H2020 SAINT project & CTI

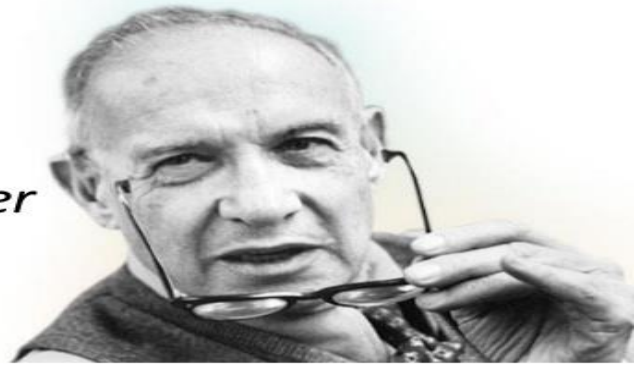
GA No: 740829 - May 2017 – April 2019

Latif Ladid - University of Luxemburg

This work is performed within the SAINT Project (Systemic Analyser in Network Threats),
with the support of the European Commission and the Horizon 2020 Program, under Grant Agreement No 740829.

SAINT Systemic Analyser In Network Threats

"Management is doing things right; leadership is doing the right things."
— *Dr. Peter F. Drucker*



Management GURU, Peter Drucker famously once said:

'If You Can't Measure It, You Can't Manage It.'

EUROPEAN COMMISSION

Brussels, 13.9.2017

JOIN(2017) 450 fina

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

EUROPOL

Europol Calls on Internet Providers to End CGNAT IP Address Sharing

SAINT & CTI

Why SAINT & CTI? ....

one of the major missing elements in **CTI & for the EU, is reliable metrics & econometrics i.e.**

- Where do the threats come from?
- Who from?
- How many?
- Cost of threats?
- Getting better or worse (trends)?
- What's the priorities?

.... so SAINT is vital for EU in awareness of threat metrics & economics..... to guide EU & Member states policy

SAINT Objectives

1 - **Metrics for CTI**, cyber-security and cyber-crime market

2 - **New economic models** for the reduction of cyber-crime as a cost-benefit operation

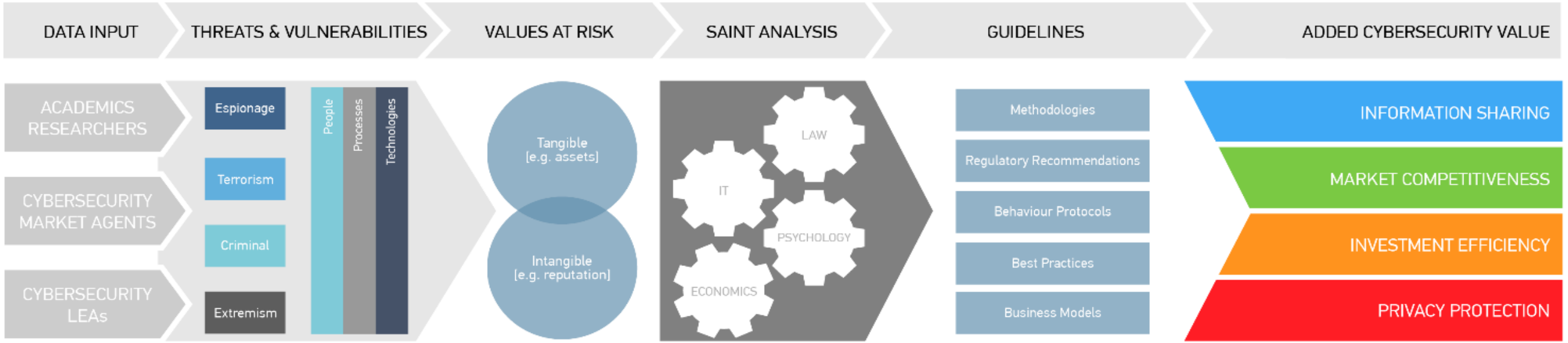
3 - **Costs / Benefits** of information sharing regarding cyber-attacks

