3

Statistical Analysis and Economic Models for Enhancing Cyber-security in SAINT

Edgardo Montes de Oca[1], John M. A. Bothos[2] and Stefan Schiffner[3]

[1]Montimage Eurl, 39 rue Bobillot, Paris, France
[2]National Center for Scientific Research “Demokritos”, Patr. Gregoriou E. & 27 Neapoleos Str, Athens, Greece
[3]University of Luxemburg
E-mail: edgardo.montesdeoca@montimage.com; jbothos@iit.demokritos.gr; Stefan.schiffner@uni.lu

SAINT analyses and identifies incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing. Analysis of the ecosystems of cyber-criminal activity, associated markets and revenues drive the development of a framework of business models appropriate for the fighting of cyber-crime. The role of regulatory approaches as a cost benefit in cyber-crime reduction is explored within a concept of greater collaboration to gain optimal attrition of cyber-criminal activities. Experimental economics aid SAINT in designing new methodologies for the development of an ongoing and searchable public database of cyber-security indicators and open source intelligence. Comparative analysis of cyber-crime victims and stakeholders within a framework of qualitative social science methodologies deliver valuable evidences and advance knowledge on privacy issues and deep web practices. Equally, comparative analysis of the failures of current cyber-security solutions underpins a model for greater effectiveness and improved cost-benefits. SAINT advances the metrics of cyber-crime through the construct of a framework of a new empirical science that challenges traditional approaches and fuses evidence-based practices with

more established disciplines. Innovative models, algorithms and automated framework for metrics benefit decision-makers, regulators, law enforcement, at national and organisational levels providing improved cost-benefit analysis and estimation of tangible and intangible costs for optimal risk and investment incentives.

3.1 Introduction

The SAINT project[1] examines the problem of failures in cyber-security using a multidisciplinary approach that goes beyond the purely technical viewpoint. Building upon the research and outcomes from preceding projects, it combines the insights gained to progress further analysis into economic, behavioural, societal and institutional views in pursuit of new methodologies that improve the cost-effectiveness of cyber-security.

SAINT analyses and identified incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing to enhance cyber-security and mitigate (a) the risk and (b) the impact from a cyber-attack, while providing, at the same time, solid economic evidence on the benefits from such improvement based on solid statistical analysis and economic models.

It is widely acknowledged that despite the sums spent annually on cyber-security, cyber-crime continues to flourish. No true or accurate picture of the situation is readily available and yet vast amounts of money continue to be employed in efforts to reduce levels of cyber-crime that do not appear to be working. There are now more than 3.6 billion Internet users[2] and 7.3 billion mobile-cellular subscriptions worldwide[3] in 2016 and rising. According to Microsoft's report [1] on "Cyberspace 2025: Today's Decisions, Tomorrow's Terrain", it is estimated that 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. In this expanding cyber-space, it is estimated that 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. The

[1] SAINT (Systemic Analyser In Network Threats) is an H2020 project. See https://cordis.europa.eu/project/rcn/210229 and https://project-saint.eu for more information.

[2] www.internetworldstats.com (30 June 2016).

[3] www.itu.int

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 represents €15 billion and up to €50 billion for security products and services [2]. Europol, in its 2015 report [3] "Exploring Tomorrow's Organized Crime" forecasts an 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. The crime-as-a-service business model is facilitated by social networking, digital infrastructures and virtual currencies that allow cyber-criminals to exchange and use financial resources anonymously on a large scale.

The EU FP7 project CyberROAD[4] successfully delivered a research roadmap for cyber-crime and cyber–terrorism using in-depth analysis into technological, social, legal, ethical, political, and economic origins of the issues. A noted research outcome was the proposed innovative cyber-crime cost-benefit reduction methodology as delivered in the paper "2020 Cybercrime Economic Costs: No Measure No Solution", [2]. In furtherance of the insights already gained in the CyberROAD project, SAINT carries out an extensive analysis of the state-of-the-art using a range of comparative studies to deliver a framework of data-driven guidelines based on mathematical analysis of the relevant quantitative variables that decision makers require for accurate resource allocation. The construct of such a framework designed with experimental economics aligns and regulates the discipline to that of an empirical science and substantiates the case for greater collaboration in information sharing.

3.2 SAINT Objectives and Results

3.2.1 Main SAINT Objectives

SAINT project studies and improves the measurement approaches and methodologies by means of constructing a framework of a new empirical science, challenge traditional approaches and fuse evidence-based practices with more established disciplines for a lasting legacy. Through the construction this framework, it gives decision makers (public policy authorities, business leaders and individuals) data-driven guidelines based on scientific analysis of relevant quantitative and qualitative variables for their decisions about dedicating resources to deal with cyber-threat risks and cyber-criminals.

[4] https://www.cyberroad-project.eu

By employing various methodologies from different scientific fields, the main objectives of SAINT are to:

1. Establish a complete set of metrics for cyber-security economic analysis, cyber-security and cyber-crime market.
2. Develop new economic models for the reduction of cyber-crime as a cost-benefit operation.
3. Estimate and evaluate the associated benefits and costs of information sharing regarding cyber-attacks.
4. Define the limits of the minimum needed privacy and security level of internet applications, services and technologies.
5. Identify potential benefits and costs of investing in cyber-security industry as a provider of cyber-security services.
6. Develop a framework of automated analysis, for behavioural, social analysis, cyber-security risk and cost assessment.
7. Provide a set of recommendations to all relevant stakeholders including policy makers, regulators, law enforcement agencies, relevant market operators and insurance companies.

