Horizon 2020 Program (2014-2020)

Cyber security, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

Cyber security cOmpeteNCefOr Research anD InnovAtion[1†]

T4.3 – Economic Perspectives (Initial Report)

Abstract: This document reviews the cyber security threats background and proposes a structured economic approach enabling the development of fine-grained economic models for the mapping of tasks, risks, and dependencies at a low level in order to approximate cost estimates related to cyber security tasks. Moreover, an analysis of threats and risks for Europe is conducted as well as the different relationships among stakeholders identified.

Authors: Muriel Franco, Bruno Rodrigues, Geetha Parangi, Burkhard Stiller
Lead: University of Zurich UZH

10.06.2019

1 The research leading to these results has received funding from the European Union Horizon 2020 Program (2014-2020) under grant agreement n° 830927.

The CONCORDIA Consortium

CODE	Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JUB	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
TUD	Technical University of Darmstadt	Germany
MUNI	Masaryk University	Czech Republik
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
ICL	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT	European Institute of Innovation + Technology	Hungary/EU
TELENOR	Telenor	Norway
ACS	Airbus Cyber security	Germany
SECT	secunet Security Networks	Germany
IFAG	Infineon	Germany
SIDN	SIDN	Netherlands
SNET	SurfNet	Netherlands
CYD	Cyber Detect	France
TID	Telefonica I+D	Spain
RD	RUAG Defence	Switzerland
BD	Bitdefender	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens	Germany
Flowmon	Flowmon Networks	Czech Republic
TVA	TV Austria	Austria
TI	Telecom Italia	Italy
EFA	EFACEC	Portugal
ALBV	Arthur's Legal B.V.	Netherlands
EI	eesy innovation	Germany
DFN-CERT	DFN-CERT	Germany
CAIXA	CaixaBank	Spain
BMW	BMW	Germany

GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece

Contents

1. Introduction

Cyber security concerns are one of the significant side effects of an increasingly interconnected world, which inevitably put economic factors into perspective either directly or indirectly. As various types of attacks are being leveraged with the democratization of Internet access, there is a greater need for companies and nations for higher protective measures concerning their cyber activities. For example, Critical National Infrastructures (CNI) are infrastructures that are crucial for the everyday life of the population of the nation. Infrastructures from different sectors can be considered as CNI, which directly affect the health of the population while others are affecting the national economy. These infrastructures should receive special attention regarding reliability and security because of their importance and the dangerous impacts if they failed.

The most dangerous threats for the few years were discussed in a recent report prediction [35]. Such threats include Cyber-Crime-as-Service, attacks related to Internet-of-Things (IoT), attacks based on artificial intelligence (*e.g.,* social engineering), and cyber bullying. Besides, attacks on cloud storages, nations, and supply chain are still rising, such as sabotages, misinformation campaigns and stealing of sensitive data. Even though those threats are being the concern of academia and industry for the past years, solutions to completely solve them are not on the horizon. Also, most of the target`s companies, although has giving attention to that, are not investing sufficient budget in protecting themselves against attackers.

Ernst & Young [13] released a survey concerning the reasons for vulnerabilities, in which almost 60% of the companies included in the survey mention that budget constraints are the reasons behind missing measures against cyber-attacks. From these, 53% of the companies stated that the lack of skilled resources, namely employees, pose a danger to the cyber security of the company. This problem could also be caused by the lack of willingness to invest in better cyber security systems and personnel by the company, since the acquisition of skilled workers expensive in general. The survey mentions that tools and methods to recognize vulnerabilities and cyber threats are many times not advanced enough to meet the need in the current environment. All these factors together form a major peril to the cyber security of companies and their system and may be responsible for a considerable number of successful cyber-attacks.

Also, it is important to mention that while most corporate business actions can be quantified, security is not straightforward to be quantified. Contrary to the popular opinion, not having suffered from a cyber-attack is not a valid indication for a secure organization. In this context, a vulnerability in a single system can put in risk all other subsystems or directly connected systems. In addition to security aspects, one must consider safety aspects in which systems can deliberately fail (*e.g.,* due to human or natural disaster factors), jeopardizing one of the fundamental aspects of security, the availability. Nonetheless, announcing that an organization implemented a 24/7 CSIRT (Computer Security Incident Response Team) is, in fact, an indicator for security, but the indicator is limited to the capacity of its professionals only. There is a need for standards to measure and reveal the security level such that all stakeholders can understand and develop a common view.

Such standards are for instance ISO27000, the Cyber security Framework of the National Institute of Standards and Security, the Control Objectives for Information and Related Technology (COBIT) of the Information Systems Audit and Control Association (ISACA) or IEC6244 of the International Electrotechnical Commission. Even though these work differently, they are following common goals. With the help of the mentioned standards, security responsible can compare themselves to other market players or even to whole industries. Committing to be certified against ISO27000 or improving one's NIST (National Institute of Standards and Technology) tier level makes investments into security justifiable for the security responsible in an organization. What this means in detail, will be discussed in the following sections.

The cybercrime economic damages go beyond of thefts of personal/financial data or intellectual property. These attacks can cause a direct loss in the company's reputation, which may even represent a total disruption of the business. In this context, it is imperative to understand the dependencies between complex and distributed systems (e.g., supply chain), as well as security and safety risks associated with each actor.

This report is divided as follows. Based on increasing risk and attack vectors, a state-of-the-art concerning Threats and Risks assessment is conducted in Section 2. Next, Section 3 elucidates possible stakeholders involved and the mapping of their actions and responsibilities. Finally, Section 4 presents SEConomy, a framework for the viability of economic models that take into account risks and threats attributed to the role of each stakeholder within an ecosystem. SEConomy proposes a cost-investment security analysis model based on the relationship between system attributes and their failure probabilities, which results in economic impacts.

2. Threats and Risks

Cybercrime-as-a-Service (CCaaS) has been indicated as one of the huge cyber threat for different stakeholders [35]. Currently, anyone with the minimum background can contract services or obtain tools to start sophisticated and powerful cyber-attacks to a target. Besides, hackers with certain expertise can use such a model to amplify and speed-up their attacks, thus enabling vast and dangerous attacks that can, for example, reflect directly in money loss and data leaking. The rising of IoT and, consequently, the growth in the number of devices, also contributes to the proliferation of malicious services. The CCaaS market includes botnets to execute large Distributed Denial-of-Service, malwares and exploits on-demand to obtain advantages (e.g., crypto mining), and also solutions that focus on the propagation of misinformation (i.e., bots that simulates legitimate users to share fake news).

The advance of attacks based on Artificial Intelligence (AI) also is a critical complaint for the next years. Different steps of the cyber-attacks (e.g., vulnerabilities identification and social engineering) have been automatized by using state-of-the-art artificial intelligence techniques. Based on that, the cyber-attacks are become more sophisticated and can many times surpass traditional security systems. These AI-based attacks can be a threat for many stakeholders (e.g., banks and governments

sectors), impacting not only by infrastructure attacks, but also by using sophisticated social engineering techniques to cause damage and/or steal sensitive data, e.g., misinformation campaigns to influence in political scenarios, information leaks, and service interruption.

Cyber weapons developed to hit industrial systems and Supervisory Control and Data Acquisition (SCADA) systems are still a threat. This kind of attack can impact directly on critical government infrastructure (*e.g.,* Venezuela blackout on March 2019) and manufacturing industries. As critical infrastructure systems are not designed to be resilient to cyber-attacks, the risks are growing according to cyber-attacks are evolving, and legacy systems are still being used. In the past, for example, the Stuxnet threat revealed to the world how evolved is cyber warfare by attacking Iran's nuclear weapon development. In the same context, the cyber espionage has been impacted directly on governments in different dimensions, such as leaking of sensitive information or also influencing directly on elections by focusing the attacks (*e.g.,* social engineering and malware) in people and devices involved directly with the election process.

