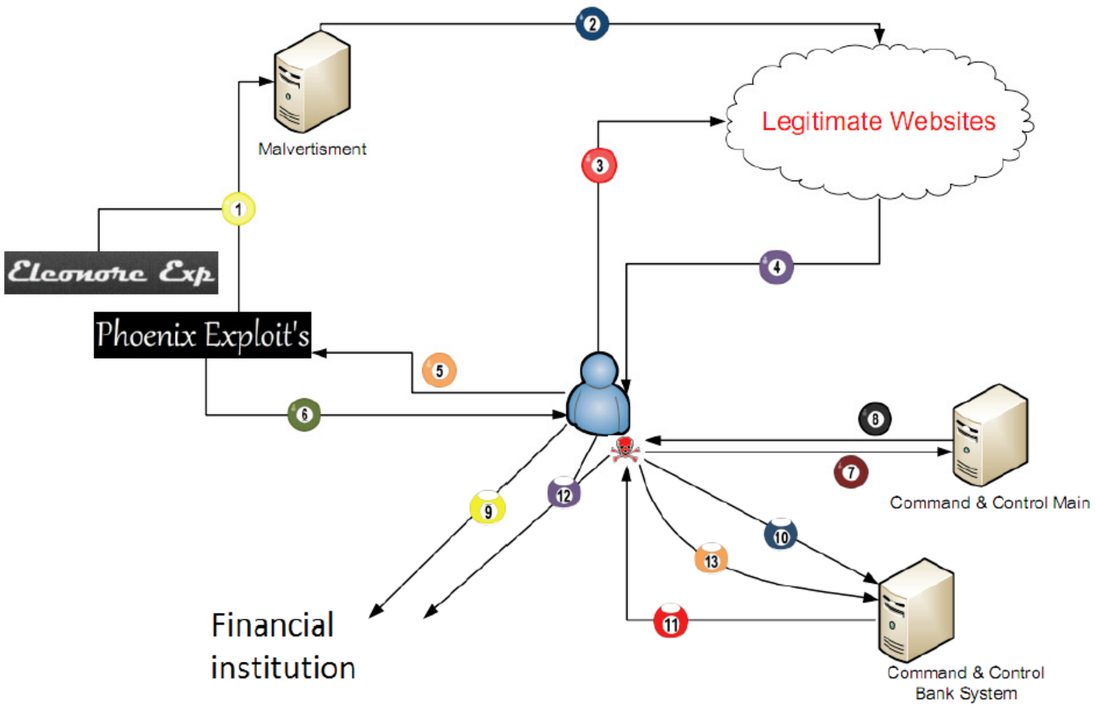
Many, including experts in the US government, believe the cyberattack against Sony was the work of hackers affiliated with the North Korean government. Could the reclusive nation *really* be involved in this latest incident?

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

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

International Business Times
- 13th May 2016 -

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



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

Source: White Paper by M86 Security: Aug 2010

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

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

CyberEspionage: *Middle East and Africa*

Desert Falcons. Victims of advanced targeted attack.

Activist · Education · Financial · Government · Industrial · Energy · Media · Political · Trade and commerce · Religious · Unknown

High infection rate (1500+)

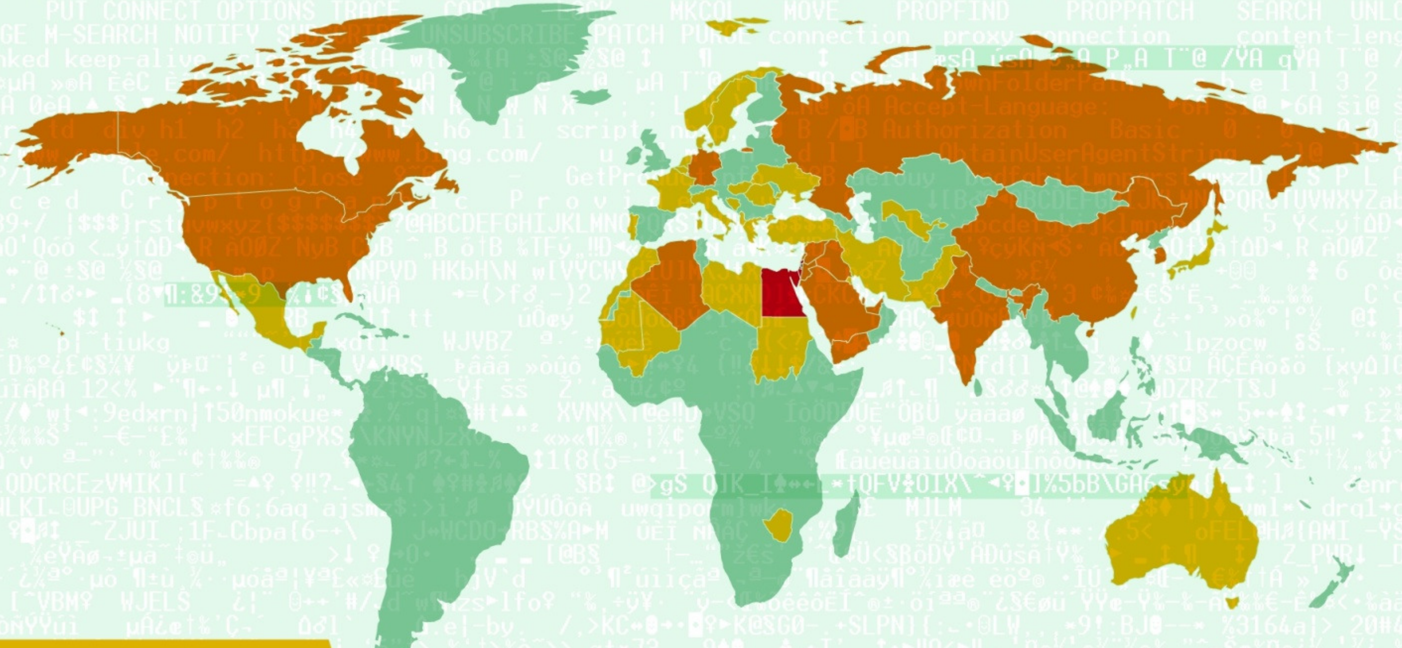
Palestine	Activist, Education, Financial, Government, Media, Political, Trade and commerce, Unknown

Medium infection rate (500+)

Egypt	Activist, Media, Political, Industrial, Religious, Trade and commerce, Unknown
Israel	Energy, Financial, Government, Industrial, Political, Trade and commerce, Unknown

Low infection rate (50+)

Jordan	Energy, Government, Industrial, Trade and commerce, Unknown
United Arabic Emirates	Media, Government, Unknown
Saudi Arabia	Government, Unknown
United States of America	Education, Unknown
South Korea	Industrial, Unknown
Russia Federation	Unknown
Lebanon	Unknown
Iraq	Unknown
Canada	Unknown
Qatar	Unknown
Germany	Unknown
China	Unknown
Syria	Unknown
Yemen	Unknown
Algeria	Unknown
India	Unknown

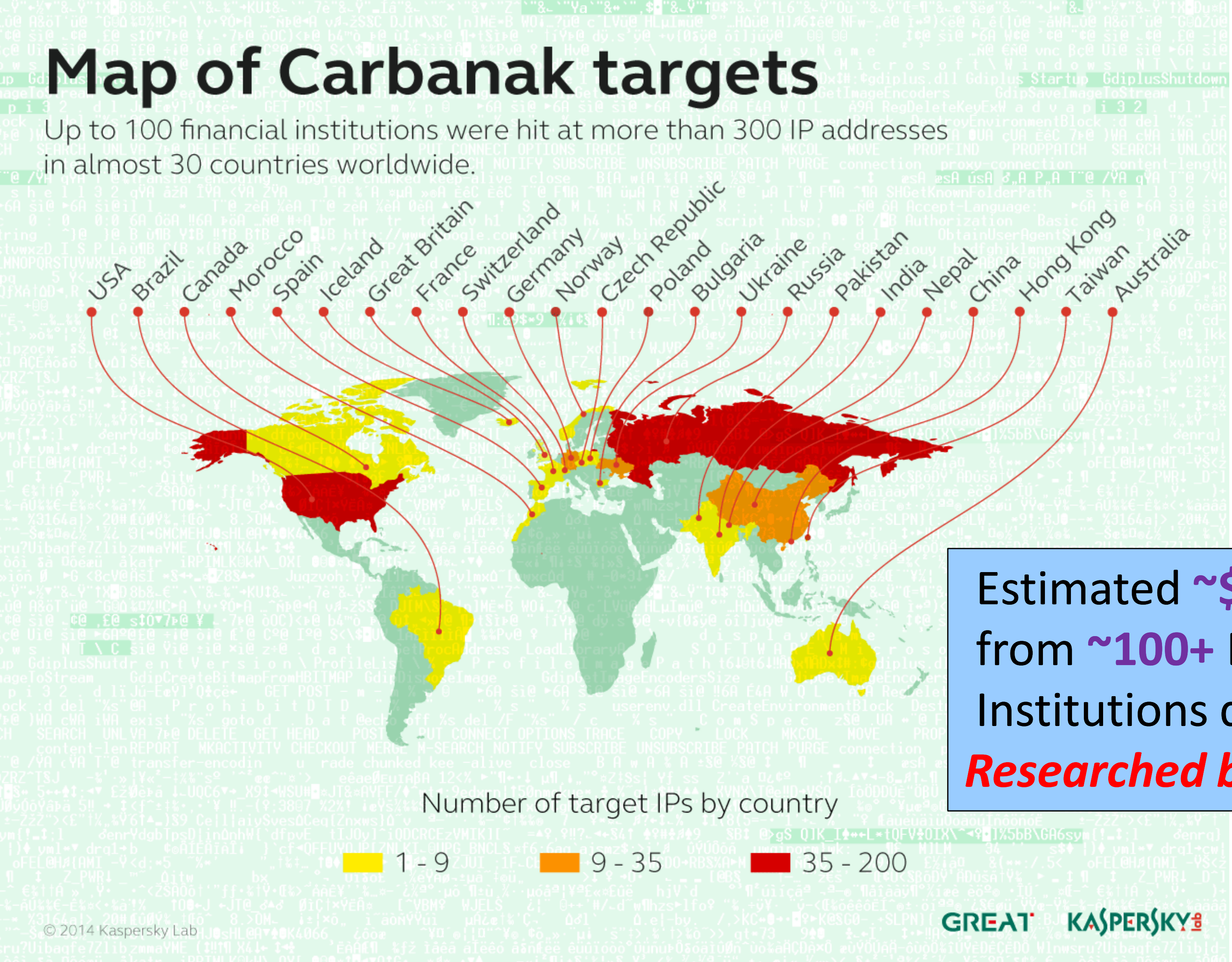


Lowest infection rate

Kuwait, Norway, Turkey, Sweden, France, Mexico, Morocco, Libya, Albania, Romania, Italy, Hungary, Australia, Japan, Zimbabwe, Uzbekistan, Ukraine, Taiwan, Sudan, Portugal, Mauritania, Mali, Iran, Greece, Cyprus, Belgium, Netherland, Pakistan, Denmark, Bosnia and Herzegovina (Unknown)

KASPERSKY lab

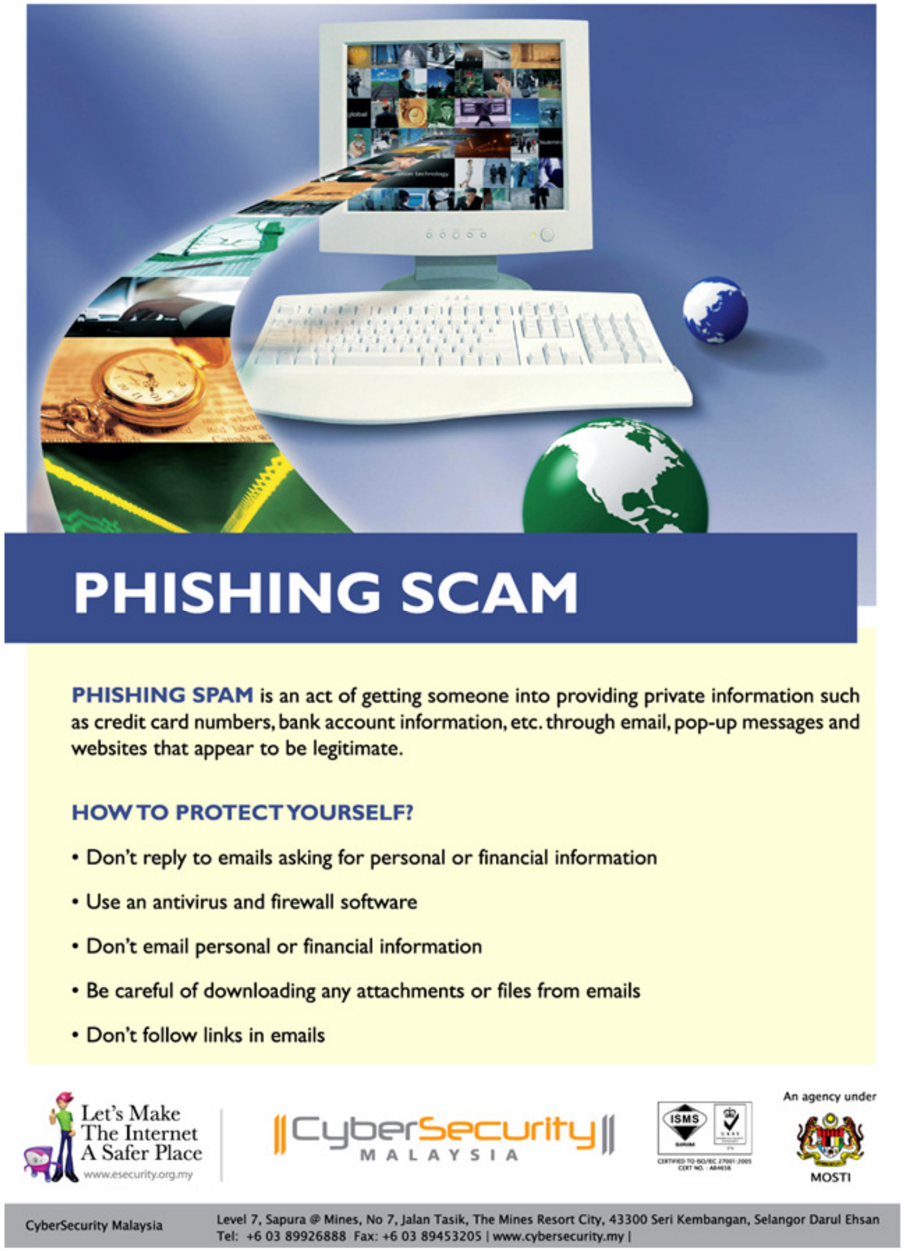
Cyber Threat: “Banking Theft”– Carbanak



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

Researched by “Kaspersky Labs”

Cyber Threats: Phishing and Identity Theft



PHISHING SCAM

PHISHING SPAM is an act of getting someone into providing private information such as credit card numbers, bank account information, etc. through email, pop-up messages and websites that appear to be legitimate.

HOW TO PROTECT YOURSELF?

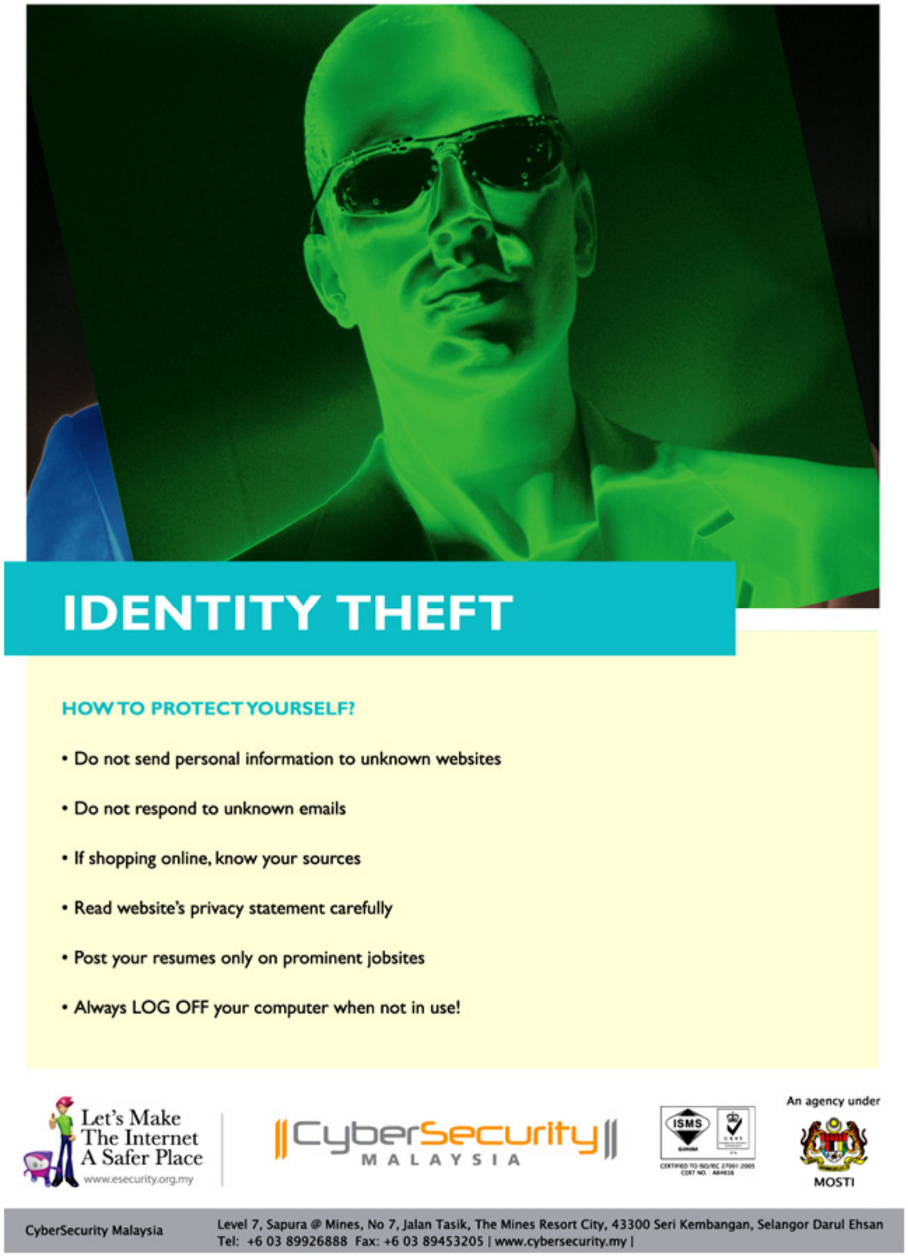
- Don't reply to emails asking for personal or financial information
- Use an antivirus and firewall software
- Don't email personal or financial information
- Be careful of downloading any attachments or files from emails
- Don't follow links in emails

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 |



IDENTITY THEFT

HOW TO PROTECT YOURSELF?

- Do not send personal information to unknown websites
- Do not respond to unknown emails
- If shopping online, know your sources
- Read website's privacy statement carefully
- Post your resumes only on prominent jobsites
- Always LOG OFF your computer when not in use!

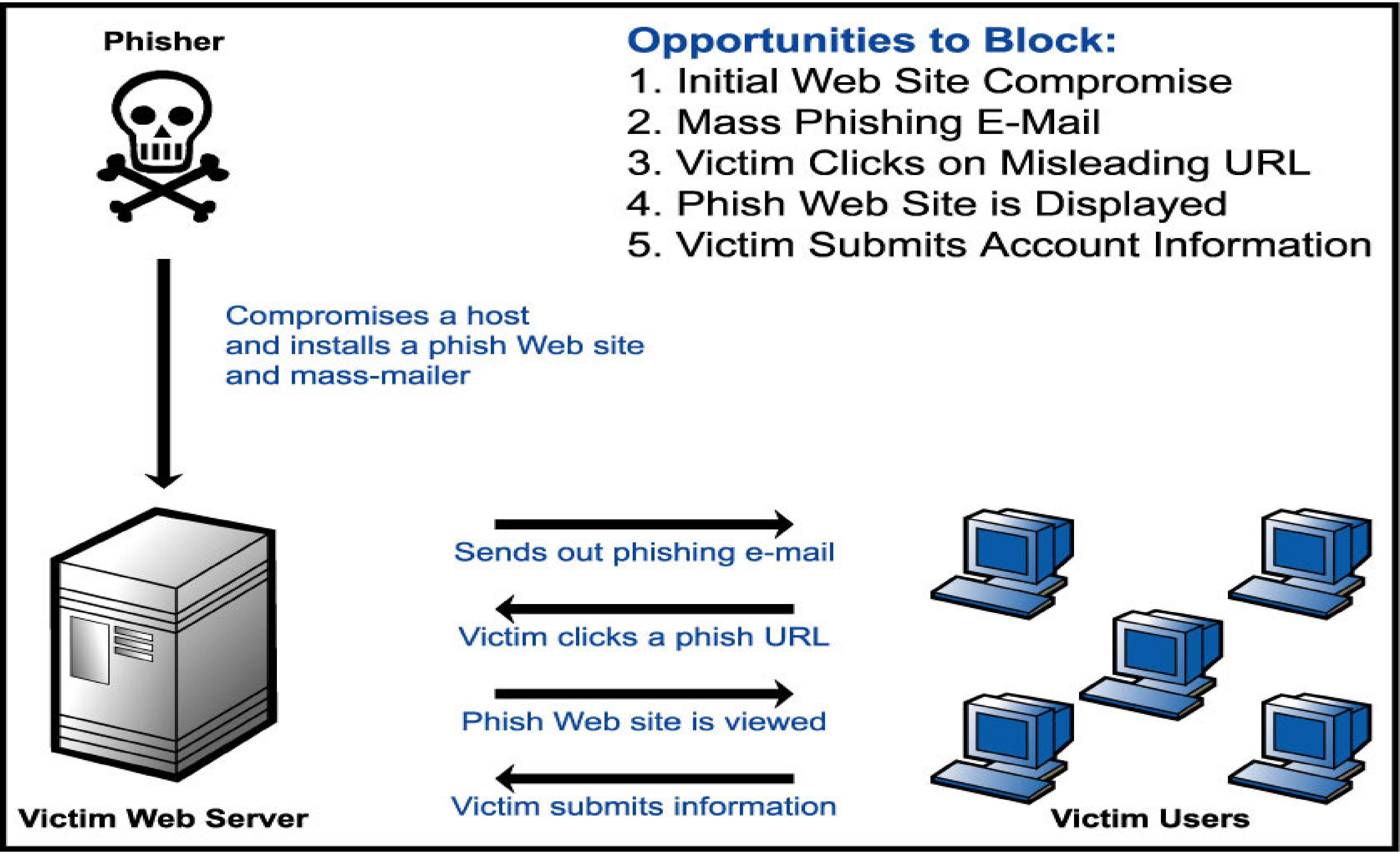
Let's Make The Internet A Safer Place
www.esecurity.org.my

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 |

Phishing Attack: Typical "Cyber Hacking" Process



Phisher

Opportunities to Block:

1. Initial Web Site Compromise
2. Mass Phishing E-Mail
3. Victim Clicks on Misleading URL
4. Phish Web Site is Displayed
5. Victim Submits Account Information

Compromises a host and installs a phish Web site and mass-mailer

Sends out phishing e-mail

Victim clicks a phish URL

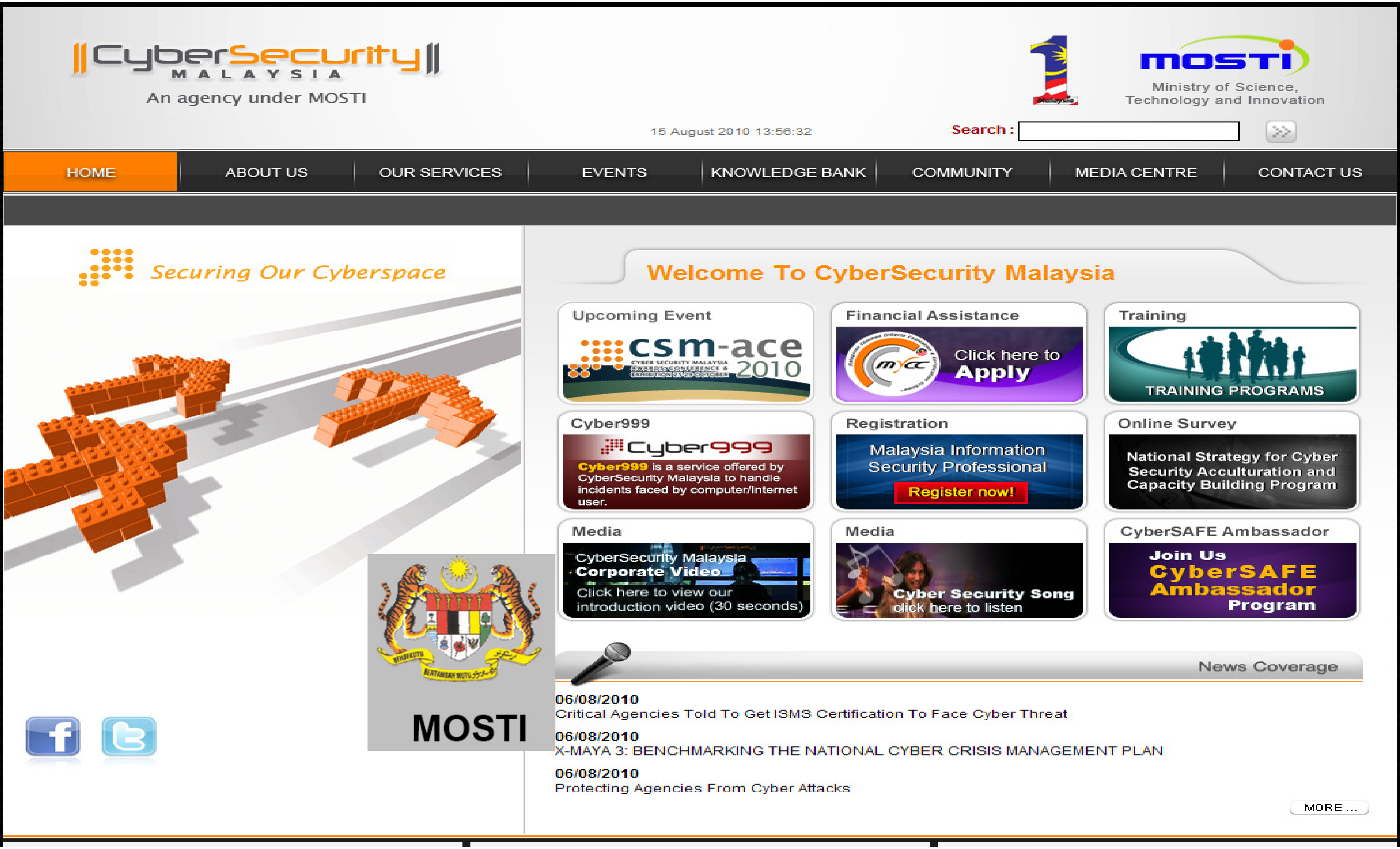
Phish Web site is viewed

Victim submits information

Victim Web Server

Victim Users

Malaysian Government: CyberSecurity



CyberSecurity MALAYSIA

An agency under MOSTI

MOSTI

Ministry of Science, Technology and Innovation

15 August 2010 13:56:32

Search :

HOME | ABOUT US | OUR SERVICES | EVENTS | KNOWLEDGE BANK | COMMUNITY | MEDIA CENTRE | CONTACT US

Securing Our Cyberspace

MOSTI

Welcome To CyberSecurity Malaysia

Upcoming Event: csm-ace 2010

Financial Assistance: Click here to Apply

Training: TRAINING PROGRAMS

Cyber999: Cyber999 is a service offered by CyberSecurity Malaysia to handle incidents faced by computer/Internet user.

Registration: Malaysia Information Security Professional. Register now!

Online Survey: National Strategy for Cyber Security Acculturation and Capacity Building Program

Media: CyberSecurity Malaysia Corporate Video. Click here to view our introduction video (30 seconds)

Media: Cyber Security Song. click here to listen

CyberSAFE Ambassador: Join Us CyberSAFE Ambassador Program

News Coverage

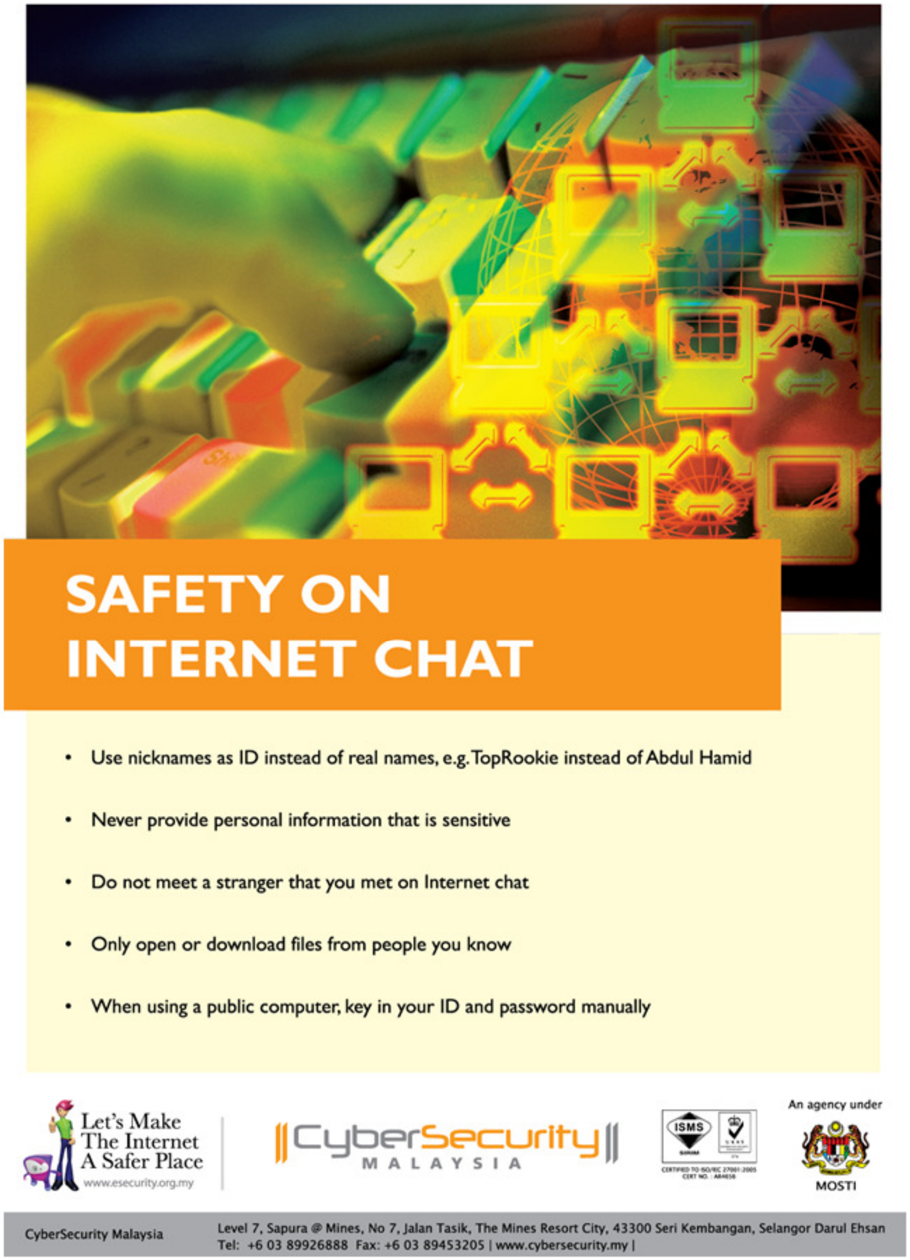
06/08/2010
Critical Agencies Told To Get ISMS Certification To Face Cyber Threat

06/08/2010
X-MAYA 3: BENCHMARKING THE NATIONAL CYBER CRISIS MANAGEMENT PLAN

06/08/2010
Protecting Agencies From Cyber Attacks

MORE ...