3.2.2 Main SAINT Results

The SAINT project examines the problem of failures in cyber-security using a multidisciplinary approach that combines economic, behavioural, societal and institutional approaches in pursuit of new methodologies that improve the cost-effectiveness of cyber-security. SAINT analyses and identifies incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing to enhance cyber-security and mitigate (a) the risk and (b) the impact from a cyber-attack, while providing, at the same time, solid economic evidence on the benefits from such improvement based on solid statistical analysis and economic models.

3.2.2.1 Metrics for cyber-security economic analysis, cyber-security and cyber-crime market

SAINT investigates and establishes accurate indicators and metrics for economic analysis, cyber-security and cyber-crime market, including the effects of regulatory analysis on the economics of cyber-security. It investigates all the open source intelligence methodologies and performs an analysis on the effect of those metrics in different scenarios and environments. The establishment of metrics for measuring privacy is also included in this effort.

With respect to the metrics and indicators (objective 1), SAINT analyses [4]: 19 open source cyber-security indicator datasets (including ENISA's top 15); two indicators of emerging cyber-threats; Blacklists, Blocklists and Whitelists; five insecurity indicators; nine security indicators; nine economic indicators; five open source intelligence methodologies for cyber-threats. It includes relevant examples, usage, statistics, and metrics for each of the above indicators.

SAINT also gathers and analyses [5] evidences from stakeholders, across multiple disciplines, with the objective to examine the problem of failures in cyber-security beyond a purely technical viewpoint and gain advanced knowledge on economics and cyber-security practices from the stakeholders, enabling the gaining of a better understanding of their needs and requirements and providing insights on cyber-security and product value for money. As a consequence of this analysis, FICORA (Finish regulator), is now proactively involved and cooperating in distributing a survey for Finland to gain supporting metrics in answer to an important question: why does Finland have one of the best quantitative track records in cyber-security, within the EU & G20[5]?

It was additionally observed as a result of a comparative analysis that the inclusion of the cost of time spent/lost by cyber-crime victims provided an important metric for ROI calculations. Results show:

- The cost of cyber-crime is estimated to be €30 billion (0.242% of EU's GDP).
- The cost in time lost or spent in 2017 due to cyber-crime amounts to an estimated €60 billion.
- Therefore, the actual total cost of cyber-crime to the EU in 2017 can be estimated to be €90 billion.

3.2.2.2 Economic models for the reduction of cyber-crime as a cost-benefit operation

Significant effort of SAINT is dedicated in the research and development of new economic models for cyber-security and cyber-crime. A rich econometric and mathematical theoretical framework is implemented for this purpose, and the final methodologies and models are validated in a controlled environment under the supervision of the Hellenic Police Cyber-Crime Unit.

In relation to objective 2, research focuses on the organisation's effective operational processes [6] to achieve efficiency in production by investigating their incentives in choosing input combinations that minimise cost and,

[5] http://www.intercomms.net/issue-30/dev-3.html

consequently, maximise profits. With the rapid evolution of Cloud Internet, organisations have an alternative solution to substitute highly qualified Information Technology working staffs that are paid high wage rates, which means excessive labour costs, with subcontracting of such Information Technology services to external providers like the newly emerged Managed Service Providers Networks. In this way, organisations avoid the excessive economic investment costs to set up and develop in-house Information Technology departments from scratch and find the means to hire or offer professional training to existing working staff, with the potential risk of economic losses resulting, in case of failures from such internally structured departments. Research in this field concerns the organisations' decisions to substitute production factors, purchased in the respective production factor markets, to minimise their production cost. It studies the dependence of the organisations' policies, concerning the outsourcing of certain Information Technology activities, by purchasing Cloud Internet computer services from automated platforms of Managed Service Provider Networks, on the price of Information Technology labour force that is the wage rates in the Information Technology sector. The empirical research performed in showed that organisations' price cross-elasticity demand for Cloud Internet computer services is significantly negative towards the wage rate in the Information Technology sector for specialised Information Technology labour force by -21.84% ($\pm 6.38\%$). The evolution of Cloud Internet in our time has given organisations many alternatives, especially in the area of Information Technology services that can be purchased online, through the participation in relevant automated platform networks, operated and managed by external providers, in the form of Managed Service Provider Networks.

SAINT identifies current cyber-security failures and requirements to improve the situation at all levels of cyber-security defences and across a variety of sectors [7]. It determines what constitutes a cyber-security failure, or what inadvertently increases the risk of a cyber-attack, using quantitative and qualitative analysis, to identify what new practices are required to improve cyber-security, reduce wasteful information technology spending and improve return on investment.

SAINT also investigates how cyber-attacks materialise, focusing on what lies behind and contributes to the materialisation of these attacks [8]. This basically represents the emergence of a whole new economy consisting of a new and fast-growing body of vulnerability markets with stakeholders selling and buying vulnerabilities to gain financial gains or avoid financial losses, associated with immaterial assets, namely the vulnerabilities and their exploits. The goal is to identify and categorise the vulnerabilities and exploits markets along with the involved stakeholders and their roles, to provide guidelines for cost-effective cyber-security methodologies that can be applied as counter-measures for defence against malicious hackers. Vulnerability announcements can inflict severe monetary and other intangible costs on the company's value.

3.2.2.3 Benefits and costs of information sharing regarding cyber-attacks

SAINT provides guidelines for information sharing between all the agents, for mitigating inefficiencies in the cyber-security investment landscape and in the total economy in general. These guidelines are based on the joint evaluation of measurable quantitative economic and technical variables regarding the influence of cyber-security information sharing in the cost structure, the rate of investment, the effective allocation of resources and the overall profitability of each agent.