The supply chain of popular softwares is also a massive target for attackers. Cyber-attacks to compromise the supply chain to hit a broad audience have been arising in recent years. This focus on corrupt libraries or other components that are part of the software to insert backdoor and create vulnerabilities in softwares trust by everyone. The main focus of this kind of attack is to steal sensitive information from the victims with any suspect. Finally, the Cloud Providers, mainly companies that provide cloud storage, are one of the most targets for cyber-attacks. As users and companies are migrating their data to the cloud, it is normal that with that, the cyberattacks migrate together. Several approaches of Cloud-based ransomware have been identified with the primary goal of obtaining financial advantage by encrypting data from one or more customers using such kind of service.

Table 1 provides an overview of the threats that compose different classes (*e.g.,* CaaS and supply chain attacks) and its main goals as well as the most affected stakeholders (*i.e.,* Targets). It is noted, by considering the provided information, that general threats are being explored in different contexts according to the end-target, such as a malware that can be used to infect millions of devices in order to create botnets, while can also have ransomware functions with financial interests in determined targets

2.1. Current Research Directions

Nowadays, different directions and dimensions have been considered to develop the next-generation of protection services. Also, improvements in the current solutions to deal with the evolving aspects of well-known attacks should receive attention as well. Thus, in the rest of this section, the current research directions are presented and reviewed to shed light on how trend technologies (e.g., AI and blockchain) and other well-known approaches are being used to support solutions for cyber security.

Social Engineering has been exhaustively investigated in literature in recent years. In a recent study, Marczak et al. [27] examined the settings and software of the devices

used by thirty potential government targets of Middle Eastern and the Horn of Africa. The results demonstrate that several vulnerabilities are presented, which can be explored by sophisticated techniques of social engineering. In another study, Postnikoff et al. [36] argued that robot social engineering is already possible and that

Table 1: Overview of threats and its main goals

Class	Threat	Main Goal	Targets
Cybercrime-as-a-Service	DDoS Malware Exploits Botnets Spam/Phishing	Amplify the access of attacks to any users and improve capacity to conduct attacks	Service providers, cloud providers, governments, end-users
Nation-state hacking	Social Engineering Malware Cyber-weapons focused on ICS/SCADA systems	Cyber espionage and sabotage	Governments and large companies
AI-based attacks	Vulnerabilities exploration Social Engineering Misinformation campaigns Phishing	Automation of some phases of the attacks	Service Providers, governments, small and large companies, banks
Supply chain attacks	Compromise libraries/softwares Insert vulnerabilities	Stealing data from a wide audience that trust in a software	Governments, small and large companies, banks, end-users
Cloud attacks	Malware (mainly Ransomware) Exploits DDoS attacks	Stealing of sensitive data, sabotage, and financial interest	Cloud providers, service providers, banks, small and big companies

there is still a lack of defences against this kind of attack. In terms of protection against social engineering, Tsinganos et al. [46] presented an automated recognition system for chat-based (e.g., Skype, Facebook, and email) social engineering attacks against companies' employees. This solution uses convolutional neural networks to recognize characteristics of an attack (e.g., influence, deception, personality, speech act, and experience) and calculate the security risk for the company according to the chat content. Others attacks can be conducted in the application layer, such as cross-site attacks and third-party tracking. In such a direction, Franken et al. [16] provided a comprehensive evaluation of third-party cookies and introduced a framework to validate the effectiveness of cross-site countermeasures solutions.

As there are many threats introduced by AI-based attacks, the academia is doing the opposite path and investigating how to use AI to avoid and mitigate cyber-attacks. Falco et al. [14] proposed a tool that uses AI techniques to identify attack pathways in an automated way. This solution is based on attack trees that can correlate causes of failures, the taxonomy of attacks, and frameworks of different stakeholders to develop a master attack method that can be used for classical planners to generated adequate protection. In the same direction, Khanna et al. [25] proposed a method based on machine learning to protect smart grid systems for false data injections attacks. For this, the method identifies the compromised meters by anticipating the correct measurements in the event of a cyber-attack. Also, in the context of smart home systems, Tertytchny et al. [45] introduced a method based on supervised machine learning to identify cyber-attacks in energy-aware smart home systems.

Efforts to identify and mitigate botnets attack have also been conducted. Falco et al. [15] developed NeuroMesh, which is a solution that uses hacker tools against the hacker. This solution provides managed security and intelligence to IoT devices thought a friendly botnet running on the Bitcoin blockchain. Also supported by the blockchain, Rodrigues et al. [40] introduced a collaborative defense against DDoS attacks and Sagirlar et al. [43] proposed AutoBotCatcher which is a blockchain based P2P botnet detection technique which dynamically analyses communities of IoT devices to detect botnets. There are researches also focusing on the infection phase of botnets. Bajitos et al. [5] created honeypots that simulate telnet devices to understand the propagation of botnets. In another study, Yamanoue [48] created a beneficial pseudo botnet to detect communication between malicious botnet. This pseudo botnet can detect communication peer-to-peer (p2p) and domain generation algorithm (DGA) communications by malwares. Others studies have improved the investigation of botnets in the context of IoT networks. Ceron et al. [8], for example, presented an approach for handling the network traffic generated by IoT botnets (*e.g.,* Mirai and Bashlite families) in an analysis environment. In another study, Chen et al. [9] explored convolutional neural networks to the effective detection of botnets. The experiment shows the technique can increase the detection accuracy of previously presented techniques up to 98.6% and decrease the false positive rate up to 0.5%.Besides that, several threats have been emerged and evolved to explore cloud environments. Among these threats, ransomware and sophisticated malware to steal sensitive data from the cloud and its consumers are the most destructive. A novel defensive approach based on the self-organizing network paradigms and emergent communication technologies has been expected to mitigate crypto-ransomware [29].

By relying on Software-Defined Networks (SDN) and Network Functions Virtualization (NFV), the researchers could achieve smart coordination and calibration of countermeasures. Another study has been proposing backup mechanisms based on containers to cloud providers survive on destructive ransomware attacks [22]. In the context of cloud services, different malwares have been arising to steal data. The task of analyzing and identifying complex and unstructured malware behaviours have been proved as a challenge. For this, Hsiao et al. have trained recurrent neural networks to detect malwares and vaccine the infrastructure against the corresponding malware families with similar behaviours [20]. Also, in other studies, a framework for real-time analysis of malware [1] and a

cloud-based tool for mitigating side-channel attacks have been investigated [18]. Table 2 presents examples of related work for each threat discussed as well as summarizes the insights obtained by analysing the state-of-the-art solutions.

Table 2: Example of efforts in literature addressing well-known threats

Threat	Solutions	Insights
DDoS	[15], [40]	Blockchain-based solutions are arising to detect and mitigate DDoS attacks.
Malware	[9], [29], [22], [20]	Trend technologies (*e.g.,* neural networks and self-organizing networks) are being used to classify malwares and to plan the security to reduce ransomware impacts.
Botnet	[15], [43], [5], [48], [8]	Machine learning is a trending topic of detecting botnets. As botnets have behavior patterns, artificial intelligence techniques could be useful. Also, honeypots have been used to collect information from botnets.
Social Engineering	[27], [36], [46], [16]	AI-based attacks are becoming a reality in the context of Social Engineering. In the same direction, solutions are using machine learning to recognize patterns to identify imminent social engineering and protect against sophisticated attacks.
Sabotage	[25], [45]	Machine learning has also been used as a tool to detect and understand the impact of cyber-attacks against governments or smart homes.
Others	[1], [18]	Several cloud-based solutions have been proposed to mitigate different cyber-attacks.

