Navigating the Cyber-Security Risks and Economics of System-of-Systems

Terese Besker
Systems Engineering
RISE Research Institutes of Sweden AB
Gothenburg, Sweden
Terese.Besker@ri.se
ORCID: 0000-0002-9811-000X

Ulrik Franke
Systems Engineering
RISE Research Institutes of Sweden AB
and
KTH Royal Institute of Technology
Kista, Sweden
Ulrik.Franke@ri.se
ORCID: 0000-0003-2017-7914

Jakob Axelsson
Mälardalen University
and
RISE Research Institutes of Sweden AB
Västerås, Sweden
Jakob.Axelsson@mdu.se
ORCID: 0000-0002-3986-1196

***Abstract*—Cybersecurity is an important concern in systems-of-systems (SoS), where the effects of cyber incidents, whether deliberate attacks or unintentional mistakes, can propagate from an individual constituent system (CS) throughout the entire SoS. Unfortunately, the security of an SoS cannot be guaranteed by separately addressing the security of each CS. Security must also be addressed at the SoS level. This paper reviews some of the most prominent cybersecurity risks within the SoS research field and combines this with the cyber and information security economics perspective. This sets the scene for a structured assessment of how various cyber risks can be addressed in different SoS architectures. More precisely, the paper discusses the effectiveness and appropriateness of five cybersecurity policy options in each of the four assessed SoS archetypes and concludes that cybersecurity risks should be addressed using both traditional design-focused and more novel policy-oriented tools.**

Keywords—System-of-Systems, Cybersecurity, Economics, Incentives, Cyber Security Investment

I. Introduction

Modern digital society offers many benefits to the users of different system-of-systems (SoS) applications. Not only can consumers share rides or apartments, but entrepreneurs can also find investors, and mature companies can source their production quickly and efficiently from networks of geographically dispersed vendors. However, such systems and SoSs are also vulnerable, both to deliberate attacks and to unintentional accidents and mistakes (for analyses from different sectors, see, e.g., [1],[2],[3],[4]).

Although there is current research that addresses cybersecurity in the form of, for example, the risk of being exposed to an attack, these studies usually model individual nodes in a network (equivalent to an individual system in an SoS), which means that these studies do not always consider the risks associated with the integration and interconnection of different systems [5]. Unfortunately, understanding and analysing risks in SoS environments are very challenging for at least three related reasons.

Complex interdependencies: By definition, an SoS consists of several independent, evolutionary, and distributed systems called constituent systems (CS) [6]. Integrating these CSs is what enables interactions, dependencies and collaborations between them [7] and clearly offers benefits (see [8] for a conceptual review and [9] for an attempt at econometric quantification), but also entails uncertainty about how the different CSs will behave under different circumstances and the risk that an incident, whether an attack or an accident, at a single CS may compromise the entire SoS.

Non-technical aspects: Risk analysis in the SoS context is not only about technical aspects but also about, e.g., lack of policy and compliance, lack of security culture (see [10] for a review of why users do not follow security regulations) and trust and other aspects that can cause or contribute to incidents in an SoS. This may be difficult for traditional engineering-centric risk management, and at least some evidence suggests that cybersecurity measures in practice are biased towards technological risk controls, leaving organizational and social controls underrepresented [11].

Diverging incentives: Risk management in the SoS context also has to address and manage the possibility of diverging incentives among the CSs. As remarked by Anderson & Moore, "*security failure is caused at least as often by bad incentives as by bad design*" [12], and if this is a correct analysis, it is certainly a challenge that SoS designers have to rise to. There is also the case where CSs evolve over time, making it necessary to have a broad and life-cycle-oriented perspective on risk analysis [13].

All three aspects are especially poignant if, as in this article, we consider not only the software part of SoSs but also take a more expansive view and include people and processes in addition to technology (both software and hardware).

This paper proposes a novel perspective on cybersecurity in SoS—the perspective of cyber and information security economics. Whereas the economics of cyber and information security has grown into a prolific discipline in the past two decades, it seems that these lines of thought have not gained attention within SoS research. More concretely, the tools from economics have the potential to be a valuable complement to traditional design-focused tools employed in SoS engineering.

The paper's contribution can be seen as wedding cybersecurity economics to SoS—hopefully, to mutual gain. To do so, small literature reviews of each field are carried out before these are synthesized in the end. Though the discussion is intended to first and foremost be applicable to SoS, part of it may also apply to complex systems in general, not just SoS.