SAINT estimates and evaluates the associated benefits and costs of information sharing regarding cyber-attacks (objective 3) [6, 9]. For this, international cooperation activities have been studied [9], such as the ITU Global Cyber-security Agenda (GCA).

The GCA is a framework launched in 2007 for international cooperation. It is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts. Within GCA, ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT) promote the deployment of solutions and services to address cyber-threats on a global scale. It is a global multi-stakeholder and public-private alliance against cyber-threats. EU addresses cyber-security through tool policies that affect the structures and capabilities of organisations while in parallel takes action by providing incentives to support and promote the development of co-operation in the area of cyber-security, for detecting cyber-incidents and responding to cyber-attacks effectively and appropriately.

The Directive on the Security of Network and Information Systems, the "NIS Directive", mentioned as the first EU-wide cyber-security law, is designed among others to foster better co-operation in reporting serious incidents and adopting effective risk management practices.

Regarding the promotion of cooperation in cyber-security domain, ENISA also serves as a focal point for information sharing and spread of knowledge in the cyber-security community, through the setting up of

Information Sharing and Analysis Centres. Their role is particularly important in creating the necessary trust for sharing information between all the different agents.

The subject of co-operation between organisations and how it influences their effective performance and allocation of their resources in terms of decreasing production cost and profitable exploitation of production inputs has been studied [6]. In this context co-operation between organisations is defined as information sharing between them. It proves empirically the importance of co-operation through information sharing in minimising production cost and achieving economic efficiency in the allocation of resources. The associated benefits of information sharing between organisations have been evaluated. In the long-run, using information sharing processes for improving the production process has an almost -13% ($\pm$ 3.58%) decreasing effect on the real (deflated) long-run average production cost for the sample of our Eurozone countries, for the time period 2009–2012.

3.2.2.4 Privacy and security level of internet applications, services and technologies

SAINT analyses the dependence of detection of cyber-security incidents, on behavioural features of network traffic flow to interpret adequately the careless behaviour of internet users, regarding the proper application of cyber-security norms and rules. For this, SAINT implemented a correlation analysis on quantitative technical and measurable qualitative behavioural variables, concerning network traffic flow characteristics and cyber-security behaviour characteristics.

Regarding the limits of the minimum needed privacy and security level of internet applications, services and technologies (objective 4), [10] devised models and mechanisms for measuring privacy and for user privacy protection mechanisms. Several formal frameworks of privacy notions, with differing assumptions, are proposed that study the relations between Anonymous Communication Networks and respective provided privacy.

Based on this work, in [18] SAINT proposes how these different frameworks can be unified by constructing a generalized indistinguishability game similar to the games used to define semantic security in cryptographic protocols [23].

Along with effective defences against website fingerprinting, such as continuous data flow, package padding and traffic morphing, adaptive padding between data packets with generic web traffic and clustering of webpages into similarity groups. Beyond this, SAINT investigates:

- Approaches for protecting publicly available databases like secure computation of elementary database queries, locally random reductions of sets to databases, zero Knowledge interactive (and non-interactive) proofs, data oblivious data transfers in private information retrieval.
- Privacy preserving credentials and authentication mechanisms like password-based authentication, cryptographic certificates, attribute-based credentials, electronic certificates and electronic Identities.
- Database content anonymisation concepts and techniques like k-anonymity, i-diversity, t-closeness, bloom filters, differential privacy.

3.2.2.5 Benefits and costs of investing in cyber-security

SAINT provides guidelines and frameworks for maximising efficiency in cyber-security services. Part of the effort is dedicated in the development of alternative ways and methods to get valuable information in measurable quantitative form of metrics and then to analyse it to highlight guidelines for competitiveness and profitability in the cyber-security industry. SAINT also determines the value of the underground and cyber-crime market within a wider investigation of information security markets including.

In relation to objective 5, SAINT proposes new models and new paradigms in cyber-security with a special focus on the incentives of the different stakeholders in the ecosystem of cyber-criminality. It was first necessary to identify the existing business models that cyber-criminals use, and to describe the different national strategies of European countries that have been put in place to fight against cyber-crime. From this, new models are proposed that provide innovative ways that help reduce cyber-crime by targeting the right incentives of both cyber-criminals and cyber-security practitioners. These models are compared among each other and their practical relevance is evaluated [11]. Some of the results obtained concern: the analysis of existing cyber-criminal business models; the analysis of national, European and international cyber-security policies and strategies and the draft of 8 innovative models to fight against cyber-crime, including: the certification and labelling services model; the insurance model; the wage model; the collaborative model; the education model; the crowdsourcing model; the bug-bounty model; the artificial intelligence model.

In relation to objective 5, SAINT demonstrates [8] that behind the materialisation of the cyber-attacks there is a new and fast-growing body of vulnerability markets with stakeholders selling and buying vulnerabilities for financial gains or to avoid financial loss. This implies that a whole new economy is rapidly evolving based on immaterial assets, the vulnerabilities and their exploits. Over the last years, ransomware attackers demanded payment in cryptocurrencies, with the Bitcoin[6] being among the most popular ones. Bitcoin offers anonymity in terms of involved parties and the amount of the transaction and their use for illicit purposes has become popular.