3. Mapping of Stakeholders

The vision of CONCORDIA is to build strong cooperation between all its stakeholders, bridge and learn that all its stakeholders have their KPIs and foster the development of IT products and solutions along the whole supply chain. As Concordia aims to develop the solutions that are important for Europe, hence it needs good cooperation involving multiple and diverse stakeholders. It also aims to combine its stakeholders in a unique way and build a strong network among them. Figure 1 shows the first step in the identification of possible stakeholders of Concordia and the interaction between those stakeholders. Several key stakeholders have been identified with which it will establish and foster liaisons. The possible stakeholders

that could be the member of the network are European entities, Research entities, Companies, National and International entities [34]. The stakeholders identified are not exhaustive and additional stakeholders could be identified.

The possible European entities could be the European Union Agency for network and Information Security (ENISA), The Computer Emergency Response Team for the EU (European Union) Institutions, bodies and agencies (CERT-EU), European Strategic Intelligence and Security Center (ESISC), and European cyber security organization (ECSO). These entities are the centre of expertise for cyber security in Europe. They actively contribute to information and network security within the union. They deliver advice, solutions, develop and implement policy and respond to information security incidents and threats. They also help to discover breaches or anomalous activity and target to catch adversaries early in the attack lifecycle. They provide awareness of the threat landscape and helps companies and national entities to understand their adversaries. This could save the companies and national entities from financial damages. They also usher strict data security laws on them by providing standards. These standards provide clear direction to the companies and national entities in the configuration management process and ensure compliance with frameworks and improve the security of the organization.

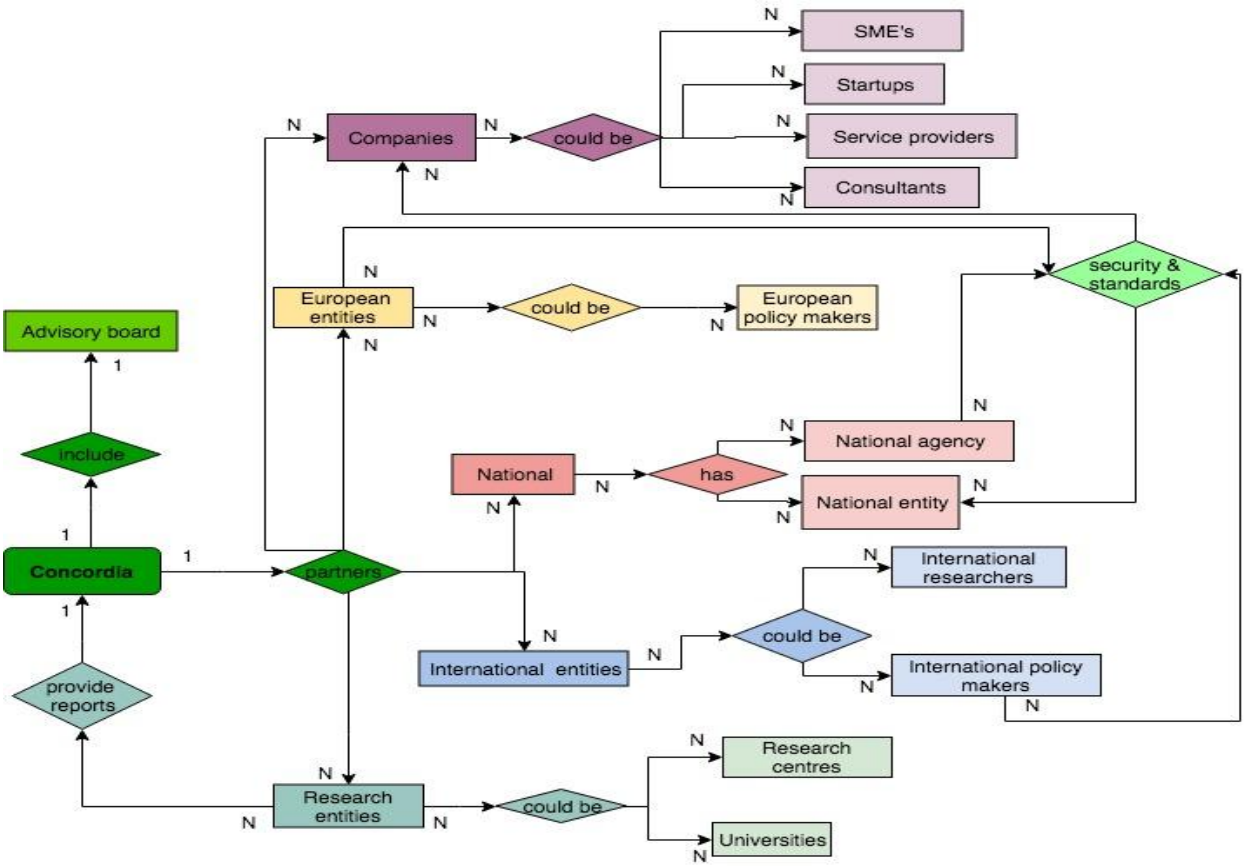

Figure 1: Concordia Stakeholders

The National has national entities and national agencies. Few examples of the national agency are Global Cyber Security Center (GCSEC), National Cyber security

Agency of France, and National Cyber Security Centre of Lithuania. National entities example include Military, Navy, Healthcare sector, and Airlines. National agencies are responsible to develop and distribute awareness and knowledge on cyber security. They provide support to the national entities and companies on policy, legal frameworks, security standards, and regulations. In some cases, they manage internet operations of national entities and propose cyber security plans and investigate cyber security attacks.

The possible sector of companies that could be the partner of Concordia are the startup companies, service providers, consultants, SME's, and large multinational company. Companies depend on the research entities for their research potential and talent to overcome cyber security challenges. The collaboration between companies and research entities help companies to increase security awareness but also help the research centers to understand concrete industry needs and requirements. Companies contribute their expertise and allow research entities to access their knowledge resources [33].

Research entities could be the Universities, and Research centers. Center for strategic and international studies (CSIS), National Counterintelligence and Security Center (NCSC) could be the possible stakeholders. Research entities contribute and participate in the research and development process and provide reports to the Concordia partners about existing solutions and increase the security awareness among them. They could also propose several pilots in the companies and national entities. They develop innovative solutions to overcome cyber security challenges faced by the companies and national entities. Research entities also provide inputs to the Concordia and emphasize the cyber security pain points and help Concordia to fight against cyber security problems.

International entities such as international researchers and policy makers could also be the partners of Concordia. Few examples of International policy makers are Women in International Security, payment card industry security standards council, and International Organization of Securities Commissions. European CERTs (Computer Emergency Response Team) in collaboration with international CERTs could build threat intelligence for Europe. The collaboration with international researchers will enable greater opportunities to witness the most recent trends and innovations worldwide in an area of cyber security.

Concordia includes Advisory Board which comprises of leaders from the companies, national entities, standardization, policy, and politics. They provide strategic advice and helps in connecting with possible clients and users. They provide advice on the current and emerging technologies and ensure that the project stays true to its goals and objectives.

3.1. Case Study: Banking Sector

Cybercrime is a term associated with activities related to the misuse of computer, information system, data, and cyberspace for personal and economic gain [2]. Cybercrimes have affected not only individuals but also groups and organizations, or even society as a whole. In the banking sector, the cybercrimes are committed using online technologies to illegally transfer or remove money to different account [12].