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

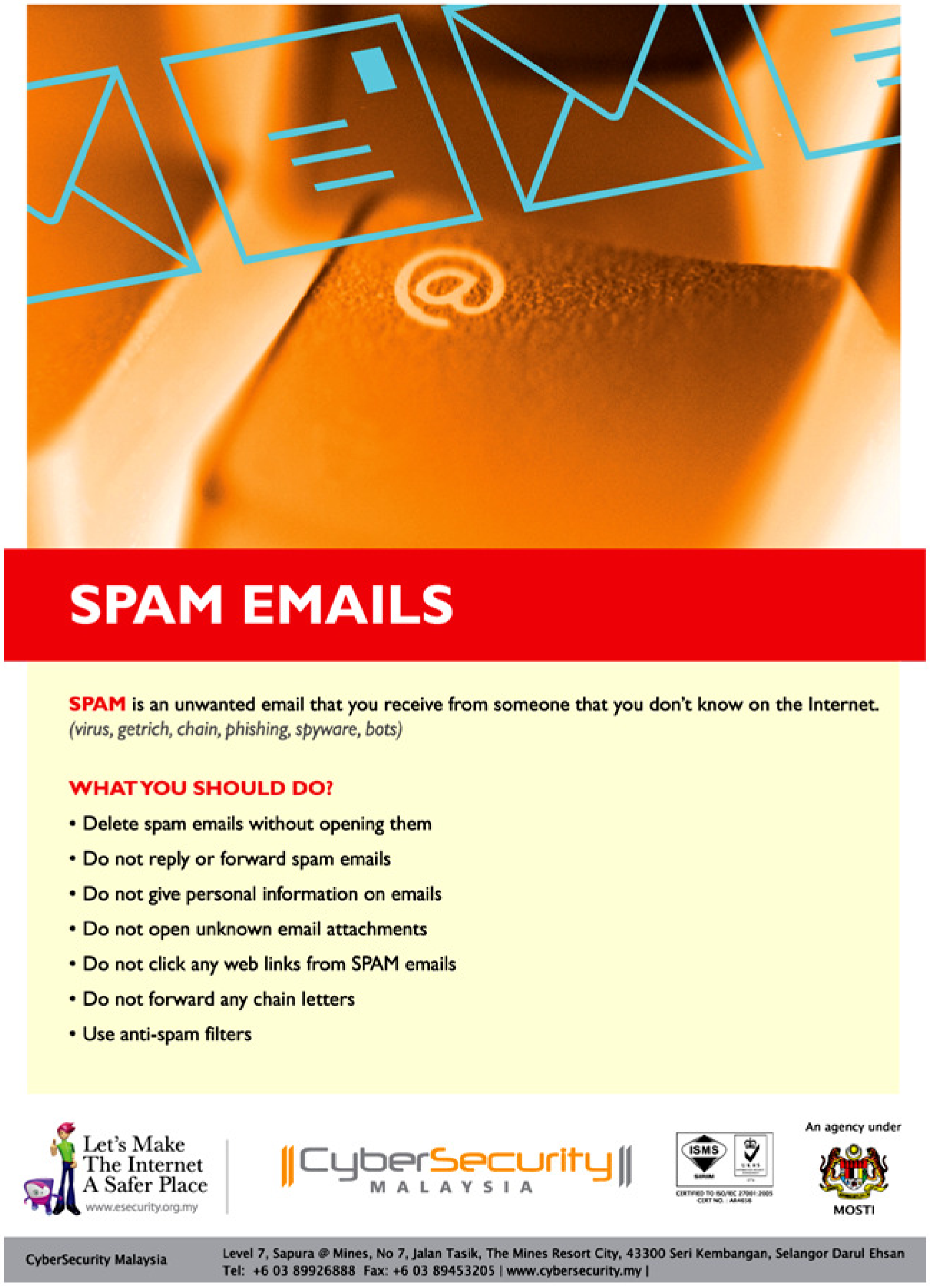
Let's Make The Internet A Safer Place
www.esecurity.org.my

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

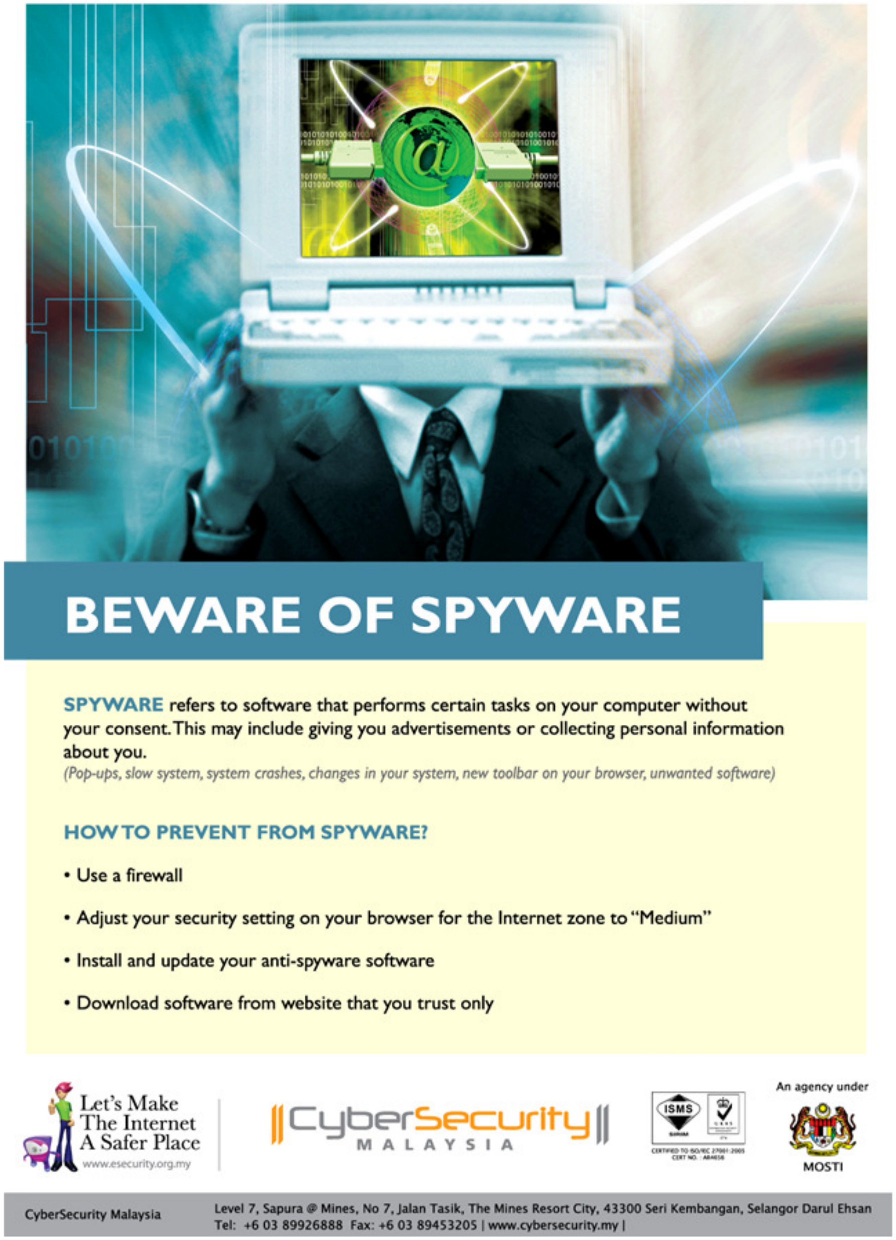
CyberSecurity MALAYSIA

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

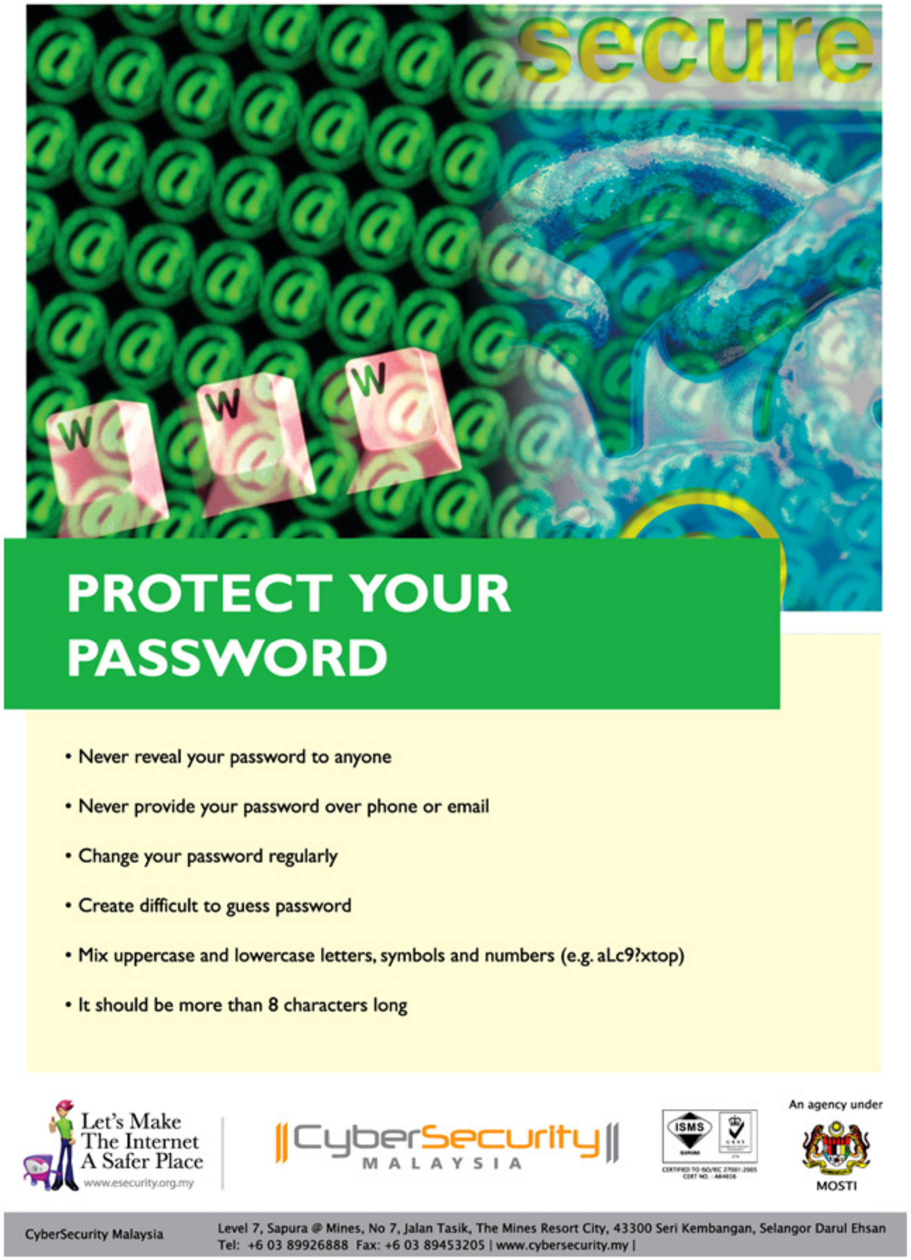
Let's Make The Internet A Safer Place
www.esecurity.org.my

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

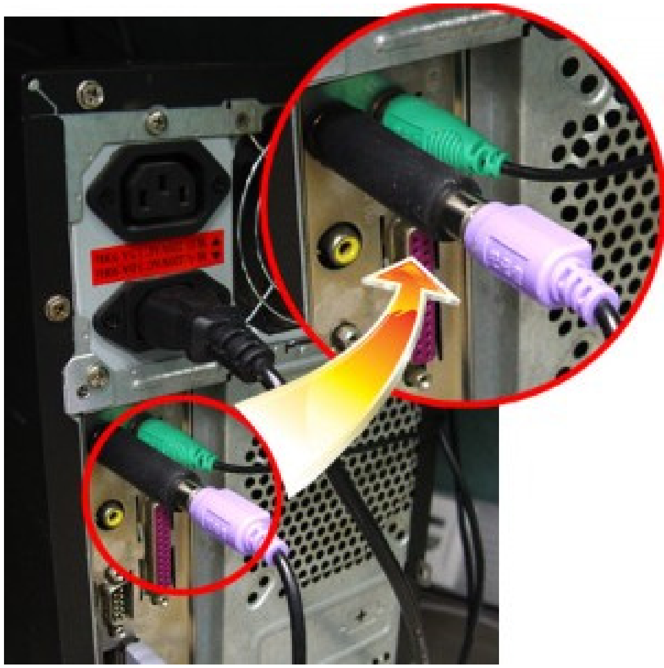
CyberSecurity Malaysia

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.

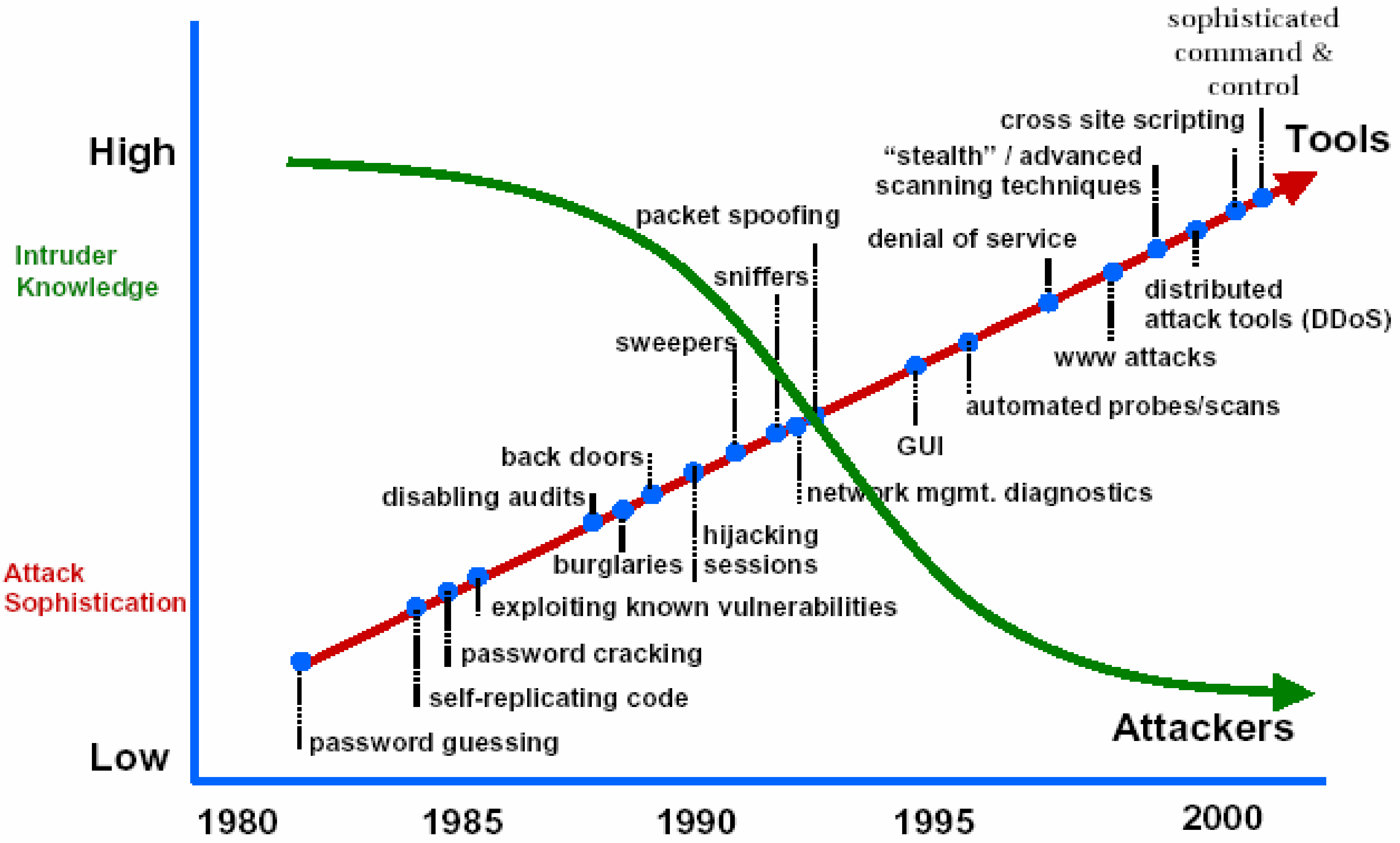
Australian Government: Cybersecurity Awareness

Australian Government

Protecting Yourself Online

What Everyone Needs to Know

Attacker Sophistication vs Intruder Knowledge



"Dark Web" *Criminal Cyber Economy*

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

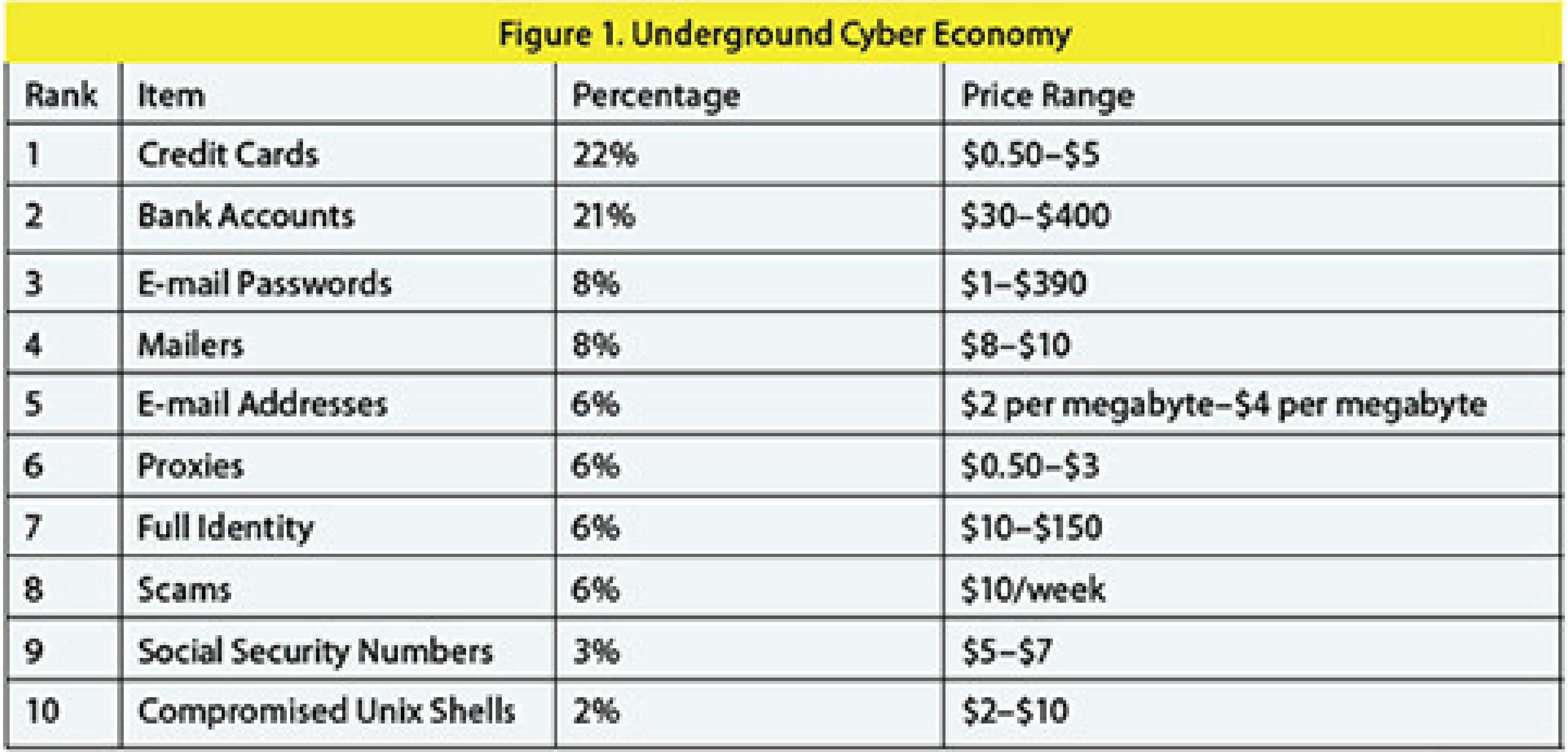


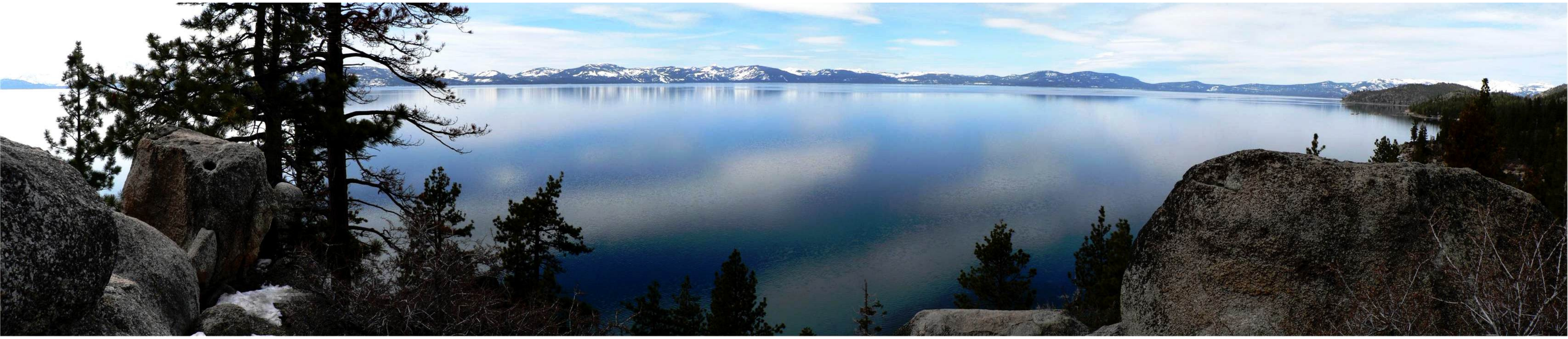
Figure 1. Underground Cyber Economy

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

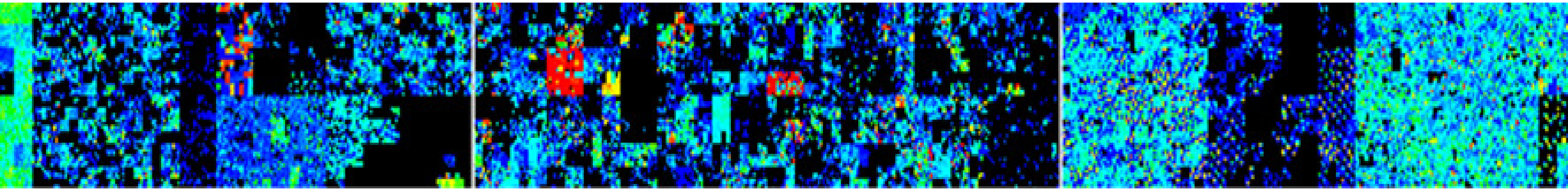
– Symantec Corp. - September 2007

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

“Practical Cyber Defence”: TOP 10 Cyber Threats!



1 – Cyber Crime, Cyber Terror & Cyber War	2 – Countdown to TOP 10 Cyber Threats!	3 – 21stC Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools “Exploration”	**5 – Cyber Entry and Exit Routes and Tools** **“Penetration”**	6 – Real-Time Cyber Alert: Hack & Attack! “Cyber Attack”
7 - In-Depth: 21stC Technical Cyber Defence	8 – *YOUR* Operational Cyber Defence	9 – *YOUR* Cyber Defence Campaign Plan!



“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

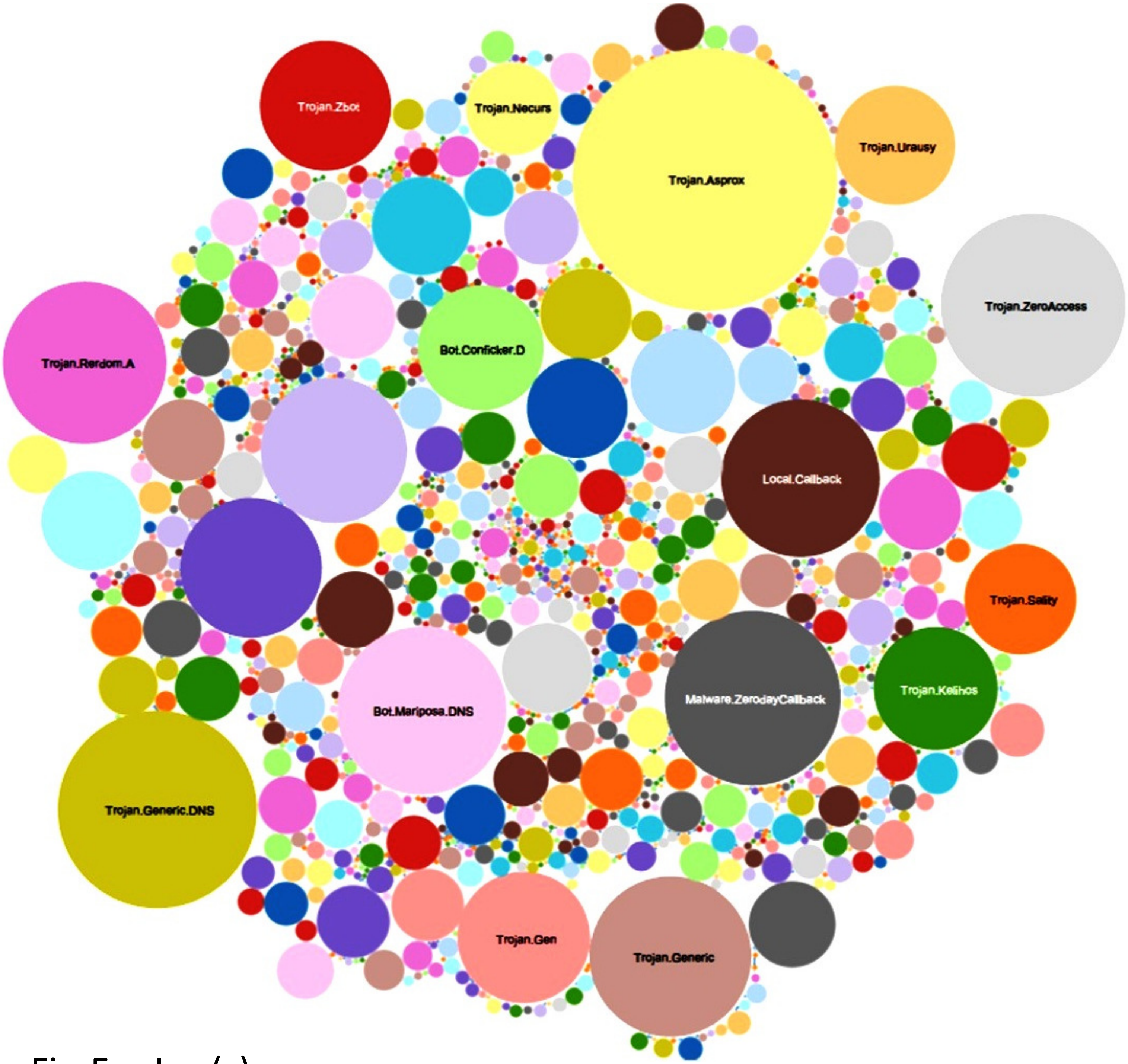
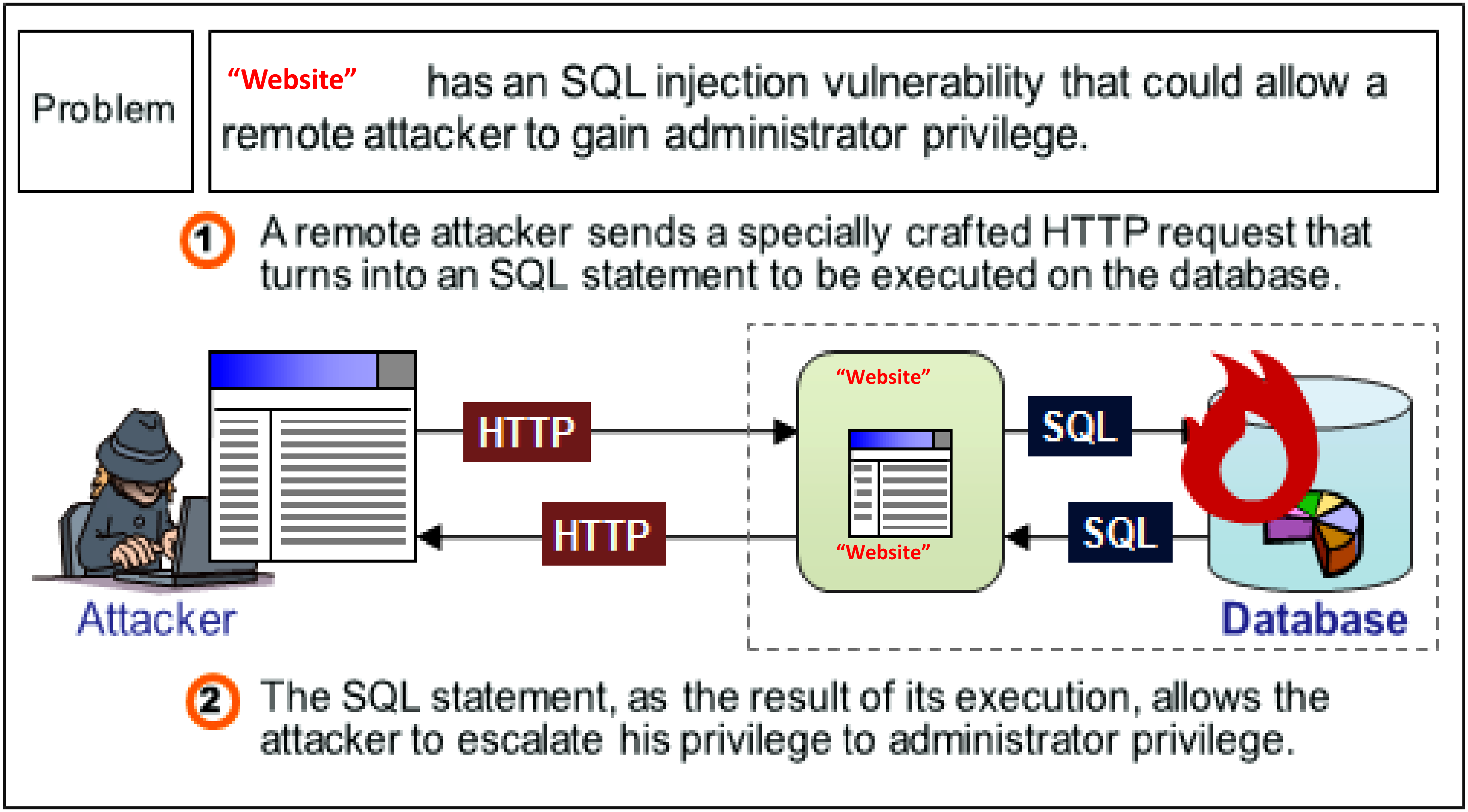