The "Execute Code"-related vulnerabilities are prevalent among all other vulnerabilities, which implies that software vendors (mainly OS developers) fail to take appropriate measures during the design and implementation stages. Most of the discovered vulnerabilities (over 50%) are severe, with a severity score at least six. This, in turn, may imply severe financial or other intangible (e.g. trust, fame) costs on affected companies. No software product or system is immune to vulnerabilities, which demonstrates that vulnerability discoverers could virtually target any vendor, operating system, or software product as long as it is either, (or both), a challenging or profitable target.

Vulnerability announcements can inflict severe monetary and other intangible costs (e.g. loss of trust and tarnished fame) on the affected company, measured by system downtime, operation disruption, loss of credibility and customers, higher assurance costs, etc.

Vulnerability announcements can lead to a negative and significant change in a software vendor's market value. According to the conducted quantitative analysis, an affected vendor can lose even 60% value in stock price when a related vulnerability is disclosed. Study has also showed that a software vendor loses more market share if the market is competitive or if the vendor is small. Moreover, as can be expected, the change in stock value is more negative if the vendor fails to provide the right patch at the time of disclosure of the vulnerability. In addition, according to the findings, key vulnerabilities have significantly more impact on the company's value.

Useful insights on the types of attacks per business sector have also been obtained [12]. Small businesses (with fewer than 250 employees) are those most targeted by cyber-attacks, making up as much as 43% of all the cyber-attacks on companies (in 2015). Large enterprises (with over 2,500 employees) accounted for 35% of all cyber-attacks, while medium-sized businesses (with between 251 and 2,500 employees) made up the remaining 22%. It is interesting to note that these results are diametrically opposed to those from 2011 where large businesses accounted for the majority (50%) of all cyber-attacks on companies, medium-sized businesses represented 32%, while small businesses accounted for 18%. Between 2011 and 2015, small businesses have been increasingly targeted by cyber-attacks. This trend can

[6] https://www.bitcoin.com/

be explained by the fact that, unlike big businesses that have the capacity to invest in proper expertise and technologies, smaller businesses may not always have the financial resources and staff to protect themselves from such threats. Consequently, cyber-attackers take advantage of smaller companies' digital vulnerability to steal confidential data and intellectual property, bring down the website, or organising phishing and spamming campaigns. Regarding the type of cyber-attacks on businesses, we have the following specificities:

- Spam: the size of a company has limited influence over its spam rate. Indeed, in 2016, the spam-rate varied between 52.6% and 54.2%, which shows that all kinds of companies are likely to be targeted, regardless of their size. Furthermore, all industry sectors receive similar quantities of spam.
- Phishing: although the overall phishing rates have declined over the past three years, companies are still targeted by these attacks. Medium-sized businesses experience the highest phishing rates. In 2016, the sector of agriculture, forestry, and fishing was the most affected by phishing, with one in 1,815 emails being classed as a phishing attempt.
- Data breaches: In 2016, the industry of services (particularly business services and health services) was the most affected by data breaches, representing 44.2% of all breaches. The sector of finance, insurance, and real estate was ranked second with 22.1%.

The private sector, particularly the cyber-security industry, plays an important role in combatting cyber-crime by providing individual users, businesses, and organisations with services and solutions to cyber-threats. In 2003, the global cyber-security market represented $2.5 billion, currently it amounts to $106 billion, and the sector will be worth $639 billion in 2023. These numbers underline the growing demand for cyber-security solutions and highlight the business opportunities in the sector.

In 2016, the commercial cyber-security vendors' market was dominated by the United States with a total of 827 vendors leading cyber-security research and products. Israel and the United Kingdom hold second and third place in the ranking with 228 and 76 vendors respectively.

While the cyber-security industry has potential for growth, in both the private and public sectors, it is still struggling to keep up with cyber-crime for three reasons:

- The variety of IoT devices: the increase in connected IoT devices increases the number of potential targets. Projections suggest that, by 2020, there will be tens of billions of connected digital devices in the EU alone.

- The multiplicity of data: an increase in connected IoT devices directly correlates with an increase in data that needs to be protected.
- The shortage of skilled workers in the cyber-security sector: in spite of the great employment opportunities and high number of open positions for IT specialists and cyber-security professionals, the cyber-security industry struggles with training them in time to keep up with growing demand. The solution to this problem may come from artificial intelligence and machine learning, which are currently being developed.

SAINT also performed a cost-benefit analysis of cyber-security solutions and products (objective 5). This is built on a cash flow analysis of cyber-security solutions, products and models. It relies on information from a market analysis established [12], on the revenue analysis of cyber-security services [13] and on the most relevant models identified. It also uses input from conducted surveys [14] and estimates the price of digital assets and the costs of intangible risks. In addition to the cash flow analysis, a sensitivity and risk analysis is implemented [15]. These recommendations serve as guidelines for various stakeholders, including cyber-security business providers. It builds on the cost-benefit implemented, as well as on the econometric analysis of cyber-security solutions, the market analysis, and the assessment of the innovative cyber-security models analysed [16].

3.2.2.6 Framework of automated analysis, for behavioural, social analysis, cyber-security risk and cost assessment

In the framework of automated analysis (objective 6), SAINT defines the different tools that constitute the Framework (Figure 3.1, [17]). This includes the cyber-security cost-benefit analysis tools and algorithms. Based on available metrics, indicators and parameters, the techniques allow the construction of models and the estimation of the price of digital assets and costs of intangible risks (e.g. reputation, non-critical service disruption). A toolset for automated analysis based on automatic information gathering and analysis tools that extract information from a variety of information sources on the Internet and the Deep Web has been designed and prototypes implemented. The tools include: Social Network Analyser and the Deep Web Crawler. The information sources include cyber-security related discussion forums, bug bounties, social network discussions and public vulnerability and data breach incident databases.

