



## Systemic Analyser in Network Threats

[www.project-saint.eu](http://www.project-saint.eu)

@saintprojecteu

#saintprojecteu



**John M.A. Bothos**  
[jbothos@iit.demokritos.gr](mailto:jbothos@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.





@saintprojecteu - #saintprojecteu

Budget: 1.998.700 € - Contract No: 740829

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

Project Coordinator: **Dr. Stelios C. A. Thomopoulos**

[scat@iit.demokritos.gr](mailto:scat@iit.demokritos.gr)

Institute Director & Director of Research

Head of Integrated Systems Laboratory

Institute of Informatics & Telecommunications

National Center for Scientific Research "DEMOKRITOS"

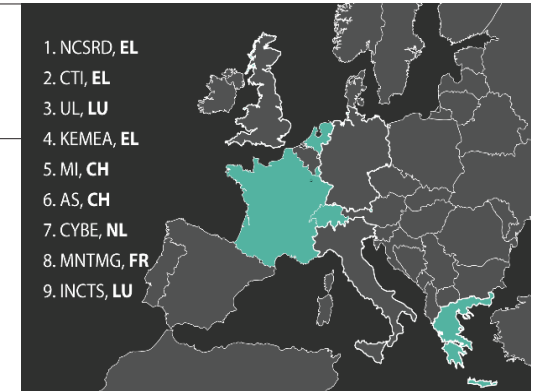


#### Consortium:

National Center for Scientific Research "Demokritos" (GR), Technology Institute & and Press "Diophantus" (GR), Center For Security Studies (GR), Universite du Luxembourg (LU), INCITES Consulting SARL (LU), Mandat International (CH), Archimede Solutions SARL (CH), Stichting CyberDefcon Netherlands Foundation (NL), Montimage EURL (FR).



1. NCSR, EL
2. CTI, EL
3. UL, LU
4. KEMEA, EL
5. MI, CH
6. AS, CH
7. CYBE, NL
8. MNTMG, FR
9. INCTS, LU



## Cybersecurity Market Potential

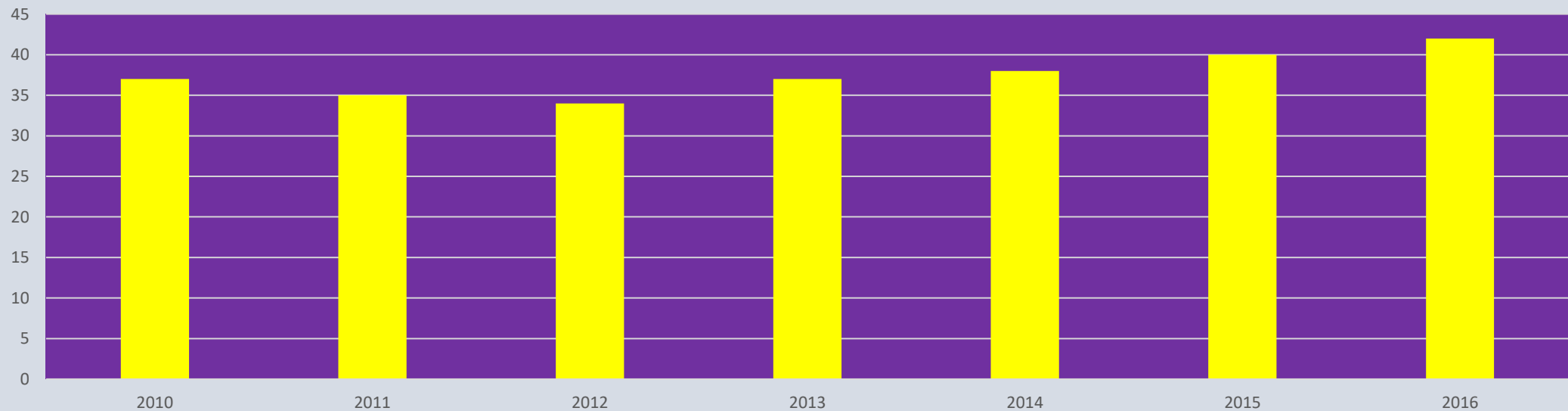
### General I&T industry related indicative data