Image: www.fireeye.com – FireEye Inc (c)

"Cyber Threat": SQL Injection Vulnerability



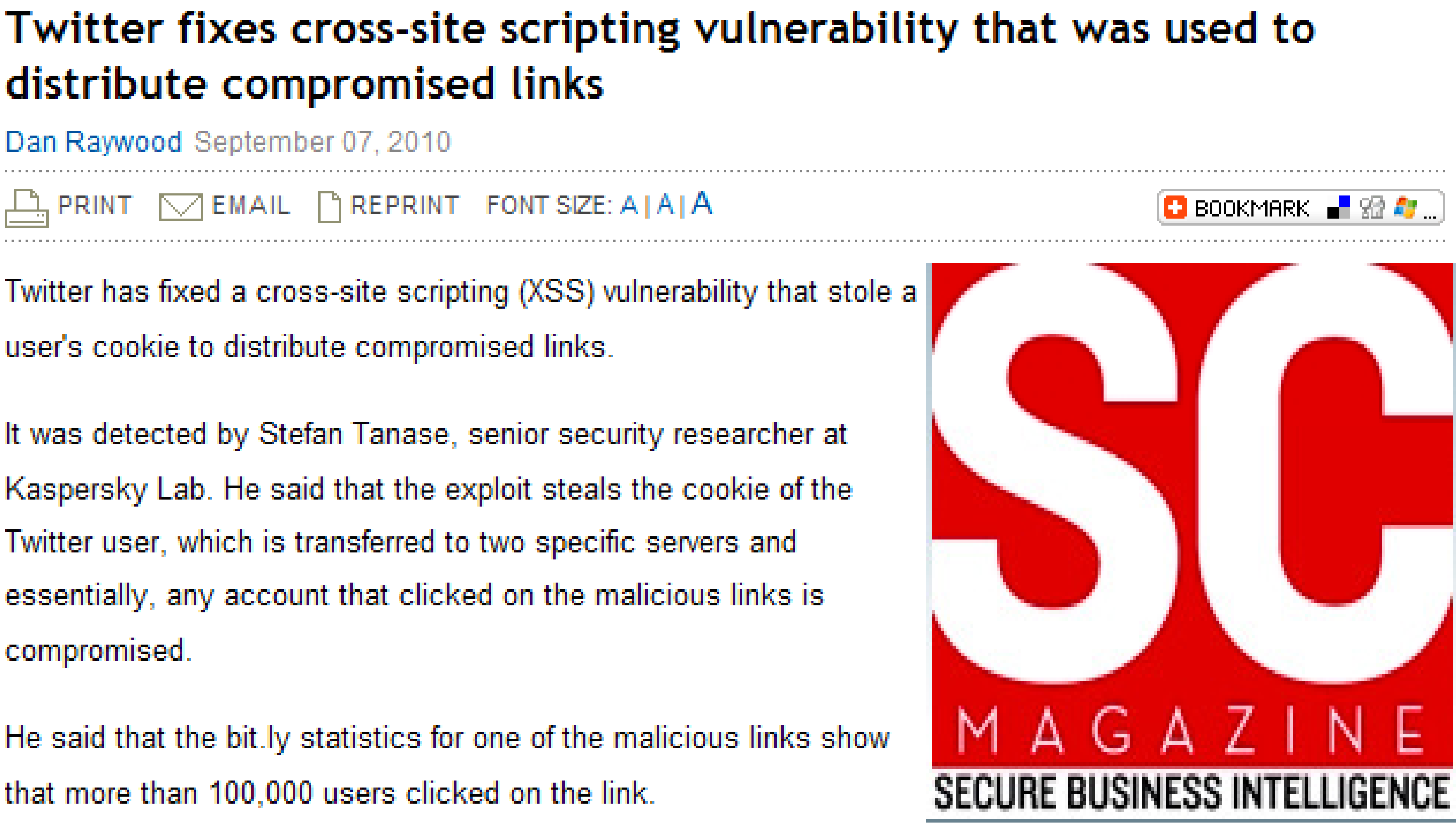
Problem	"Website" has an SQL injection vulnerability that could allow a remote attacker to gain administrator privilege.

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

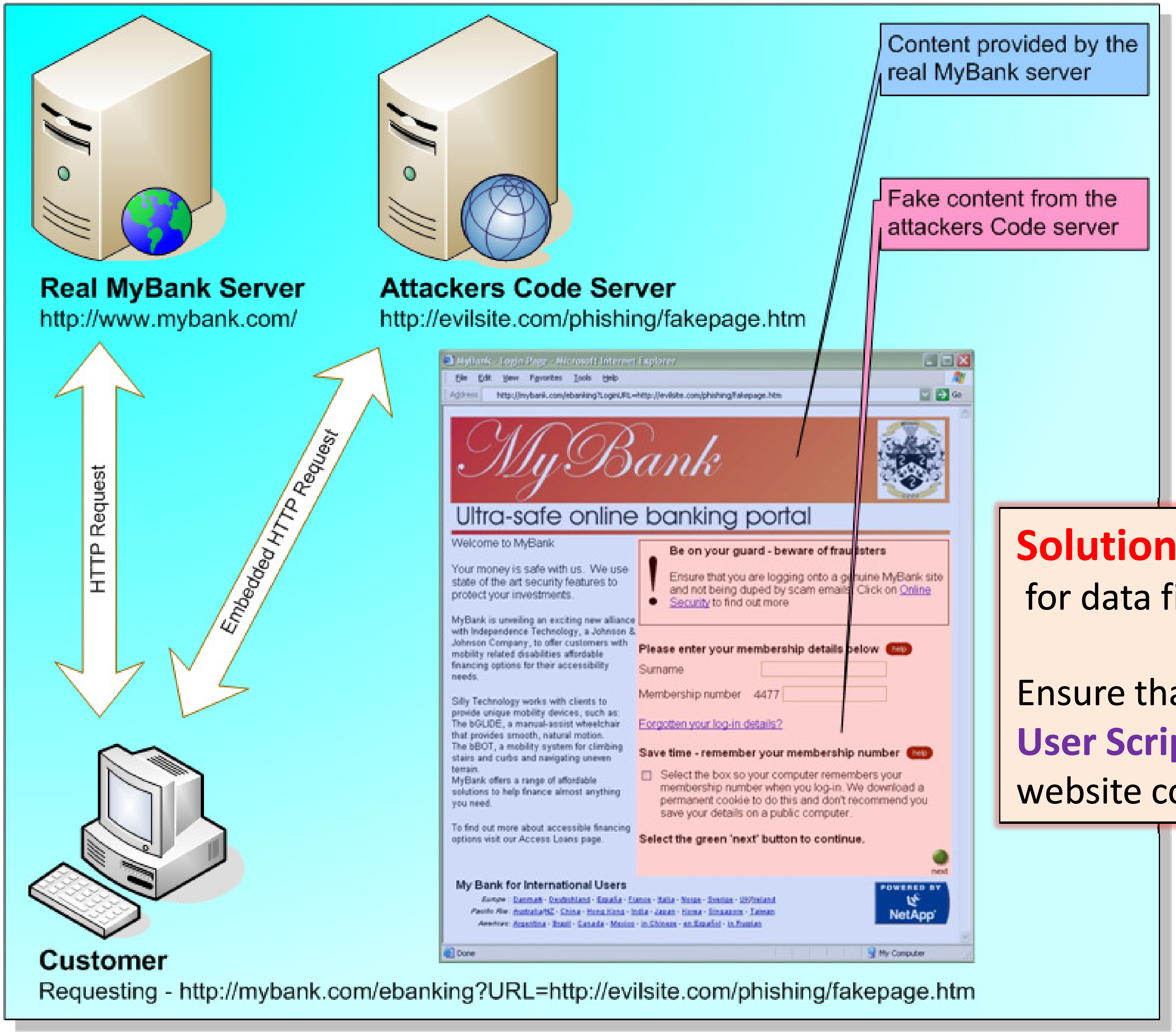
Dan Raywood September 07, 2010

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.

Impact of **XSS** Cross-Site Scripting **“Cyber Threat”**


Content provided by the real MyBank server
Fake content from the attackers Code server
Real MyBank Server
http://www.mybank.com/
Attackers Code Server
http://evilsite.com/phishing/fakepage.htm
HTTP Request
Embedded HTTP Request
Customer
Requesting - http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm
MyBank - Login Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
help
next
POWERED BY NetApp
Done
My Computer

http://mybank.com/ebanking?LoginURL=http://evilsite.com/phishing/fakepage.htm

MyBank

Ultra-safe online banking portal

Welcome to MyBank

Your money is safe with us. We use state of the art security features to protect your investments.

MyBank is unveiling an exciting new alliance with Independence Technology, a Johnson & Johnson Company, to offer customers with mobility related disabilities affordable financing options for their accessibility needs.

Silly Technology works with clients to provide unique mobility devices, such as: The bGLIDE, a manual-assist wheelchair that provides smooth, natural motion. The bBOT, a mobility system for climbing stairs and curbs and navigating uneven terrain. MyBank offers a range of affordable solutions to help finance almost anything you need.

To find out more about accessible financing options visit our Access Loans page.

Be on your guard - beware of fraudsters

Ensure that you are logging onto a genuine MyBank site and not being duped by scam emails. Click on Online Security to find out more

Please enter your membership details below

Surname

Membership number 4477

Forgotten your log-in details?

Save time - remember your membership number

□ Select the box so your computer remembers your membership number when you log-in. We download a permanent cookie to do this and don't recommend you save your details on a public computer.

Select the green 'next' button to continue.

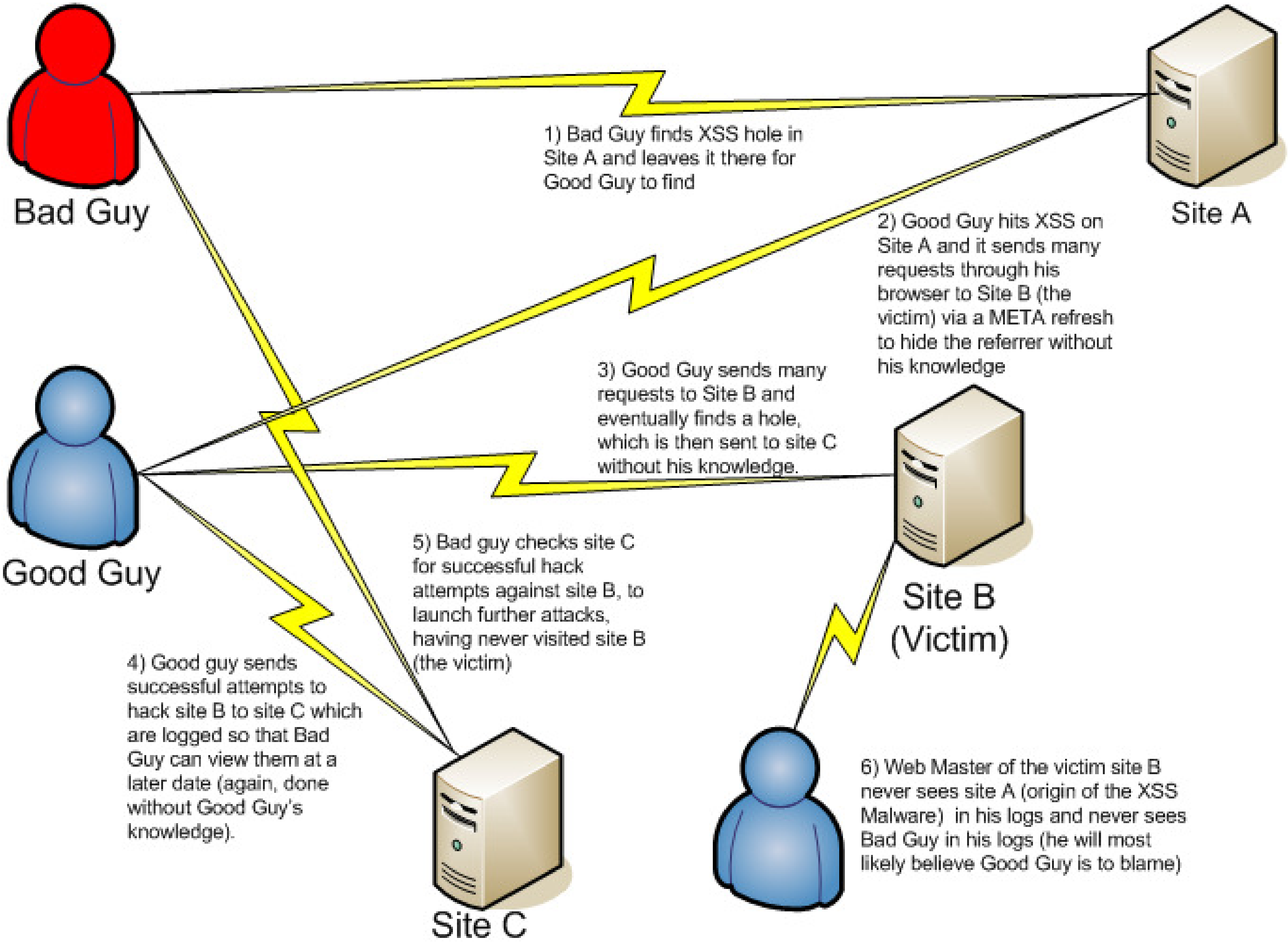
My Bank for International Users

Europe: Danmark - Deutschland - España - France - Italia - Norge - Sverige - UK/Ireland
Pacific Rim: Australia/NZ - China - Hong Kong - India - Japan - Korea - Singapore - Taiwan
Americas: Argentina - Brazil - Canada - Mexico - in Chinese - en Español - in Russian

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



1) Bad Guy finds XSS hole in Site A and leaves it there for Good Guy to find

2) Good Guy hits XSS on Site A and it sends many requests through his browser to Site B (the victim) via a META refresh to hide the referrer without his knowledge

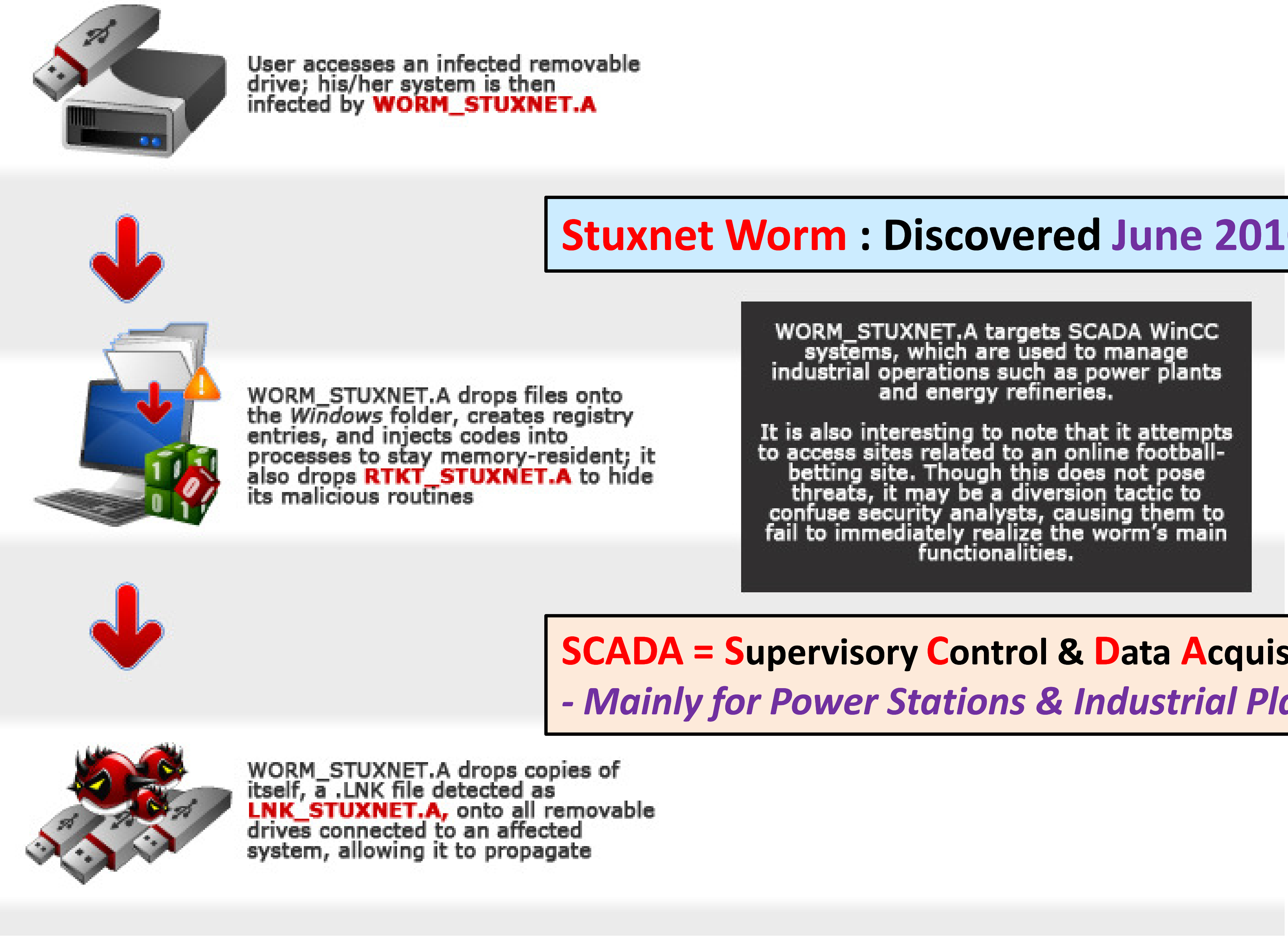
3) Good Guy sends many requests to Site B and eventually finds a hole, which is then sent to site C without his knowledge.

4) Good guy sends successful attempts to hack site B to site C which are logged so that Bad Guy can view them at a later date (again, done without Good Guy's knowledge).

5) Bad guy checks site C for successful hack attempts against site B, to launch further attacks, having never visited site B (the victim)

6) Web Master of the victim site B never sees site A (origin of the XSS Malware) in his logs and never sees Bad Guy in his logs (he will most likely believe Good Guy is to blame)

Designer "StuxNet" Worm - Industrial "SCADA" Systems



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

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 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

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

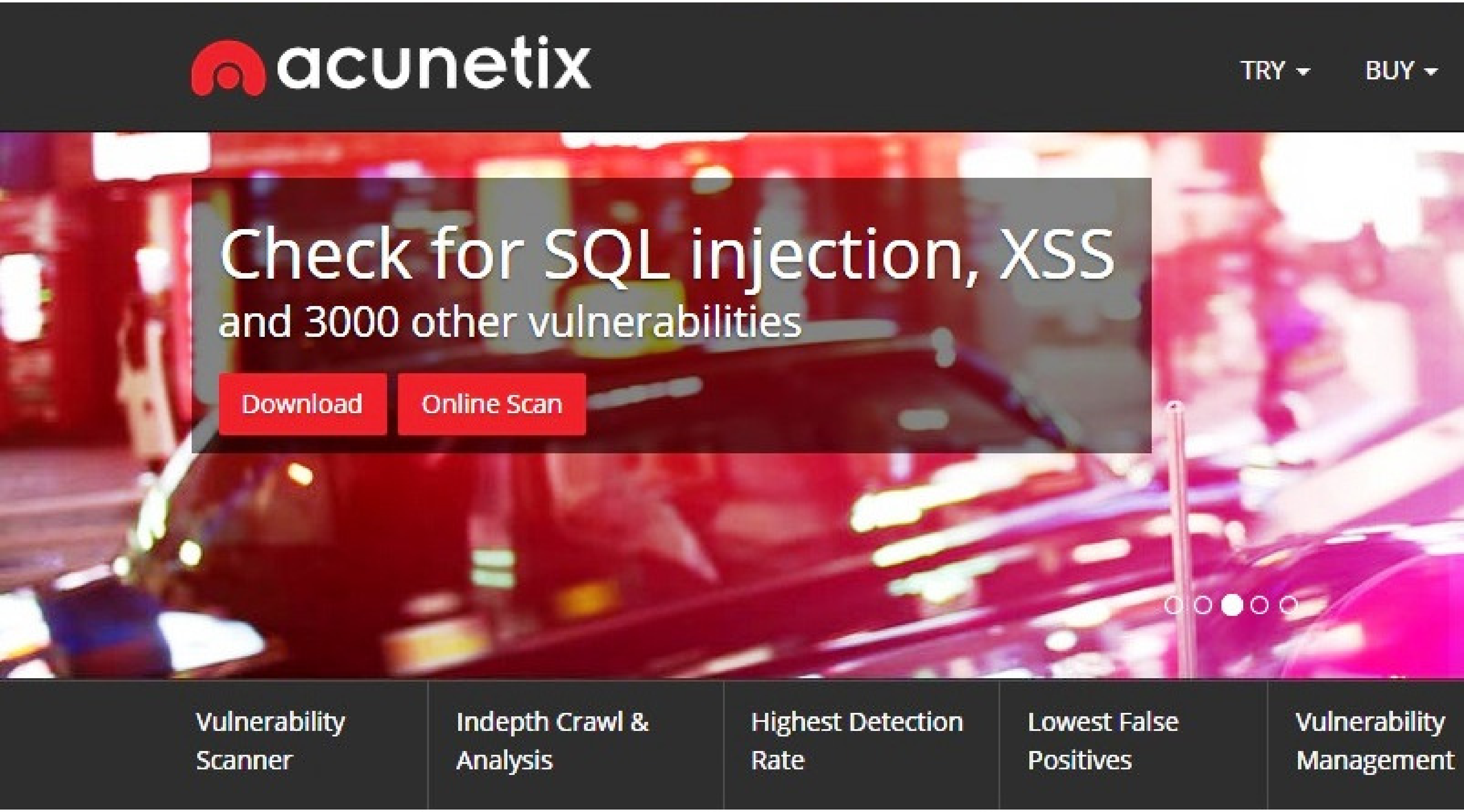
It is also interesting to note that it attempts to access sites related to an online football-betting site. Though this does not pose threats, it may be a diversion tactic to confuse security analysts, causing them to fail to immediately realize the worm's main functionalities.

Stuxnet Worm : Discovered June 2010

SCADA = Supervisory Control & Data Acquisition

- Mainly for Power Stations & Industrial Plants

Cyber Tool: Web-Site Security - Acunetix

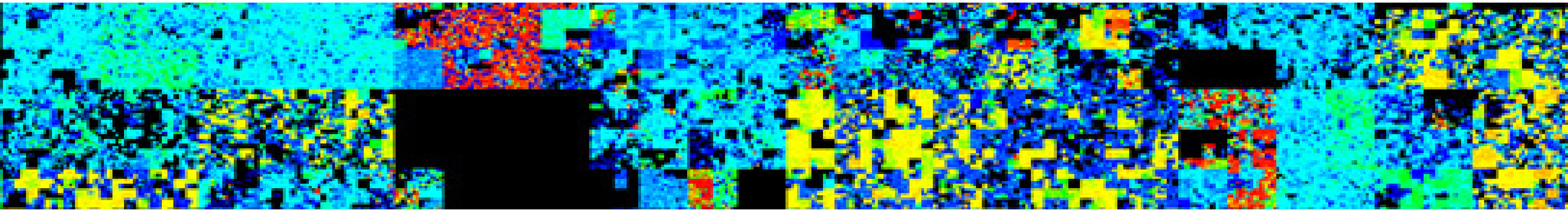


Check for SQL injection, XSS

and 3000 other vulnerabilities

“Practical Cyber Defence”: TOP 10 Cyber Threats!

1 – Cyber Crime, Cyber Terror & Cyber War	2 – Countdown to TOP 10 Cyber Threats!	3 – 21stC Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools “Exploration”	5 – Cyber Entry & Exit Routes & Tools “Penetration”	6 – Real-Time Cyber Alert: Hack & Attack “Cyber Attack”
7 – In-Depth: 21stC Technical Cyber Defence	8 – *YOUR* Operational Cyber Defence	9 – *YOUR* Cyber Defence Campaign Plan!

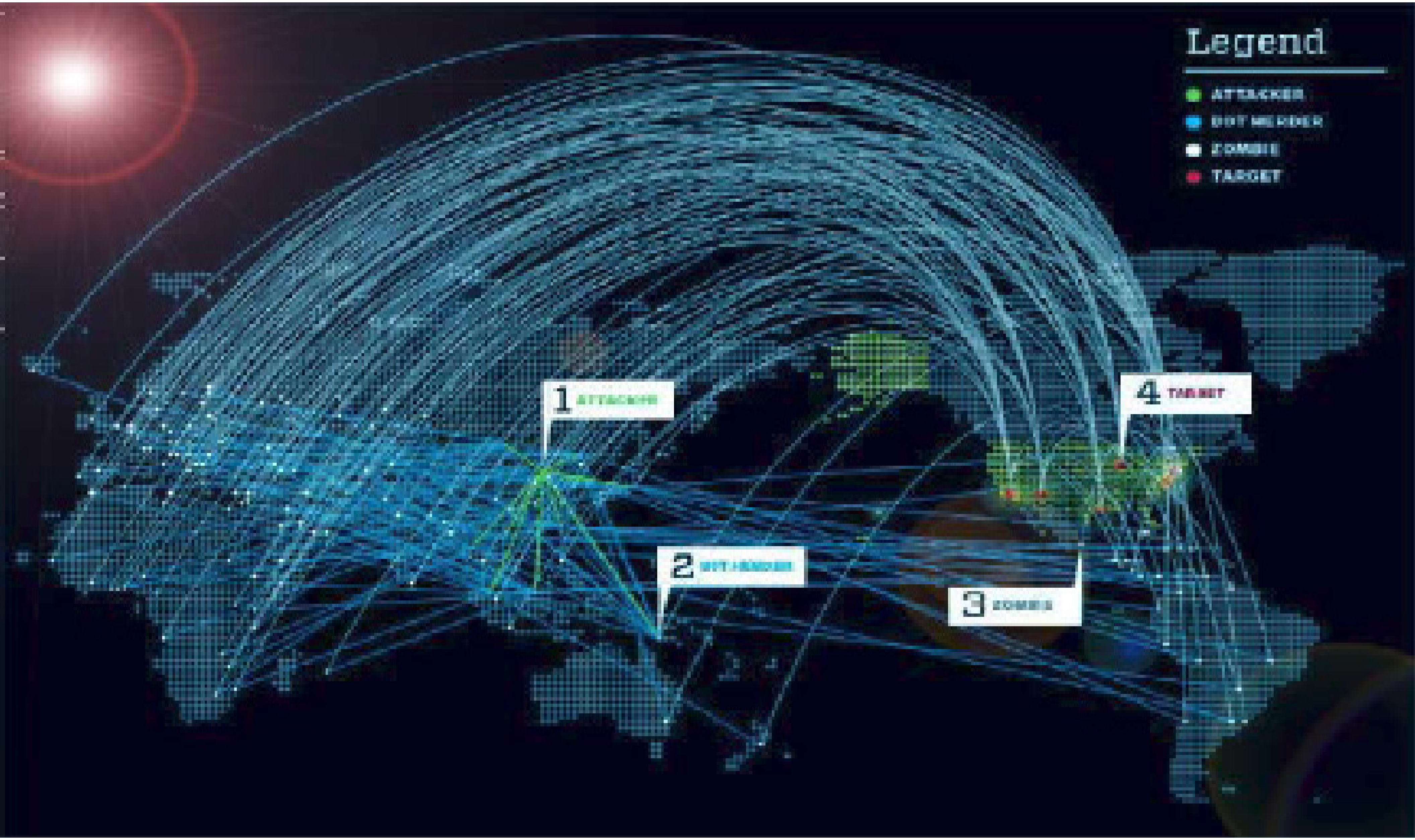


"Real-Time Cyber Alert: *Hack & Attack*"

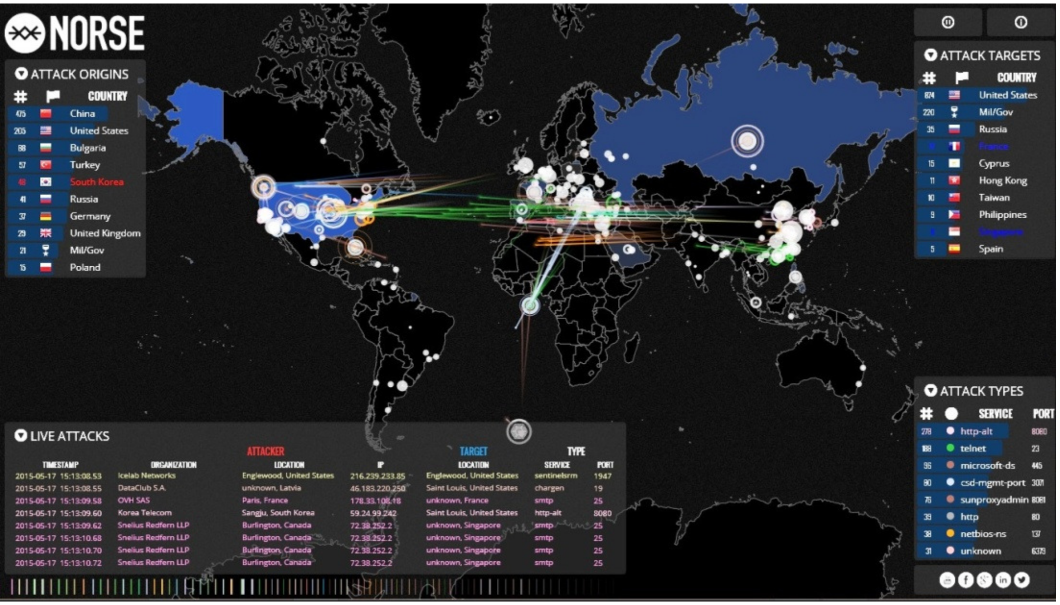
*** CYBER ATTACK ***

- 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!



