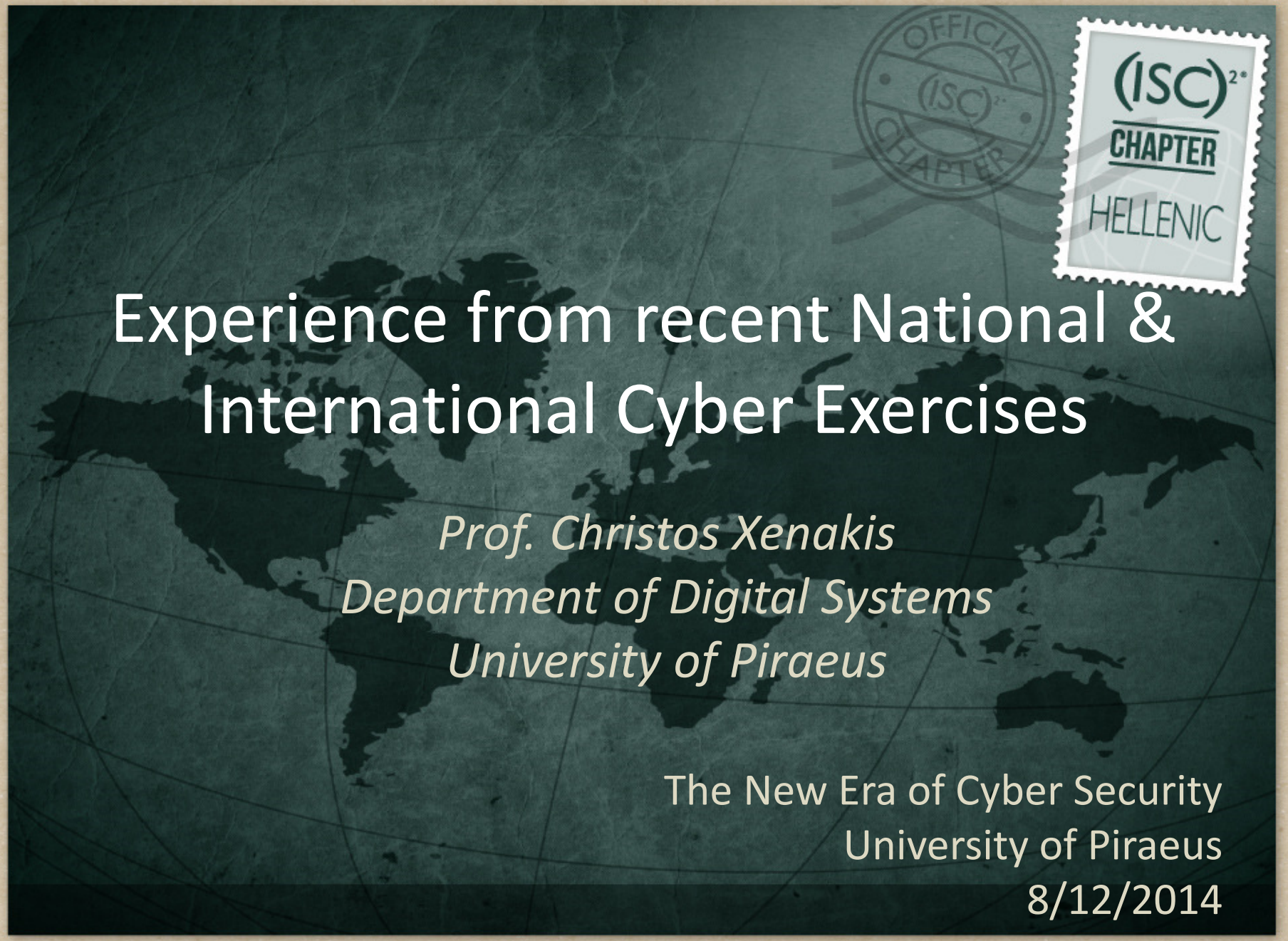


Experience from recent National & International Cyber Exercises

Prof. Christos Xenakis
Department of Digital Systems
University of Piraeus

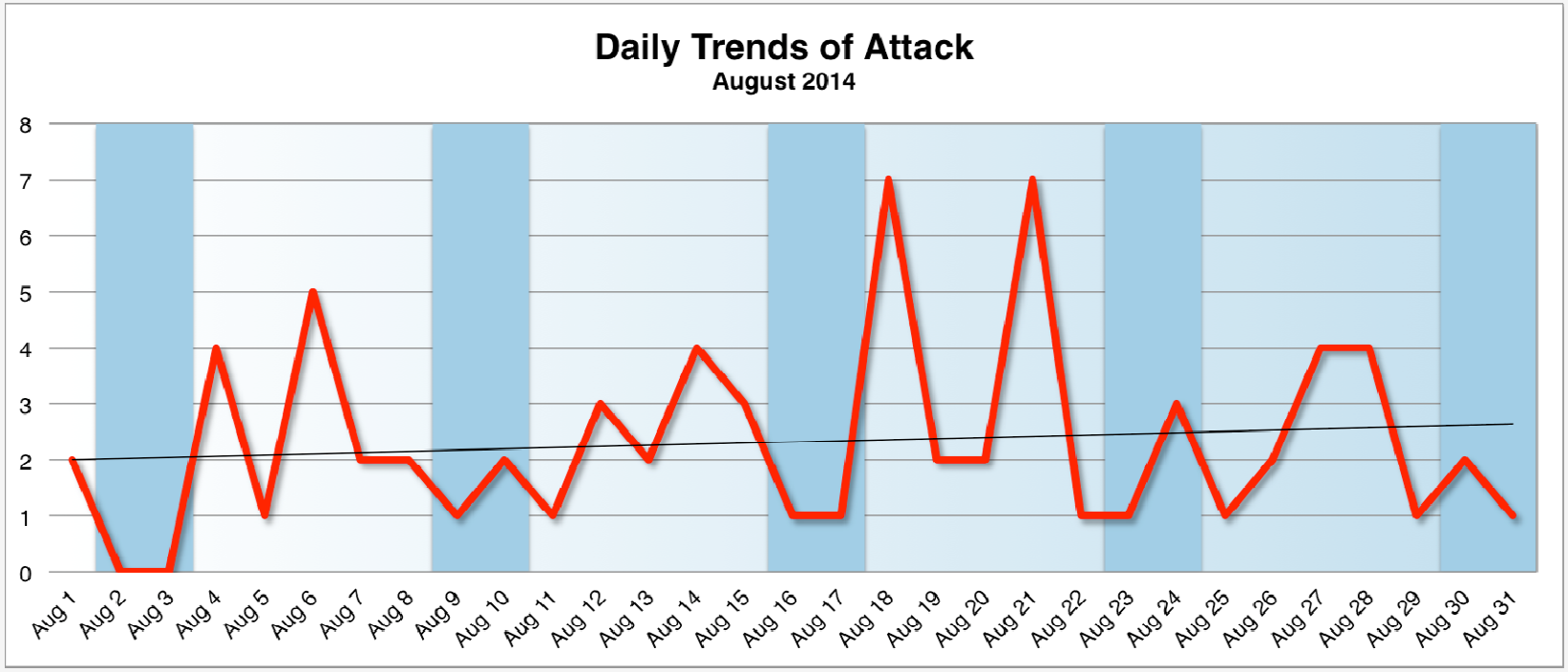
The New Era of Cyber Security
University of Piraeus
8/12/2014

A few words about us …

- University of Piraeus, Greece
- School of Information and Communication Technologies
- Department of Digital Systems
- System Security Laboratory founded in 2008
- Research Development & Education
  - systems security, network security
  - computer security, forensics
  - risk analysis & management
- MSc course on "Digital Systems Security" since 2009