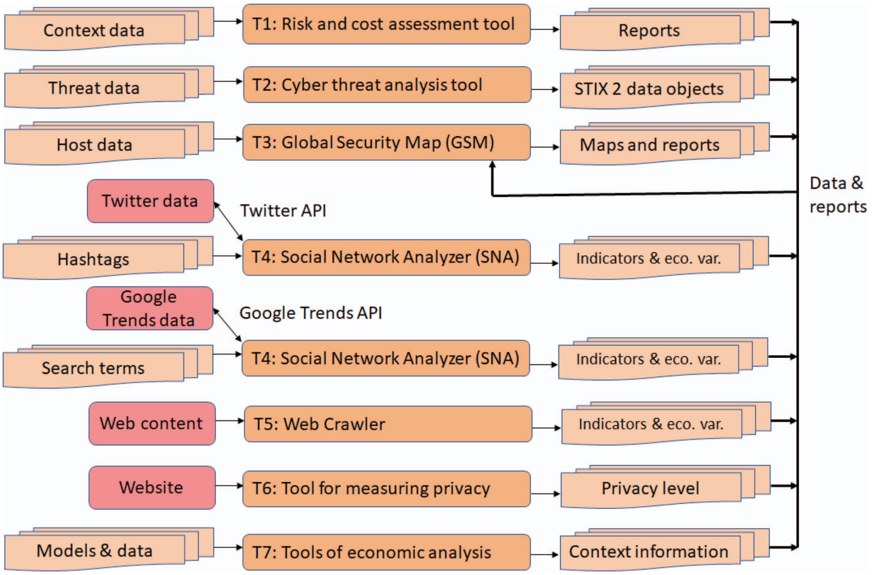


Figure 3.1 High-level architecture of the SAINT framework.

The developed Twitter Social Network Analyser (SNA) utilizes the social network, Twitter, to extract trends on the cyber-crime activity. To this end, a dictionary of #hashtags of interest is created. The SAINT SNA mines only publicly available tweets and accounts for the specific hashtags and extracts the related information.

The Google Trends SNA utilizes the popular Google Trends platform to extract trends that are related to cyber-crime activity. Google Trends is a public web facility of Google Inc. It is based on Google Search and shows how often a particular search term is entered with respect to the total searches in different regions of the world and in various languages.

Crawling and Scraping the Web and Deep Web can be categorized into two different large types, where each one includes a number of considerations and design decisions, depending to the target web sites that are searched (Web and Deep/Dark Web). The first type is Web Scraping of a website and the second one Crawling. The Tor network was found to be the ideal place for investigating cyber-criminal activity while browsing anonymously Deep Web sites to avoid of being hacked or traced. For the implementation of our scripts, we run Tor in the background to avoid being detected by users of the Deep and the Dark Web.

SAINT's Global Security Map (GSM)[7] gathers data on selected ENISA indicators using a variety of suitable open source feeds and presents the results visually on a global map. It is an interactive tool which enables visualization of the geographic distribution of the sources of cyber-crime and quantitative comparative metrics, with the aim to provide a simple and accurate method of displaying the global hotspots for the location and quantification of the top cyber-threat indicators: malware, phishing, spam, cyber-attacks, and other malicious activities. The unique combination of detailed data and simplified visualizations make the tool ideal for research and comparative analysis purposes by governments, law enforcement, CERTs, academia, Infosec, financial institutions and the public sector (also related to objective 7).

One more tool developed in the scope of SAINT project is Tool for measuring privacy in encrypted networks [18]. Resent research [19, 20] showed that user's privacy can be endangered even if he is using anonymization networks such as TOR [21] or JAP [22]. By means of an attack known as *website fingerprinting*, it is possible to identify which website a user is visiting and, thereby, to identify both two communicators and the content of the communication. However, different websites have different degrees of finger printability. Thereby, SAINT developed a tool which allows any user to estimate his vulnerability level to the website fingerprinting attack when visiting a website. Afterward, the user can decide if visiting this website costs the possible risks.

3.2.2.7 Recommendations to stakeholders

Reference model (Figure 3.2, [12]) illustrates the interactions between the different stakeholders involved in the cyber-crime and cyber-security ecosystem.

Related to objective 7, SAINT provides a set of recommendations to all relevant stakeholders (policy-makers, regulators, law enforcement agencies, relevant market operators and insurance companies) [16]. This builds on the input of various sources from different partners, including the stakeholder surveys that were conducted. An initial set of recommendations has been defined that includes:

- Adopting in-depth comparative analysis for the application of successful practices of individual countries, i.e. Finland (see Figure 3.3).