With the enhancement in technology such as ATM, online banking, the banking sector has witnessed different forms of cybercrimes like ATM frauds, Phishing, identity theft, DDoS, cyber money laundering, and credit card frauds. The threats and security breaches have highly increased in recent years due to the reason that banking increasingly relies on computer technologies and the internet to operate its businesses and market interactions [41]. As Banks adopts modern trends of doing business, they have to protect themselves against cyber-crimes [12]. In general, all these frauds are executed with the ultimate aim to gain access to the user's bank account, steal funds, and transfer money to a different account [37]. Banking fraud is a major issue being experienced globally and is continuing to prove costly to Banks and its stakeholders [7]. Figure 2 shows the possible stakeholders that are involved in the Bank cyber security domain and the interaction among them. The actors are categorized into four main categories, such as exploiters, victims, security providers, and regulators. The stakeholders identified and listed below are not exhaustive and can evolve according to Concordia's pilots.

Malicious exploiters are usually motivated by political or financial gain or human factors such as revenge or curiosity [2]. Malicious exploiters range from the cybercriminals, internal employee, government, organization. Internal employees are those who are working within the bank to leak out important information in order to harm the reputation of the bank. They inadvertently cause a data breach through carelessness or might intentionally cause the breach. They could be influenced by financial rewards or blackmail to steal valuable information [2]. Cybercriminals are highly organized and very knowledgeable who seek to find security holes in the system to overcome protection measures adopted by the banks for their own profit [37]. The malicious attempt could also be from the organization and government to breach the information system of the Banks.

When malicious exploiters attack the Banks, they could breach the confidentiality of user's or customer's data such as customer's bank details or bank's intellectual property. The attack on the bank could have a direct or indirect impact on its customers, Business partners, and insurance company in terms of financial or identity fraud [2]. Customers are often concerned about privacy and identity theft. The exploiters might alter the customer's credit rating which could lead to that person's inability to secure the financial loan and could also prevent the authorized user from accessing his or her user account, data, or information. When such attacks take place, the banks are responsible for all these fraudulent activities perpetrated via the internet channel. Banks are responsible for reimbursing most customers losses [41]. Insurance company equalizes the cost when a cyber-threat event happens at an organization and also helps to prevent an attack and respond to mitigate when cyber security fail [7]. It helps the Banks to prepare for cyber threats by contributing to minimizing the said loss or damage and bringing the situation back to normal [34].

Security guardians help in mitigating banking frauds. They improve the existing banking system and help in removing the vulnerabilities. The security guardians could be the bank itself, third-party security provider hired by the bank to ensure security from the threats, or cyber intelligence. The security guardians within the bank could be the security team, board members, senior management, auditors, and consultants [37]. The sophistication of contemporary attacks requires a

sophisticated response. The Banks ensure that they have the right resources to manage the cyber security risks. Therefore, the Banks increasingly look to the third-party cyber security solution provider to better manage the risk. Cyber intelligence could be professional external parties or internal. They obtain information about the different types of attacks targeting the organization. They assess and manage cyber risk. They enable the banks to respond to cyber threats with actionable cyber investigations and remediation [7]. The banks implement the security guideline, procedure, policy, and privacy components [41]. The security team within the bank is responsible for securing information and data. They create a cyber-threat protection strategy and build layers of security to protect the business process and data integrity. They are constantly vigilant, set to defend, and ready to respond creatively and rapidly in the event of an attack. They utilize the standards provided by the policymakers in their configuration management process and ensure compliance with frameworks and improve the security posture of their organization. Senior management could be part of the security planning process. They take input and guidance from their security team on security issues and are responsible for overall budgetary and strategic decisions [34].

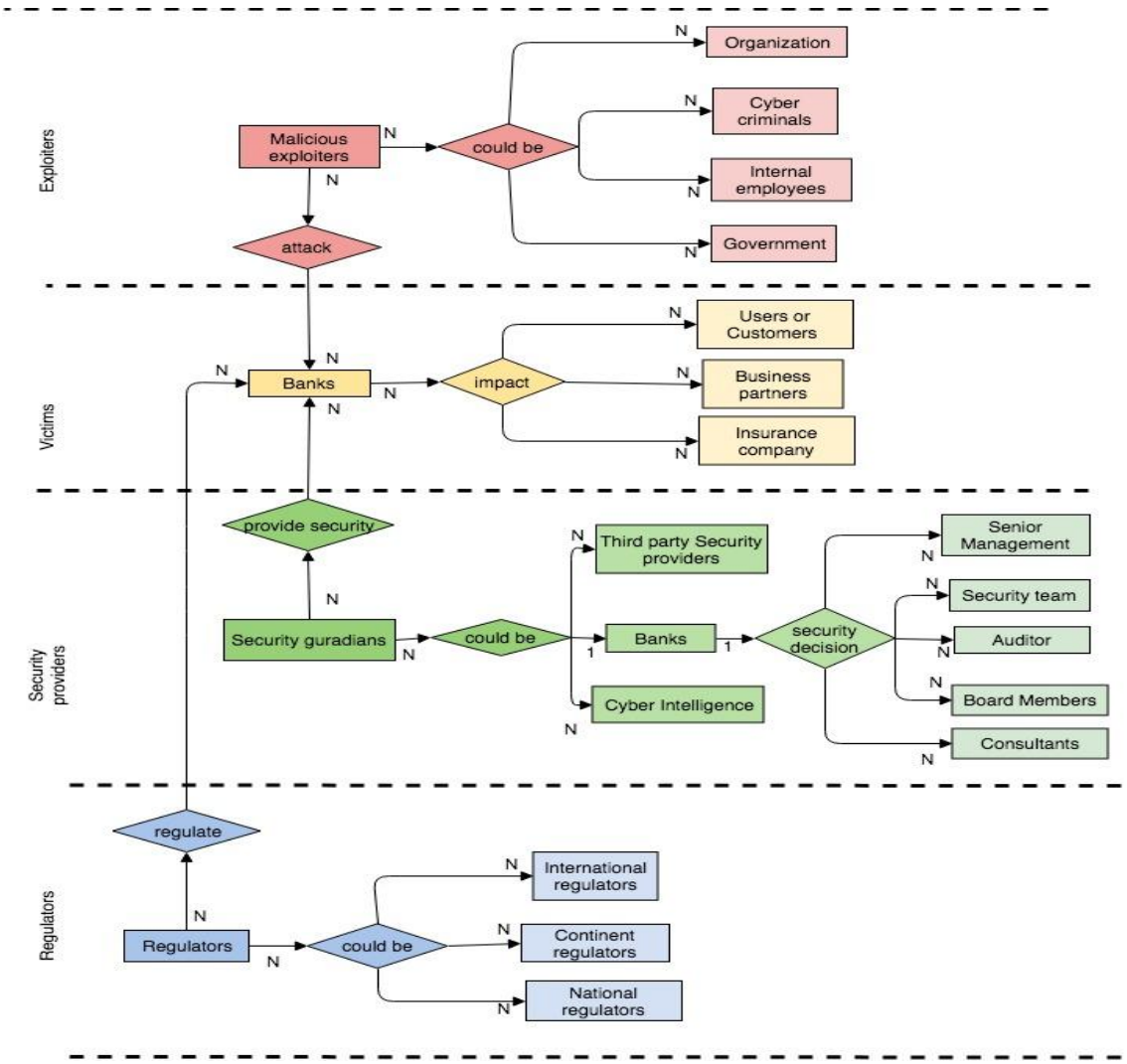

***Figure 1**: Bank Cyber security Stakeholders*

Regulation in banking is the preservation of solvency and stability of the system [42]. Regulators make policies and adopt measures to protect banking platforms from cyber threats [41]. Banks must face compliance mandate or regulatory requirement, for example, the regulations such as Payment Card Industry Data Security Standard, National Institute of Standards and Technology, Cyber Essentials, EU General Data Protection Regulation. These regulations include requirements for data privacy. Banks must integrate compliance and regulations into their assessment. Regulation imposed by the regulators provide stability to the banking system and avoid the important negative consequences of panics [42]. For example, GDPR has introduced greater enforcement powers for regulators and greater privacy rights for the consumers backed by the threat of a large fine.