Successive "Real-Time" *DarkNet* CyberAttacks



ATTACK ORIGINS

#	COUNTRY
475	China
205	United States
68	Bulgaria
57	Turkey
46	South Korea
41	Russia
37	Germany
29	United Kingdom
21	Mil/Gov
15	Poland

ATTACK TARGETS

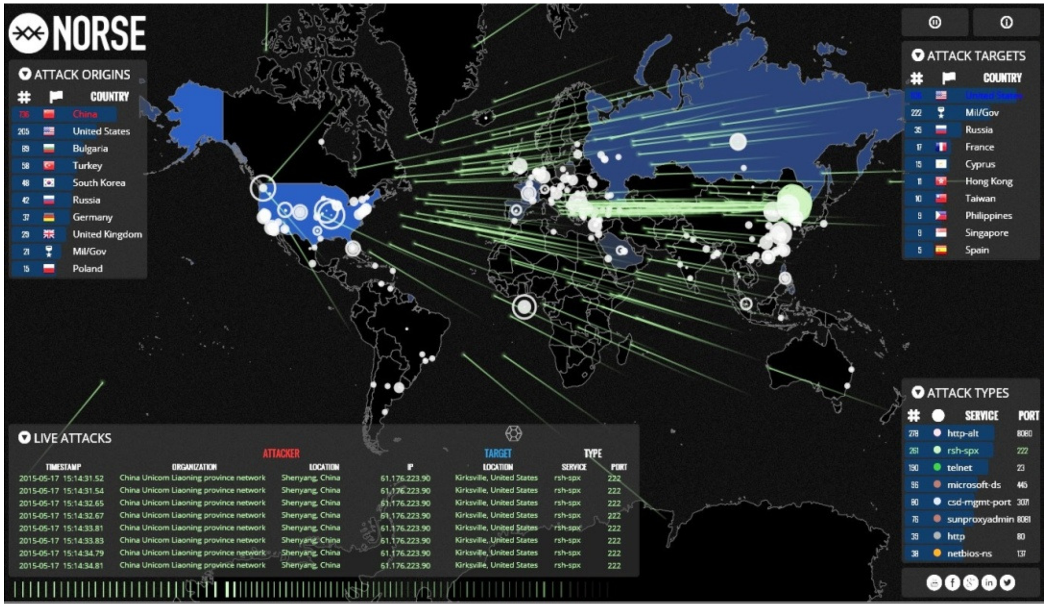
#	COUNTRY
874	United States
220	Mil/Gov
35	Russia
[illegible]	France
15	Cyprus
11	Hong Kong
10	Taiwan
9	Philippines
[illegible]	Singapore
5	Spain

ATTACK TYPES

#	SERVICE	PORT
278	http-alt	8080
188	telnet	23
96	microsoft-ds	445
80	csd-mgmt-port	3071
76	sunproxyadmin	8081
39	http	80
38	netbios-ns	137
31	unknown	6379

LIVE ATTACKS

	ATTACKER			TARGET	TYPE	
TIMESTAMP	ORGANIZATION	LOCATION	IP	LOCATION	SERVICE	PORT
2015-05-17 15:13:08.53	Icelab Networks	Englewood, United States	216.239.233.85	Englewood, United States	sentinelsrm	1947
2015-05-17 15:13:08.55	DataClub S.A.	unknown, Latvia	46.183.220.250	Saint Louis, United States	chargen	19
2015-05-17 15:13:09.58	OVH SAS	Paris, France	178.33.108.18	unknown, France	smtp	25
2015-05-17 15:13:09.60	Korea Telecom	Sangju, South Korea	59.24.99.242	Saint Louis, United States	http-alt	8080
2015-05-17 15:13:09.62	Snelius Redfern LLP	Burlington, Canada	72.38.252.2	unknown, Singapore	smtp	25
2015-05-17 15:13:10.68	Snelius Redfern LLP	Burlington, Canada	72.38.252.2	unknown, Singapore	smtp	25
2015-05-17 15:13:10.70	Snelius Redfern LLP	Burlington, Canada	72.38.252.2	unknown, Singapore	smtp	25
2015-05-17 15:13:10.72	Snelius Redfern LLP	Burlington, Canada	72.38.252.2	unknown, Singapore	smtp	25



ATTACK ORIGINS

#	COUNTRY
736	China
205	United States
69	Bulgaria
58	Turkey
48	South Korea
42	Russia
37	Germany
29	United Kingdom
21	Mil/Gov
15	Poland

ATTACK TARGETS

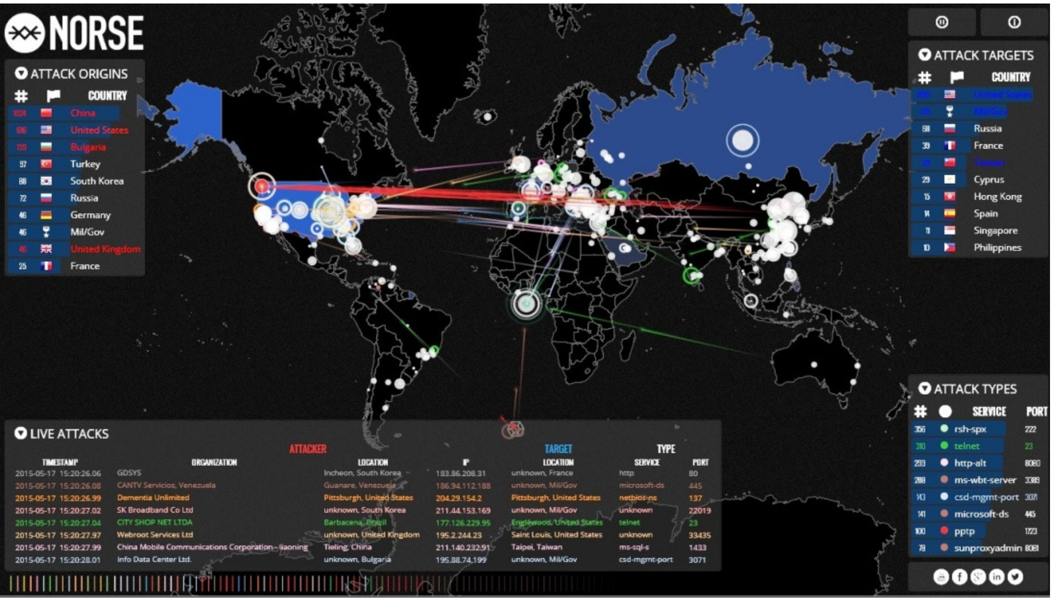
#	COUNTRY
[illegible]	United States
222	Mil/Gov
35	Russia
17	France
15	Cyprus
11	Hong Kong
10	Taiwan
9	Philippines
9	Singapore
5	Spain

ATTACK TYPES

#	SERVICE	PORT
278	http-alt	8080
261	rsh-spx	222
190	telnet	23
96	microsoft-ds	445
80	csd-mgmt-port	3071
76	sunproxyadmin	8081
39	http	80
38	netbios-ns	137

LIVE ATTACKS

	ATTACKER			TARGET	TYPE	
TIMESTAMP	ORGANIZATION	LOCATION	IP	LOCATION	SERVICE	PORT
2015-05-17 15:14:31.52	China Unicom Liaoning province network	Shenyang, China	61.176.223.90	Kirksville, United States	rsh-spx	222
2015-05-17 15:14:31.54	China Unicom Liaoning province network	Shenyang, China	61.176.223.90	Kirksville, United States	rsh-spx	222
2015-05-17 15:14:32.65	China Unicom Liaoning province network	Shenyang, China	61.176.223.90	Kirksville, United States	rsh-spx	222
2015-05-17 15:14:32.67	China Unicom Liaoning province network	Shenyang, China	61.176.223.90	Kirksville, United States	rsh-spx	222
2015-05-17 15:14:33.81	China Unicom Liaoning province network	Shenyang, China	61.176.223.90	Kirksville, United States	rsh-spx	222
2015-05-17 15:14:33.83	China Unicom Liaoning province network	Shenyang, China	61.176.223.90	Kirksville, United States	rsh-spx	222
2015-05-17 15:14:34.79	China Unicom Liaoning province network	Shenyang, China	61.176.223.90	Kirksville, United States	rsh-spx	222
2015-05-17 15:14:34.81	China Unicom Liaoning province network	Shenyang, China	61.176.223.90	Kirksville, United States	rsh-spx	222



ATTACK ORIGINS

#	COUNTRY
1029	China
616	United States
159	Bulgaria
97	Turkey
88	South Korea
72	Russia
46	Germany
46	Mil/Gov
46	United Kingdom
25	France

ATTACK TARGETS

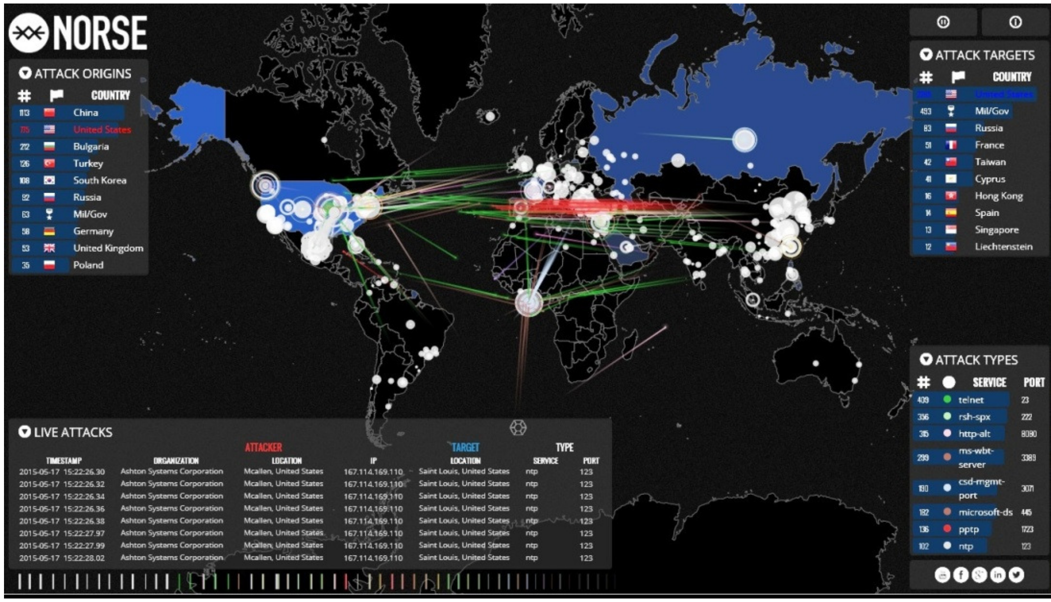
#	COUNTRY
[illegible]	United States
[illegible]	Mil/Gov
68	Russia
39	France
[illegible]	Taiwan
29	Cyprus
15	Hong Kong
14	Spain
11	Singapore
10	Philippines

ATTACK TYPES

#	SERVICE	PORT
356	rsh-spx	222
310	telnet	23
299	http-alt	8080
288	ms-wbt-server	3389
143	csd-mgmt-port	3071
141	microsoft-ds	445
100	pptp	1723
78	sunproxyadmin	8081

LIVE ATTACKS

	ATTACKER			TARGET	TYPE	
TIMESTAMP	ORGANIZATION	LOCATION	IP	LOCATION	SERVICE	PORT
2015-05-17 15:20:26.06	GDSYS	Incheon, South Korea	183.86.208.31	unknown, France	http	80
2015-05-17 15:20:26.08	CANTV Servicios, Venezuela	Guanare, Venezuela	186.94.112.188	unknown, Mil/Gov	microsoft-ds	445
2015-05-17 15:20:26.99	Dementia Unlimited	Pittsburgh, United States	204.29.154.2	Pittsburgh, United States	netbios-ns	137
2015-05-17 15:20:27.02	SK Broadband Co Ltd	unknown, South Korea	211.44.153.169	unknown, Mil/Gov	unknown	22019
2015-05-17 15:20:27.04	CITY SHOP NET LTDA	Barbacena, Brazil	177.126.229.95	Englewood, United States	telnet	23
2015-05-17 15:20:27.97	Webroot Services Ltd	unknown, United Kingdom	195.2.244.23	Saint Louis, United States	unknown	33435
2015-05-17 15:20:27.99	China Mobile Communications Corporation - liaoning	Tieling, China	211.140.232.91	Taipei, Taiwan	ms-sql-s	1433
2015-05-17 15:20:28.01	Info Data Center Ltd.	unknown, Bulgaria	195.88.74.199	unknown, Mil/Gov	csd-mgmt-port	3071



ATTACK ORIGINS

#	COUNTRY
113	China
775	United States
212	Bulgaria
126	Turkey
108	South Korea
92	Russia
63	Mil/Gov
58	Germany
53	United Kingdom
35	Poland

ATTACK TARGETS

#	COUNTRY
[illegible]	United States
493	Mil/Gov
83	Russia
51	France
42	Taiwan
41	Cyprus
16	Hong Kong
14	Spain
13	Singapore
12	Liechtenstein

ATTACK TYPES

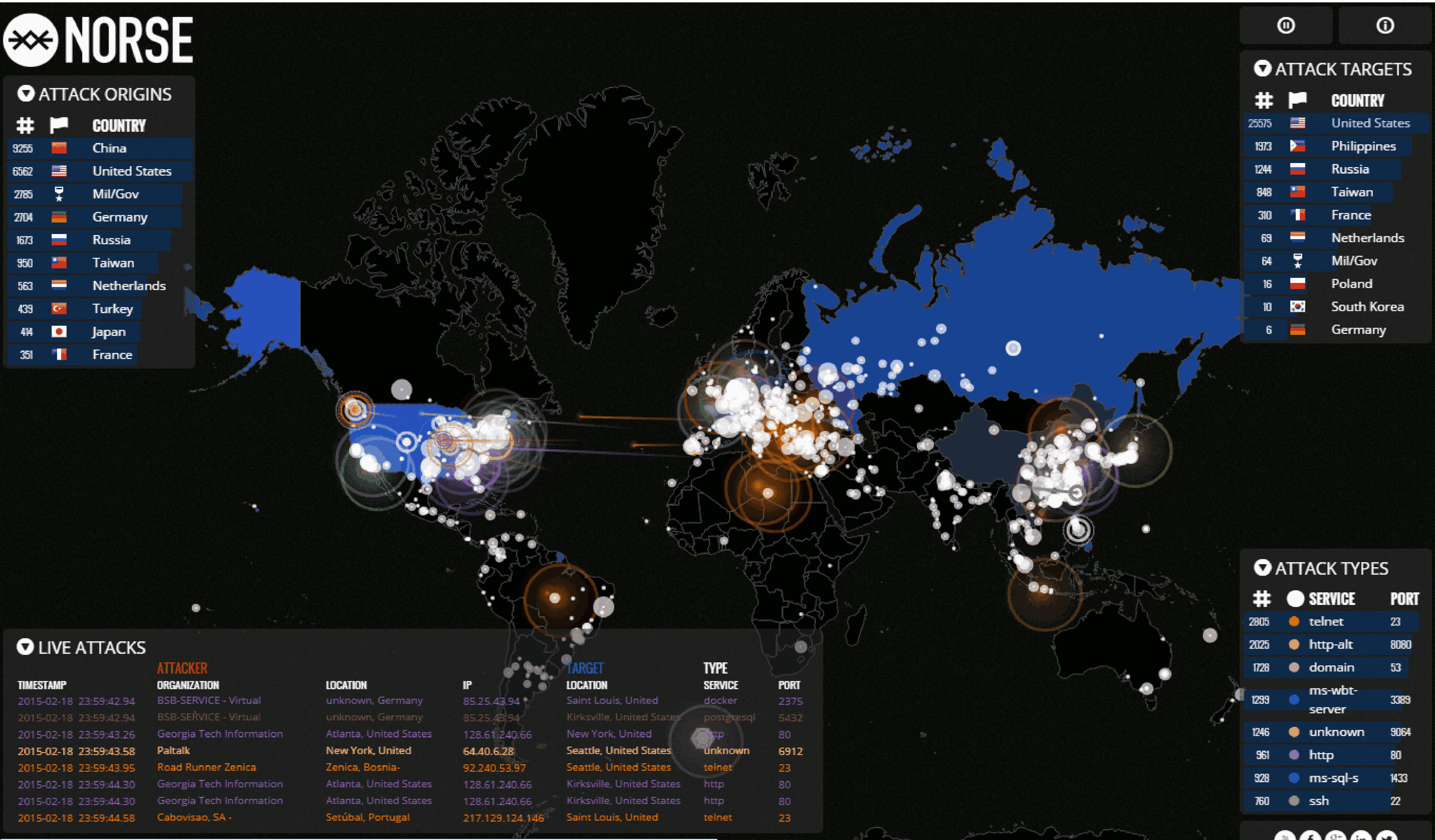
#	SERVICE	PORT
409	telnet	23
356	rsh-spx	222
315	http-alt	8080
299	ms-wbt-server	3389
190	csd-mgmt-port	3071
182	microsoft-ds	445
136	pptp	1723
102	ntp	123

LIVE ATTACKS

	ATTACKER			TARGET	TYPE	
TIMESTAMP	ORGANIZATION	LOCATION	IP	LOCATION	SERVICE	PORT
2015-05-17 15:22:26.30	Ashton Systems Corporation	Mcallen, United States	167.114.169.110	Saint Louis, United States	ntp	123
2015-05-17 15:22:26.32	Ashton Systems Corporation	Mcallen, United States	167.114.169.110	Saint Louis, United States	ntp	123
2015-05-17 15:22:26.34	Ashton Systems Corporation	Mcallen, United States	167.114.169.110	Saint Louis, United States	ntp	123
2015-05-17 15:22:26.36	Ashton Systems Corporation	Mcallen, United States	167.114.169.110	Saint Louis, United States	ntp	123
2015-05-17 15:22:26.38	Ashton Systems Corporation	Mcallen, United States	167.114.169.110	Saint Louis, United States	ntp	123
2015-05-17 15:22:27.97	Ashton Systems Corporation	Mcallen, United States	167.114.169.110	Saint Louis, United States	ntp	123
2015-05-17 15:22:27.99	Ashton Systems Corporation	Mcallen, United States	167.114.169.110	Saint Louis, United States	ntp	123
2015-05-17 15:22:28.02	Ashton Systems Corporation	Mcallen, United States	167.114.169.110	Saint Louis, United States	ntp	123

Link: map.norsecorp.com - Norse Corporation

Real-Time Global DDoS “BotNet” Attack



ATTACK ORIGINS

#	COUNTRY
9255	China
6562	United States
2785	Mil/Gov
2704	Germany
1673	Russia
950	Taiwan
563	Netherlands
439	Turkey
414	Japan
351	France

ATTACK TARGETS

#	COUNTRY
25575	United States
1973	Philippines
1244	Russia
848	Taiwan
310	France
69	Netherlands
64	Mil/Gov
16	Poland
10	South Korea
6	Germany

ATTACK TYPES

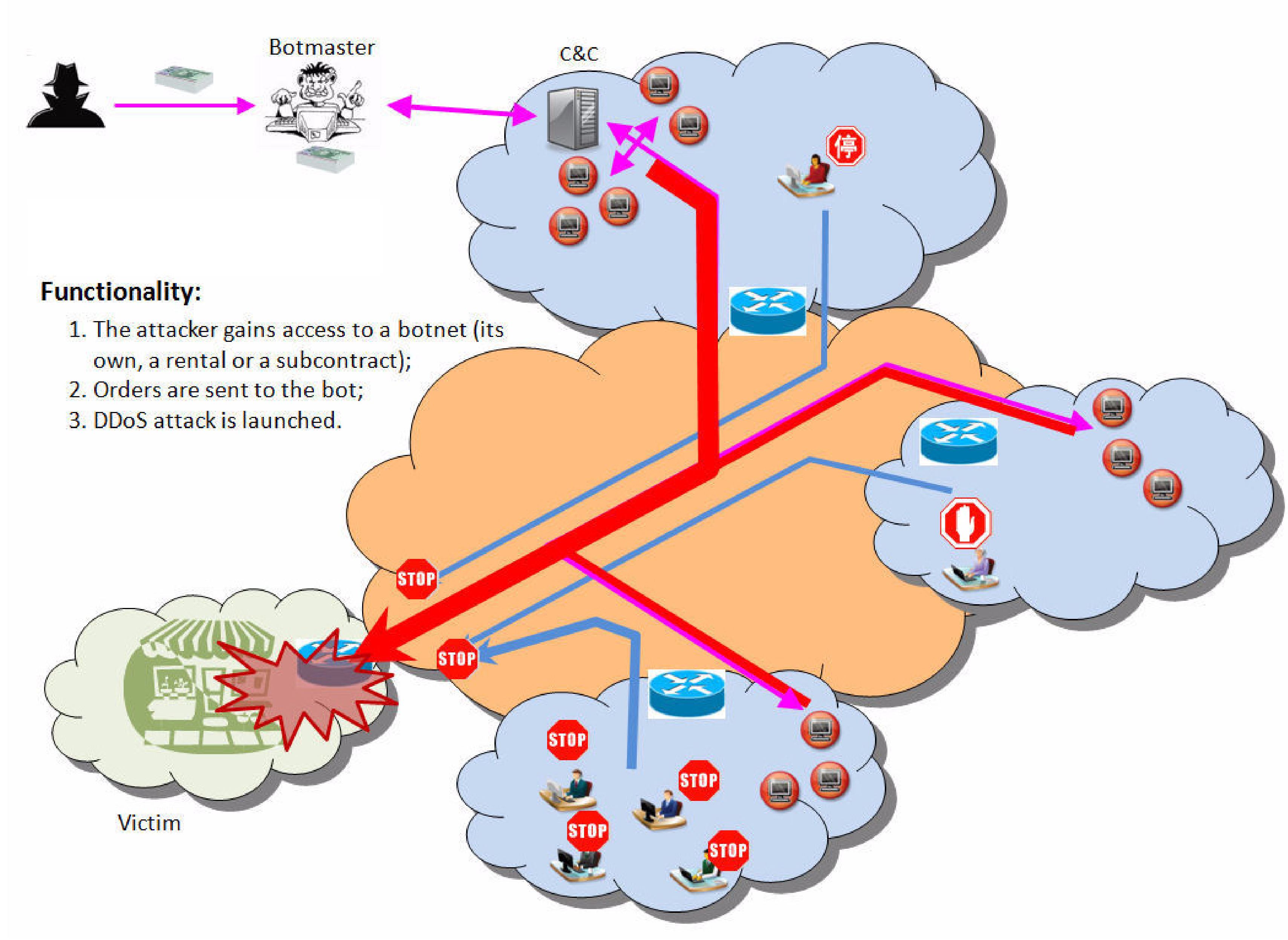
#	SERVICE	PORT
2805	telnet	23
2025	http-alt	8080
1728	domain	53
1299	ms-wbt-server	3389
1246	unknown	9064
961	http	80
928	ms-sql-s	1433
760	ssh	22

LIVE ATTACKS

	ATTACKER			TARGET	TYPE	
TIMESTAMP	ORGANIZATION	LOCATION	IP	LOCATION	SERVICE	PORT
2015-02-18 23:59:42.94	BSB-SERVICE - Virtual	unknown, Germany	85.25.43.94	Saint Louis, United	docker	2375
2015-02-18 23:59:42.94	BSB-SERVICE - Virtual	unknown, Germany	85.25.43.94	Kirksville, United States	postgresql	5432
2015-02-18 23:59:43.26	Georgia Tech Information	Atlanta, United States	128.61.240.66	New York, United	http	80
2015-02-18 23:59:43.58	Paltalk	New York, United	64.40.6.28	Seattle, United States	unknown	6912
2015-02-18 23:59:43.95	Road Runner Zenica	Zenica, Bosnia-	92.240.53.97	Seattle, United States	telnet	23
2015-02-18 23:59:44.30	Georgia Tech Information	Atlanta, United States	128.61.240.66	Kirksville, United States	http	80
2015-02-18 23:59:44.30	Georgia Tech Information	Atlanta, United States	128.61.240.66	Kirksville, United States	http	80
2015-02-18 23:59:44.58	Cabovisao, SA -	Setúbal, Portugal	217.129.124.146	Saint Louis, United	telnet	23

Link: map.norsecorp.com - Norse Corporation

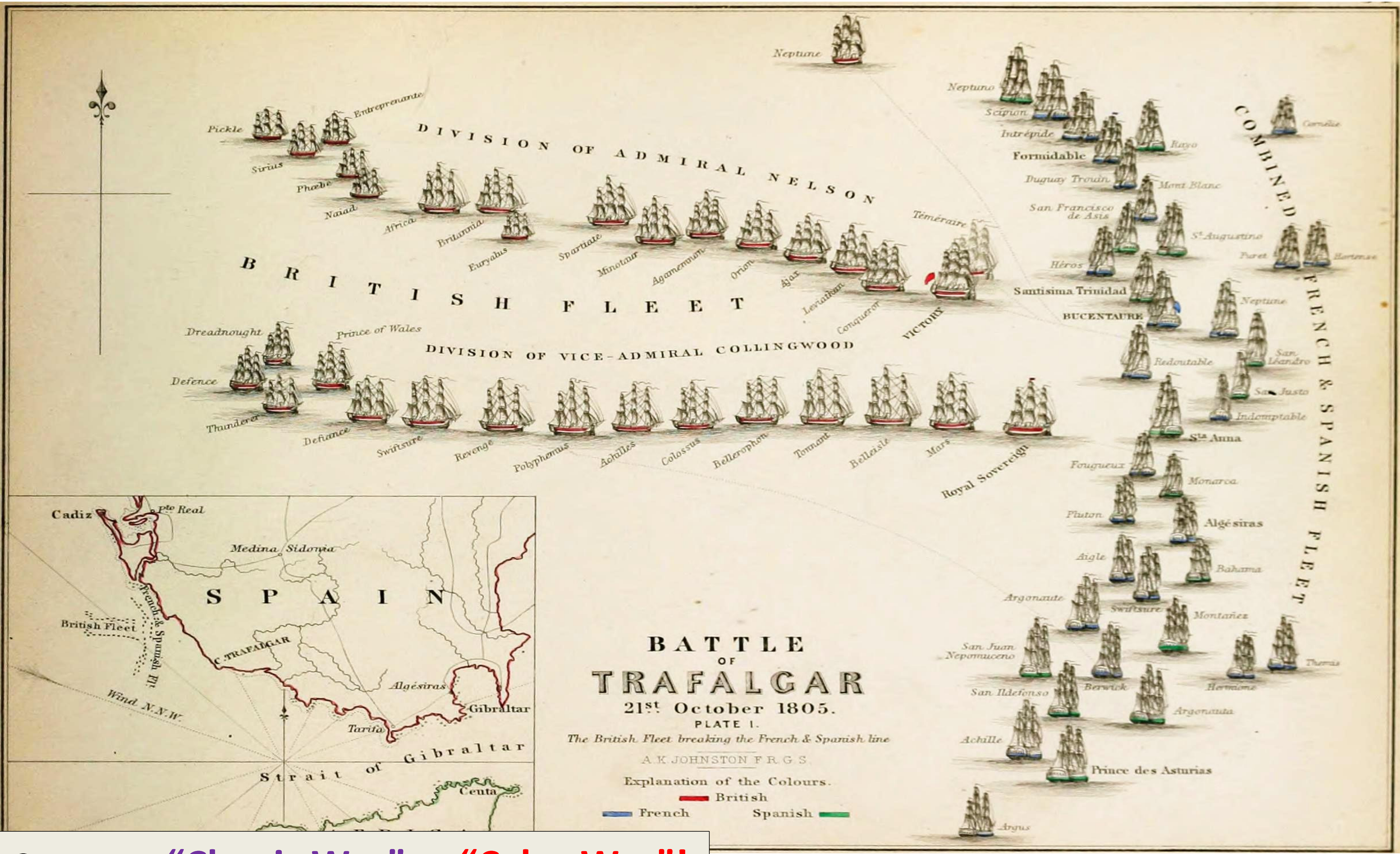
Typical DDOS "BotNet" Attack



Functionality:

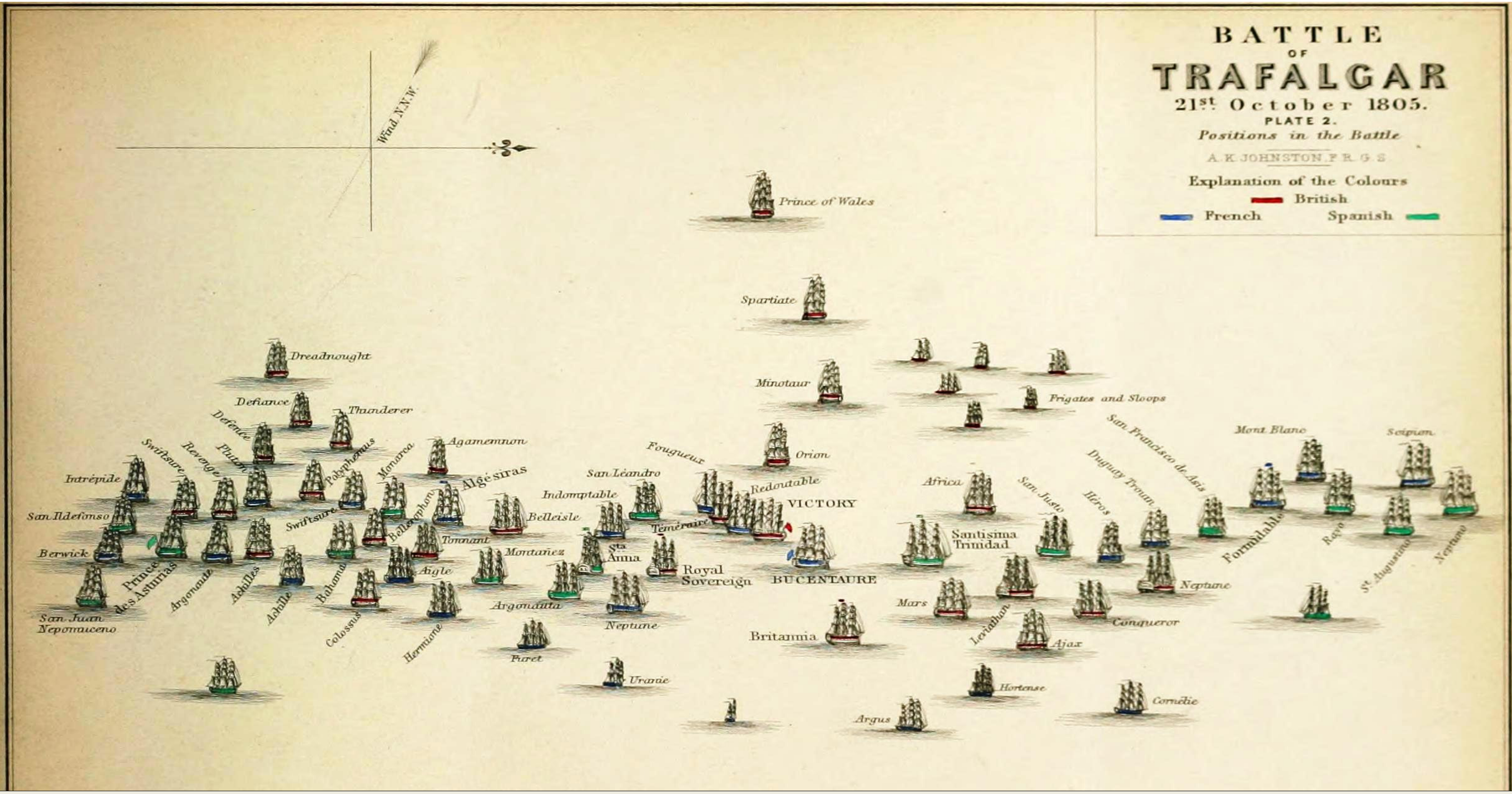
1. The attacker gains access to a botnet (its own, a rental or a subcontract);
2. Orders are sent to the bot;
3. DDoS attack is launched.