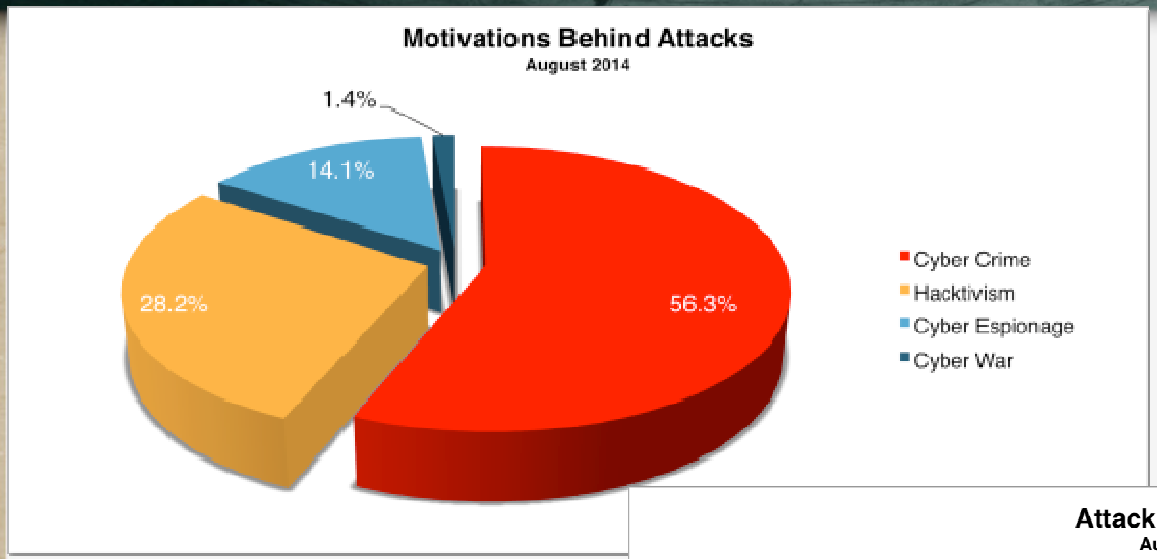
Cyber Attacks

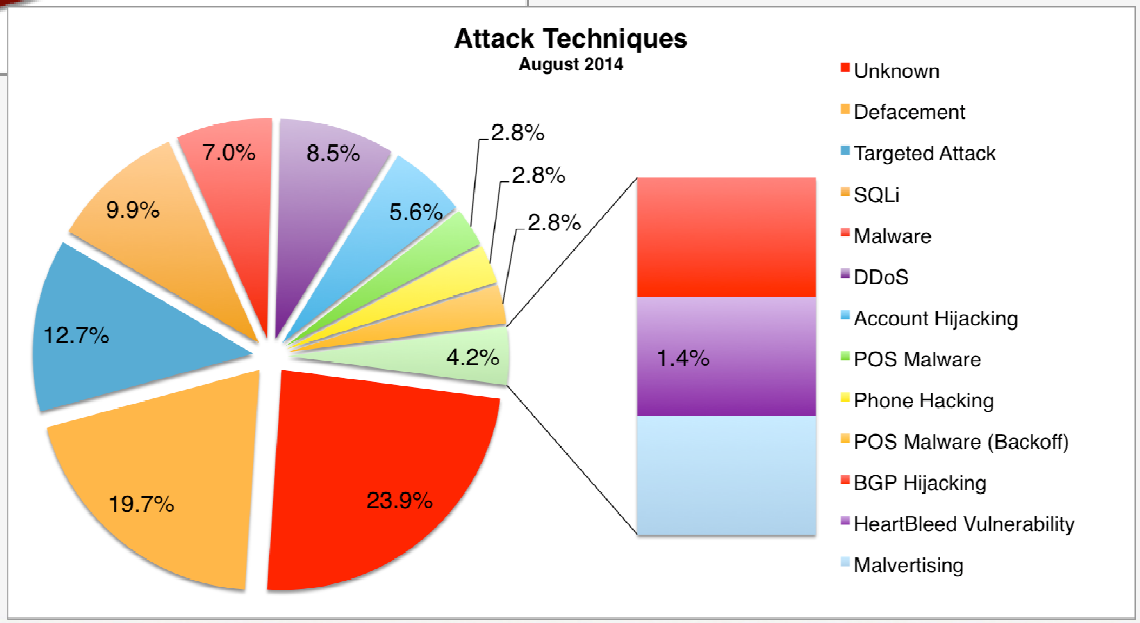
- Hundred of thousands of cyber attacks are being performed every day.