The rest of the paper is organised as follows. Section II offers a short introduction to the economics of cyber and information security, followed by an overview in Section III describing different SoS archetypes and their related cybersecurity concerns. Section IV focuses on security assessment in SoS, and Section V describes the importance of balancing security investments among different CS in SoS. These sections set the stage for the main contribution in Section VI, which discusses how cybersecurity economics tools can be used in the design and governance of SoS. Section VII concludes the paper.

II. Economics of Cyber and Information Security

As the introduction mentions, cyber and information security economics has been increasingly studied over the past two decades. While this short introduction cannot cover the entire field, a few key tenets, important in the SoS context, can be identified.

A. Externalities

In an interconnected environment, poor security is what economists refer to as an *externality* [12], i.e., there is a spillover effect whereby someone's poor security also potentially impacts everyone else. A recent literature review on cybersecurity investments, including a discussion of various spillover effects, is presented by Fedele and Roner [14]. Several examples have been of SoS being subjected to cyberattacks in recent years. Some of these attacks resulted from an attack on one CS that sequentially triggered damage and harm to other CSs in the same SoS [15].

An example of a cyberattack is cyber blackmail against the Coop food chain in Sweden in 2021, which made the company's payment system completely unusable. This attack was in the form of digital ransomware that locked the payment system in stores, making transactions impossible. The attack was not aimed at Coop in particular but at the American company Kaseya, whose software, in turn, was used by Coop's supplier Visma Esscom. In Sweden, the pharmacy Apotek Hjärtat, the petrol chain St1, and the railway operator SJ also suffered from disruptions in their systems due to this attack.

The insight from economics is that there is often underinvestment in preventing externalities. Since a CS does not bear the total cost of an incident but exports some of it to the rest of the SoS, this CS cannot be expected to invest as much in security as desirable from the SoS perspective. In this sense, poor cyber security is not unlike pollution (for further treatments of this parallel, see [16] and [17]).

B. Asymmetric Information

Different actors often have access to different information. For example, software vendors typically know more about their products than buyers. This may seem like a trivial insight, but it offers a profound perception of why insecure software is not just outcompeted on the market [12]. From the buyer's perspective, if secure software cannot be told from insecure software, then there is no reason to pay more for security. From the vendor's perspective, spending the resources necessary to create secure software is difficult if no buyer is ready to pay more for security.

Thus, even if both parties would agree to a higher price for software *known* to be secure, they cannot reach this agreement if the security of the software is *unknown*. (This general mechanism was famously identified by Akerlof [18] and later underpinned his Nobel prize in economics.) Such *information asymmetries* are common in SoS contexts.

C. The Difficulties of Risk Sharing

Cyber risks can be managed in many ways beyond investing in controls to minimise them. In particular, risks can be *shared* with others. Indeed, this happens all the time in SoS contexts—the question is whether it happens deliberately or as an unexpected by-product. Inspired by the case reported in [19], we can ask who bears the responsibility—and the cost—when, e.g., a remote-controlled hauler in a mine loses connectivity? The miner? The hauler provider, who might be selling hauling-as-a-service? The provider of the telecom infrastructure? The telecom service provider? In the absence of contracts and agreements beforehand, the answer to such a question might be found the hard way, ex-post, in a court.

This points to a more considerable problem: Immature risk management in emerging SoS could stifle innovation so that technically feasible and value-generating collaborations never get off the ground because the parties cannot agree on how to share the risks involved. A highly relevant but somewhat discouraging risk-sharing insight from the cybersecurity economics literature is that it can be difficult. Even insurers—arguably the best quantitative risk-management experts around—have serious problems properly assessing cyber risks. The premiums they would charge a CS or an SoS collectively to underwrite cyber-risks may be too high or too low—no one really knows (see, e.g., [20],[21]).

In recent years, ransomware attacks such as the Kaseya incident mentioned above have upended previous pricing models and raised the entry barrier for insureds, leaving many organizations unable to insure themselves [22]. Nevertheless, the cyber insurance literature contains some valuable lessons for SoS since there has been a prolific discussion about what insurers can or cannot achieve from a security governance perspective (see, e.g., [23], [24] and [25]). Some of the roles envisioned for insurers may also be feasible for other SoS actors.

D. Allocation of Liabilities

Generalising from the previous tenets, the SoS-relevant insights from cybersecurity economics can be summarized — as put by Moore [16] —as follows: "*policy and legislation must coherently allocate responsibilities and liabilities so that the parties in a position to fix problems have an incentive to do so*". Though this dictum originally refers to government policy and legislation, it is equally applicable to SoS policy and legislation, and SoS researchers and designers have ample reason to ponder it, as further discussed in Section VI.

