H2020 SAINT project

Dr. Andreas Zalonis

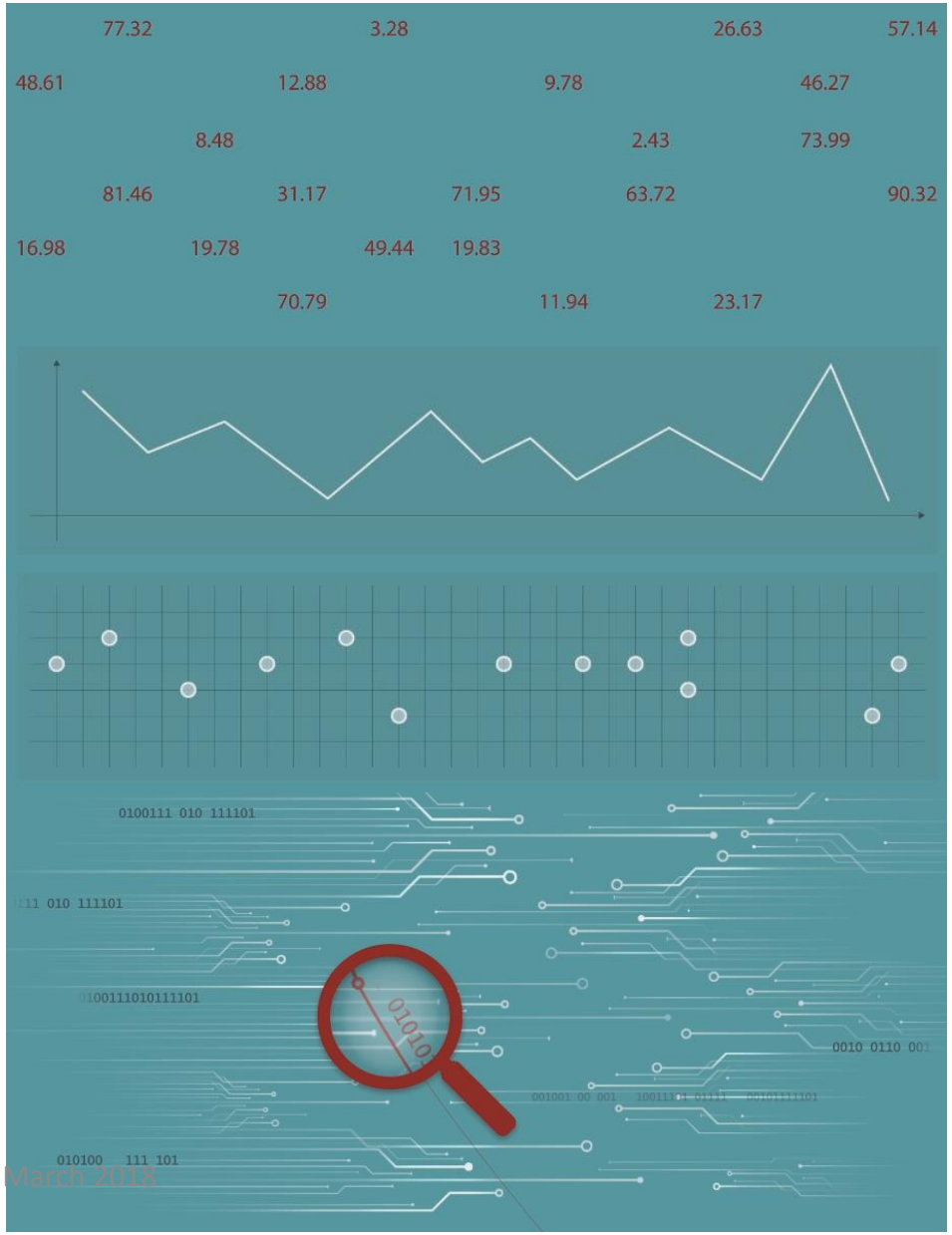
azalonis@iit.demokritos.gr

Integrated System Laboratory
Institute of Informatics & Telecommunication
NCSR 'Demokritos'

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.