[7] https://3hz6pq.staging.cyberdefcon.com/

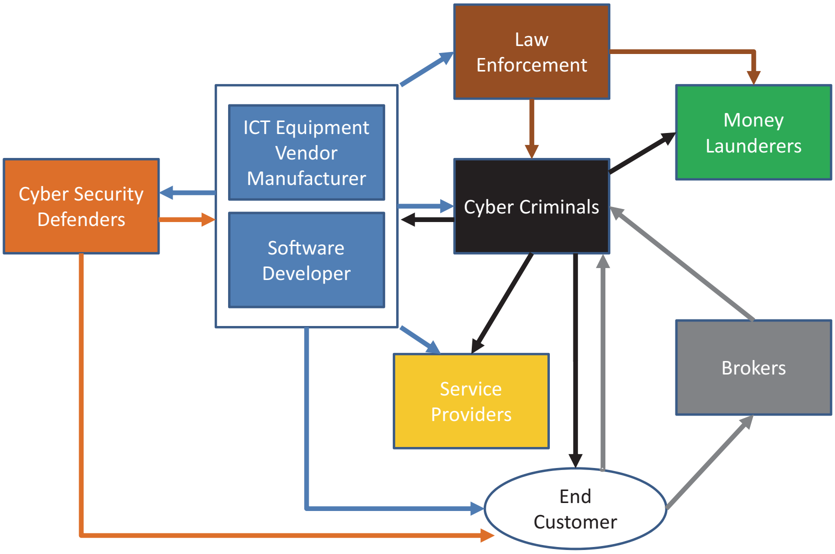
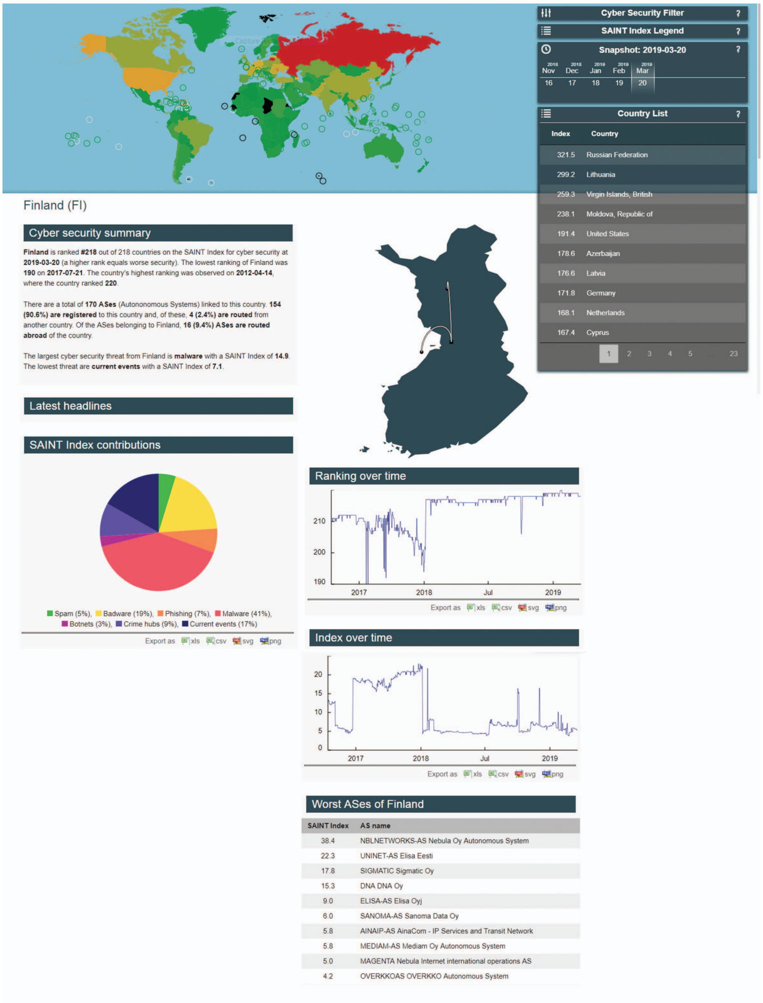


Figure 3.2 Stakeholder reference model.

- Improving the cost of cyber-crime metrics and econometrics for enhanced ROI calculations by the inclusion of the time spent or lost by cyber-crime victims.
- Improving the transparency of cyber-security matters within the workplace.
- Educating the workforce on the costs and risks to the workplace of cyber-practices.
- Furthering cyber-security training & education within the EU to alleviate the acknowledged lack of trained staff.
- Improving the complementarity among standards and best practices in cyber-security within the EU.
- Standardising the metrics to enable accurate comparative analysis between surveys/reports.

In Finland, FICORA has the role of a CERT that is a regulator but also acts to prevent and remediate cyber-security issues. The problem in other countries is that the regulators are only telecom regulators whereas in Finland FICORA is both a telecom and cyber-security regulator. Telecom operators are not really concerned about the security of customers. They just want to make sure that their services work, that the pricing brings profits and that the competition is regulated to their advantage. Most CERTs in Europe have a limited role that



Cyber Security Filter

SAINT Index Legend

Snapshot: 2019-03-20

2018 Nov	2018 Dec	2019 Jan	2019 Feb	2019 Mar
16	17	18	19	20

Country List

Index	Country
321.5	Russian Federation
299.2	Lithuania
259.3	Virgin Islands, British
238.1	Moldova, Republic of
191.4	United States
178.6	Azerbaijan
176.6	Latvia
171.8	Germany
168.1	Netherlands
167.4	Cyprus

1 2 3 4 5 … 23

Finland (FI)

Cyber security summary

Finland is ranked **#218** out of 218 countries on the SAINT Index for cyber security at **2019-03-20** (a higher rank equals worse security). The lowest ranking of Finland was **190** on **2017-07-21**. The country's highest ranking was observed on **2012-04-14**, where the country ranked **220**.

There are a total of **170 ASes** (Autononomous Systems) linked to this country. **154 (90.6%) are registered** to this country and, of these, **4 (2.4%) are routed** from another country. Of the ASes belonging to Finland, **16 (9.4%) ASes are routed abroad** of the country.

The largest cyber security threat from Finland is **malware** with a SAINT Index of **14.9**. The lowest threat are **current events** with a SAINT Index of **7.1**.