[Source: Hackmageddon.com]

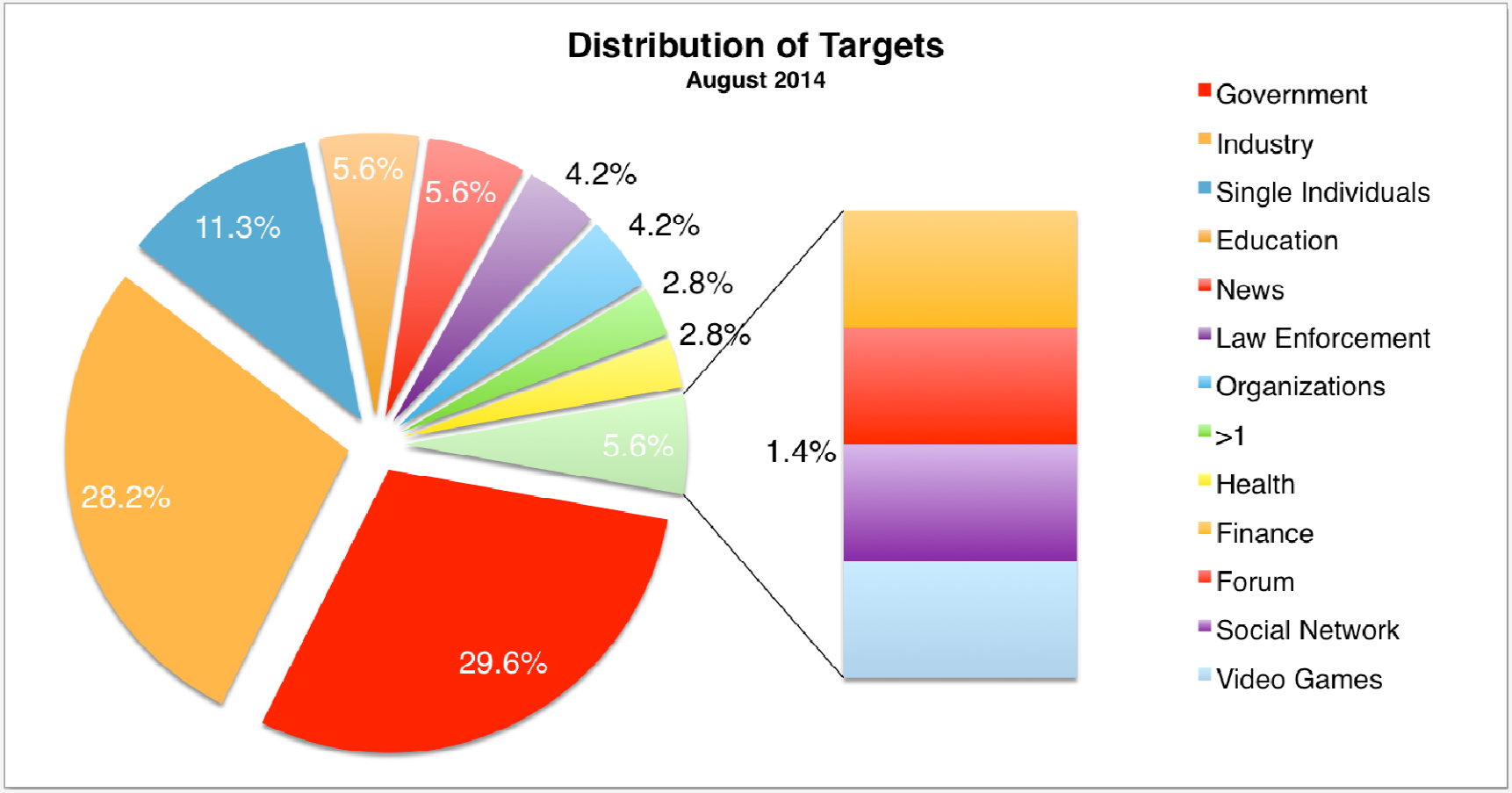
Cyber Attacks





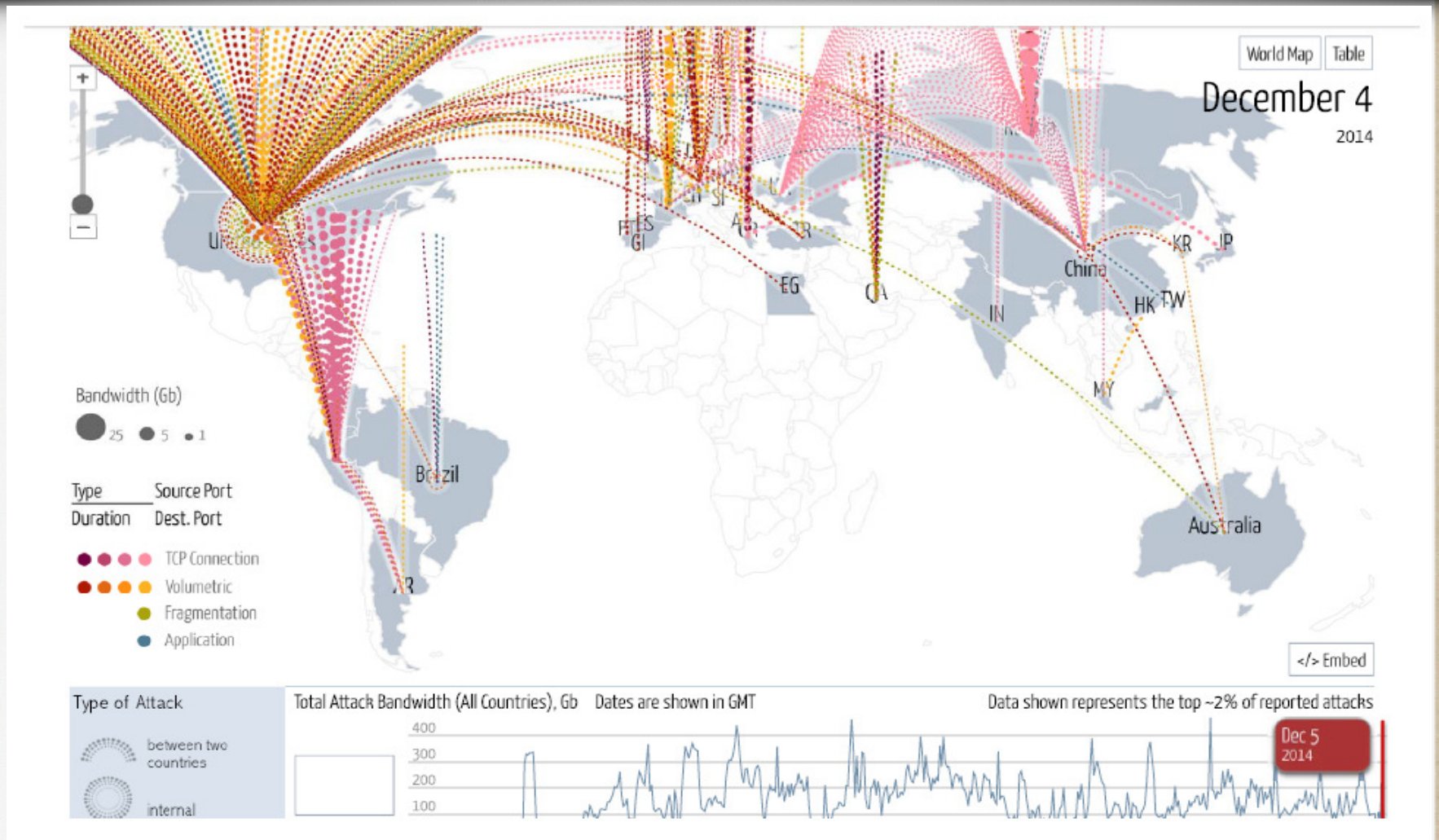
[Source: Hackmageddon.com]

Cyber Attacks



Source: Hackmageddon.com

Cyber Attacks



http://www.digitalattackmap.com/

Cyber Attacks

What is a Cyber Exercise ?

- A **Cyber exercise** is a controlled environment (a game), where **cyber attack incidents** occur with the purpose of **evaluating** and **testing** the capabilities of:

1. **Cyber security readiness,**
2. **Cyber protection,**
3. **Incident response.**

Categories of Cyber Exercises

- Cyber exercises are performed in a **closed/controlled environment** in order to **prevent actual attacks** to take place on **real networks**.
- Trainees are mainly divided in **two groups**:
  - **Red Team (attackers)**
  - **Blue Team (defenders)**
  - **CeRTs, Government bodies**, etc.
- There are **two different kinds** of Cyber Exercises
  - **Real-time exercises**
  - **Offline exercises**

Categories of Cyber Exercises

- **Real-time exercises**:
  - The **blue team** controls a set of computer machines:
    - SCADA Systems, Web Servers, DataBase Servers, Workstations, Routers, Firewalls, IDSs, etc
  - The **red team** tries in **real time** to exploit the **vulnerabilities** of the infrastructure.
  - The **blue team** has to **keep** and **maintain** the necessary services **up** and **running**.
- **Offline exercises** :
  - The **red team** designs and executes the **security incidents, offline**
  - The incidents are **distributed** to the **bleu team**, e.g., forensic analysis of a compromised web server, .exe files, log files, etc.
  - **Virtual machines** and the necessary files are also distributed to the players.