4 - **Privacy** and security level of internet applications, services and technologies

5 - **Automated analysis**, for behavioral, social analysis, cyber-security risk and cost assessment

6 - **Recommendations** to all relevant stakeholders including **policy makers, regulators, law enforcement agencies, relevant market operators and insurance companies**

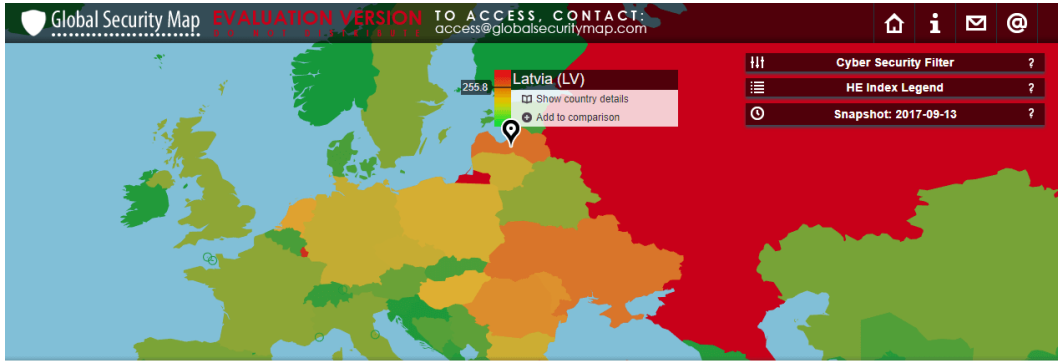
Research Methodology and Outcome



Scientific activities:

- Applied cyber-security metrics analysis
- Regulation focused comparative analysis
- Data mining and data processing automated analysis for the development
- Economic and behavioral theoretic analysis for the development of econometric and behavioral models

Mapping the threats (LV)



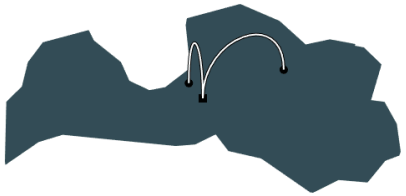
Latvia (LV)

Cyber security summary

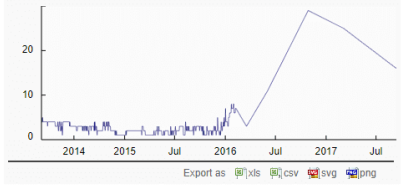
Latvia is ranked **#16** out of 224 countries on the Host Exploit index for cyber security (HE-index) at **2017-09-13** (a higher rank equals worse security). The lowest ranking of Latvia was **1** on **2014-05-20**. The country's highest ranking was observed on **2013-02-27**, where the country ranked **29**.

There are a total of **200 ASs** (Autononomous Systems) linked to this country. **197 (98.5%) are registered** to this country and, of these, **7 (3.5%) are routed** from another country. Of the ASs belonging to Latvia, **3 (1.5%) ASs are routed abroad** of the country.

The largest cyber security threat from Latvia are **botnets** with a HE-index of **550.1**. The lowest threat are **current events** with a HE-index of **33.1**.



Ranking over time

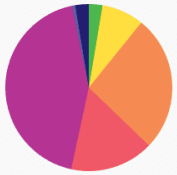


Latest headlines

Russia may have tested cyber warfare on Latvia, Western officials say	more
Russia Breaks into US Soldiers' iPhones in Apparent Hybrid Warfare	more
War Games: Russia Is Testing Out Live Bombings and Shutting Down	more
NATO, Latvia Claim More Russian Cyber-Attacks	more
Daily News 02 / 10 / 2017	more
Total Defense: How the Baltic States Are Integrating Citizenry Into Their	more
PM May calls for European cyber-cooperation; Norway joins Nato CCD	more
Was it something she said? Theresa May is shunted to the back of the	more
NATO Secretary General Jens Stoltenberg: Romania is key ally in	more
Norway to join the NATO Cyber Defence Centre of Excellence	more