- ❑ 3.6 billion Internet users worldwide in 2016 [www.internetworldstats.com](http://www.internetworldstats.com)
- ❑ 7.3 billion mobile-cellular subscriptions worldwide in 2016 [www.itu.int](http://www.itu.int)
- ❑ By 2025, more than 91% of people in developed countries and nearly 69% of those in emerging economies will be using the Internet, with the total number of Internet users estimated to be 4.7 billion. [Microsoft , “Cyberspace 2025: Today’s Decisions, Tomorrow’s Terrain”](#)
- ❑ At least 7% of URLs are malicious, 85% of the 200 billion emails processed per day are spam, 1.4 million browser agents are botnets, consisting 20% of mobile browser agents and measurable cyber-attacks rise up to 1 million plus every day Microsoft’s report. [Microsoft , “Cyberspace 2025: Today’s Decisions, Tomorrow’s Terrain”](#)
- ❑ The annual cost to the global economy from cyber-crime is € 300 billion, with the average annualized cost of data breaches only, being € 7.9 million. The global cyber-crime market sizes up to € 15 billion and up to € 50 billion for security products and services. [Microsoft , “Cyberspace 2025: Today’s Decisions, Tomorrow’s Terrain”](#)
- ❑ Forecasts about expansion of cyber-crime, in the form of a project-basis where cyber-criminals lend their knowledge, experience and expertise as part of a crime-as-a-service business model. [Europol, “Exploring Tomorrow’s Organized Crime” , 2015](#)