Of course, this brief section has not exhaustively covered the economics of cyber and information security. The article by Anderson & Moore in *Science* [12] remains an excellent introduction to the field, though it is getting somewhat dated. A more recent review is given by [26], and some challenges, along with a research agenda to address them, are offered by [27].

III. SoS Archetypes and Security Concerns

An SoS is a collection of systems that work together to provide a capability that none of its CS can accomplish on its own. The collaboration in the SoS can have different characteristics, mainly depending on the level of alignment regarding goals and to what extent there is central management.

Based on this, the three SoS archetypes, *directed, collaborative, and virtual,* were introduced in [28]. A fourth archetype, *acknowledged,* was later added [29]. Over the years, different interpretations of them have been proposed in the literature. This paper will use fairly recent definitions in the ISO standard on SoS [30].

Since there are different archetypes of SoS architectures, there may be differences in how susceptible each type is to various cyberattacks. With this knowledge, the choice of SoS architecture can thus guide decisions regarding, for example, the initial design of the SoS, but also when planning updates and modifications of the SoS [31]. The critical factor is how the CSs communicate and interact since the security issues affecting an SoS vary depending on its architecture.

A similar analysis was provided in [29] but with a focus on security testing. In this paper, the scope is extended to security issues in general to provide a background for the economic perspective covered later. In this section, security concerns related to each of the archetypes will be presented and discussed.

A. Directed SoS

The SoS is centrally managed, and the CSs are built primarily to fulfil the purposes of the SoS. A directed SoS is created and maintained to fulfil a specific purpose, and the CSs are directly subordinate to the management of the SoS. Independent operation is a secondary goal, meaning that even though the individual CSs can operate independently, their normal operational mode is subordinate to the centrally managed purpose of the SoS [30].

This category of SoS is most easily achieved if the SoS is both implemented and operated by a single organisation or company, thus having similar authority, resources, common standards, and a common platform with uniform protocols [32]. Consequently, this type of SoS has well-defined CSs that drive and influence the development and capabilities of the SoS, which also usually has full access to all available information within the SoS and has extensive authority in negotiations between the CSs in the overall SoS [33].

The central management is sometimes referred to as the "Key Stone" (KS) component or actor [33]. It is thus a component or stand-alone system with a clear and reinforced mandate to, for example, guide and control the cooperative behaviour and capabilities of the SoS.

An example of a directed SoS is an "Emergency response system". In this type of SoS, individual CS, such as fire and police alarm systems, transportation systems, and medical response systems, are interconnected and managed by a central authority to coordinate emergency response efforts during a crisis.

Analysing the SoS security in a directed SoS is perhaps the most straightforward case since it essentially relies on the communication of each CS with the central one, which is responsible for security negotiation among the CSs. This implies that communications, security requirements, and properties may be managed in a centralised way [34].

B. Acknowledged SoS

An acknowledged SoS also has a specific purpose and objective, but the CSs have a more independent role in the SoS. Usually, these CSs have their own, more independent ownership (i.e. can be owned by different organisations or companies in the SoS) and thus also their own budget and funding and their own development and sustainment strategies [30]. All of this can potentially affect the SoS's development opportunities [32].

This SoS archetype also has a KS or a central entity. However, compared to the mandate of a KS in a directed SoS, both the authority and control of the KS in an acknowledged SoS are more limited [33]. Hence, an acknowledged SoS is not controlled by a KS or any central entity but may abide by an agreement on performing specific tasks.

An example of an acknowledged SoS is "Environmental monitoring systems", where individual environmental monitoring systems from different countries or organizations operate independently but are coordinated by a central authority to monitor and track global environmental changes.

Managing the security in this type of architecture requires a distributed and decentralised organisation, where each CS administers the mutual agreements and should cooperate and coordinate with the CSs. The central entity does not have a sufficient mandate to control the fulfilment of the security requirement of each CS. This means that each CS must guarantee to behave correctly, i.e., in a compliant way concerning the set of security requirements agreed upon. Although SoS security is a common goal to achieve, individual interests of the CSs may arise and create security vulnerabilities, and privacy may also be affected in this type of architecture [6].

Since the CSs may move from one SoS to another according to their availability or potentially also being part of more than one SoS, there is a potential risk that a CS may make improper use of the collective data for their own or third parties' profit. This means that a lack of trust or responsibilities among the CSs in an acknowledged SoS architecture could potentially become a considerable risk for the shared data and functionalities. The security testing in this type of SoS is hence more complex than in the previous case since the central system assisting in negotiating the security requirements, in which each system shall conduct this negotiation for its own sake, is lacking [6].