Participation in Cyber Exercises

- **Panoptis 2010**: 1st National Cyber Defense Exercise
- **Panoptis 2011**: 2nd
- **Panoptis 2012**: 3rd
- **Panoptis 2014**: 4th

Cyber Europe 2014

enisa European Network and Information Security Agency

https://cyberprotector2014.com

Cyber Coalition 2014

Participation in Cyber Exercises

- **Training incidents** include:
  - Network packet capture analysis
  - Malware analysis
  - Digital and Mobile Forensics
  - Log Analysis
  - Insider attacks
  - Steganography analysis
  - Detection of vulnerabilities
  - Port scanning
  - Service scanning and patching of vulnerable versions of software.
  - Real Time network traffic monitoring
  - IDS and firewall monitoring and configuration
  - Security of FTP, Windows Server and Linux operating system.

Participation in Cyber Exercises

- **Training incidents** include:
  - Forensics Investigation
  - Compromised Website Analysis
  - Impact Analysis
  - Infected System Malware Analysis
  - Mobile Device Infection
  - Advanced Malware Analysis
  - Attacks on Ipv6 Corporate Networks
  - DDoS Attacks against a friendly server
  - Attack co-ordination via social media
  - Insider man attacks in corporate networks
  - SCADA attacks based on insider
  - Manipulation of SCADA field Devices in complex ICT systems

Participation in Cyber Exercises

- **Training incidents** include:
  - Script Kiddie attacks (website defacements, password brute-force, portscanning)
  - Web Application Attacks (data exfiltration, malicious file uploads, content modification)
  - Insider Threats (malicious USB sticks containing malware)
  - Targeted Attacks (via phishing based attacks)
  - Anti Virus bypassing via malicious payloads

Participation in Cyber Exercises

- **Cyber Coalition 2014:** Cyber exercise organized by **NATO**.
  - **CC2014** contained both **live** and **offline** scenarios.
  - **Offline Scenarios**
    - Android Malware analysis
    - Ransomware analysis
    - Backdoored motherboard. Motherboard that it's UEFI BIOS is infected with malware
  - The participants **were trained** at
    - Reverse Engineering
    - Digital Forensics
    - Malware analysis
    - Network Packet capture
    - Real time **monitoring** and **immediate response** to incidents