4. Economic Analysis Approach

Cyber security concerns are one of the significant side effects of an increasingly interconnected world, which inevitably put economic factors into perspective either directly or indirectly. In this context, it is imperative to understand the significant dependencies between complex and distributed systems (*e.g.*, supply-chain), as well as security and safety risks associated with each actor. SEConomy is a framework to measure economic impact of cyber security activities in a distributed ecosystem with several actors. Through the mapping of actors, responsibilities, inter-dependencies, and risks, it is possible to develop specific economic models, which can provide in a combined manner an accurate picture of cyber security economic impacts.

It is imperative to understand the economics behind cyber security activities. For example, the United States of America (U.S.A.) released in 2018 an estimate of costs related to malicious cyber activities of around 57 and 109 billion USD for incidents appearing only in 2016 [47]. These numbers involve not only losses at the initial target and economically linked firms derived from attacks, but also incurs in costs involving the maintenance and improvement of systems security [6]. Further, Moore [31] corroborates with the U.S.A. estimate, predicting in 2018 a cost of 114 and 124 billion USD in 2019, representing an increase of 8% for one country only. While cost numbers are not precise on a global scale, there are estimates that predict costs related to cyber security activities to exceed 1 trillion USD cumulatively for the five years from 2017-2021 [32], taking into account the growing number of Internet of Things (IoT) devices.

Systems often fail because organizations do not take into account the full costs of failure, which includes two critical categories: security (prevention of malicious activities) and safety (prevention of accidents or faults) [30]. Security investments are typically complex because malicious activities typically expose externalities as a result of underinvestment in cyber security, *i.e.*, they usually exploit vulnerabilities unforeseen in the design space. Safety, however, originates from requirements, which take systems failures due to unexpected events (*i.e.,* natural disaster or human failures) into account to prevent the loss of lives. In a setup where major actors want to minimize costs while maximizing security and safety aspects [30,38], it is essential to understand all key cyber security impacts or the lack thereof within a specifically determined economy [3].

4.1. Background and Related Work

Although reasons behind cyber-attacks can be widely diverse, %ranging from identity phishing and information security breaches to the exploiting of vulnerabilities on Critical National Infrastructures (CNI), it is notorious that these attacks have become increasingly driven by financial motives. Therefore, the related work focus here is on models analyzing economic aspects behind cyber-attacks. For this reason, the United States Department of Defense declares the cyberspace as the fifth dimension of defense areas, complementing the traditional land, water, sea, and air warfare dimensions [28].

A purely economic analysis was released in 2018 by the U.S. White House [47] revealing estimates of economic impacts in the year of 2016, the year in which one of the largest Distributed Denial-of-Service (DDoS) attack was launched on the content provider Dyn-DNS, which interrupted the delivery of content for significant Internet services (*e.g.,* Twitter, PayPal, and Spotify) for a few hours. These numbers corroborate with the influence of cyber-attacks in the economy (whether it is a nation or large private organizations).

The AFCEA, which is a non-profit organization serving military, government, industry and academia, presented a discussion on cyber security economics in a practical framework. The framework guides private organizations and the U.S. government highlighting principles to guide investments mapping risks their associated economic impacts. Threats are categorized according to its complexity *i.e.,* sophisticated or not and its mission criticality *i.e.,* define how certain vulnerability could impair a service/process.

Concerning the mapping of risks and threats (without a direct analysis of economic impacts), the National Institute for Standards and Technology (NIST) developed a model for guiding the investment in cyber security countermeasures. Specifically, NIST's Special Publication 800-37 [24] and 800-53 [23] define the Cyber security Risk Management Framework (RMF) including a method for assessing the implementation of controls to mitigate risk. Although 800-37 and 800-53 do not present an analysis directly related to economic aspects, the NIST framework to classify risks, as well as the AFCEA mapping of risks, allows for the establishment of economic models based on threats.

Moore [30] discusses under economic directions impacts of cyber-attacks in a national context. He bases the analysis of attacks on Critical National Infrastructures that could harm or collapse its economy. Also, Moore puts those principles into perspective, which motivate these attacks and policy options to prevent or respond to attacks. Thus, he proposes regulatory options to overcome barriers in cyber security, such as safety regulation, post liability, and others. According to the knowledge of the authors economically-driven frameworks for a suitable and detailed assessment are not yet in place.

Aiming at the evaluation of economic risks, Rich *et al.* [38] proposes a proactive model to simulate economic risks of CNI's with integrated operations, *i.e.*, that links many vendors, suppliers into the same ecosystem. Thus, the authors seek to map inter-dependencies amongst actors to establish a causal relation, which can then be

used to estimate economic risk under various scenarios. However, despite of providing a view on the inter-dependencies between the actors, the proposed model does not consider problems that may later occur because of a rush to attain initial economic gains [11].

4.2. SEConomy Framework

In ecosystems involving different actors ensuring certain security/safety levels is not a straightforward task. Due to the number of participants potentially managing sensitive information or critical tasks, the risk assessment of a supply chain, for example, becomes complicated [3, 11]. The framework proposed in Figure 3 takes into consideration the economic analysis of complex systems by structuring to five stages of mapping and modeling, allowing the creation of economic models with fine-grained estimates.

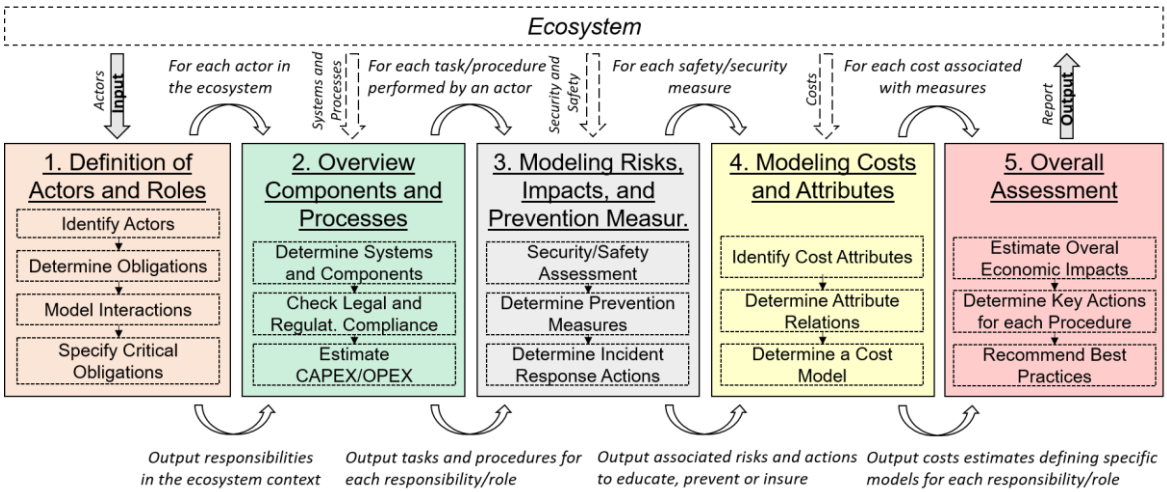

Figure 2: *SEConomy Framework*

Stage 1 is concerned with the definition of actors and their functions, whose interactions should be mapped as well as which critical functions should be specified. Stage 2 to determines which systems/components and processes are performed by these actors and their legal implications for an initial attribution of investment and operating costs. Based on the mapping of actors, systems, and processes, Stage 3 is responsible for the production of risk models and possible impacts as well as preventive and training measures based, for example, on NIST risk assessment guides 800-37 and 800-53 [24, 23]. Stage 4 takes into consideration this risk analysis to map costs in a fine-grained manner, i.e., for each risk of each task performed by each actor previously mapped. Lastly, Stage 5 gathers outputs of Stage 4 to a produce general feedback in terms of overall economic impacts, the determination of improvement actions, and best practices.