Objectives

- Metrics and Indicators for cyber-security economic analysis
- New economic models
- Information sharing cost-benefit analysis
- Privacy vs. Security
- Cyber security Investment cost-benefit analysis
- Tools for automated analysis
- Recommendations and Best Practices



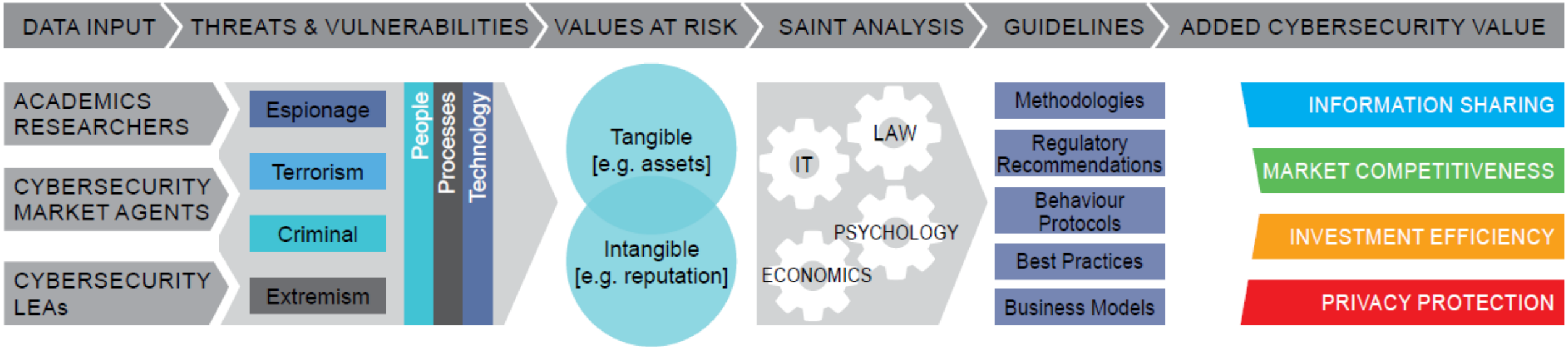
Concept

Quantitative & Research Studies
Theoretical Research
Policies & Regulations

Consumers reports, preferences, practices
Business interests
Ethics & Privacy

Observation & Event driven studies
Cyber security practitioners & expert groups
Service providers
Technology experts
Legal & Law enforcement

Methodology



Research

Scientific research areas:

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

Presentations:

- Comparative Metrics of Cybercrime & Cyber Security – Jart Armin (CyberDefcon)
- Applied economic research on factors influencing firms' production cost and their incentives to cooperate – John Bothos (NCSR “Demokritos”)
- Automated analysis of cybersecurity related information sources and indicators – V. Vlachos and Y. Stamatiou (CTI “Diophantus”)