Latest headlines

SAINT Index contributions

🟩 Spam (5%), 🟨 Badware (19%), 🟧 Phishing (7%), 🟥 Malware (41%),
🟪 Botnets (3%), 🟪 Crime hubs (9%), 🟦 Current events (17%)
Export as xls csv svg png

Ranking over time

Index over time

Worst ASes of Finland

SAINT Index	AS name
38.4	NBLNETWORKS-AS Nebula Oy Autonomous System
22.3	UNINET-AS Elisa Eesti
17.8	SIGMATIC Sigmatic Oy
15.3	DNA DNA Oy
9.0	ELISA-AS Elisa Oyj
6.0	SANOMA-AS Sanoma Data Oy
5.8	AINAIP-AS AinaCom - IP Services and Transit Network
5.8	MEDIAM-AS Mediam Oy Autonomous System
5.0	MAGENTA Nebula Internet international operations AS
4.2	OVERKKOAS OVERKKO Autonomous System

Figure 3.3 Global security map of Finland.

consists in reporting threats, building cyber-threat intelligence frameworks, and stimulating or developing cyber-threat solutions. When the safety and security of citizens is concerned we need entities that act and are proactive as is the case in the health and food sectors. FICORA is the best qualitatively and quantitatively. It bases its cyber-security activity on technologically efficient techniques, such as darknets or reverse network telescopes, but also it obtains results through sound organisation, clear objectives, close collaboration with all the stakeholders, and has the budget to do it.

Another aspect that should be emphasised is the legal one. The U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs) has resulted in an almost immediate reduction of botnets in the US. Operators started taking down botnets and collaborating to do so. What can be derived from this experience is that when a law is passed that identifies responsibilities and penalties, companies and individuals are incentivised. Telecom operators will start taking down botnets and fighting cyber-criminality only when it becomes financially interesting for them. Unfortunately, there is yet no law in Europe that is equivalent to ABC. The examples of collaborative actions since 2014 [9] show progress but the need remains to obtain a more systematic approach for fighting cyber-crime that is better and more globally organized. This can only be achieved with effective laws, regulations, incentivisation and cooperation at the national and international levels.

3.3 Conclusion

The SAINT project has worked on and advanced in the comprehension of the stakes involved in the cyber-security domain. It has analysed the risks and cost of security threats by compiling a complete set of metrics for the analysis of cyber-security economics, cyber-security risks, and the cyber-crime market. New economic models and algorithms have been developed to find optimised cost-benefit solutions for reducing cyber-crime.

The deep analysis of the benefits obtained from cyber-attacks information sharing (in particular, cooperative and regulatory approaches), positive impact of investments in cyber-security by industry, and the risks and costs of security breaches have resulted in a set of recommendations valuable for all relevant stakeholders (e.g. policy makers, regulators, law enforcement agencies, industry). The studies and surveys conducted have also allowed to better understanding the limitations and needs involved when finding the equilibrium between privacy and security of internet-based applications, services and technologies.

SAINT has also developed a framework that facilitates the automated analysis for behavioural, social, cyber-security risk and cost assessment. Research gaps have been addressed that can help policy makers make more informed decision on where economic investments should be directed to return the best possible outcomes. The different tools that constitute the SAINT Framework target improving the automation of certain analysis tasks and present the results in an integrated way, at least partially. The resulting system serves as a proof of concept that will show the usefulness of the integration of data from different sources and tools. In the future, the Framework will be extended and include a tighter integration so that researchers can process different types of security intelligence information and obtain results in a methodical way.

The main challenge identified by SAINT is to find the best approaches to:

- Coordinate cyber-security related issues and actions (i.e., related to legislative, regulatory, law enforcing and cooperative) between different organisations and countries;
- Measure the effectiveness of the actions;
- Achieve long-term impact to improve the security of ICT users;
- Implement and enforce laws and regulations in a virtualised and often conflicting international context;
- Make security an integral part of ICT design;
- Reverse the tendency that makes economic incentives better for criminals that those who need to protect their systems;
- Achieve consensus between stakeholders and countries;
- Improve education related to cyber-security;
- Find a good balance between security and privacy.

Having analysed different regulations and practices our conclusion is that we need to attack the cyber-threat problem from all fronts at the same time, in other words we need to:

- Improve the laws and regulations and make them more comprehensive;
- Coordinate better the regulatory processes and incentivize cooperation;
- Make cyber-security and privacy protection an obligation of service providers (including operators) to their customers;
- Greatly improve the awareness of the individuals to the risks;
- Change the economics to reduce the benefits of cyber-criminal activities and improve the perceived benefits of cyber-security measures. This includes reforming the international finance system to eliminate, or at least greatly reduce, the money laundering possibilities (e.g., tax havens, bitcoins).

Many of the challenges are addressed in the case of Finland, except maybe for the challenges related to the privacy concerns and the economics and financial aspects. Collaborative actions need to be done in a more systematic, global and organised way for fighting cyber-crime. This can only be achieved with effective laws, regulations, incentivisation and cooperation at the national and international levels. Currently, cyber-crime is more incentivized and even cooperates better than organisations that fight it. This situation needs to be reversed and obtaining profits by cyber-criminals should be made much more complicated.