4.2.1. Definition of Actors and Roles

It is possible to consider as input, for example, the production chain of an aircraft system as a complex ecosystem that requires an assurance of security and safety levels based on a detailed risk analysis of all its major control components. A comparative between Airbus and Boeing supply-chains [19] have shown, for example, that the manufacture of the wide-body Airbus A300 and Boeing 737 aircraft involves multiple suppliers from 30 and 67 countries, respectively. Hence, it is essential in Stage 1 to identify all actors involved in the supply chain, and their roles (and determination of which tasks/functions are critical).

Figure 4 shows as a first step the identification of actors involved (*e.g.,* producers of flight control systems, software for engines) as well as their obligations and interactions with other actors. In this regard, Boeing and NIST defined a guideline on cyber security supply-chain risk management [39], where the organizations that provide software for their aircrafts must undergo a rigorous inspection process.

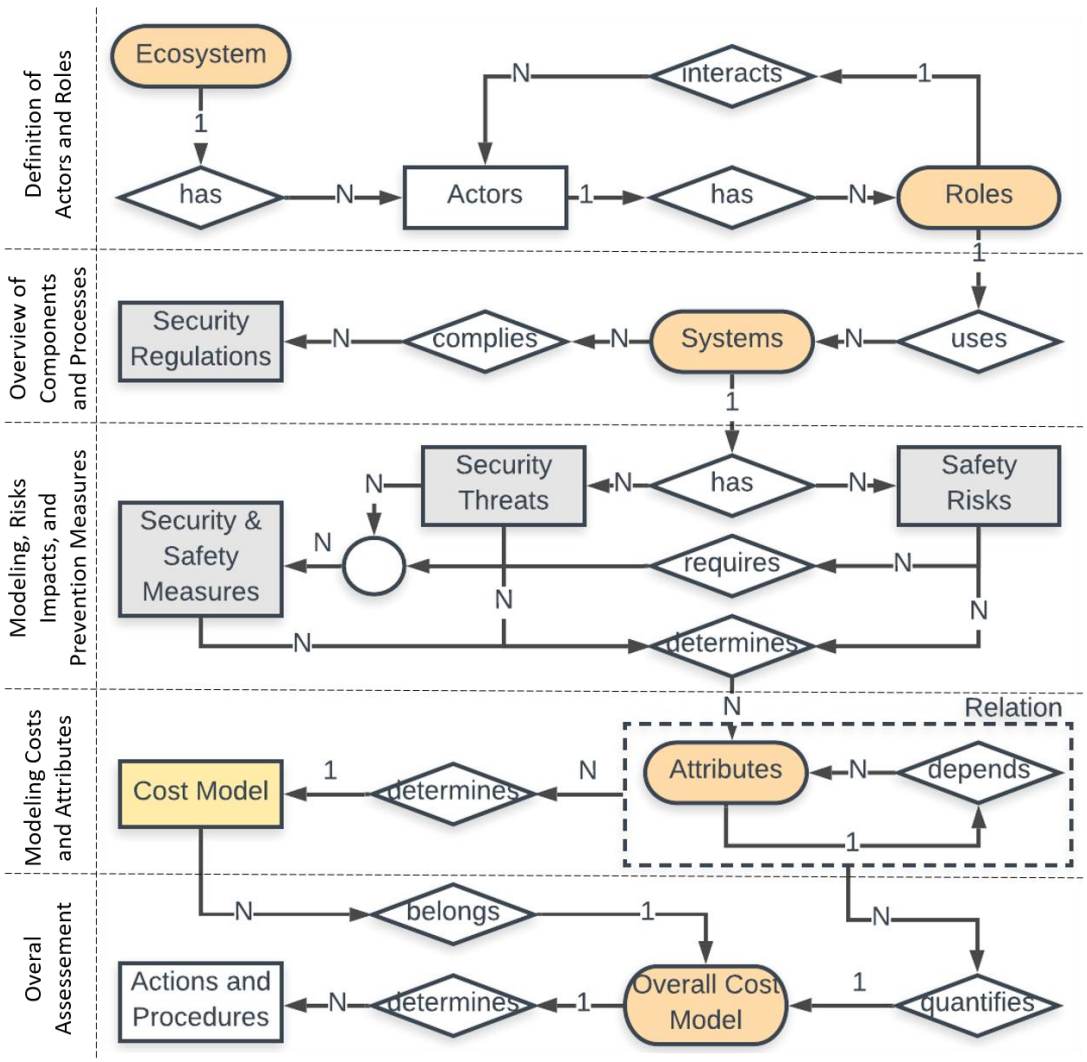

Figure 3: *SEConomy entity-relation model between stages*

4.2.2. Overview of Components and Processes

Among the actors' obligations, it is necessary to identify the ones whose roles involve critical processes/systems and components. In the case of the aviation sector, these include producers of navigation and communication systems, traffic collision avoidance, and Fly-By-Wire (FBW) systems [39]. The mapping of systems and components is crucial for the analysis of risk, which involves not only technical, but also human aspects. For example, critical systems require not only a guarantee of safety and security aspects, but also whether actors operating these systems can monitor and react. Also, these systems should comply with security and safety regulations/recommendations, which measurably lead to implications of Capital or Operational Expenditures (CAPEX/OPEX). For example, the Airbus A320 FBW system uses five different computers running four flight control software packages to ensure reliability/availability [26], complying with the U.S.A. Federal Aviation Administration agency requirements for safety matters in the design of FBW systems.

4.2.3. Modeling Risks, Impacts, and Prevention Measures

As presented in Figure 4, each system requires an analysis of its potential security/safety threats, and measures to respond to these threats. A rational approach in defining what is "appropriate" involves (a) identification of risks by examining potential vulnerabilities and their chances of a successful exploitation, (b) the cost of these results if vulnerabilities are exploited, and (c) the cost of mitigating vulnerabilities. The analysis of threats/risks can be based, for example, on frameworks such as the NIST 800-37/800-53 [24, 23]. Also, it is necessary to determine measures to be taken in response to each threat and their associated costs. For example, the ROI (Return On Investment) of proactive approaches (education/training of personnel, prevention, and redundancy of critical systems) is a better economic alternative than reactive approaches (active monitoring and recovery). However, the remaining difficulty is to determine efficiently thresholds for CAPEX and OPEX.

4.2.4. Modeling Costs and Attributes

The challenge of this stage is to translate risks and several measures of security in terms of costs, which includes the mapping of interdependence between failures. In this regard, such correlations can be mapped as the correlation between two Bernoulli random variables (A, B) [10]:

$$Dependence(A,B) = p_X = \frac{p_X - p_A * p_B}{\sqrt{p_A(1-p_A) * p_B(1-p_B)}} \quad (1)$$

pA and *pB* provide the probability of failure in a system A and B, respectively. *pX* describes the probability of a failure in both A and B. The SECeconomy approach is based on the ROSI (Return On Security Investment) model that determines the cost/benefit ratio related to security strategies [44, 6]: Threat exposure Costs

(*Tcosts*) in Eqn. (2) estimates the total cost of vulnerabilities given their probable occurrences within a time frame $deltaT(prob\ (Nocurrences)/time)$:

$$T_{costs}(A,B) = \Delta T * \left(\sum_{i=1}^{N_{Threats}} ThreatCost * Dependence(A,B) \right) \quad (2)$$

There are two significant challenges to quantify vulnerability costs in Eqn. (2): (a) economic impacts of vulnerabilities identified (*Tcost*) and (b) potential impacts given by a probability on the *K* dependent systems. However, impacts on dependencies are equally not straightforward to be estimated because the failure of one component may not always lead to the failure of another dependent system (*e.g.*, the use of a layered defense or a "sufficient" redundancy level may reduce such risks). For example, a failure in a fuel control subsystem may not always impair an aircraft's turbine, because a redundancy level of computers exists to provide input for the FBW and, typically, more than one turbine is used in a commercial wide/narrow-body aircraft.