"Naval Campaign: Battle of Trafalgar-1805



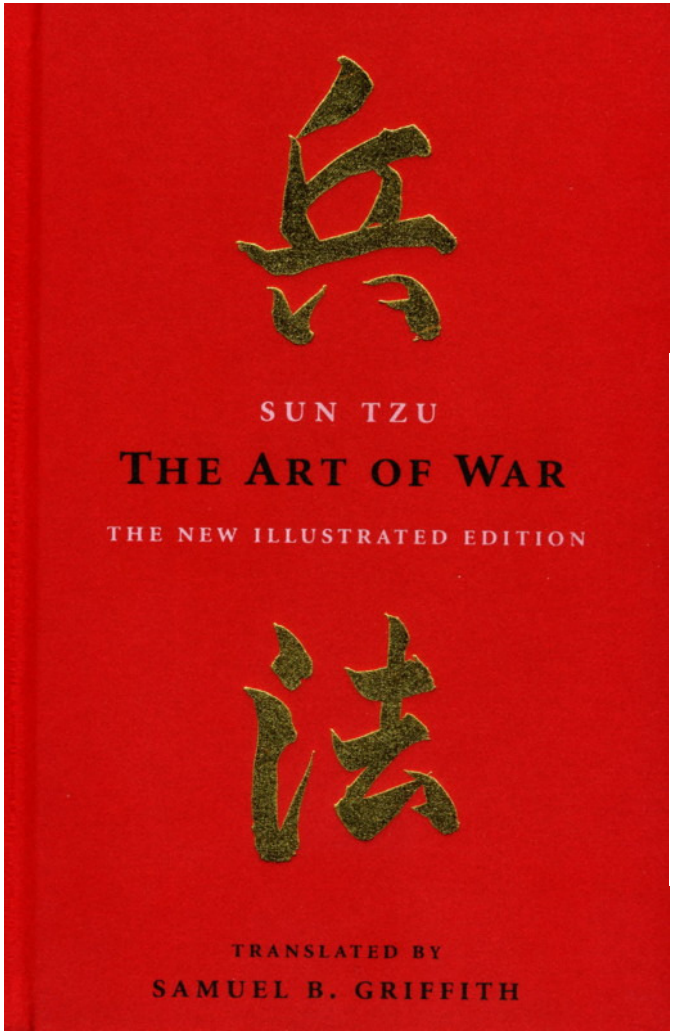
Compare "Classic War" to "CyberWar"!

Naval Campaign: Battle of Trafalgar-1805

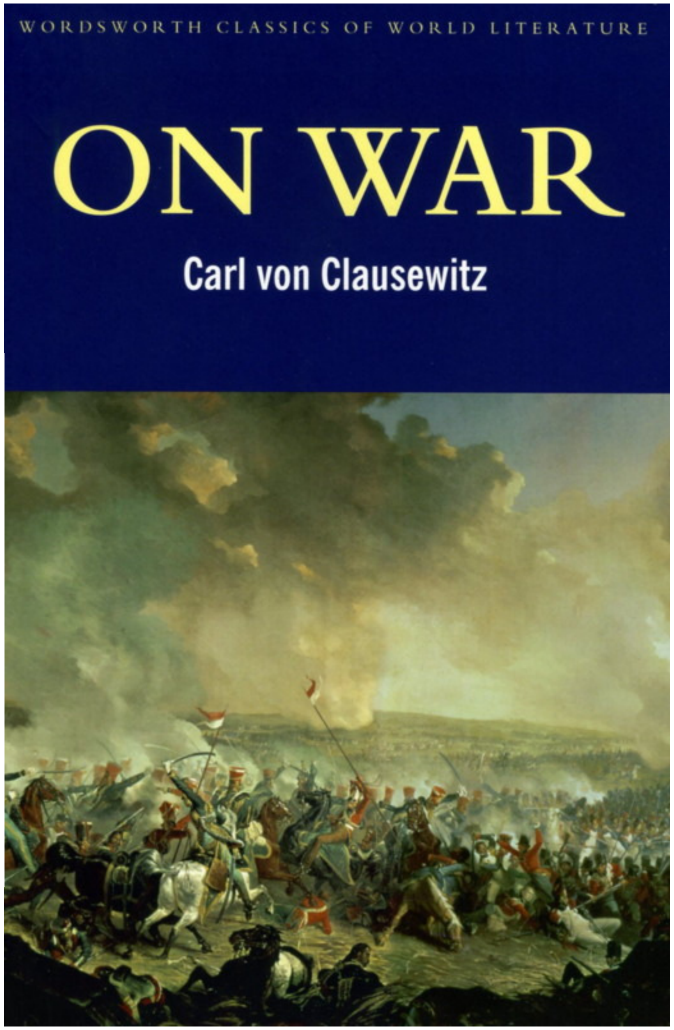


"Cyber Attack Strategies & Campaigns have *Similarities* with Classical Warfare!...
...But they occur ***1Million X Faster*** @ "Speed of Light" rather than "Speed of Sound"!

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



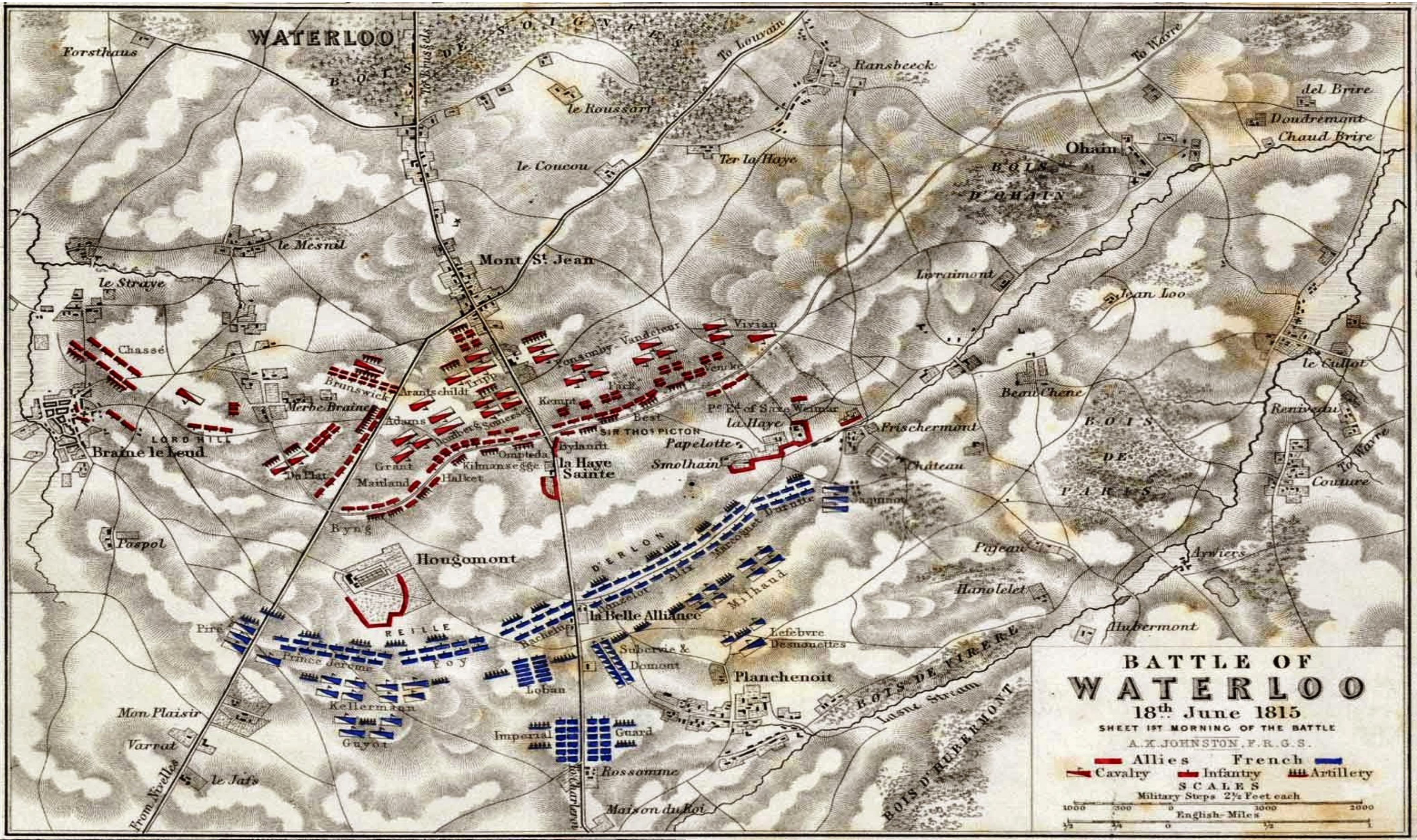
Recommended "Bedtime Reading" *for* Cybersecurity Specialists!



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

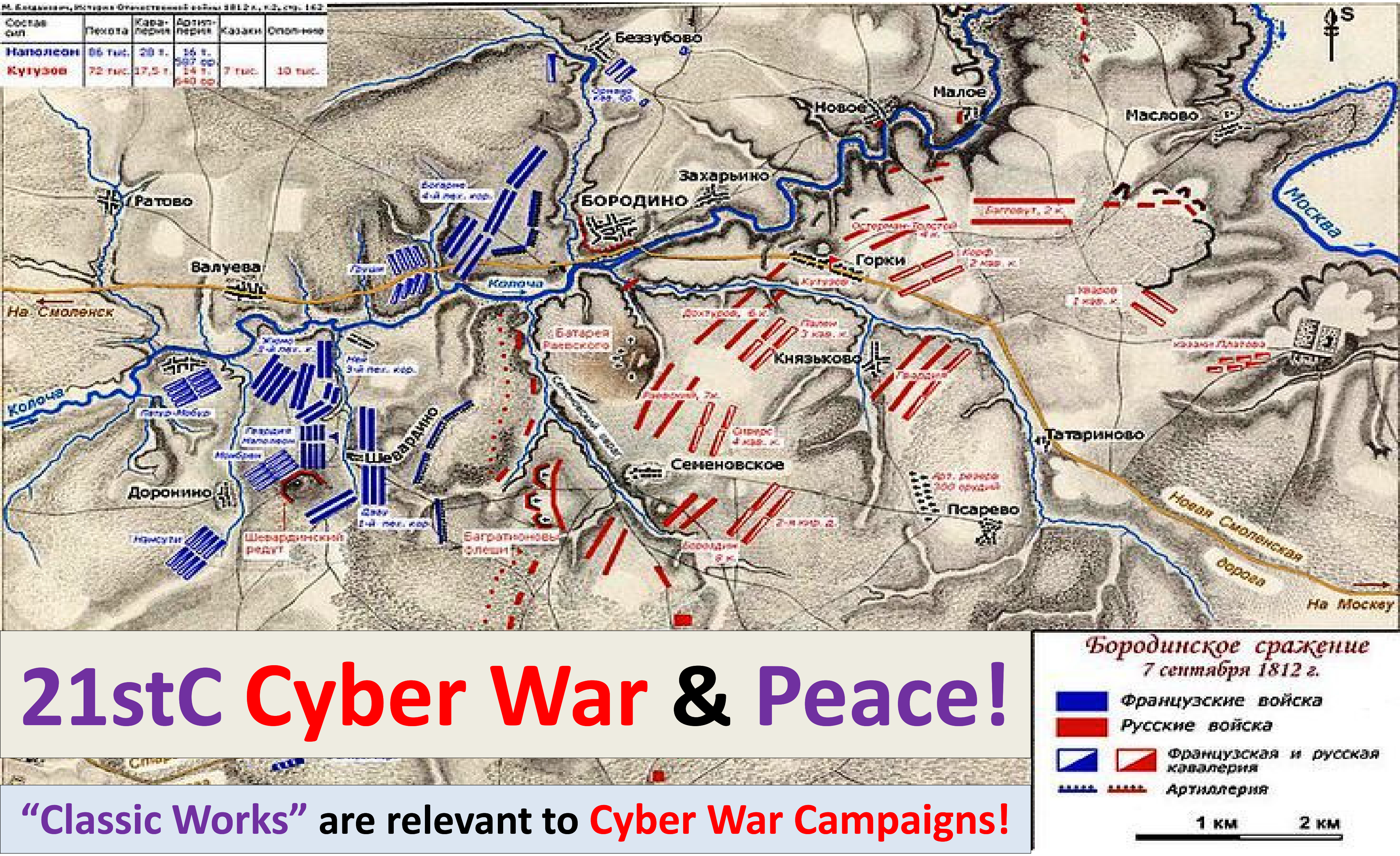
Cyber Criminals now plan Cyber Campaigns & Attacks with In-Depth Research & 21st Weapons!

Classic Campaigns: Battle of Waterloo-1815



"Clauzewitz" is relevant to Cyber Campaigns!

Classical Warfare: Battle of Borodino-1812



М. Богданович, История Отечественной войны 1812 г., т.2, стр. 162

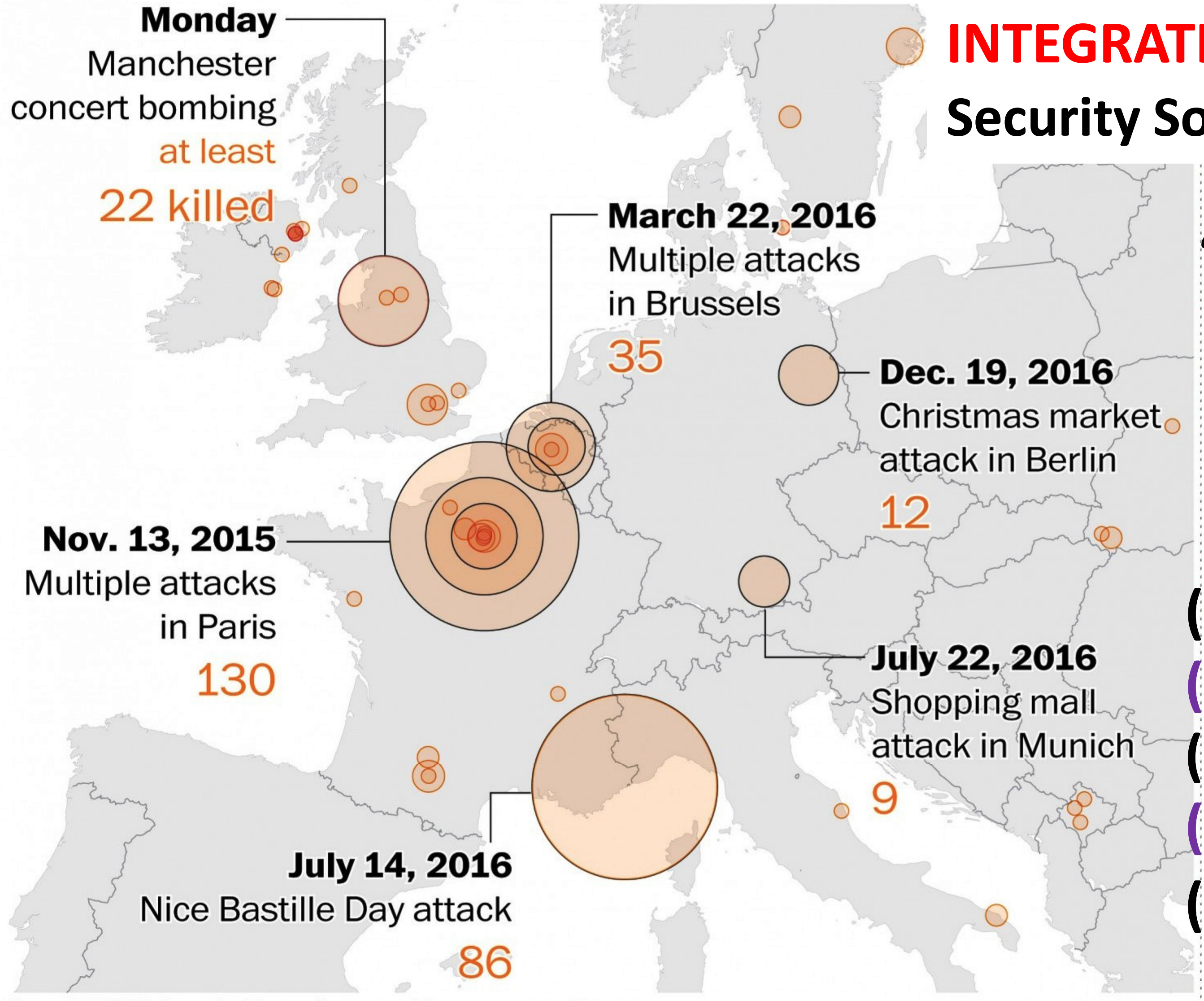
Состав сил	Пехота	Кава-лерия	Артил-лерия	Казаки	Ополч-ние
Наполеон	86 тыс.	28 т.	16 т. 587 ор.		
Кутузов	72 тыс.	17,5 т.	14 т. 640 ор.	7 тыс.	10 тыс.

21stC Cyber War & Peace!

"Classic Works" are relevant to Cyber War Campaigns!

21stC Warfare: "Urban Terrorism"

Terror attacks in Western Europe since 2012



Source: IHS Jane's Terrorism and Insurgency Center

THE WASHINGTON POST

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!**

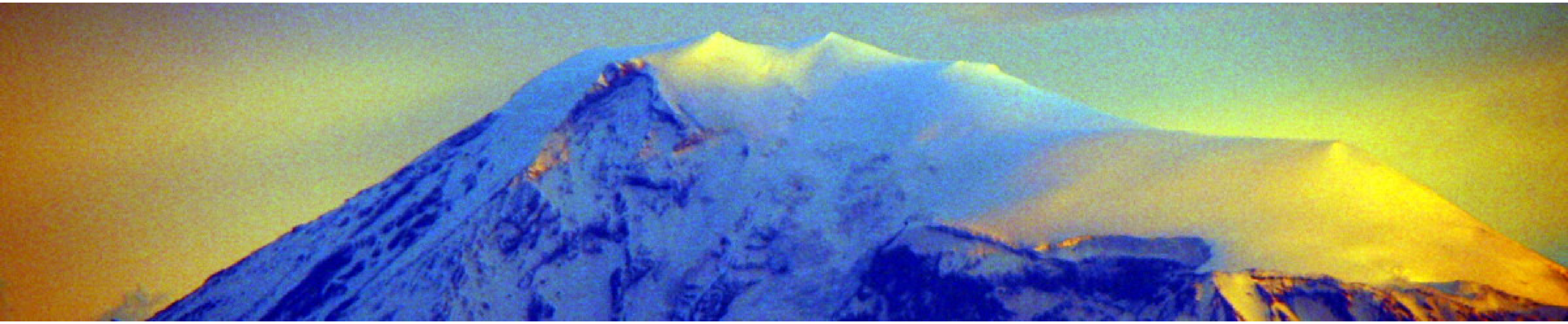
(2) **Research** Urban Targets

(3) **Social Media** for Comms

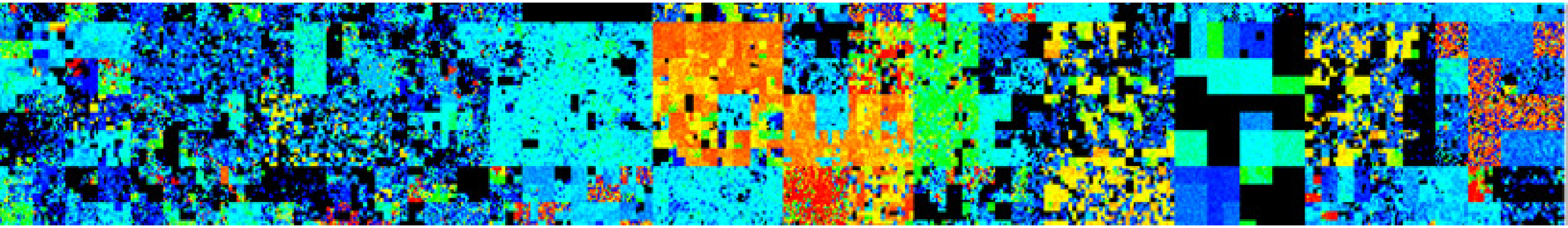
(4) **Recruitment** & Training

(5) **Ransomware** for CA$H..

"Practical Cyber Defence": TOP 10 Cyber Threats!



1 – Cyber Crime, Cyber Terror & Cyber War	2 – Countdown to TOP 10 Cyber Threats!	3 – 21stC Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert: Hack & Attack! **"Cyber Attack"**
7 – In-Depth: 21st Technical Cyber Defence	8 – *YOUR* Operational Cyber Defence	9 – *YOUR* Cyber Defence Campaign Plan!

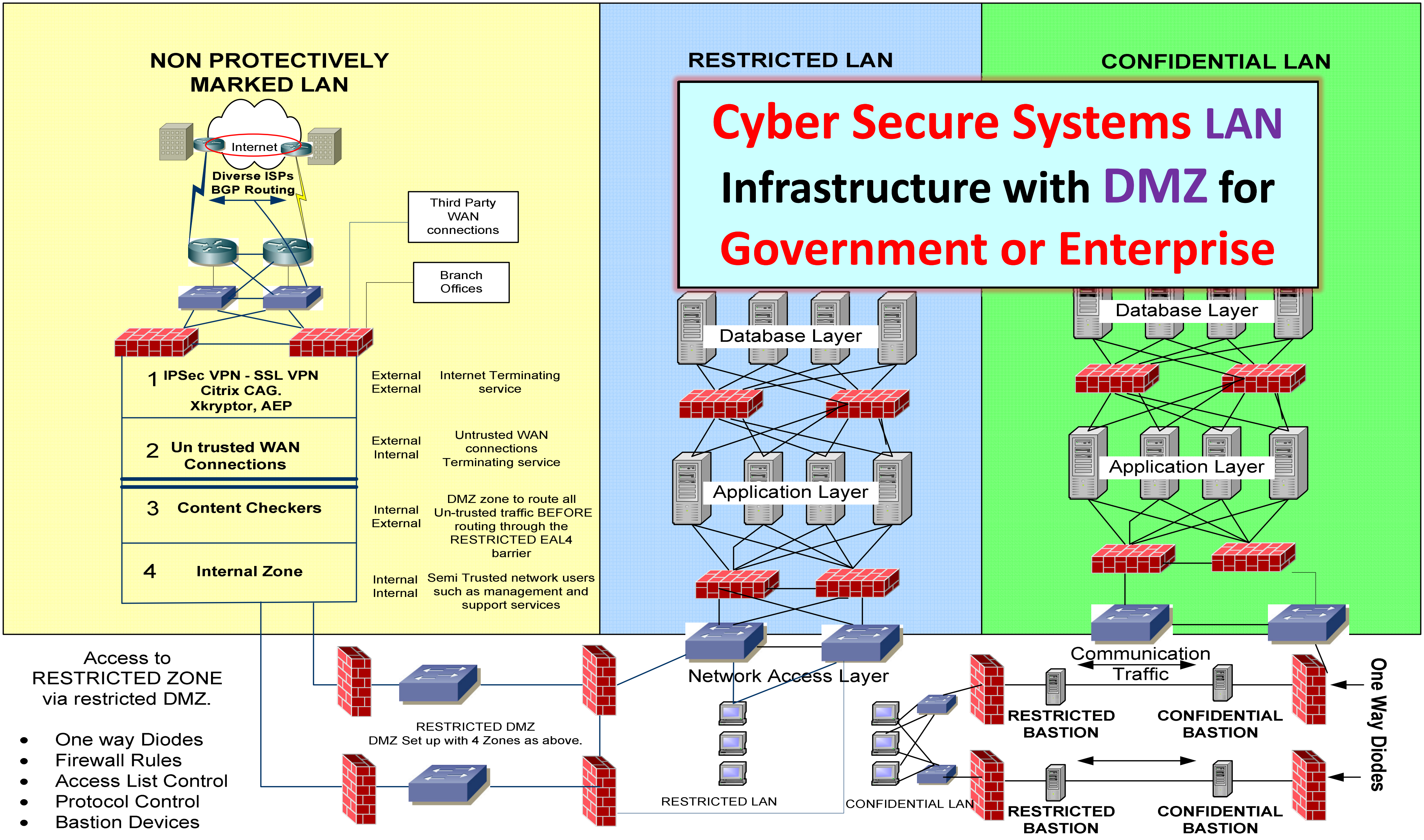


"In-Depth 21stC Technical Cyber Defence"

- 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

TOP Security for Critical Sectors: Govt, Banks, Energy, Transport..



Cyber Secure Systems LAN Infrastructure with DMZ for Government or Enterprise

NON PROTECTIVELY MARKED LAN

Internet

Diverse ISPs BGP Routing

Third Party WAN connections

Branch Offices

1 IPSec VPN - SSL VPN Citrix CAG. Xkryptor, AEP — External External — Internet Terminating service

2 Un trusted WAN Connections — External Internal — Untrusted WAN connections Terminating service

3 Content Checkers — Internal External — DMZ zone to route all Un-trusted traffic BEFORE routing through the RESTRICTED EAL4 barrier

4 Internal Zone — Internal Internal — Semi Trusted network users such as management and support services

RESTRICTED LAN

Database Layer

Application Layer

Network Access Layer

RESTRICTED LAN

CONFIDENTIAL LAN

Database Layer

Application Layer

Communication Traffic

RESTRICTED BASTION

CONFIDENTIAL BASTION

RESTRICTED BASTION

CONFIDENTIAL BASTION

CONFIDENTIAL LAN

One Way Diodes

RESTRICTED DMZ
DMZ Set up with 4 Zones as above.

Access to RESTRICTED ZONE via restricted DMZ.