Index over time

HE Index contributions



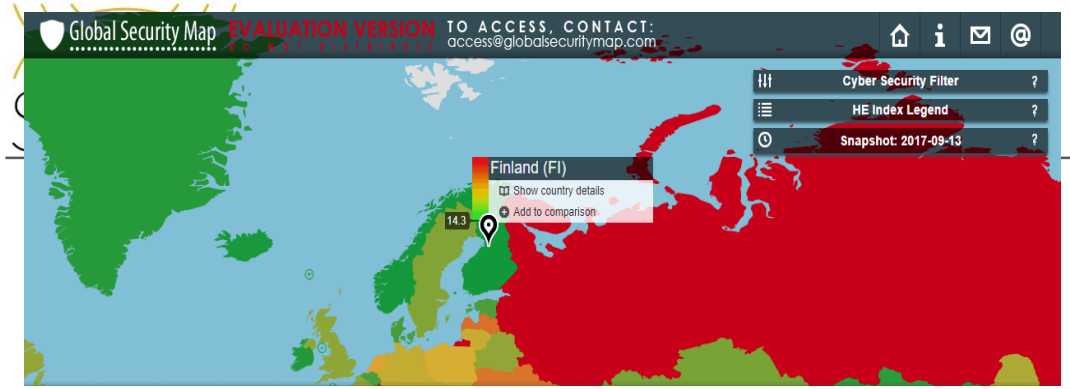
Spam (3%), Badware (8%), Phishing (26%), Malware (16%), Botnets (43%), Crime hubs (1%), Current events (3%)

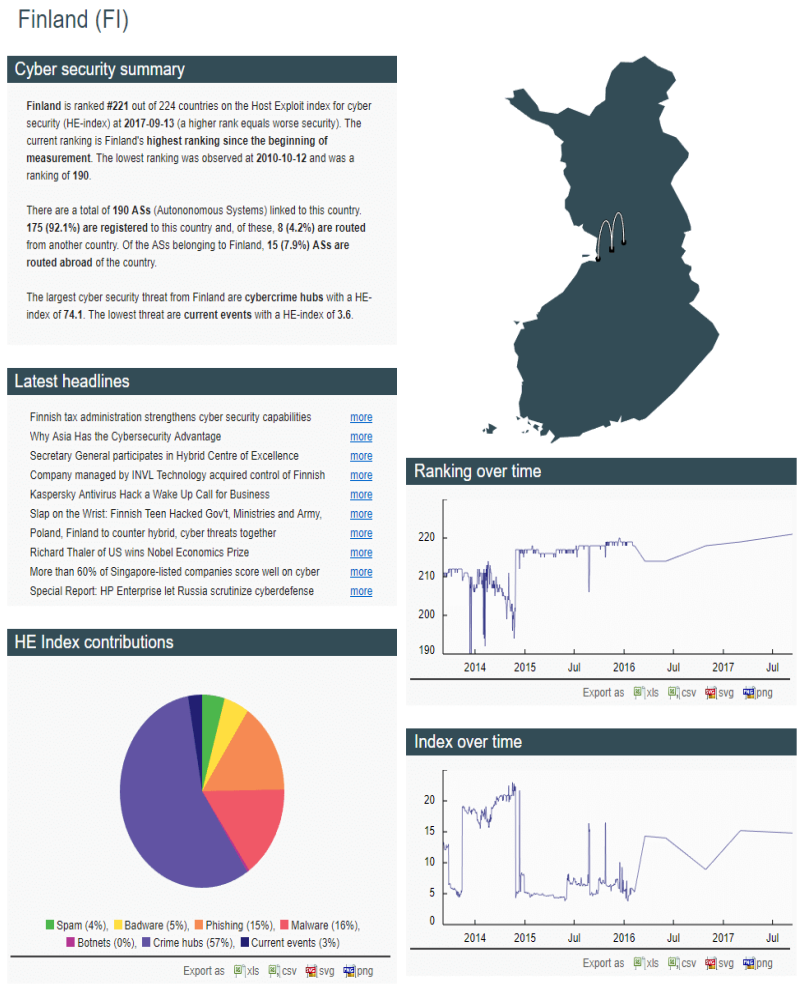
Export as xls csv svg png

Comparable examples of measurable threats of x 2 EU countries (Sept 17):