Mitigation Costs (*Mcosts*) presented in Eqn. (3) are equally challenging to be estimated, since failures are typically originated from unforeseen design aspects. However, it is possible to include an *InsuranceCost* that allows the recovery of *Tcost* costs.

$$M_{costs}(A) = \sum_{i=1}^{N_{Threat.}} \Delta T * MitigationCost + InsuranceCost \quad (3)$$

The cost of mitigation, termed *MitigationCost*, in Eqn. (3) does not foretell the economic impact on dependent systems, which relies on the probabilistic dependence of Eqn. (1). Failures/vulnerabilities can trigger cascading failures on correlated systems/subsystems potentially impairing the functioning of the entire system. An alternative is to adopt an insurance model (simplified as *InsuranceCost*) to cover potential impacts of subsystems or directly connected systems. Finally, Eqn. (4) calculates the ROSI for a single system taking as input Threat (*Tcost*), Mitigation (*Mcosts*), and initial investments in security (*InitSecCost*).

$$ROSI = \sum_{i=1}^{N_{System}} \frac{(T_{costs} * M_{costs}) - InitSecCost}{InitSecCost} \quad (4)$$

In the last stage, it is necessary to calculate the overall economic impact based on ROSI from all *S* systems, required by *R* roles of *A* actors. Therefore, as illustrated in Figure 4, the *N* economic models will define an overall estimate of costs for the entire ecosystem, as illustrated by Algorithm 1.

Algorithm 1: Overall Economic Assessment (OEA)

```
1 begin
2     for each Actor ∈ Ecosystem:
3         for each Role ∈ Actor:
4             for each System ∈ Role:
                  /* Correlation between linked systems in Equation 1  */
5                 p(x) ← dependence(System, ∀ linkedSystems)
                  /* Estimate exposure costs in Equation 2             */
6                 threat_costs ← T_costs(A, p(x))
                  /* Estimate mitigation costs in Equation 3           */
7                 mitigation_costs ← M_costs(A)
                  /* Get Overal Economic Assessment (OEA) in Equation 4
                     */
8                 OEA ← ROSI(threat_costs, mitigation_costs, InitSecCost)
```

5. Summary

The predictions for 2019 are emphatic in affirm that the Cyber-crime-as-a-Service are stronger than ever [35]. This model is one key factor for the growth of the cybercrime ecosystem and, consequently, can impact negatively in the global and local economy. The misinformation campaigns around the world (e.g., Russia playbook [17] and Brazil`s presidential race [21]), as well as the nation-state hacking, is becoming as an emergency for the next few years. Also, the number of IoT attacks is rising faster as the IoT networks are becoming a reality. Thus, the academia and industry should spend efforts to analyze not only risks for companies and its stakeholders but also the impacts of those threats on the economy and society as a whole. Most of such impacts may be reduced by increasing the investments in protection services, adequate cyber security planning for companies (e.g., risk analysis and training of response teams), and education of the end-users.

As support for the planning and decision process for cyber security, the SEConomy framework was introduced to detail economic estimates for security measures in complex distributed systems. Such framework can be used for stakeholders, as those mapped in Chapter 3 (e.g., the bank and telecom sectors), to evaluate the drawbacks and advantages of cyber security approaches, taking into account their business models and risks involved. Thus, such a framework is an initial step to define an overall model for economic perspectives verifications.

However, although SEConomy can provide estimates based on historical events and probabilities, failures and vulnerabilities in critical systems typically result in failures of sub-components or related systems, impacting the overall costs. For example, despite all recent technological advances, the introduction of a new warning component in the Boeing 737 Max caused two accidents with hundreds of fatalities [4]. Specialists stated that a software failure (*i.e.,* not properly implemented/tested) in the "Angle-Of-Attack (AOA)" sensors were triggering the flight control system to push the nose of the aircraft down repeatedly. In this regard,

the calculation of risks through mutual vulnerability exposure along with other horizontal (i.e., subsystems of a system) and vertical (i.e., systems of other actor relations) is a complex task of potential security and safety consequences.

Thus, the presented SEConomy is a new framework for estimating costs in complex distributed systems, which provide models for cost estimations and the mapping of relations between interdependent systems. Thus, the need to refine these models for specific applications becomes visible. Future work will run this refinement as well as the proposal of cyber-insurance models capable of covering the mitigation of threats not foreseen in design. In addition, SEConomy will be applied in different use cases such as Finance and e-Health sectors, with specific models and stakeholders from each sector for economic estimates.

References

[1] S. Agarwal, G. Raj: FRAME: Framework for Real Time Analysis of Malware; 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, November 2018, pp. 14-15.

[2] B. Arief, M. A. B. Adzmi, T. Gross: Understanding cybercrime from its Stakeholders Perspectives: Part 1–Attackers; IEEE Security & Privacy, vol. 13, February 2015, pp. 71-76.

[3] J. Bauer, M. Van Eeten: Introduction to the Economics of Cyber security. Communications and Strategies vol. 81, 2011, pp. 13–22.

[4] BBC: Boeing Admits it 'Fell Short' on Safety Alert for 737; BBC News, 2019, [On-line] https://www.bbc.com/news/business-48461110, last visit June 3, 2019.

[5] T. Bajtoš, P. Sokol, and T. Mézešová: Virtual Honeypots and Detection of Telnet Botnets; Central European Cyber security Conference (CEC), Ljubljana, Slovenia, November 2018, pp. 1-6.

[6] M. Brecht, T. Nowey: A Closer Look at Information Security Costs; The economics of Information Security and Privacy, Springer, October 2013, pp. 3–24.

[7] M. Camillo: Cyber Security: Risks and Management of Risks for Global Banks and Financial Institutions; Journal of Risk Management in Financial Institutions, vol. 10, 2017, pp. 196-200.

[8] J. Ceron, K. Steding-Jessen, C. Hoepers, L. Granville, C. Margi: Improving IoT Botnet Investigation Using an Adaptive Network Layer; Sensors, vol. 19, no. 727. February 2019, pp. 1-16.

[9] S. Chen, Y. Chen, W. Tzeng: Effective Botnet Detection Through Neural Networks on Convolutional Features; 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom), New York, USA, August 2018, pp. 372-378.

[10] P. Y. Chen, G. Kataria, R. Krishnan: Correlated Failures, Diversification, and Information Security Risk Management; MIS quarterly, 2011, pp. 397–422.

[11] S. Dynes, E. Goetz, M. Freeman: Cyber Security: Are Economic Incentives Adequate?; Critical Infrastructure Protection, Springer, 2008, pp. 15–27.

[12] S. Dzomira: Electronic Fraud (Cyber Fraud) Risk in the Banking Industry, Zimbabwe; Risk Governance and Control: Financial Markets and Institutions, vol. 4, January 2014, pp. 16-26.