During the collaboration and interconnections among different CS, the CS may generate a cascade vulnerability problem [35], intensifying the attack and magnifying its effect [36]. This may occur when e.g. a system with high-security levels is sharing data with a system with lower security. Different levels of security among the CSs may cause the CS with lower security levels to become the weakest link in the SoS. Thus, it is important to conduct an extensive analysis of the CSs to detect the weakest CSs and determine if any of them could potentially create a cascade problem within the SoS [34].

C. Collaborative SoS

In a collaborative SoS, the CSs interact relatively voluntarily to fulfil agreed and central objectives within the SoS [30]. This archetype of SoS is best suited to SoS, where the stand-alone systems are primarily "owned" by different organisations or companies but where every CS has a reasonably equal position, without any dominant organisation [32] and no clearly stated KS or a central entity. In the collaborative SoS category, the SoS lacks authority over the CSs and has no coercive power to run the SoS, meaning that the CSs choose to collaborate to fulfil the SoS's goal voluntarily and agree with the central purposes of the SoS [28].

Examples of collaborative SoS are "Transportation networks", where individual transportation providers such as airlines, rail companies, and bus companies operate independently but voluntarily collaborate to provide integrated transportation services to passengers.

From a security perspective, functionalities may manipulate the data shared with the CSs out of the scope of the SoS, which introduces vulnerabilities to the privacy of the data in the SoS. One key challenge for the security in this SoS type is establishing the general criteria that define the shared security concept. This means that every CS coordinating with the central entity must agree with the security requirements. It is, however, essential to note that governing the security requirements may require a negotiation phase among the CSs. This implies that it would be possible for a CS to use information from other CSs for its own purposes, intentionally or unintentionally. However, this issue may be solved by clearly stating (e.g., in guidelines) the essential data each CS requires to avoid providing data that are not strictly necessary.

The issue of not sharing more than strictly needed data is commonly referred to as a non-disclosure or data-sharing agreement. The result may be that during an attack, the attacker could access data shared among the different CSs and reconstruct sensitive information about the SoS that may be used to exploit its security in other attacks [34].

D. Virtual SoS

In a virtual SoS, the independent CSs have no central management (i.e., no explicit KS or a central entity) and no centrally agreed purpose for the SoS [30]. This type of SoS thus relies on relatively invisible mechanisms to maintain its structure and interaction between the constituent systems [32].

Large-scale desirable behaviour may emerge based on market forces, which may incentivise adapting to cooperation and compliance with core standards within the SoS [37]. Thus, a virtual SoS emerges in unpredictable ways due to individual CS joining the SoS [34], meaning that large-scale behaviour may emerge either deliberately or accidentally within the SoS [38].

An example of a virtual SoS could be the "*Transportation networks*" mentioned in Section III.C, but with the modification that the individual transport providers do not interact with each other to combine their services. Instead, each user manages the coordination of their own travel by interacting with the providers individually.

From a security perspective, this SoS architecture presents more difficulties when analysing its vulnerabilities because there is not a central entity that may guarantee security, and no agreement defines which should be the proper behaviour. As a result of this environment, a central system does not coordinate the CSs, and the CSs may not even consider themselves as part of an SoS. However, due to the loose collaboration between the CSs, the vulnerabilities might have minimal impact on each single CS on average.

Moreover, testing the security requirements in a virtual SoS cannot be easily done since there is uncertainty about how the CS will communicate in the future. However, it could be analysed by considering previous SoS collaborations. Taken together, there are most likely no explicit defensive mechanisms that clearly can solve this issue, but contingency plans can be defined to mitigate the exploitation of the security [34].

IV. Security Analysis of an SoS

In an SoS environment, security is a significant concern due to the complexity and interconnectedness of the CSs involved. In the previous section, security concerns were enlisted for each commonly used SoS archetype. However, these archetypes only capture some aspects of a complex and heterogeneous SoS, and in practice, it is often difficult to unambiguously relate a given SoS to only one of the archetypes. Hence, it is necessary to conduct a deeper review of the security concerns for each specific application to understand the appropriate mitigation steps fully. Security analysis is thus an important step in removing risks, and in this section, some approaches to security analysis in the SoS domain will be reviewed.