- One way Diodes
- Firewall Rules
- Access List Control
- Protocol Control
- Bastion Devices

DDoS Mitigation : "Packet Filter"

Packet Filtering

Advantage:

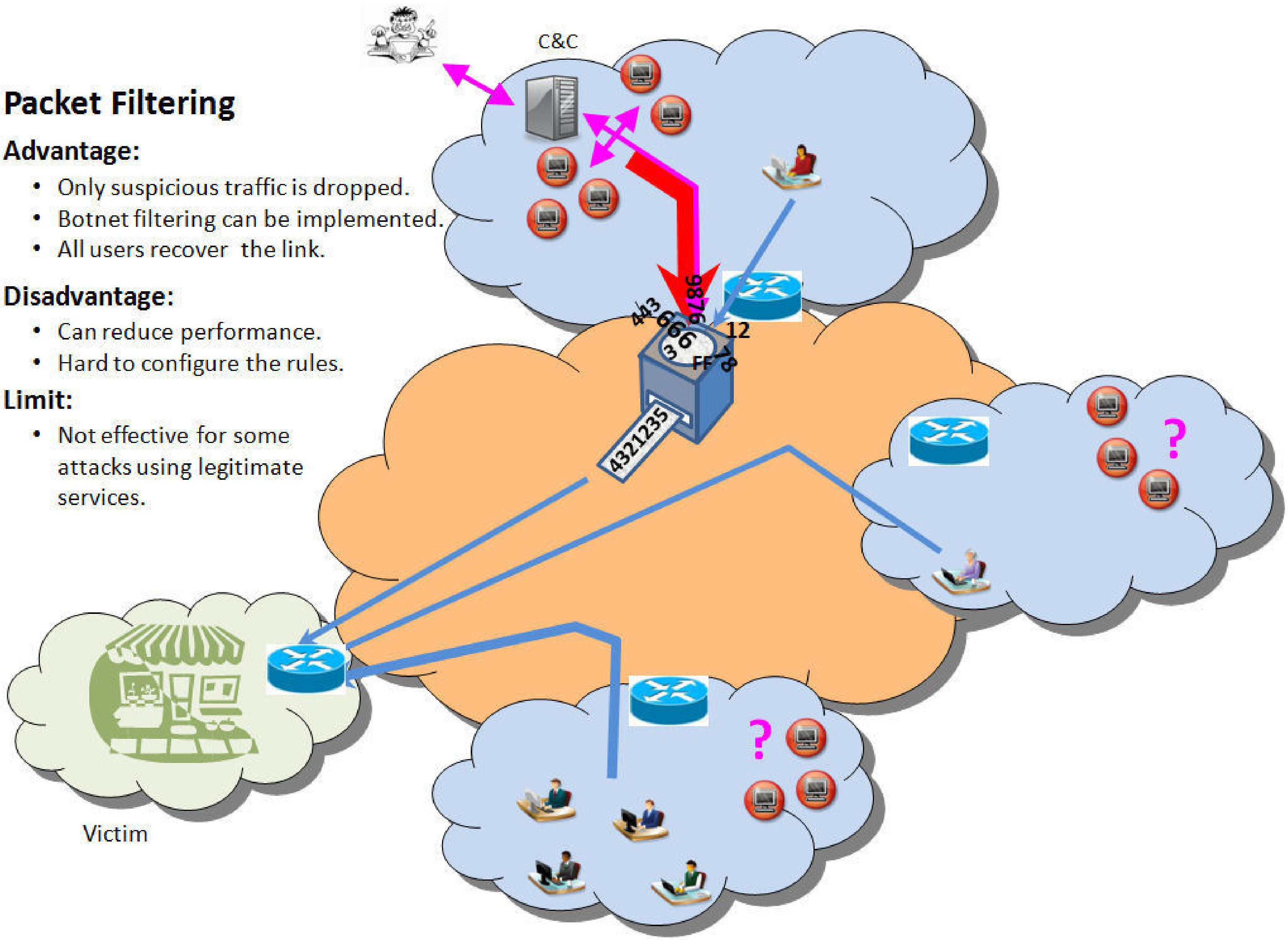
- Only suspicious traffic is dropped.
- Botnet filtering can be implemented.
- All users recover the link.

Disadvantage:

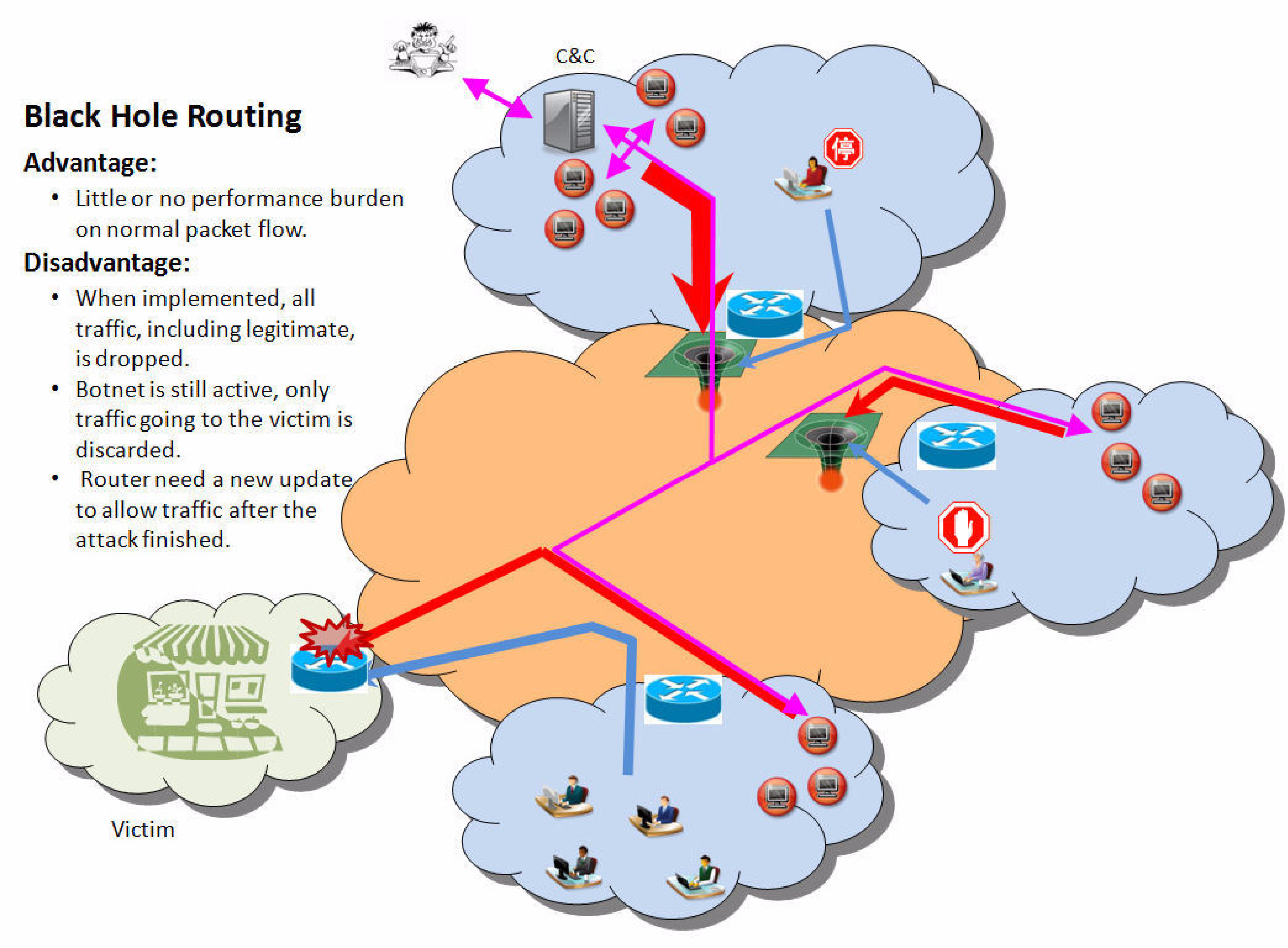
- Can reduce performance.
- Hard to configure the rules.

Limit:

- Not effective for some attacks using legitimate services.



Mitigate DDoS Attack: “Black-Holing”



Black Hole Routing

Advantage:

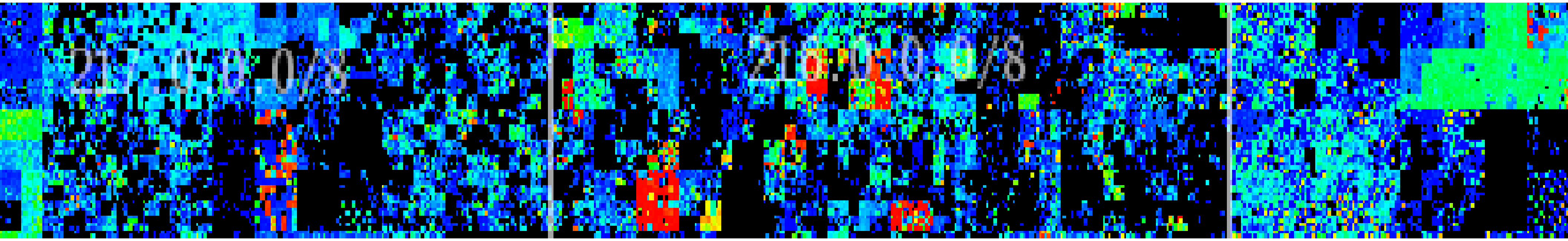
- Little or no performance burden on normal packet flow.

Disadvantage:

- When implemented, all traffic, including legitimate, is dropped.
- Botnet is still active, only traffic going to the victim is discarded.
- Router need a new update to allow traffic after the attack finished.

"Practical Cyber Defence": TOP 10 Cyber Threats!

1 – Cyber Crime, Cyber Terror & Cyber War	2 – Countdown to TOP 10 Cyber Threats!	3 – 21stC Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **"Exploration"**	5 – Cyber Entry & Exit Routes & Tools **"Penetration"**	6 – Real-Time Cyber Alert: Hack & Attack! **"Cyber Attack"**
7 – In-Depth: 21stC Technical Cyber Defence	8 – ***YOUR*** Operational Cyber Defence	9 – ***YOUR*** Cyber Defence Campaign Plan!



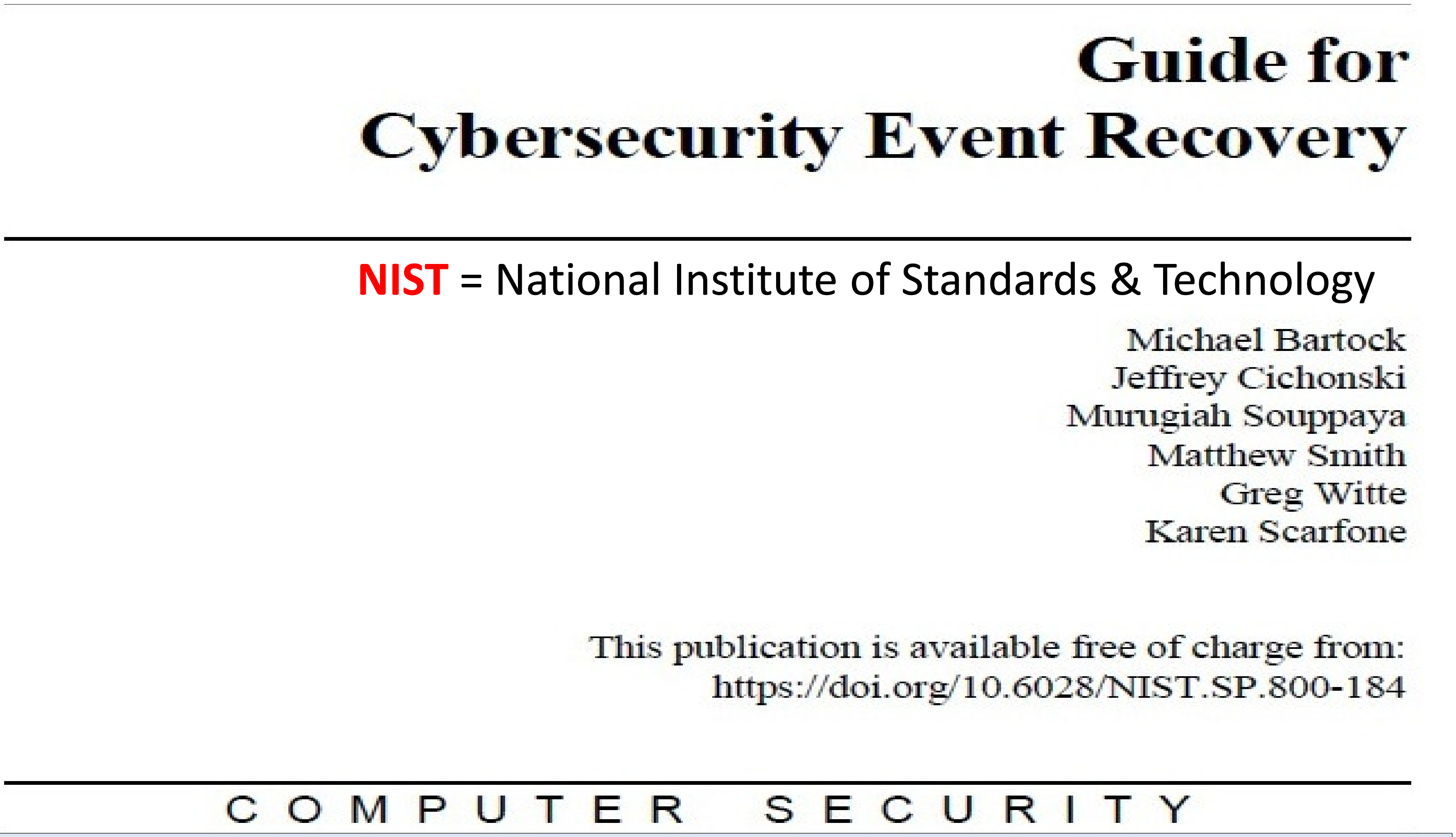
"YOUR Operational Cyber Defence"

- **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

Recommended Technical Handbook: **January 2017**



Guide for Cybersecurity Event Recovery

NIST = National Institute of Standards & Technology

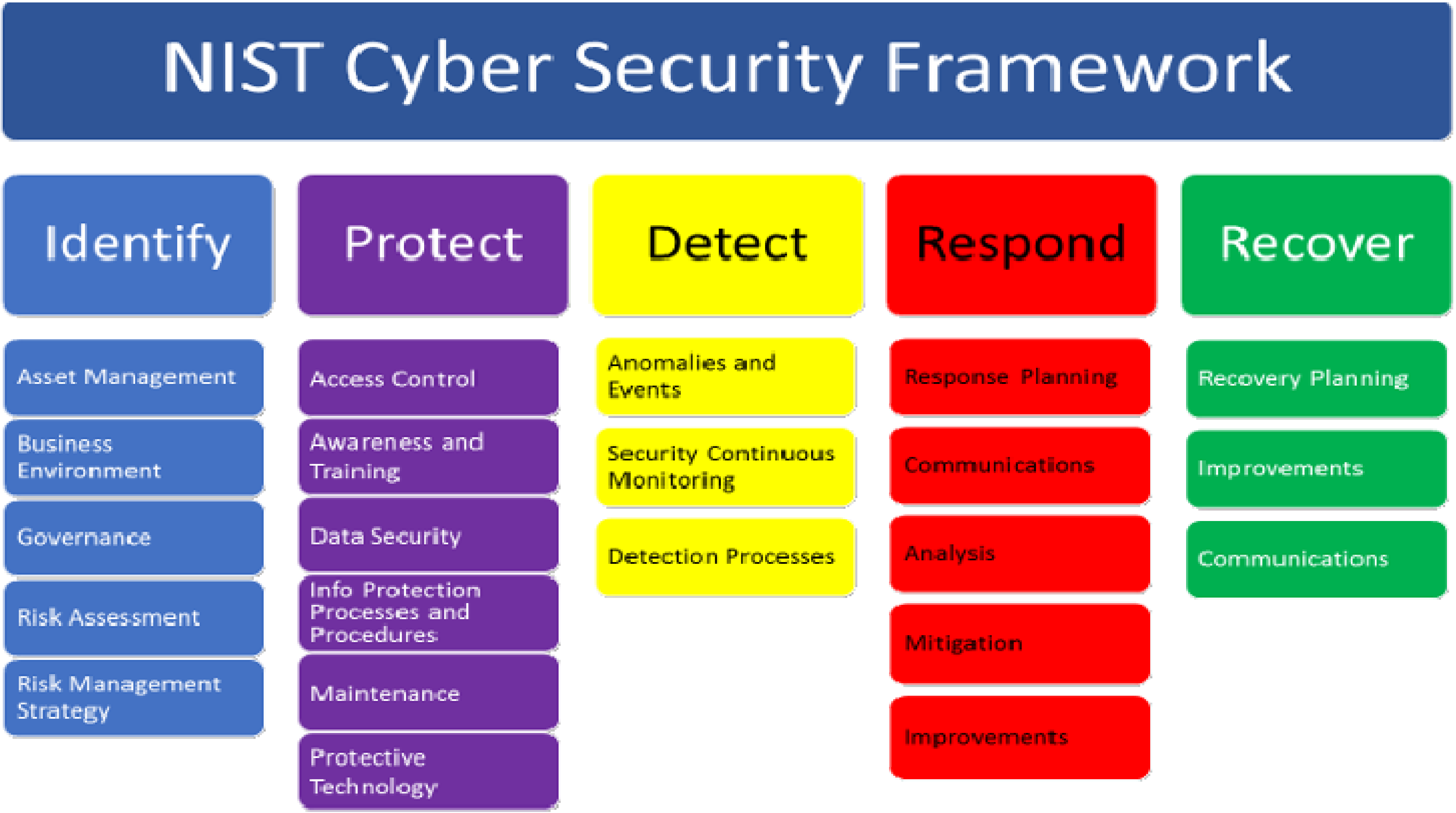
Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
Matthew Smith
Greg Witte
Karen Scarfone

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

COMPUTER SECURITY

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

Guide to CyberSecurity Event Recovery:NIST



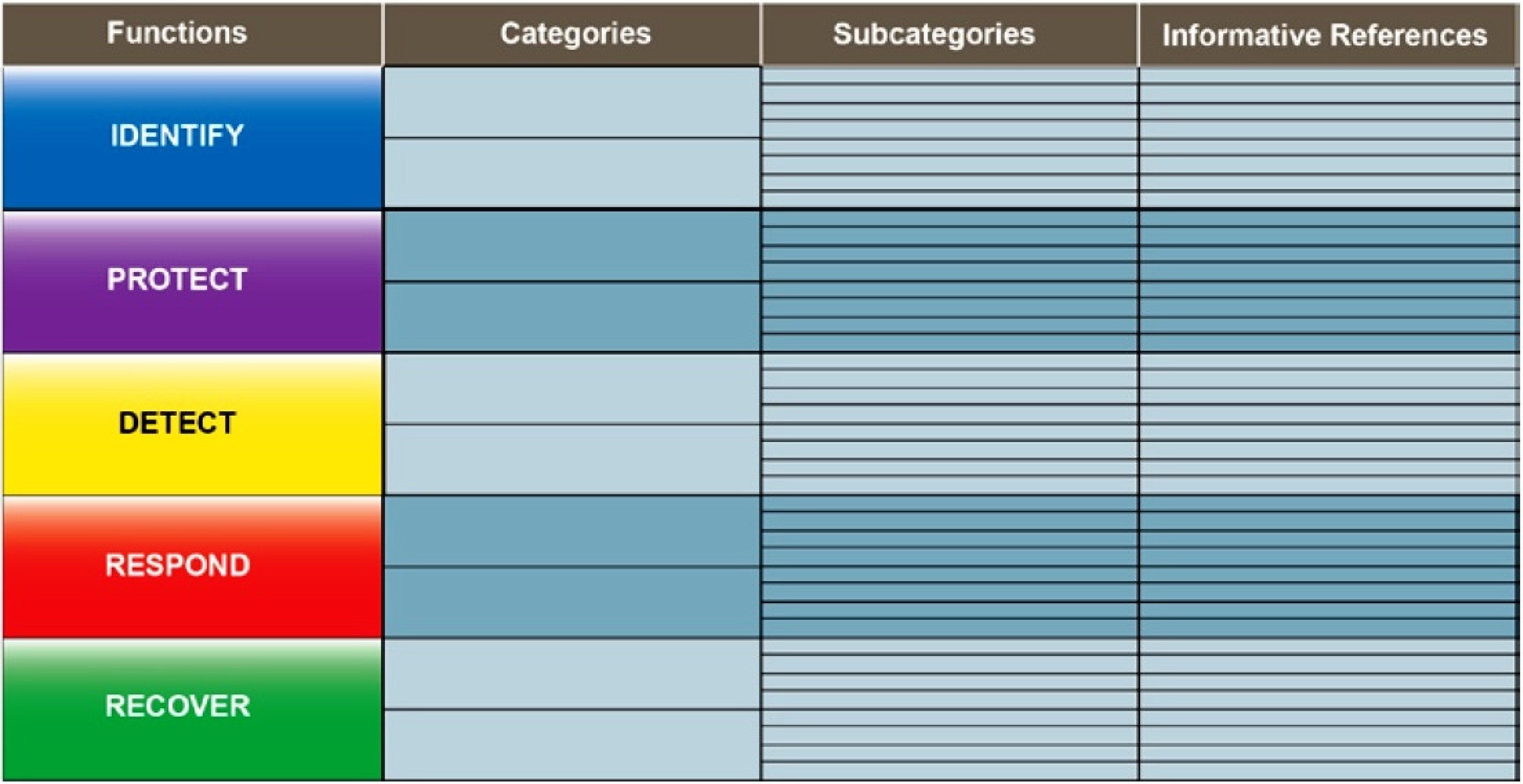
NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

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

NIST *Cybersecurity* Framework

National Institute of Standards & Technology

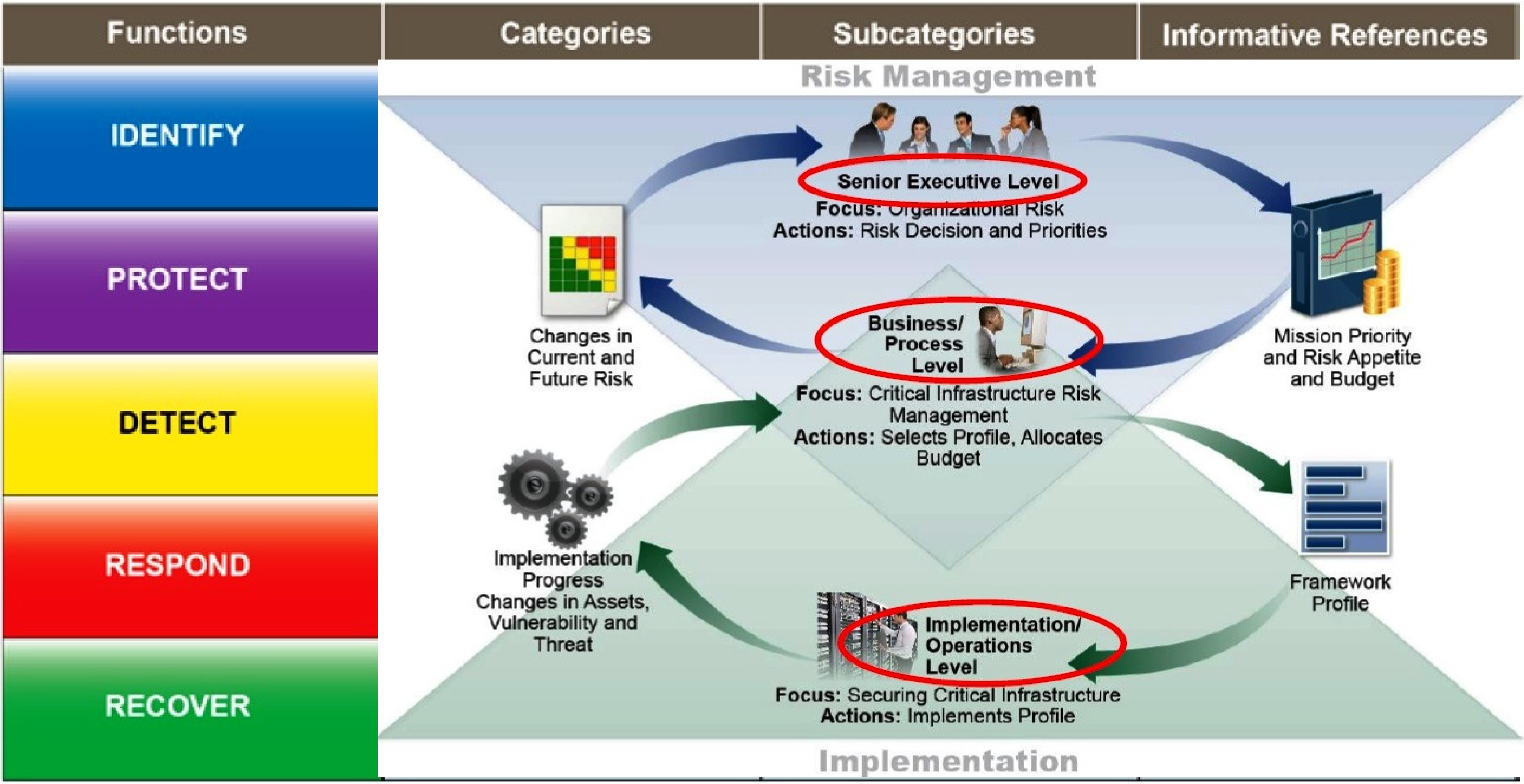


Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Web: www.nist.gov/cyberframework/

NIST *Cybersecurity* Framework

National Institute of Standards & Technology



Functions | Categories | Subcategories | Informative References

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Risk Management

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

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

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

Implementation Progress Changes in Assets, Vulnerability and Threat

Framework Profile

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

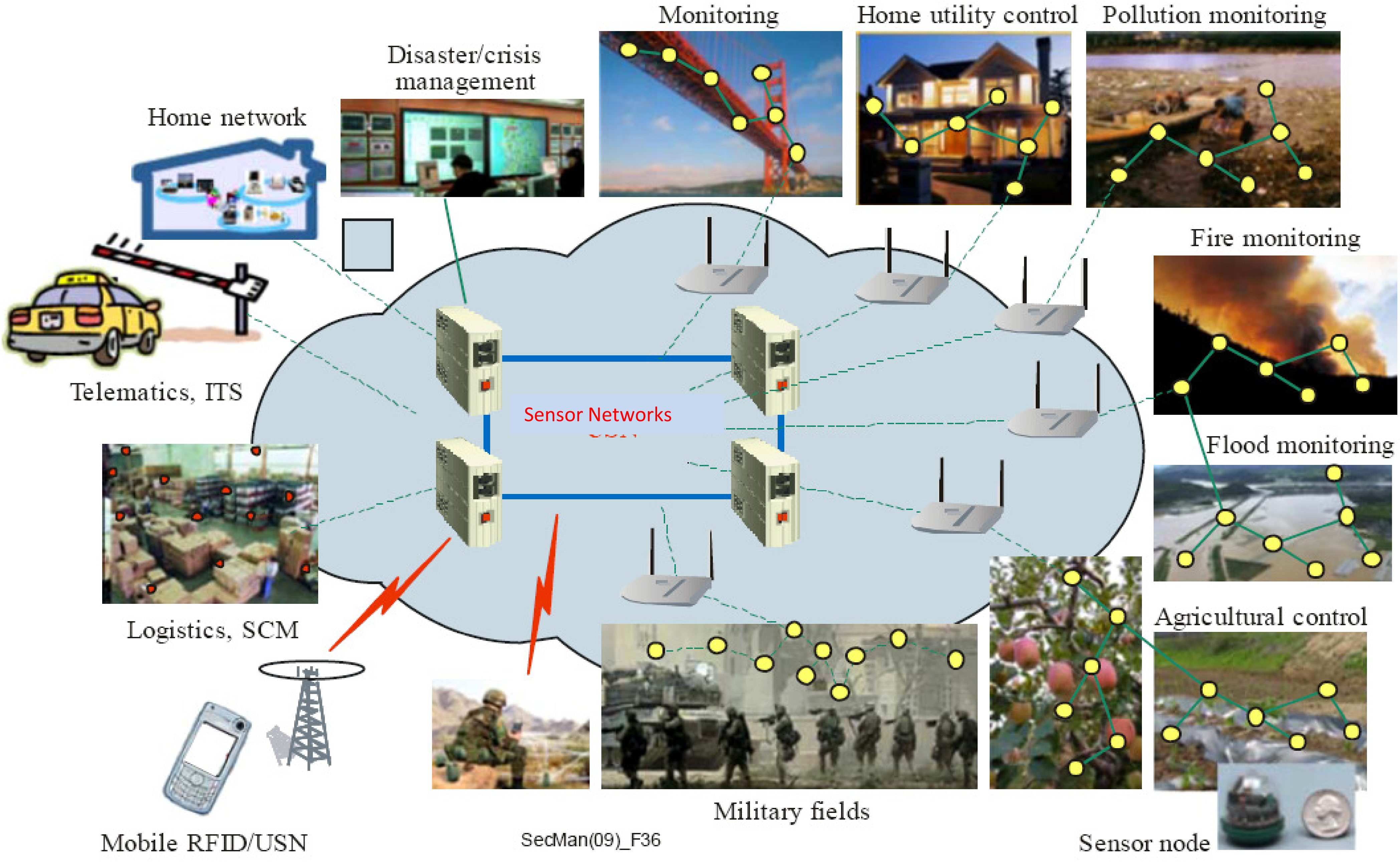
Implementation

Web: www.nist.gov/cyberframework/

35th International East/West Security Conference

- Practical Defence: TOP 10 Cyber Threats -
"Real-Time Tools, Operations & Training"
*** Genoa, Italy – 5th & 6th June 2017 ***
© *Dr David E. Probert : www.VAZA.com* ©

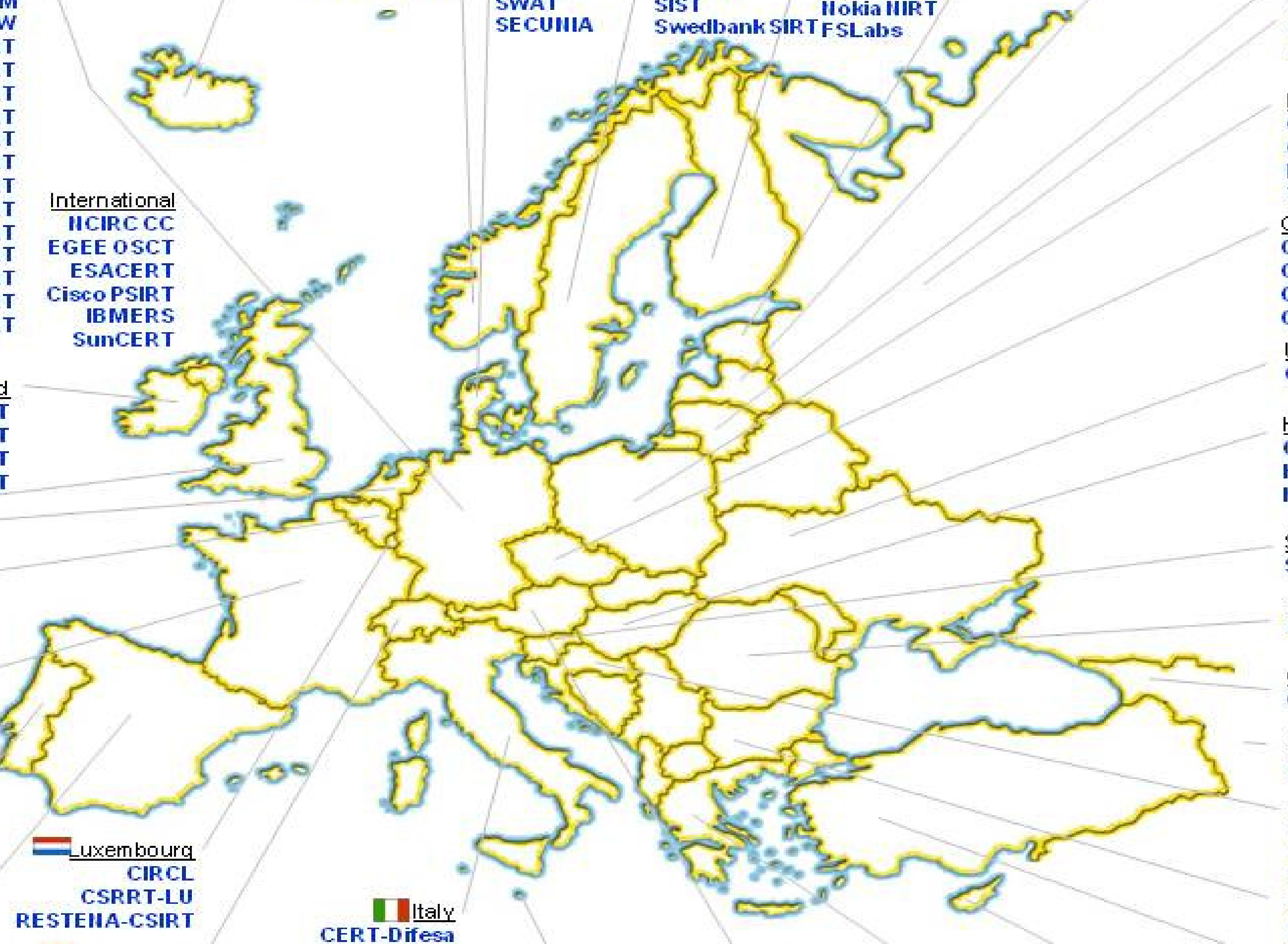
Cybersecurity for Critical Sector "Sensor Networks" (IoT)