## Cybersecurity Market Potential

- General I&T industry related indicative graph

percentage of enterprises having purchases via computer mediated networks



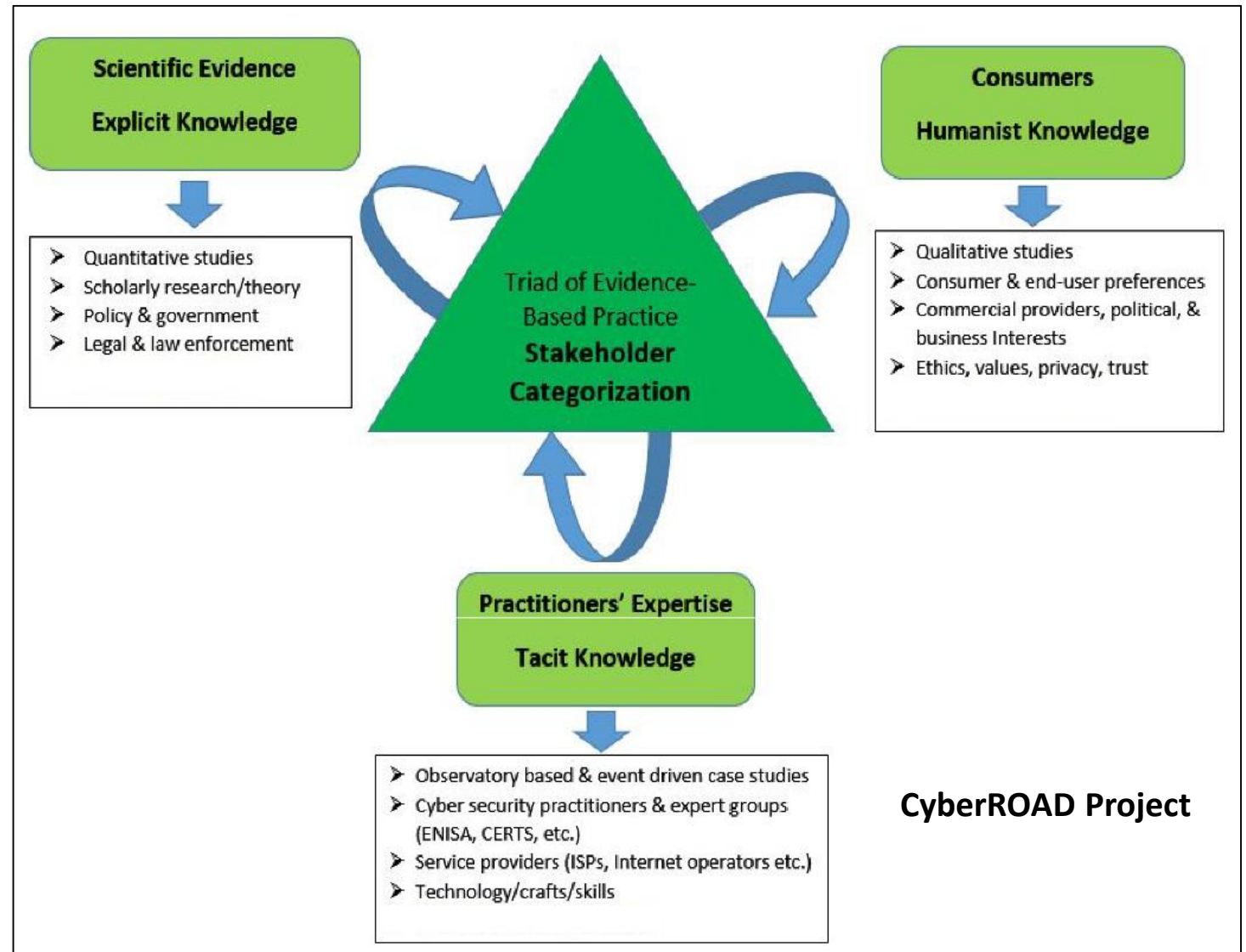
## SAINT Objectives

- Establish a complete set of metrics for cybersecurity technical and economic analysis.
- Estimate and evaluate the associated benefits and costs of information sharing regarding cyberthreats and cyberattacks and define limits of the minimum needed privacy and security level of internet applications, services and technologies.
- Identify potential benefits and costs of investing in cybersecurity industry as a provider of cybersecurity services and products and develop cost assessment models about the cost-benefit of cybersecurity investments.
- Outline the basic institutional framework of the cybersecurity industry and its relevant markets in Europe.
- Develop an automated platform for behavioural, social and economic analysis of the cybersecurity risks and the cybercrime market.
- Provide a set of recommendations about the reduction of cybercrime to all relevant stakeholders including policy makers, regulators, law enforcement agencies, relevant market operators and insurance companies

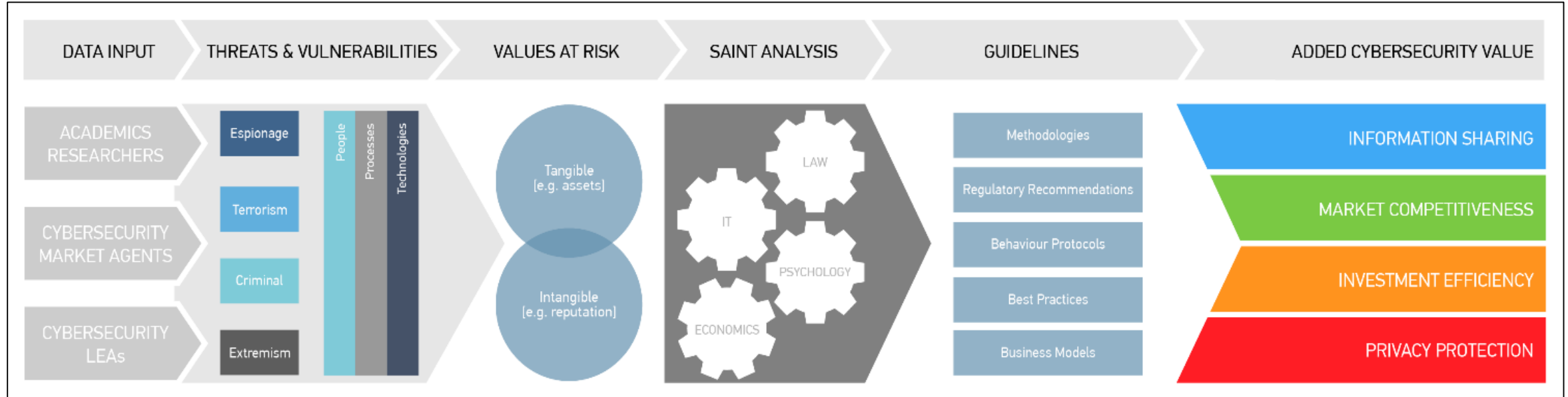
## Former Basis of Research Concept

### Stakeholders collaboration:

- Analyse and identify incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing in order to enhance cybersecurity
- Mitigate the risk and the impact from a cyberattack
- Provide solid economic evidence on the benefits from such improvement based on solid statistical analysis and economic models



## New Advanced Research Concept

































### Multidisciplinary Research Approach

- Applied metrics analysis
- Economic and behavioural theoretic analysis
- Ecosystem comparative analysis
- Automated data analysis