It is essential to conduct an analysis and simulation of the security already early in the architectural phase of an SoS [36], thereby reducing the time and costs of subsequent changes. However, the SoS evolves throughout its life cycle, and therefore security risks must be considered continuously as the SoS structure changes.

Although an identified vulnerability within an individual CS could initially be evaluated as having a relatively small impact on the SoS, this vulnerability can trigger a sequence of damage to the SoS through the dependencies and integration between the individual CSs. A cyberattack can thus be further intensified so that the end result on the SoS as a whole will be much more harmful [15], [36]. This implies that the SoS environment may create new constraints on the threat analysis processes, both in terms of, e.g., their evolutionary nature and emergent properties [39]. It is, therefore, especially important to conduct a security analysis not only on the individual CSs but also to carry out an analysis on the entire SoS.

A model-driven method for security analysis in the architectural phase of an SoS is CVSS (Common Vulnerability Scoring System). This method is based on Bayesian network theory and can be described in terms of sensitivity analysis to detect the potential spread of cyberattacks and thereby estimate the likelihood of possible security flaws as well as their impact on the SoS [15].

Another method for conducting a security analysis with a focus on a network of systems (for example, an SoS with several different CSs) is game theory [40] methods that take into account several different security characteristics such as inherent vulnerability, spread probability, number of CSs, attack probability, and risk propagation. Such analyses can be based on both theoretical and numerical methods [41], [5].

Taken together, due to the fact that it is relatively costly, time-consuming and labour-intensive to generate extensive test cases for the entire SoS, it is desirable to fully or partially automate the security testing process. To streamline this process, one can, for example, use the automatic generation of test data and communicate sequential processes together with formal models [42].

It is also worth considering that SoS are often cyber-physical in nature. Therefore, the effects of a cyber-attack can lead to physical damage. Approaches for unifying the analysis of security with safety and other risks in the context of SoS have been proposed [43]. A key aspect here is the distribution of responsibility between actors representing the SoS as a whole, such as the KS, and the individual CS owners. This includes both responsibility for analysis and mitigating systemic risks that may emerge from interactions within the SoS. The information asymmetry (see Section II.B) constrains how those responsibilities can be allocated.

V. Balancing Security in Different CS within an SoS

In an SoS context, each CS has unique security needs and requirements. Balancing the security of these different CSs within an SoS can be challenging. Vital factors for this balancing are, e.g., the allocation of budget and the level of security, which we elaborate on in this section.

As different CSs interact with each other, the risk of these systems being attacked and exposed to cyberattacks also increases. These attacks often occur with the aim of either accessing information or, for example, damaging the systems or threatening the owner/user of the system. This means that the companies that own a CS must invest in security technology to minimise these risks, but as explained in Section II, they may underinvest in this.

It is usually relatively challenging to determine how much funds each CS in the SoS should allocate for this type of investment and to determine a necessary or reasonable *budget* to ensure, for example, software security. The integration and dependencies between the different CSs in the SoS thus also mean that decisions about how much funds should be invested for security in the individual CS do not depend solely on an individual investment decision in an individual CS, but also on other CS's decisions in the SoS [5].

Completely eliminating these cybersecurity risks is usually very difficult or even impossible and is often not even desirable because of the high costs such a strategy would entail. This means it is both a critical and challenging task to determine the *optimal and desired level of security* with the associated budget a company should spend on this type of investment. Since these companies' systems are CSs in an SoS, the other CSs in the SoS also need to be considered when making such decisions.

Various CSs in an SoS are commonly interdependent via their integration (e.g., data sharing). Physical integration patterns between these different CSs can thus pose a risk, as there is a possibility that a specific CS will be the subject of an attack. Thus potentially, other interconnected CSs in the SoS can also be subject to the same attack. As mentioned in Section II, this risk spillover effect is often referred to as a negative externality of the respective CS security investment.

Today's cyberattacks are increasingly shifting from being random and opportunistic to becoming increasingly strategic and targeting specific victims or companies. This means there is an obvious risk that a rational and strategic attacker primarily targets the more vulnerable CSs in the SoS, i.e., those CSs who probably invested less in their security.

Taken together, these dependencies between different CSs in an SoS can be a balancing act in how an individual CS may decide on the individual level of security that one wants to achieve. This means, for example, that security investments in one CS can benefit another CS within the same SoS. A CS invests in its security, it not only protects itself from direct attacks but can also protect other interacting CS from indirect attacks (i.e. positive externality) [41], [17]. However, there is a possible risk of being part of the same SoS as a CS that has higher security than yourself, as this makes it a less attractive target for the attacker to attack that specific CS in the SoS having the highest security, with the result that the attacker instead directs its resources to attack the CS that have lower security (i.e. negative externality) [5].