ENISA: European Computer Emergency Response Network

enisa
European Network and Information Security Agency

CERTs in Europe



United Kingdom
BP DSAC
BTCERTCC
CITIGROUP (UK)
CSIRTUK
DAN-CERT
DCSIRT
E-CERT
EUCS-IRT
GovCertUK
JANET-CSIRT
MLCIRT (UK)
MODCERT
OxCERT
Q-CIRT
RBSG-ISIRT
RMCSIRT

Netherlands (The)
AAB GCIRT
AMC-CERT
CERT-IDC
CERT-KUN
CERT-RUG
CERT-UU
GOVCERT.NL
KPN-CERT
ING Global CIRT
SURFCERT
UvA-CERT
RABOBANK SOC
Edutel-CSIRT

France
CERTA
Cert-IST
CERT-LEXSI
CERT-Renater
CERT-Societe General
ISIRT
APOGEESecWatch
CSIRT BNP Paribas

Germany
BFK
CERT-BUND
CERTBw
CERTCOM
CERT-VW
ComCERT
dCERT
DFN-CERT
FSC-CERT
GNS-CERT
PRE-CERT
RUS-CERT
S-CERT
SAP CERT
SECU-CERT
Siemens-CERT
Telekom-CERT
KIT-CERT

Ireland
HEANET-CERT
POP CAP-CSIRT
Jumper CSIRT
IRISS CERT

Belgium
BELNET CERT
CERT.BE

Portugal
CERT.PT
CERT-IPN
CSIRT.FEUP

Spain
CCN-CERT
CSIRTCV
e-LC CSIRT
esCERT-UPC
INTECO-CERT
IRIS-CERT

Iceland
RHnet CERT

International
NCIRC CC
EGEE OSCT
ESACERT
Cisco PSIRT
IBMERS
SunCERT

Luxembourg
CIRCL
CSRRT-LU
RESTENA-CSIRT

Switzerland
CC-SEC
CERN CERT
IP+ CERT
OS-CIRT
SWITCH-CERT

Norway
NorCERT
UiO-CERT
UniNett CERT

Italy
CERT-Difesa
CERT ENEL
CERT-IT
CERT-RAFVG
GARR-CERT
GovCERT.IT
S2OC
SICEI-CERT

Denmark
CSIRT.DK
DK-CERT
KMD IAC
SWAT
SECUNIA

Malta
mtCERT

Sweden
SITIC
SUNet CERT
TS-CERT
SIST
Swedbank SIRT

Finland
CERT-FI
Ericsson PSIRT
Funet CERT
Nokia NIRT
FSLabs

Austria
ACOnet-CERT
CERT.AT
GOVCERT
R-IT CERT

Estonia
CERT-EE
SKY-CERT

Greece
AUTH-CERT
FORTH CERT
GRNET-CERT

Latvia
DDIRV
CERT NIC.LV

Lithuania
CERT-LT
LITNET CERT
IST-SVDPT

Russia
RU-CERT
WebPlus ISP

Poland
CERT GOVPL
CERT POLSKA
PIONIER-CERT
TP CERT

Czech Republic
CESNET-CERTS
CSIRT.CZ
CZNIC-CSIRT
CSIRT-MU

Ukraine
CERT-UA

Hungary
CERT-Hungary
HUN-CERT
NIIF-CSIRT

Slovenia
SI-CERT

Romania
RoCSIRT

Georgia
CERT-GE

Azerbaijan
CERT AzEduNET

Croatia
CARNet CERT
CERT ZSIS
HR-CERT

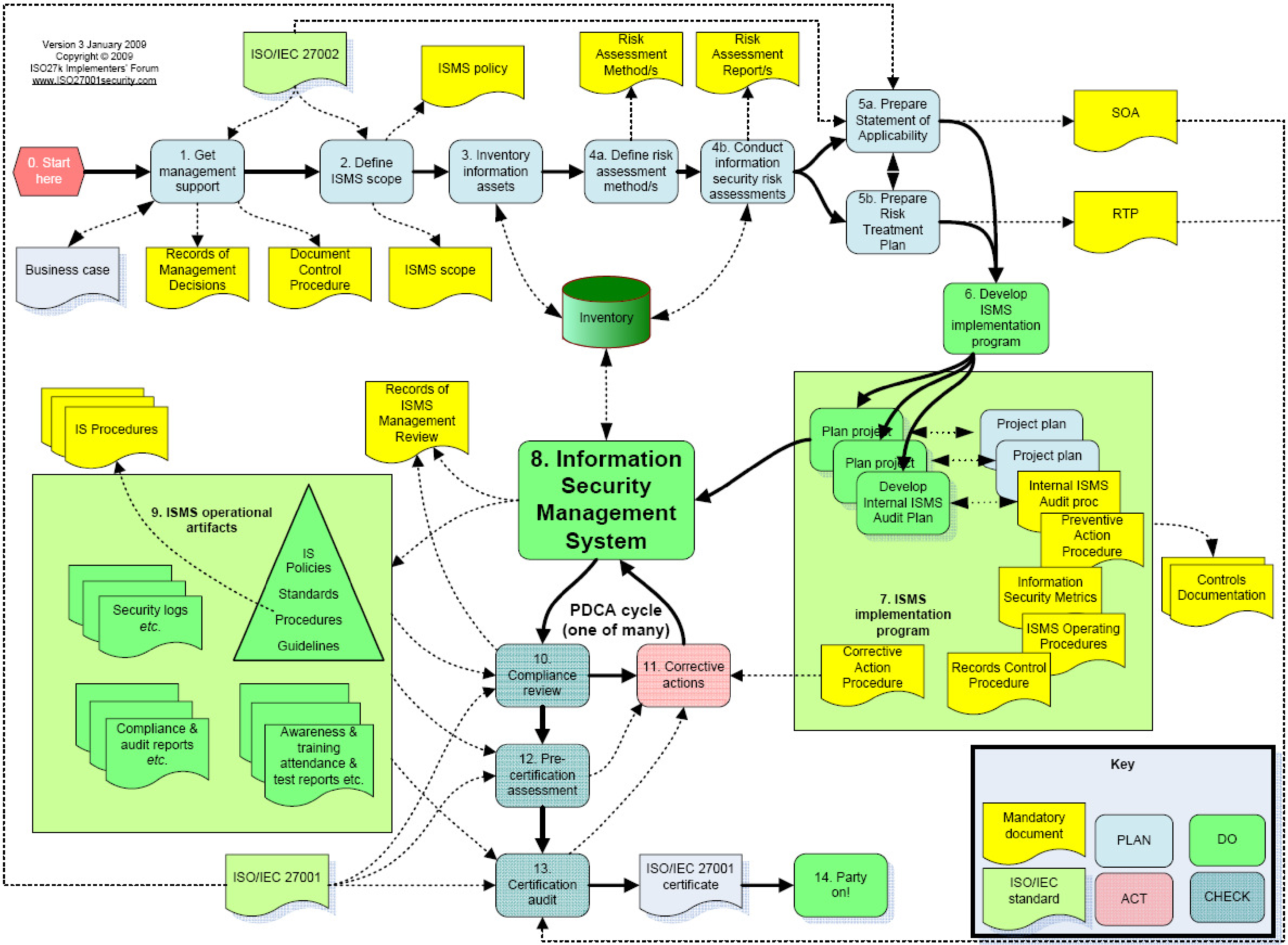
Bulgaria
CERT Bulgaria

Turkey
TR-CERT
Ulak-CSIRT

Cyprus
CYPRUS

CERTS in Europe map, June 2010 v2.0 http://www.enisa.europa.eu/act/cert/background/inv © European Network and Information Security Agency (ENISA)

Flow-Chart: ISO27001 CyberSecurity Certification



Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com

ISO/IEC 27002

ISMS policy

Risk Assessment Method/s

Risk Assessment Report/s

5a. Prepare Statement of Applicability

SOA

0. Start here

1. Get management support

2. Define ISMS scope

3. Inventory information assets

4a. Define risk assessment method/s

4b. Conduct information security risk assessments

5b. Prepare Risk Treatment Plan

RTP

Business case

Records of Management Decisions

Document Control Procedure

ISMS scope

Inventory

6. Develop ISMS implementation program

IS Procedures

Records of ISMS Management Review

8. Information Security Management System

Plan project

Plan project

Develop Internal ISMS Audit Plan

Project plan

Project plan

Internal ISMS Audit proc

Preventive Action Procedure

Controls Documentation

9. ISMS operational artifacts

IS Policies

Standards

Procedures

Guidelines

Security logs *etc.*

Information Security Metrics

ISMS Operating Procedures

7. ISMS implementation program

PDCA cycle (one of many)

10. Compliance review

11. Corrective actions

Corrective Action Procedure

Records Control Procedure

Compliance & audit reports *etc.*

Awareness & training attendance & test reports etc.

12. Pre-certification assessment

Key

Mandatory document

PLAN

DO

ISO/IEC standard

ACT

CHECK

ISO/IEC 27001

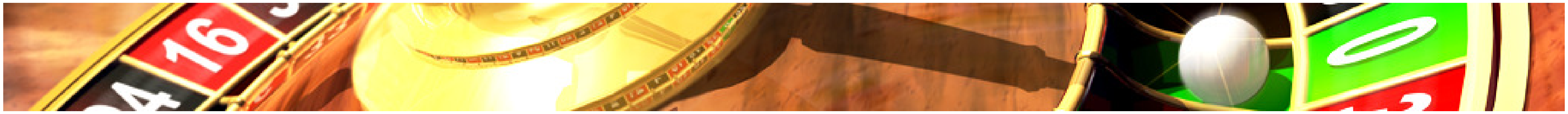
13. Certification audit

ISO/IEC 27001 certificate

14. Party on!

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...*



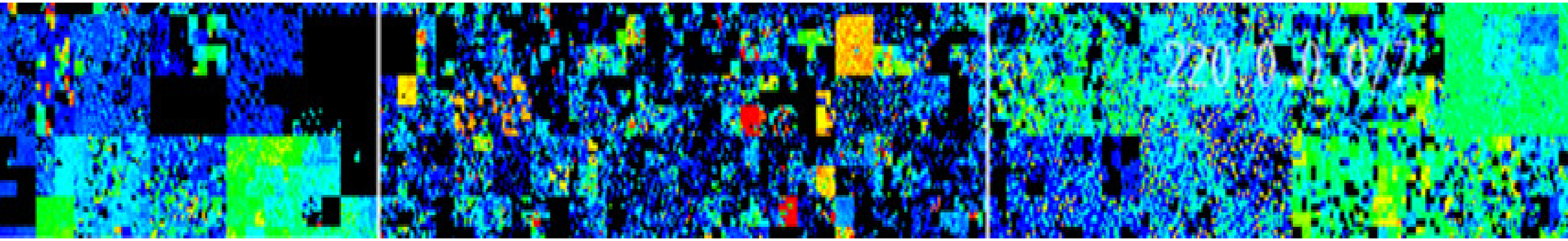
.....Research Programme initiated following ***UN/ITU*** *CyberSecurity Training @* ***UTECH – September 2010....***

UN/ITU: 5-day Cybersecurity Workshop - Jamaica 2010

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

“Practical Cyber Defence”: TOP 10 Cyber Threats!

1 – Cyber Crime, Cyber Terror & Cyber War	2 – Countdown to TOP 10 Cyber Threats!	3 – 21stC Cyber Hack & Attack Campaigns
4 – Cyber Intelligence Gathering Tools **“Exploration”**	5 – Cyber Entry & Exit Routes & Tools **“Penetration”**	6 – Real-Time Cyber Alert: Hack & Attack! **“Cyber Attack”**
7 – In-Depth: 21stC Technical Cyber Defence	8 – *YOUR* Operational Cyber Defence	9 – *YOUR* Cyber Campaign Action 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

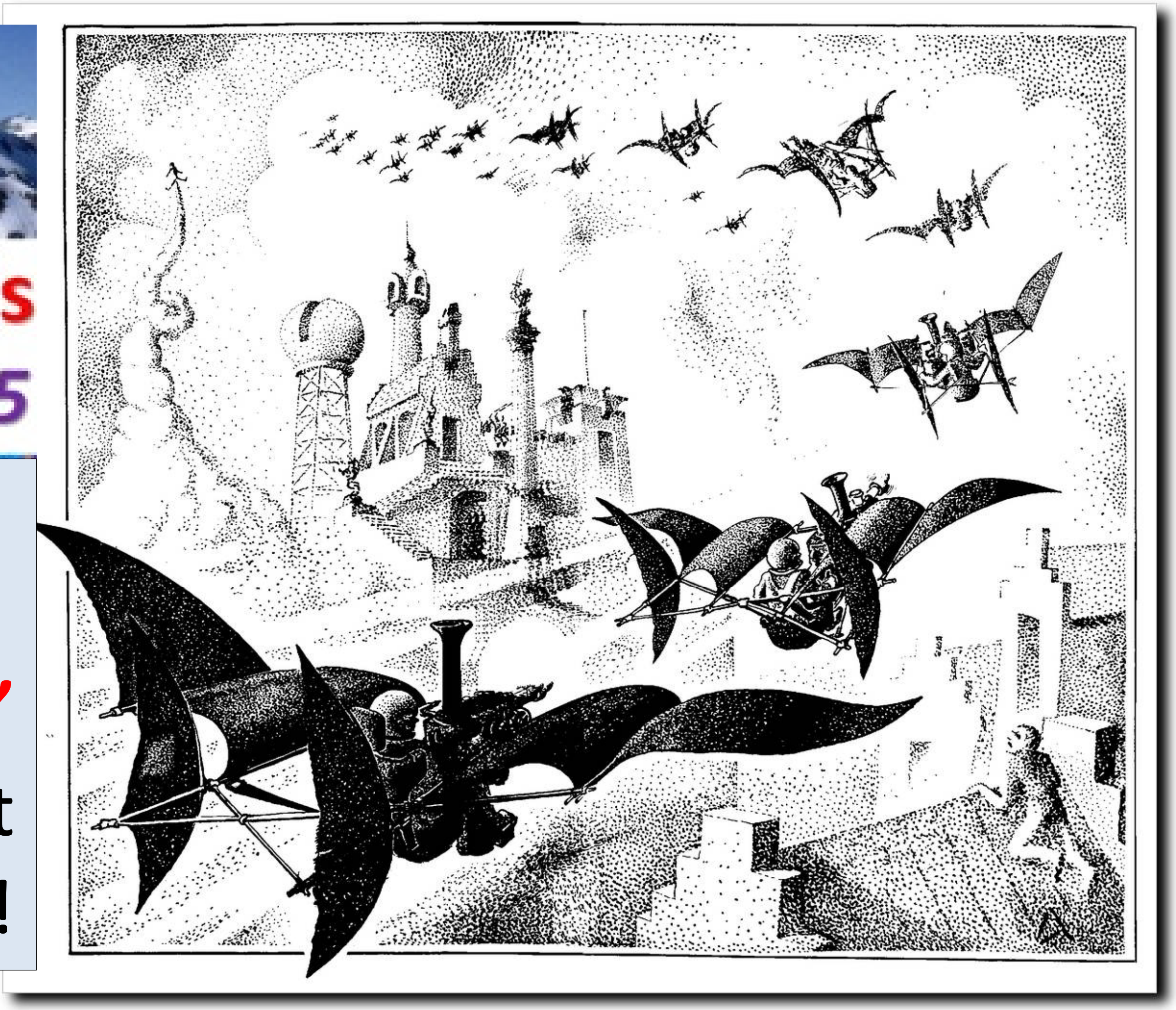
....**CyberSecurity** is Continuously Evolving so keep up with **Conferences & Professional Memberships**!....

“Cyber Defence” *against* “Alien Invaders”

Cyber Tools and Trends

Next 7 Years: 2018 - 2025

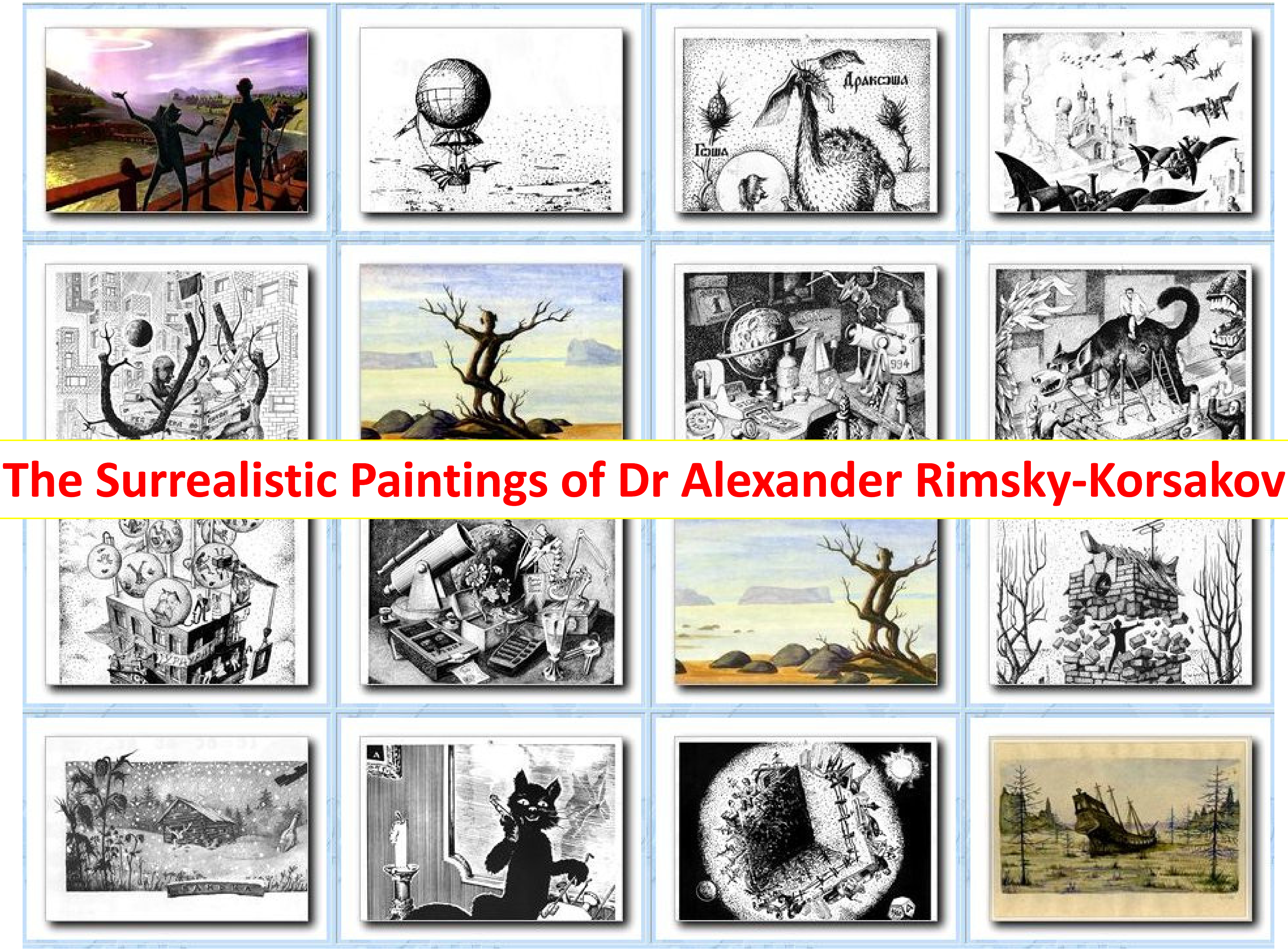
A.I. & Machine Learning CyberSecurity Tools will Provide ***“Speed of Light”*** Real-Time Defence against ***TOP 10*** Threats & Attacks!



“Steam Powered Birds arrive over our Cities! - 1981

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

The Surrealistic Paintings of Dr Alexander Rimsky-Korsakov



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

"Practical Cyber Defence": Top 10 Cyber Threats

International East-West Security Conference: Genoa

Download Presentation Slides:

www.Valentina.net/Genoa2017/

"Practical Cyber Defence": Top 10 Cyber Threats

International East-West Security Conference: Genoa

Thank-You!

Download Presentation Slides:

www.Valentina.net/Genoa2017/

East-West Security Conference – Genoa 2017

-"21stC CyberSecurity Trends"-

Practical Cyber Defence

-TOP 10 Cyber Threats-

Dr David E. Probert
VAZA International

Dedicated to Grand-Sons: Ethan, Matthew, Roscoe & Hugh – Securing YOUR Future!

35th International East/West Security Conference

- Practical Defence: TOP 10 Cyber Threats -
"Real-Time Tools, Operations & Training"
*** Genoa, Italy – 5th & 6th June 2017 ***
© Dr David E. Probert : www.VAZA.com ©

1

Cyber Tools and Trends

Next 7 Years: 2018 - 2025

Dr David E. Probert
VAZA International

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

35th International East/West Security Conference

- CyberSecurity Tools and Trends -
"From 2018 to 2025 and Beyond! "
*** Genoa, Italy – 5th & 6th June 2017 ***
© Dr David E. Probert : www.VAZA.com ©

1

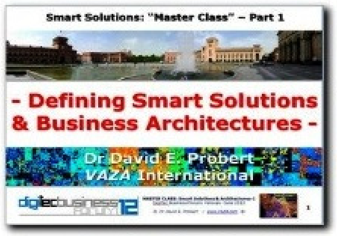
Theme (1) –"TOP 10 Cyber Threats" **Theme (2) –"CyberTrends: 2018-2025"**

Download Link: www.valentina.net/Genoa2017/

Download Presentation Slides: *www.Valentina.net/Genoa2017/*

Thank you for your time!

Additional *Cybersecurity* Resources


Smart Solutions: "Master Class" – Part 1

- Defining Smart Solutions & Business Architectures -

Dr David E. Probert
VAZA International

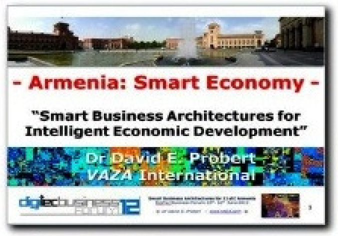
"Master Class - Smart Theory & Practice

Smart Solutions: "Master Class" – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

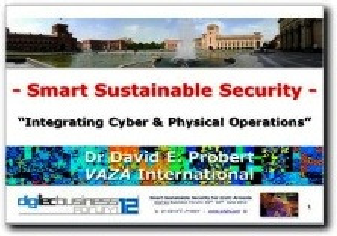
"Master Class 2012 - Smart Design"


- Armenia: Smart Economy -

"Smart Business Architectures for Intelligent Economic Development"

Dr David E. Probert
VAZA International

"21stC Armenia- 2012: Smart Economy"


- Smart Sustainable Security -

"Integrating Cyber & Physical Operations"

Dr David E. Probert
VAZA International

"21stC Armenia - 2012: Smart Security"

- Smart Governance -

"Stimulating Innovation & Economic Growth"

Dr David E. Probert
VAZA International

"21stC Armenia: Smart Governance"

"Real-Time Armenia"

"Securing Government & Financial Enterprise Operations"

"Real-Time Armenia" - White Paper

"Real-Time" ARMENIA!...

...Securing Government & Financial Enterprise Operations

Dr David E Probert
VAZA International

"Real-Time Armenia" - Slides

"Awesome Armenia!"
Photos and Panoramas

Armenia - Spring - 2009

Armenia - Summer 2009

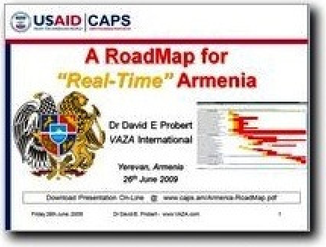
Armenian Panoramas - Summer - 2009

Awesome Armenia: In Photos

"Roadmap for Real-Time Armenia"

USAID | CAPS

Roadmap for Real-Time Armenia- Report

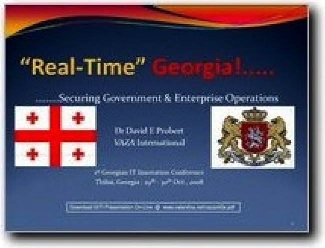

USAID | CAPS

A RoadMap for "Real-Time" Armenia

Dr David E Probert
VAZA International

Yerevan, Armenia
26th June 2009

RoadMap for Real-Time Armenia- Slides


"Real-Time" Georgia!.....

...Securing Government & Enterprise Operations

Dr David E Probert
VAZA International

"Real-Time Georgia" - GITI 2008 Slides

"Real-Time Georgia"

"Securing Government & Enterprise Operations"

"Real-Time Georgia" - GITI 2008 Paper

"Republic of Georgia"
- Photos and Panoramas -

Georgian Panoramas Autumn 2007

Caucasus Aerial Panoramas

Georgian Panoramas Autumn 2008

Georgia 2008

Gorgeous Georgia: In Photos

..."21stC Georgia"...

..."Cyber-Vardzia"...

21stC Georgia: "CyberVardzia" - Paper

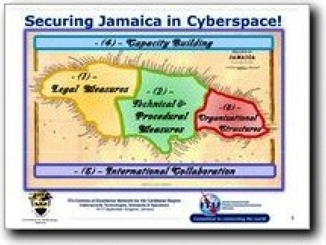
21stC Georgia – "Cyber Vardzia"

"Integrated Cyber & Physical Security"

for e-Government & e-Georgia

Dr David E. Probert
VAZA International

21stC Georgia - "CyberVardzia" - Slides


Securing Jamaica in Cyberspace!

- (4) - Capacity Building

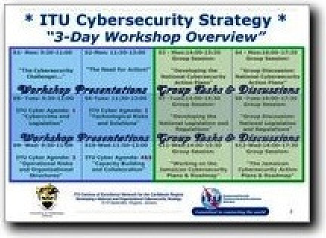
- (1) - Legal Measures

- (2) - Technical & Procedural Measures

- (3) - Organisational Structures

- (5) - International Collaboration

Jamaica: Cybersecurity Technology- Slides

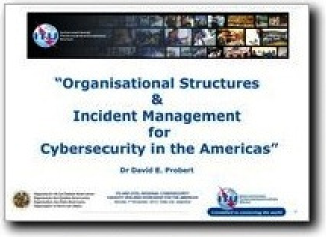

* ITU Cybersecurity Strategy *
"3-Day Workshop Overview"

Workshop Presentations

Group Tasks & Discussions

Jamaica: Cybersecurity Strategy- Slides

"Short Professional Bio"


"Organisational Structures & Incident Management for Cybersecurity in the Americas"

Dr David E. Probert

ITU/CITEL: Cybersecurity in the Americas

"Cybersecurity Capacity Building & International Collaboration "

Dr David E. Probert

ITU/CITEL: Cybersecurity Skills Building

Link: www.valentina.net/vaza/CyberDocs

Professional Profile - *Dr David E. Probert*

- ***Computer Integrated Telephony (CIT)*** – Established and led British Telecom's £25M EIGER Project during the mid-1980s' to integrate computers with telephone switches (PABX's). This resulted in the successful development and launch of CIT software applications for telesales & telemarketing
- ***Blueprint for Business Communities*** – Visionary Programme for Digital Equipment Corporation during late-1980's that included the creation of the "knowledge lens" and "community networks". The Blueprint provided the strategic framework for Digital's Value-Added Networks Business
- ***European Internet Business Group (EIBG***) – Established and led Digital Equipment Corporation's European Internet Group for 5 years. Projects included support for the national Internet infrastructure for countries across EMEA as well as major enterprise, government & educational Intranet deployments. Dr David Probert was a sponsoring member of the European Board for Academic & Research Networking (EARN/TERENA) for 7 years (1991 ➔1998)
- ***Supersonic Car (ThrustSSC)*** – Worked with Richard Noble OBE, and the Mach One Club to set up and manage the 1st Multi-Media and e-Commerce Web-Site for the World's 1st Supersonic Car – ThrustSSC – for the World Speed Record.
- ***Secure Wireless Networking*** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.
- ***Networked Enterprise Security*** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional engineers & a diverse portfolio of hi-tech security products.
- ***Republic of Georgia*** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament, 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.