[13] Ernst & Young: Swiss Organization Better Prepared to Predict and Resist Cyber-attacks but Still a Long Way to go: EY Global Information Security Survey. 2017, [On-line] https://www.ey.com/ch/en/newsroom/news-releases/news-release-ey-swiss-organizations-better-prepared-to-predict-and-resist-cyber-attacks, last visit June 3, 2019

[14] G. Falco, A. Viswanathan, C. Caldera, H. Shrobe: A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities; IEEE Access, Vol. 6, August 2018, pp. 48360-48373.

[15] G. Falco, C. Li, P. Fedorov, C. Caldera, R. Arora, K. Jackson: NeuroMesh: IoT Security Enabled by a Blockchain Powered Botnet Vaccine; International Conference on Omni-Layer Intelligent Systems (COINS '19), New York, NY, USA, May 2019, pp. 1-6.

[16] G. Franken, T. V. Goethem, W. Joosen: Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies; 28thUSENIX Security Symposium (USENIX'18), Baltimore, USA, August 2018. pp. 1-19.

[17] S. Frenkel, K. Conger, K. Roose: Russia`s Playbook for Social Media Disinformation Has Gone Global. The New York Times, January 2019, [On-line] https://www.nytimes.com/2019/01/31/technology/twitter-disinformation-united-states-russia.html, last visit 4 June, 2019.

[18] R. B. Gomes, R. D. Medina, F. G. Moro: Cloud Aid - A Cloud Computing Tool for Mitigating Side-Channel Attacks; IEEE/IFIP Network Operations and Management Symposium (NOMS), Taipei, Taiwan, April 2018, pp. 1-5.

[19] T. C. Horng: A Comparative Analysis of Supply Chain Management Practices by Boeing and Airbus: Long-term Strategic Implications; Ph.D. thesis, Massachusetts Institute of Technology, 2006.

[20] S. Hsiao, F. Yu: Malware Family Characterization with Recurrent Neural Network and GHSOM Using System Calls; International Conference on Cloud Computing Technology and Science (CloudCom), Nicosia, Cyprus, December 2018, pp. 226-229.

[21] M. Isaac and K. Roose: Disinformation Spreads on WhatsApp Ahead of Brazilian Election. The New York Times, December 2018, [On-line] https://www.nytimes.com/2018/10/19/technology/whatsapp-brazil-presidential-election.html, last visit 4 June, 2019.

[22] Y. Jin, M. Tomoishi, S. Matsuura, Y. Kitaguchi: A Secure Container-based Backup Mechanism to Survive Destructive Ransomware Attacks; International Conference on Computing, Networking and Communications (ICNC), Maui, Hawaii, USA, March 2018, pp. 1-6.

[23] Joint Task Force Transformation Force Initiative: Security and privacy controls for federal information systems and organizations; NIST Special Publication, vol. 800, 2013, pp. 8–13.

[24] Joint Task Force Transformation Initiative: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach; Technical Report, National Institute of Standards and Technology, 2014.

[25] K. Khanna, B. K. Panigrahi, A. Joshi: AI-based Approach to Identify Compromised Meters in Data Integrity Attacks on Smart Grid; IET Generation, Transmission & Distribution, vol. 12, no. 5, March 2018, pp. 1052-1066.

[26] A. J. Kornecki, K. Hall: Approaches to Assure Safety in Fly-By-Wire Systems: Airbus vs. Boeing; IASTED Conference on Software Engineering and Applications, 2004, pp. 1-6.

[27] W. Marczak, V. Paxson: Social Engineering Attacks on Government Opponents: Target Perspectives; Privacy Enhancing Technologies, Minneapolis, USA, July 2017, pp. 172-185.

[28] C. McGuffin, P. Mitchell: On Domains: Cyber and the Practice of Warfare; International Journal vol. 69, 2014, pp. 394–412.

[29] M. Monge, J. Vidal, L. Villalba: A Novel Self-Organizing Network Solution Towards Crypto-ransomware Mitigation; 13th International Conference on Availability, Reliability and Security (ARES 2018), Hamburg, Germany, August 2018, pp. 1-10.

[30] T. Moore: The Economics of Cyber Security: Principles and Policy Options. International Journal of Critical Infrastructure Protection (IJCNIP) vol. 3, 2010, pp. 103 – 117.

[31] S. Moore: Gartner Forecasts Worldwide Information Security Spending to Exceed 124 million in 2019. Gartner, 2018.

[32] S. Morgan: 2019 Official Annual Cybercrime Report. Herjavec Group, 2019, [On-line] https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf, last visit June 3, 2019

[33] H. Österle, B. Otto: Consortium Research; Business & Information Systems Engineering, vol. 2, no. 5, October 2010, pp. 283-293.

[34] P. Pagani (Editor-in-Chief): Cyber Defense Magazine (CDM); Cyber Defense Media Group, March 2019.

[35] P. Pagani (Editor-in-Chief): 2019 Predictions; Cyber Defense Magazine (CDM), Cyber Defense Media Group, March 2019.

[36] B. Postnikoff, I. Goldberg: Robot Social Engineering: Attacking Human Factors with Non-Human Actors; International Conference on Human-Robot Interaction (HRI '18), New York, USA, March 2018, pp. 313-314.

[37] A. R. Raghavan, L. Parthiban: The Effect of Cybercrime on a Bank's Finances; International Journal of Current Research & Academic Review, vol. 2, January 2014, pp. 173-178.

[38] E. Rich, J. Gonzalez, Y. Qian, F. Sveen, J. Radianti, S. Hillen: Emergent Vulnerabilities in Integrated Operations: A Proactive Simulation Study of Economic Risk; International Journal of Critical Infrastructure Protection vol. 2, 2009, pp. 110-123.

[39] S. Robert, T. Vijay, Z. Tim: Best Practices in Cyber Supply Chain Risk Management; US Resilience Project pp, 2016, pp. 1–14.

[40] B. Rodrigues, T. Bocek, D. Hausheer, A. Lareida, S. Rafati, B. Stiller:A Blockchain-based Architecture for Collaborative DDoS Mitigation with Smart Contracts and SDN; 11th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2017), Zürich, Switzerland, July 2017, pp 16–29.

[41] M. Ula, W. Fuadi: A Method for Evaluating Information Security Governance (ISG) Components in Banking Environment; Journal of Physics: Conference Series, vol. 812, 2017, pp. 12-31.

[42] X. Vives: Regulatory Reform in European Banking; European Economic Review, vol. 35, 1991, pp. 505-515.

[43] G. Sagirlar, B. Carminati, E. Ferrari: AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things; 4th International Conference on Collaboration and Internet Computing (CIC), Philadelphia, Pennsyslvania, USA, November 2018, pp. 1–8.

[44] W. Sonnenreich, J. Albanese, B. Stout: Return On Security Investment (ROSI) - A Practical Quantitative Model; Journal of Research and practice in Information Technology, vol. 38, 2006, pp. 45–52.

[45] G. Tertytchny, N. Nicolaou, M. K. Michael: Differentiating Attacks and Faults in Energy Aware Smart Home System using Supervised Machine Learning; International Conference on Omni-Layer Intelligent Systems (COINS '19), New York, NY, USA, May 2019, pp. 122-127.

[46] N. Tsinganos, G. Sakellariou, P. Fouliras, and I. Mavridis: Towards an Automated Recognition System for Chat-based Social Engineering Attacks in Enterprise Environments; 13th International Conference on Availability, Reliability and Security (ARES 2018), Hamburg, Germany, August 2018, pp. 1-10.

[47] WhiteHouse: The Cost of Malicious Cyber Activity to the U.S. Economy. White House, 2018, [On-line] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, last visit June 3, 2019

[48] T. Yamanoue: A Botnet Detecting Infrastructure Using a Beneficial Botnet; SIGUCCS Annual Conference (SIGUCCS '18), Orlando, USA, October 2018, pp. 35-42.