## Applied CyberSecurity Metrics Analysis Methodology

### Development of a database of cybersecurity indicators and metrics

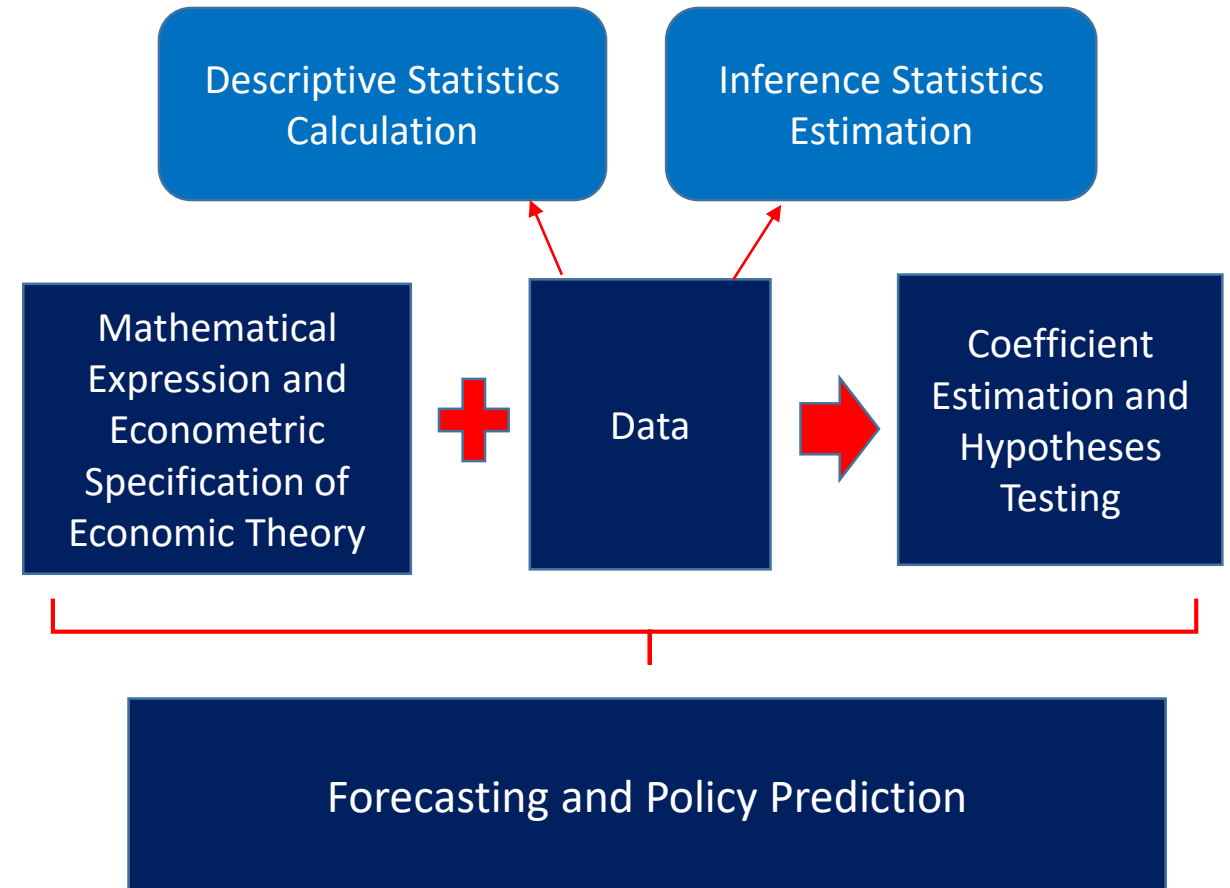
- Information sharing relevant metrics.
- Metrics for measuring privacy.
- Profitability metrics related to cybersecurity market.
- Cybersecurity investment efficiency metrics.
- Metrics enable decision-makers to take action (digital epidemiology).
- Metrics be definable in numbers (capable of expressing meaningful figures).
- Metrics be firmly founded on evidence-based practice (data to be used allowing communication with stakeholders at all levels).
- Metrics be repeatable (automation – easy to collect, update and show trends and all these at a reasonable cost).