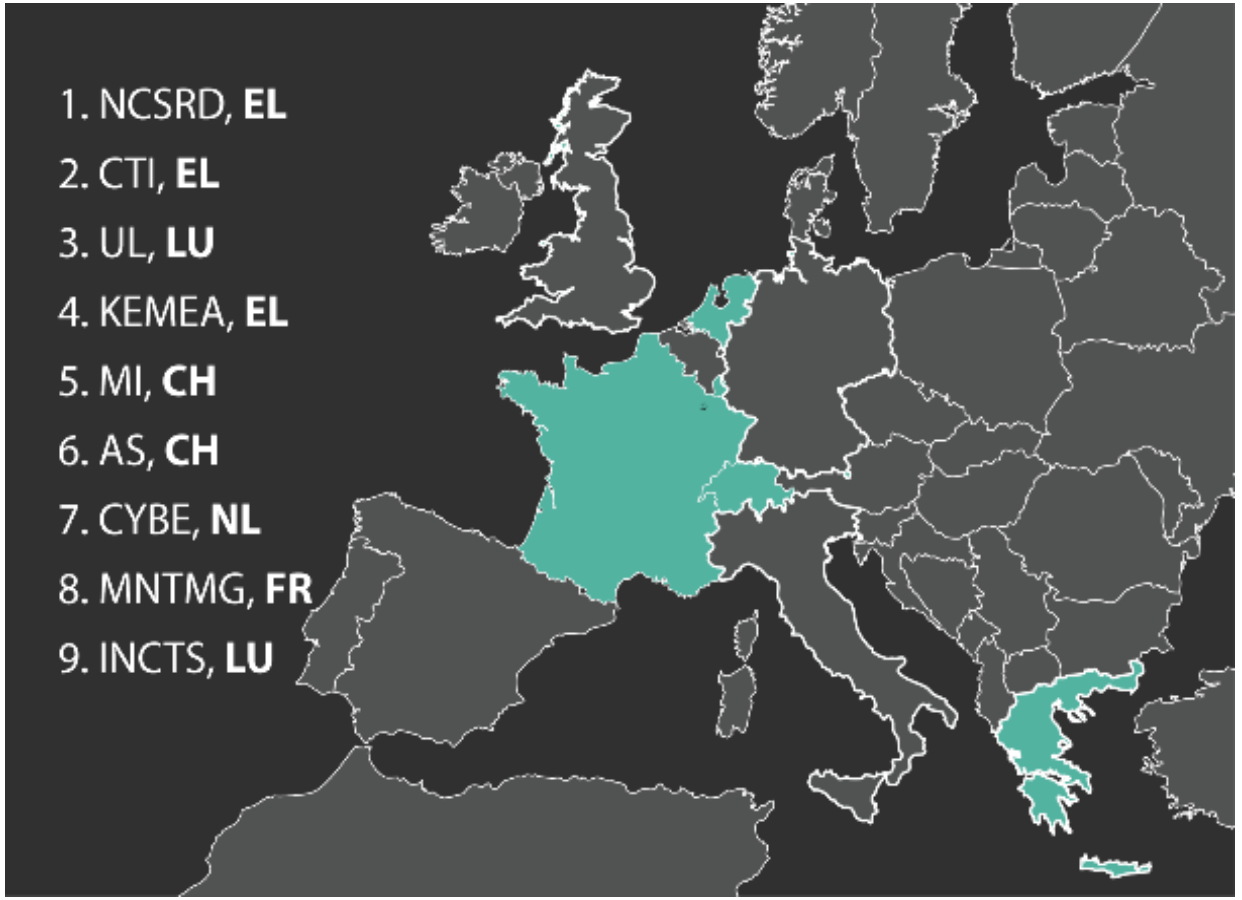
Expected Impact

- Improve social, institutional and economic comprehension of cyber-security failures
- Improve decision making, governance and investments by stakeholders (e.g. policy makers, regulators, law enforcement agencies, market operators and insurance companies)
- Facilitate information dissemination and sharing
- Improve efficiency of cyber security solutions
- Provide a set of recommendations through systemic approach impacting the economic and incentive models of cybercrime

Consortium

- 5 academic research partners (NCSRD, CTI, UL, MI, KEMEA)
- 4 business firms (AS, CYBE, MNTMG, INCTS)
- Hellenic Police Cybercrime Unit, as part of KEMEA

- **Duration: 2 years (May 1, 2017 – April 30, 2019)**



Additional information on research activities

Applied Cyber-Security Metrics Analysis

- Development of a database of cyber-security indicators and metrics
- Information sharing relevant metrics: blacklists, cyber-attack measurements, malware listing, infected websites, phishing activity, price of digital assets and costs of intangible risks (reputation, non-critical service disruption)
- Metrics for measuring privacy
- Profitability metrics related to cyber-security market
- Cyber-security investment efficiency metrics

Regulation Focused Comparative Analysis

- Assess the effectiveness of industry standards and regulations
- Compare/develop business models aiming to address and mitigate the effects of cyber-crime – identify potential incentive mechanisms
- Cost-benefit based comparative analysis of cyber-security solutions/products
- Provide a set of recommendations related to standards and benchmark used against cyber-crime

Data Mining, Data Processing and Automated Analysis

- Develop an Automated Analysis framework taking into consideration the multitude of openly available information sources
- Information sources:
  - privacy/security discussion forums and blocks, security product companies' incident reporting web pages, bug bounties discussions and reward announcements, public police reports, etc.
  - Deep Web
- Scope:
  - Build a methodological framework that will rely on big data gathering, storing, processing, correlating, and organizing these massive information sources
  - Estimate the economic impact by developing revenue models for criminal activities and provide revenue models for Deep Web activities

Economic and Behavioral Theoretic Analysis

- Investigate the role of cyber-security information sharing in the investment behavior
- Assessment of the relationship between information sharing and the number and severity of cyber-security incidents
- Construction of a methodological framework consisting of guidelines about information sharing policies
- Quantitative analysis relating technical and behavioral variables about network traffic flow characteristics – to identify network conditions indicative of cyber-threats
- Analysis of economic factors shaping the conditions for competition and profitability in the security industry
- Investigate the relation between vulnerabilities and supply and demand in the cyber-security market
- cost-benefit cyber-security methodologies - optimal investment in cyber-security and expected profitability or loss