Acknowledgements

This work is performed within the SAINT Project (Systemic Analyser in Network Threats) with the support from the H2020 Programme of the European Commission, under Grant Agreement No. 740829. It has been carried out by the partners involved in the project:

- National Center for Scientific Research "Demokritos", Integrated Systems Laboratory, Greece
- Computer Technology Institute and Press DIOFANTUS, Greece
- University of Luxembourg, Luxemburg
- Center for Security Studies – KEMEA, Greece
- Mandat International, Switzerland
- Archimede Solutions SARL, Switzerland
- Stichting CyberDefcon Netherlands Foundation, Netherlands
- Montimage EURL, France
- Incites Consulting SARL, Luxemburg

Thus, we would like to thank the different contributors from these organizations:

Eirini Papadopoulou, Konstantinos Georgios Thanos, Andreas Zalonis, Constantinos Rizogiannis, Antonis Danelakis, Ioannis Neokosmidis, Theodoros Rokkas, Dimitrios Xydias, Jart Armin, Bryn Thompson, Jane Ginn, Pantelis Tzamalis, Vasileios Vlachos, Yannis Stamatiou, Marharyta Aleksandrova, Latif Ladid, Dimitris Kavallieros, George Kokkinis, Cesar Andres, Christopher Hemmens, Anna Brékine, Sebastien Ziegler, Olivia Doell, Gabriela Znamenackova, Gabriela Hrasko.

We would also like to thank FICORA (Finland) for their help.

References

[1] Burt, Kleiner, Nicholas, Sullivan, "Cyberspace 2025 Today's Decisions, Tomorrow's Terrain, Navigating the Future of Cyber-security Policy", Microsoft Corporation, June 2014.

[2] Armin, Thompson, Kijewski, Ariu, Giacinto, Roli, "2020 Cybercrime Economic Costs: No measure No solution", 10th International

Conference on Availability, Reliability and Security, Toulouse, August 2015.

[3] European Police Office, "Exploring Tomorrow's Organised Crime", 2015 available at: https://www.europol.europa.eu

[4] Jart Armin, Bryn Thompson et al., "Final report on Cyber-security Indicators & Open Source Intelligence Methodologies", SAINT D2.1 Deliverable. Not yet available.

[5] Jart Armin, Bryn Thompson et al., "Final Report on the Comparative Analysis of Cyber-Crime Victims", SAINT D2.3 Deliverable. Not yet available.

[6] John M.A. Bothos et al., "Cyber-security Empirical Stochastic Econometric Modelling of Information Sharing and Behavioural Attitude", SAINT D3.1 Deliverable available at: https://project-saint.eu/deliverables

[7] Bryn Thompson, Jart Armin et al., "Final Analysis on Cyber-security Failures and Requirements", SAINT D3.3 Confidential Deliverable.

[8] Yannis Stamatiou et al., "Analysis of Legal and Illegal Vulnerability Markets and Specification of the Data Acquisition Mechanisms", SAINT D3.5 Deliverable available at: https://project-saint.eu/deliverables

[9] Edgardo Montes de Oca, Cesar Andres et al., "Comparative Analysis of Incentivised Cooperative and Regulatory Processes in Cyber-security", SAINT D2.5 Deliverable available at: https://project-saint.eu/deliverables

[10] Stefan Schiffner, Marharyta Aleksandrova et al., "Metrics for Measuring and Assessing Privacy of Network Communication", SAINT D2.6 Deliverable available at: https://project-saint.eu/deliverables

[11] Olivia Döll, Gabriela Hrasko et al., "Business Modelling Report", SAINT D4.3 Deliverable. Not yet available.

[12] Christopher Hemmens, Anna Brékine et al., "Stakeholder and Ecosystem Market Analysis", SAINT D4.1 Deliverable available at: https://project-saint.eu/deliverables

[13] John M.A. Bothos, Eirini Papadopoulou, Konstantinos Georgios Thanos, "Cyber-security and Cyber-crime Market & Revenue Analysis", SAINT D4.2 Deliverable. Not yet available.

[14] Bryn Thompson et al., "Stakeholder and Consumer Requirements Survey Report", SAINT D6.2 Deliverable available at: https://project-saint.eu/sites/deliverables

[15] Theodoros Rokkas, Ioannis Neokosmidis, Dimitris Xydias et al., “Report on Cost-Benefit Analysis of Cyber-security Solutions, Products and Models”, SAINT D4.4 Deliverable. Not yet available.

[16] Archimede Solutions et al., “Recommendations on Investment, Risk Management and Cyber-Security Insurance”, SAINT D4.5 Deliverable. Not yet available.

[17] Edgardo Montes de Oca, Cesar Andres et al., “Requirements Specification & Architectural Design of The SAINT Tool Framework”, SAINT D5.1 Deliverable available at: https://project-saint.eu/deliverables

[18] Stefan Schiffner, Marharyta Aleksandrova et al., “Semi-automated Traffic Analysis of Encrypted Network Traffic”, SAINT D5.2. Not yet available.

[19] A. Panchenko, L. Niessen, A. Zinnen, and T. Engel, “Website fingerprinting in onion routing based anonymization networks,” in Proceedings of ACM WPES. Chicago, IL, USA: ACM Press, pp. 103–114, October 2011.

[20] A. Panchenko, A. Mitseva, M. Henze, F. Lanze, K.Wehrle, and T. Engel, “Analysis of fingerprinting techniques for tor hidden services,” in Proceedings of the Workshop on Privacy in the Electronic Society, pp. 165–175, ACM, 2017.

[21] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The second generation onion router,” in Proceedings of USENIX Security, San Diego, CA, USA: USENIX Association, 18 p, 2004.

[22] O. Berthold, H. Federrath, and S. Kopsell, “Web mixes: A system for anonymous and unobservable internet access,” in Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, pp. 115–129, July 2000.

[23] C. Kuhn, M. Beck, S Schiffner, T. Strufe, and E. Jorswieck “Privacy framework for anonymous communication”, 20 pages, in print (poPETS, 2019).