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		



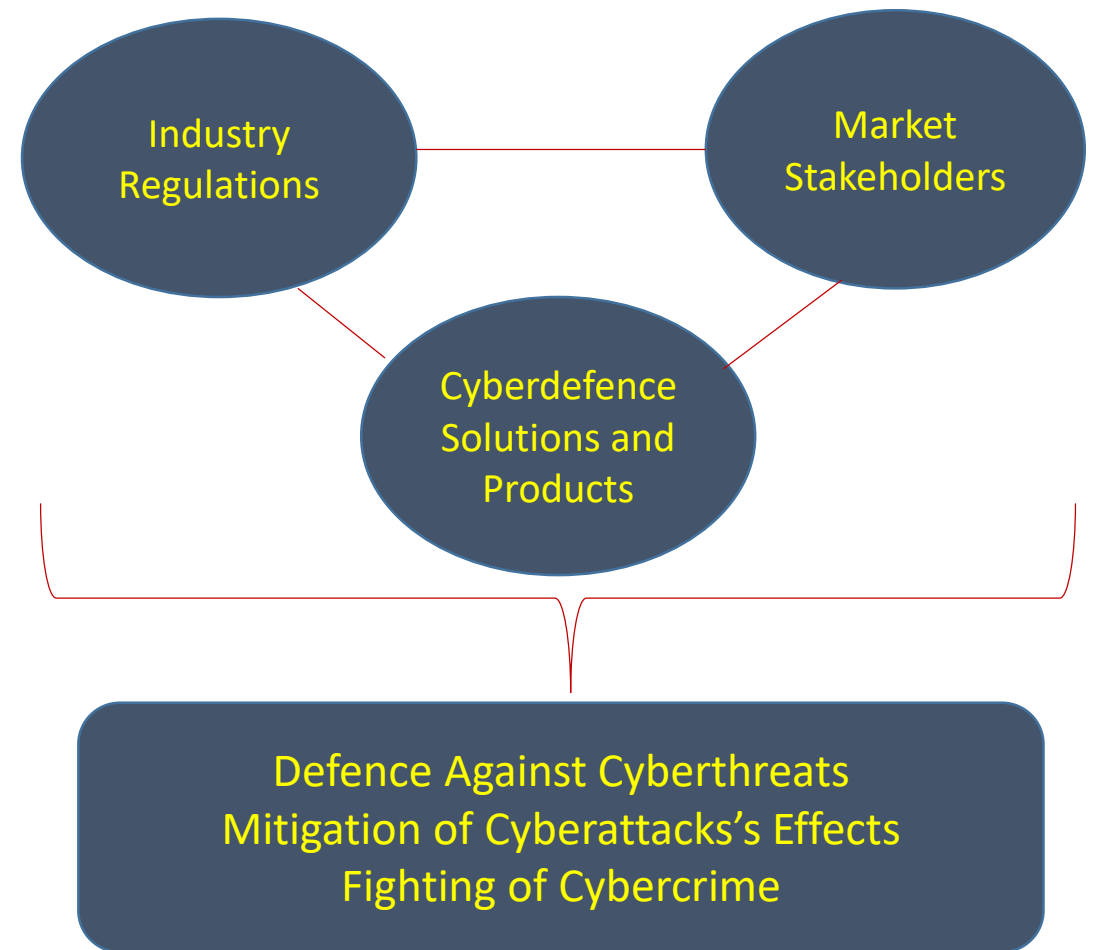
## Economic and Behavioural Theoretic Analysis Methodology

- Investigate the role of information sharing in the cybersecurity investment and assess the relationship between information sharing and the number and severity of cybersecurity incidents.
- Quantitative analysis relating technical and behavioural variables with network traffic flow characteristics in order to identify network conditions indicative of cyberthreats.
- Analysis of economic factors shaping the supply and demand conditions for competition and profitability in the cybersecurity market.
- Investigate the relation between vulnerabilities and cybersecurity investment.



## Ecosystem Comparative Analysis Methodology

- **Comparative and correlation analysis on:**
  - Cybersecurity industry regulations
  - Cybercrime market stakeholders
  - Cyberdefence solutions and products
- **Output results: recommendations and business models to:**
  - Address cyberthreats
  - Mitigate cyberattacks' effects
  - Fight cybercrime



## Automated Data Analysis Methodology

### Multiple intelligent information feeds gathering and storage and multiple analysis deployment

- Exploitation of massive intelligent information feeds from multiple information sources.
- Estimation of the economic impact of criminal activities in the Deep Web.
- Incident reporting and alerting.
- Securing the supporting ICT infrastructure.
- Deployment of multiple techniques for big data automated analysis of network traffic, for maximising the capabilities of the platform's data analysis tool, to exploit acquired encrypted and non encrypted data.
- Risk and cost analysis integrated on the platform tools, for developing and providing revenue models for cybercriminals.
- Impact analysis of identified threats.

cybersecurity/privacy  
discussion  
forums/blocks

bug bounties  
discussions/reward  
announcements

cybersecurity  
product/service  
incident reporting  
web pages

police public  
reports

deep web

network traffic big data

encrypted and non  
encrypted data

impact of identified threats

cost and risk of  
cybercriminals' revenue  
models

## SAINT's expected impact

- ✓ Improved social, institutional and economic comprehension of cybersecurity failures.
- ✓ Improved decision making, governance and investments by stakeholders (e.g. policy makers, regulators, law enforcement agencies, market operators and insurance companies).
- ✓ Provision of new models (that take into account cybersecurity economics, risks, social and market aspects) for improving institutional and private initiatives in their quest for societal resilience to cybersecurity risks.
- ✓ Facilitated information dissemination and sharing for the public and registered users.
- ✓ Provide a set of recommendations to fight cybercrime through systemic approach impacting the economic and incentive models of cybercrime.