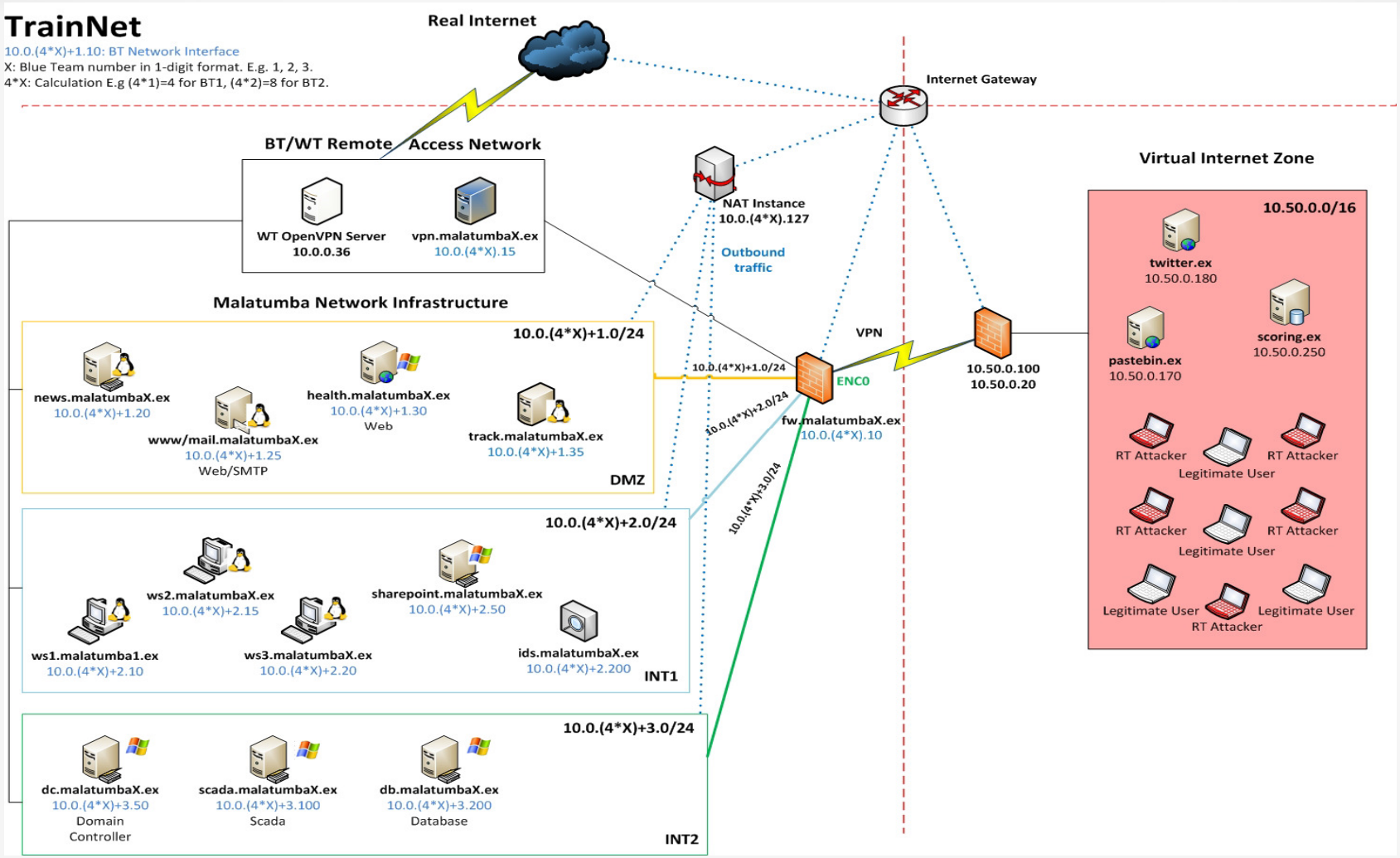
Objective of a Cyber Exercises

- In general the **main objectives** of a **Cyber Exercise** are:
  - **Assess** security **controls**, **tools**, **process** and **procedures** deployed for operational networks
  - **Train** the blue teams to **distinguish** between **'normal' traffic** and **malicious traffic**.
  - **Identify security gaps** blue teams may have with regards to **Incident Response**
  - Develop **lessons Identified database**
  - Get acquainted with **New Technologies** and **New Cyber Security Solutions**
  - Get trained and learn **different strategies** and **tactics**.

Objective of a Cyber Exercises

- **Training objectives are**:
  - **Learning the network:** assets and vulnerabilities, assign priorities to the assets, etc.
  - **System administration and prevention of attacks**: administrative tasks and hardening configurations were continuous activities
  - **Monitoring networks, detecting and responding to attacks:**
  - **Handling cyber incidents**: prioritisation, reaction time, and clarity of shared information
  - **Teamwork**

Infrastructure a Cyber Exercise



How objectives are achieved

- Identify **when** the **attack began**
- Identify **what** is being **attacked**
- Identify what **resources** are involved in **carrying** the **attack**
- Identify the **way** the **attack** is being **carried** out
- Identify **where** the attack **came from**
- **Suggest** ways of **mitigating** the attack

Secnews-Unipi Challenge Attack!

- Discover the vulnerabilities that exist at http://attack.secnews.gr/pz1.php
- Exploit them to get access to the server
- Provide a documented report

Conclusions

- **Cyber exercises** & **security challenges** are tools for evaluating and testing the **infrastructure**, **procedures** and **personnel**.
- They also provide **training**.
- They can be performed at International, National, Sector and Organization level.
- We believe that **Cyber exercises** & **security challenges** can be used to achieve **life long learning.**

Thank you for Attention

Dr. Christos Xenakis

http://cgi.di.uoa.gr/~xenakis/index.html

xenakis@unipi.gr