- **LV = 16 of 224 (lower the number = higher threats)**
- **HE Index of 255.8 (Mid to High CTI index)**
- **Main threat from LV = botnet (C&Cs)**

Mapping the threats (FI)





Comparable examples of measurable threats of x 2 EU countries (Sept 17):

- **FI = 221 of 224 (lower the number = higher threats)**
- **HE Index of 14.3 (Low CTI index)**

- So why comparing LV & FI is there such a quantitative difference?

SAINT Outputs and challenges - Practical

Practical challenge = Application of Metrics of Cybersecurity - to – CTI – examples:

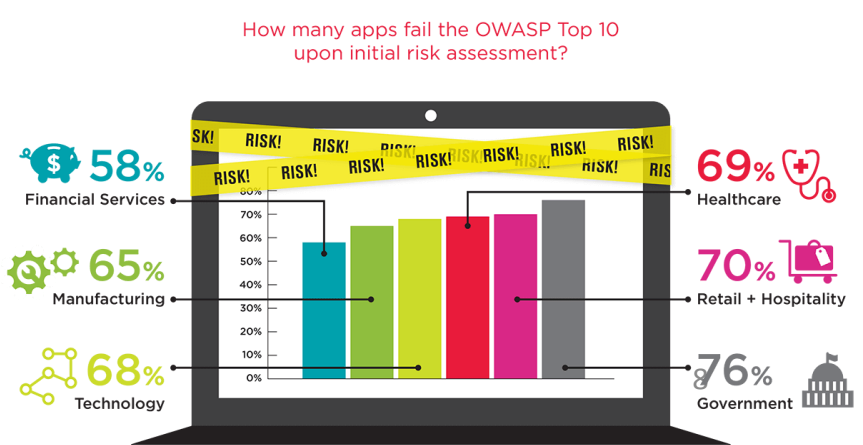
- **Determine, Quantify & Rank ENISA's ETL - metrics**
- **Economic analysis & metrics**
- **OWASP Top 10 – Web Security - Vulnerabilities**