“Master Class”: Armenia - *DigiTec2012*

- Smart Security, Economy & Governance -

Smart Solutions: “Master Class” – Part 1

- Defining Smart Solutions & Business Architectures -

Dr David E. Probert
VAZA International

MASTER CLASS: Smart Solutions & Architectures-1
DigiTec Business Forum: Yerevan - June 2012
© Dr David E. Probert : www.VAZA.com ©
1

"Master Class - Smart Theory"

Smart Solutions: “Master Class” – Part 2

- Smart Solutions in Practice for 21stC Armenia -

Dr David E. Probert
VAZA International

MASTER CLASS: Smart Solutions & Architectures-2
DigiTec Business Forum: Yerevan - June 2012
© Dr David E. Probert : www.VAZA.com ©
1

"Master Class - Smart Practice"

Smart Solutions: “Master Class” – Part 3

- Designing & Engineering Smart Solutions -

Dr David E. Probert
VAZA International

MASTER CLASS: Smart Solutions & Architectures-3
DigiTec Business Forum: Yerevan - June 2012
© Dr David E. Probert : www.VAZA.com ©
1

"Master Class - Smart Design"

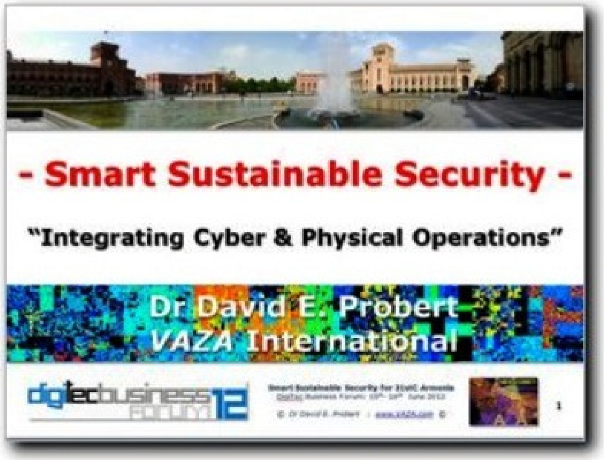
- Armenia: Smart Economy -

“Smart Business Architectures for Intelligent Economic Development”

Dr David E. Probert
VAZA International

Smart Business Architectures for 21stC Armenia
DigiTec Business Forum: 15th - 16th June 2012
© Dr David E. Probert : www.VAZA.com ©
1

"Armenia: Smart Economy"



- Smart Sustainable Security -

“Integrating Cyber & Physical Operations”

Dr David E. Probert
VAZA International

Smart Sustainable Security for 21stC Armenia
DigiTec Business Forum: 15th - 16th June 2012
© Dr David E. Probert : www.VAZA.com ©
1

"Armenia: Smart Sustainable Security"

- Smart Governance -

“Stimulating Innovation & Economic Growth”

Dr David E. Probert
VAZA International

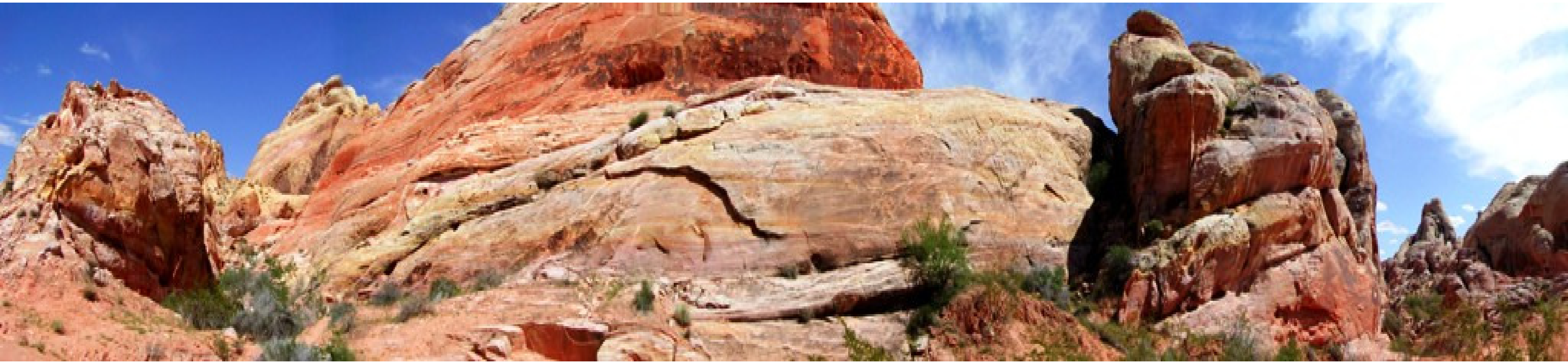
Smart Governance for 21stC Armenia
DigiTec Business Forum: 15th - 16th June 2012
© Dr David E. Probert : www.VAZA.com ©
1

"Armenia: Smart Governance"

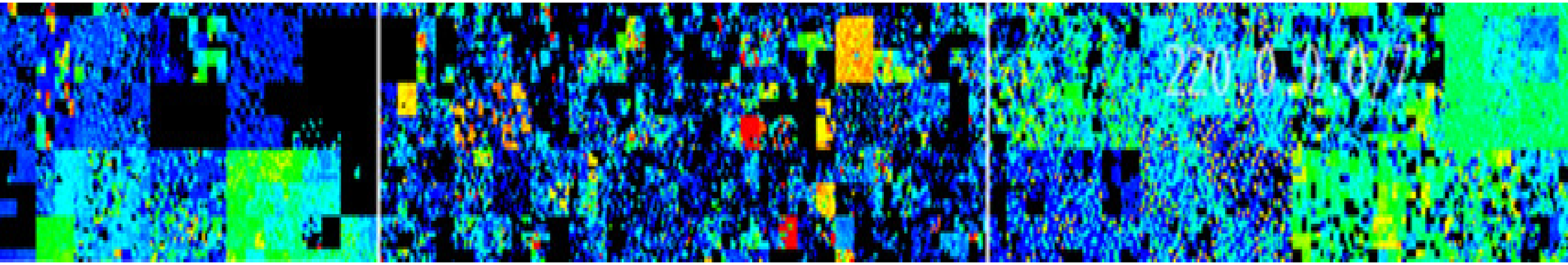
Download: www.valentina.net/DigiTec2012/

"Practical Defence: TOP 10 Cyber Threats!"

35th International East-West Security Conference: Genoa, Italy



BACK-UP SLIDES



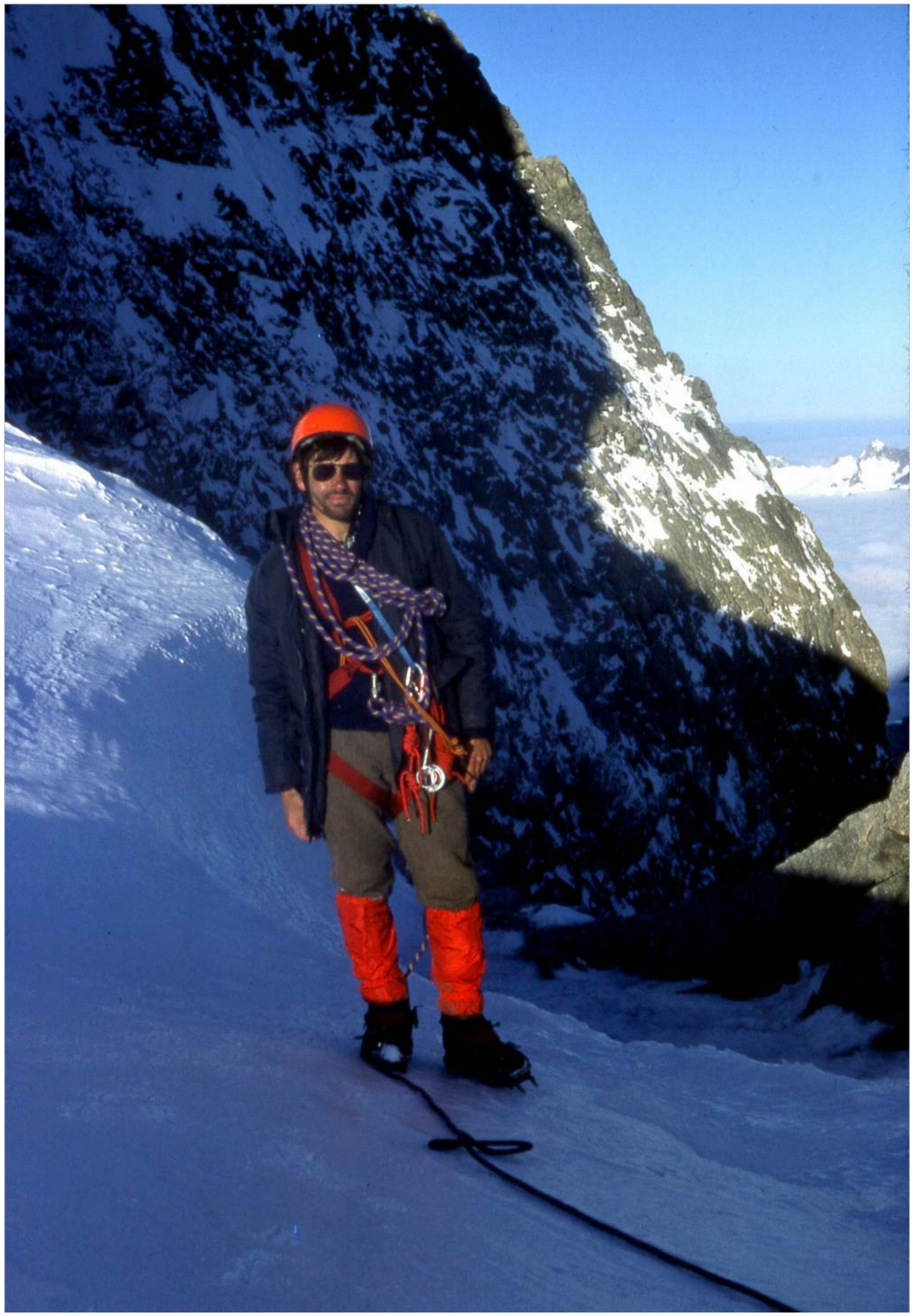
*** Security Equipment for Alpine Climbing ***

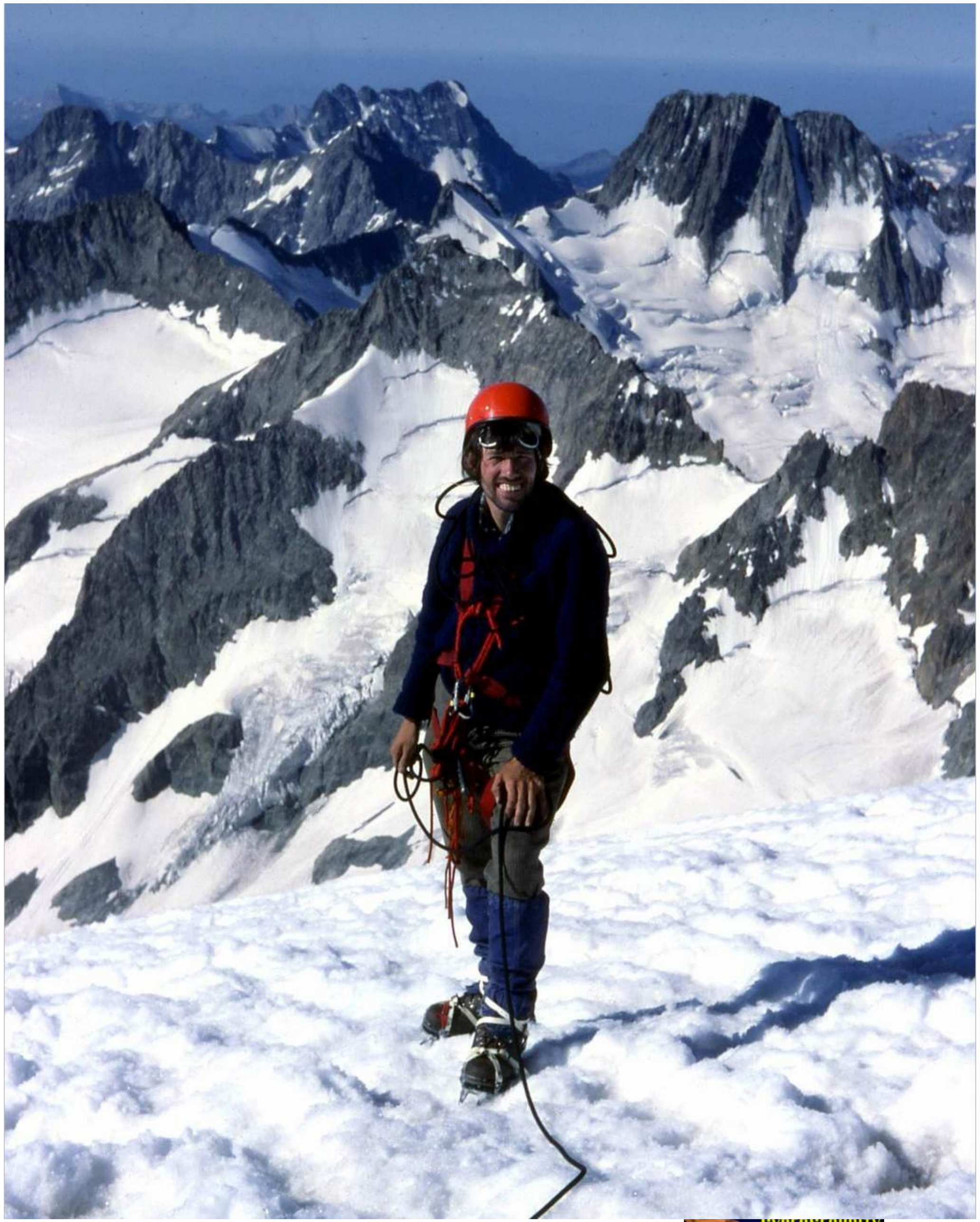
Sunrise on « Barre des Écrins » – 4102metres

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

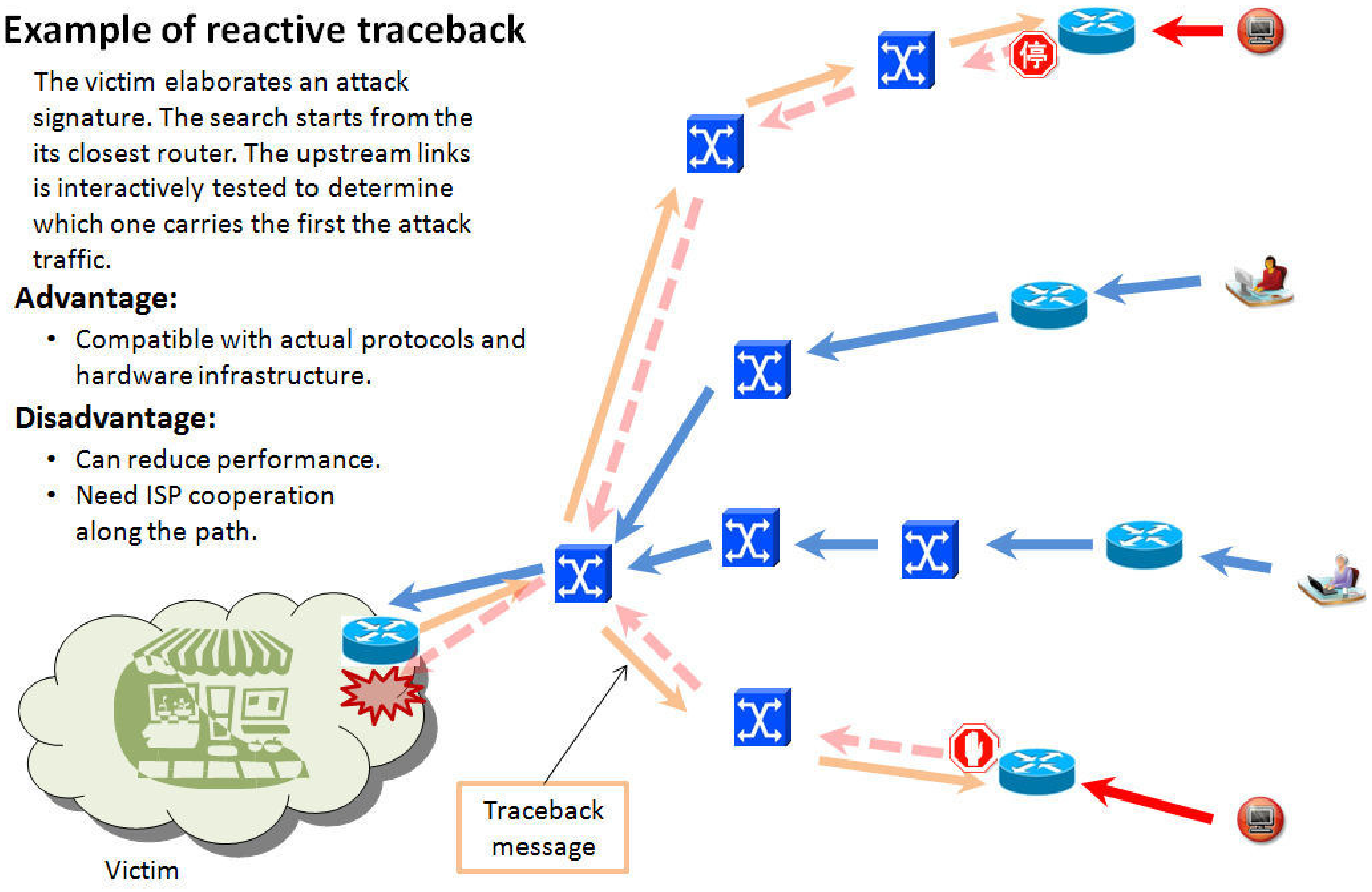
15th Sept 2015: « 7 Alpinistes died in Avalanche »

Security Equipment for *Alpine Ascents*





DDOS Mitigation: “Reactive Trace Back”



Example of reactive traceback

The victim elaborates an attack signature. The search starts from the its closest router. The upstream links is interactively tested to determine which one carries the first the attack traffic.

Advantage:

- Compatible with actual protocols and hardware infrastructure.

Disadvantage:

- Can reduce performance.
- Need ISP cooperation along the path.

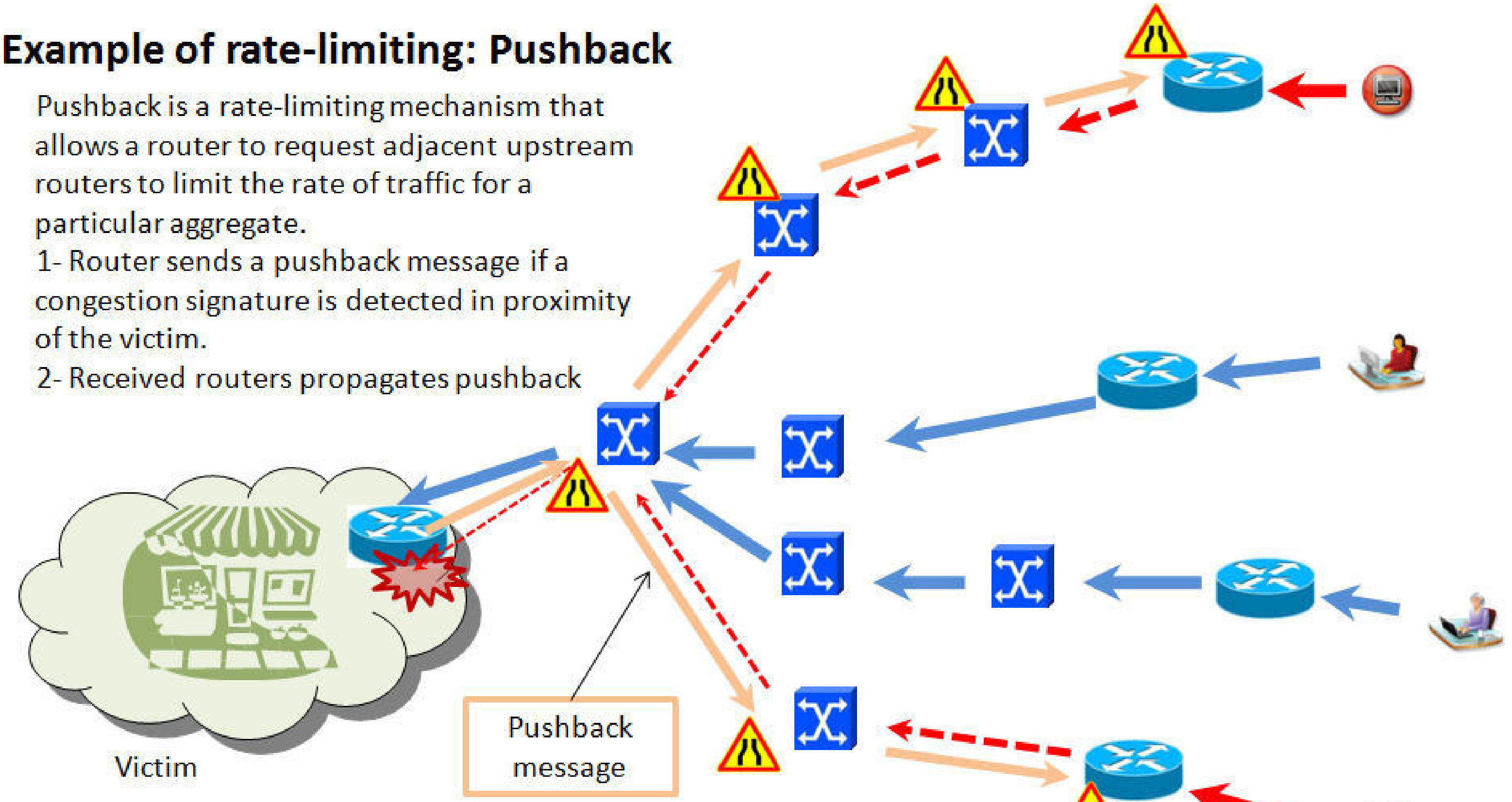
DDOS Mitigation: “Traffic Rate Limiting”

Example of rate-limiting: Pushback

Pushback is a rate-limiting mechanism that allows a router to request adjacent upstream routers to limit the rate of traffic for a particular aggregate.

1- Router sends a pushback message if a congestion signature is detected in proximity of the victim.

2- Received routers propagates pushback



Advantage:

- Prevents bandwidth from being wasted on packets that will later be dropped.

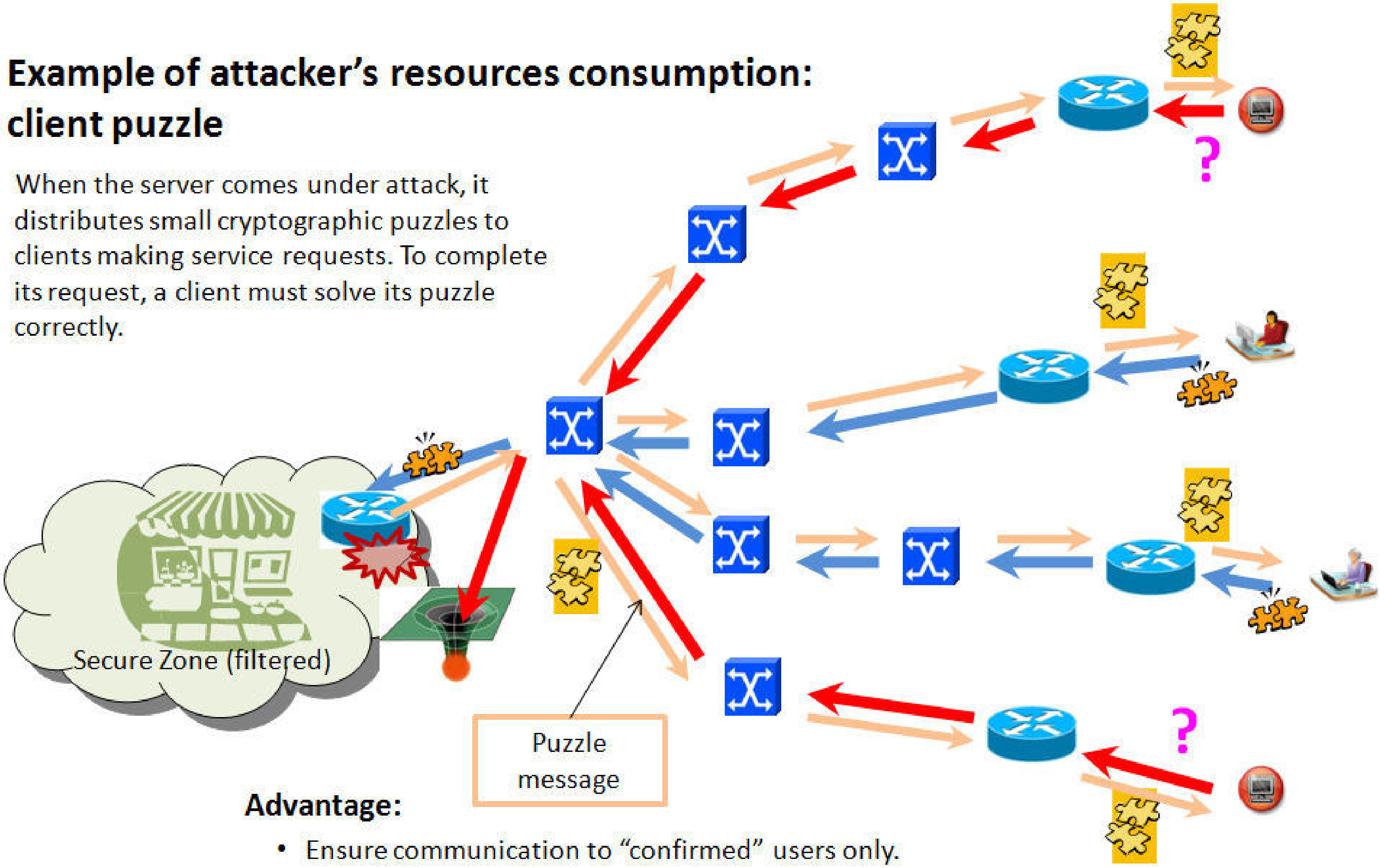
Disadvantage:

- False positives and false negatives.
- Can reduce performance.
- Need ISP cooperation along the path.

DDOS Mitigation: “Cryptographic Puzzles”

Example of attacker’s resources consumption: client puzzle

When the server comes under attack, it distributes small cryptographic puzzles to clients making service requests. To complete its request, a client must solve its puzzle correctly.



Advantage:

- Ensure communication to “confirmed” users only.

Disadvantage:

- Does not work for public services.
- Reduce performance.

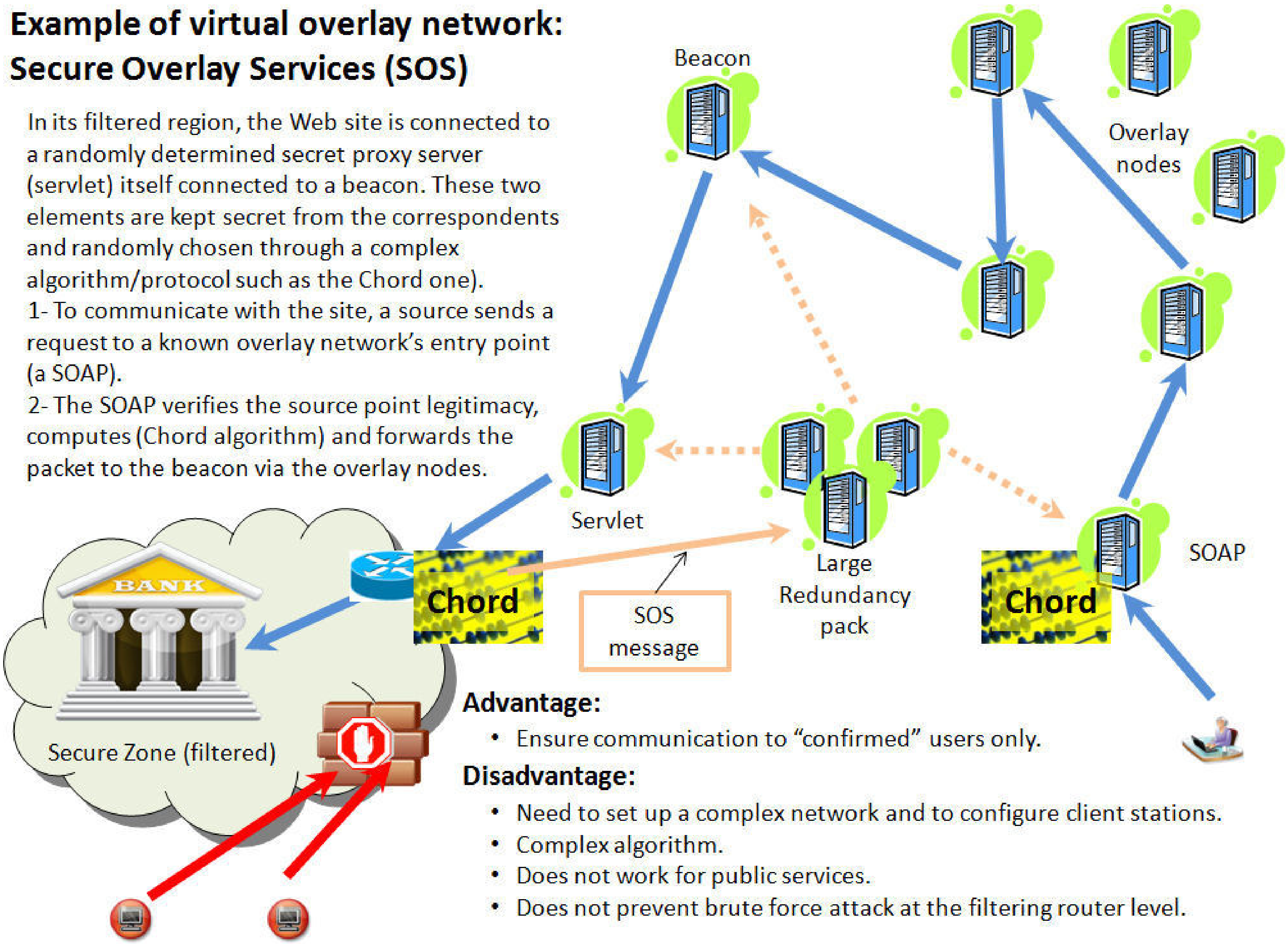
DDOS Mitigation: “Virtual Overlay Network”

Example of virtual overlay network: Secure Overlay Services (SOS)

In its filtered region, the Web site is connected to a randomly determined secret proxy server (servlet) itself connected to a beacon. These two elements are kept secret from the correspondents and randomly chosen through a complex algorithm/protocol such as the Chord one).

1- To communicate with the site, a source sends a request to a known overlay network’s entry point (a SOAP).

2- The SOAP verifies the source point legitimacy, computes (Chord algorithm) and forwards the packet to the beacon via the overlay nodes.



Advantage:

- Ensure communication to “confirmed” users only.

Disadvantage:

- Need to set up a complex network and to configure client stations.
- Complex algorithm.
- Does not work for public services.
- Does not prevent brute force attack at the filtering router level.