ENISA's Top 15 Threats

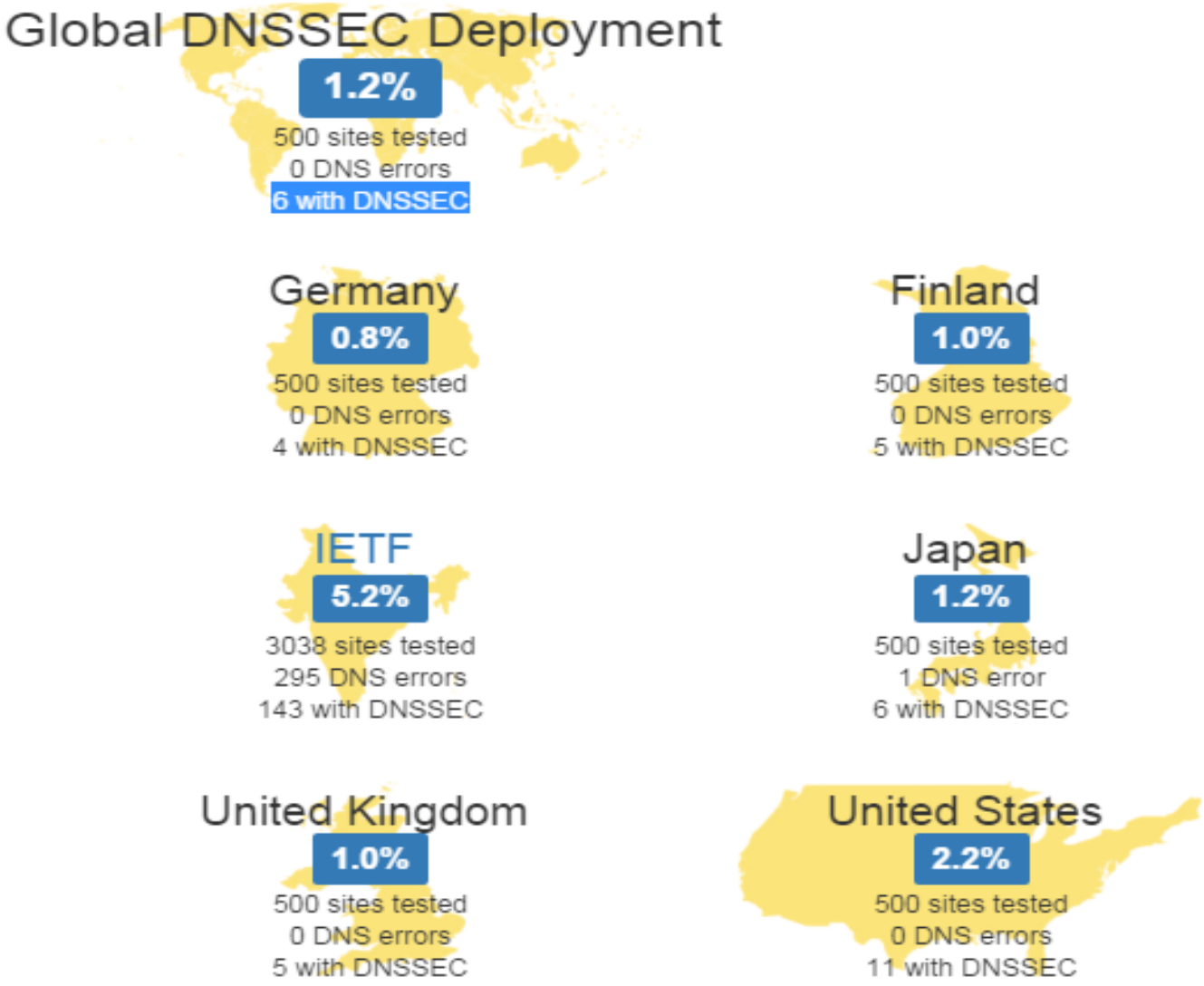
Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware		→
2. Web based attacks		→
3. Web application attacks		→
4. Denial of service		↑
5. Botnets		↓
6. Phishing		↑
7. Spam		↑
8. Ransomware		↑
9. Insider threat (malicious, accidental)		↓
10. Physical manipulation/damage/ theft/loss		↓
11. Exploit kits		↓
12. Data breaches		↓
13. Identity theft		↓
14. Information leakage		↓
15. Cyber espionage		→

OWASP Top 10 (2017)

OWASP Top 10 – 2017 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities
A10 – Underprotected APIs (NEW)



SAINT


Global DNSSEC Deployment
1.2%
500 sites tested
0 DNS errors
6 with DNSSEC
China
0.2%
500 sites tested
1 DNS error
1 with DNSSEC
Germany
0.8%
500 sites tested
0 DNS errors
4 with DNSSEC
Finland
1.0%
500 sites tested
0 DNS errors
5 with DNSSEC
India
0.6%
500 sites tested
1 DNS error
3 with DNSSEC
IETF
5.2%
3038 sites tested
295 DNS errors
143 with DNSSEC
Japan
1.2%
500 sites tested
1 DNS error
6 with DNSSEC
South Korea
0.8%
500 sites tested
0 DNS errors
4 with DNSSEC
United Kingdom
1.0%
500 sites tested
0 DNS errors
5 with DNSSEC
United States
2.2%
500 sites tested
0 DNS errors
11 with DNSSEC