VI. Security Economics and SoS Governance

The previous sections have outlined risk analysis and security challenges in the different SoS archetypes and how they are typically addressed in the extant SoS literature. However, as Sections I and II indicated, SoS security also benefits from the information and cybersecurity economics literature. More precisely, the following observations can be made:

First, the set of governance tools *formally* available is more extensive if central entities or central interaction guidelines exist in the SoS. To see this, note that a central entity or a keystone (KS) may elect not to exercise its power and guidelines for interaction may be empty, thus making whatever governance tools are available in their absence also available in their presence.

Second, however, this formal observation may be wrong in practice. The very existence of a central entity may entail expectations (from itself and others) that it uses its authority. Similarly, the existence of interaction guidelines may entail expectations that they are substantial. Thus, in practice, the second observation amounts to the hypothesis that the effectiveness and appropriateness of different governance tools will vary over the different circumstances characterising the SoS archetypes.

To illustrate and exemplify this hypothesis, we now proceed to discuss the effectiveness and appropriateness of five cybersecurity policy options identified by Moore [16]: *ex ante* regulation, *ex post* liability, information disclosure, insurance, and indirect intermediary liability in each of the SoS archetypes. The overarching question is: What can be done to increase SoS cybersecurity in different circumstances?

A. Ex Ante Regulation

Ex ante regulation means that systems are designed to prevent incidents by adhering to rules—compliance. This is the default thinking in design-oriented security engineering. *Ex ante* regulation is only possible if there are rules. If interaction guidelines are the only kind of rules, then *ex ante* regulation is only possible in collaborative or acknowledged SoS. If other kinds of rules may include security standards, *ex ante* regulation may also be possible in the other SoS archetypes. In a directed or collaborative SoS, a central entity can enforce the regulation by excluding non-compliant CSs. If a virtual SoS completely lacks rules, there is, by definition no *ex ante* regulation. Taken together, this *ex ante* regulation depends on the specific content in the interaction guidelines.

B. Ex Post Liability

Ex post liability means that anyone causing an incident has to bear the cost of it afterwards, hopefully deterring incidents in the first place. Extracting such a cost up-front from the guilty party may require a central entity—and possibly a broader legal regime where courts outside the SoS acknowledge the authority of the central entity to do so.

However, extracting the opportunity cost of future gains from being in the SoS may be less complicated—even in the absence of a central entity, other CS may refuse to cooperate with the guilty party, in essence expelling it from the SoS.

This may be possible also in a collaborative or virtual CS. However, even if such expulsion of malicious or negligent entities does not require centralised power *per se*, it may require information that is hard to come by, as we discuss next.

C. Information Disclosure

The logic of information disclosure is that if asymmetric information can destroy both supply of and demand for security (see Section II), then supplying the missing information may rectify this. For example, if vendor A has a thousand cyber incidents per year and vendor B has ten, buyers may shift from A to B if this is disclosed. Information disclosure is a widely applicable mechanism in the sense that it does not require central entities or interaction guidelines *per se*—in this sense, it is feasible across all the SoS archetypes. However, since there are powerful incentives *not* to disclose incidents, guidelines mandating disclosure and a central entity to enforce the guidelines may help. Still, mandatory disclosure with enforcement may not be as powerful an instrument as one might believe if—realistically—data quality is poor [44] or enforcement imperfect [45].

D. Insurance

Insurance against cyber incidents offers two promises: First, it shares risk with an insurance collective, removing the need for large cash reserves. It may not be such a bad idea to be moderately risk-averse and pay $101 a year to be indemnified $100 000 in the event that a costly incident with a probability of 1/1000 occurs, even though the expected value is negative.

Second, insurance can use the premiums to incentivize firms and individuals to be more secure. First and foremost, this second aspect has attracted policymakers' attention (see, e.g., [46]. Like information disclosure, insurance is a widely applicable mechanism which does not require central entities or interaction guidelines. However, without good data for actuarial pricing, cyber insurance may struggle to offer the desired incentives (see, e.g., [20], [25], making it subject to some of the same difficulties as information disclosure.

E. Indirect Intermediary Liability

Indirect intermediary liability means that a third party is held responsible for someone else's wrong. This may seem counterintuitive, but it may be a helpful regime when (i) it is difficult to apprehend the actual wrongdoer (e.g., a cyber-criminal in a foreign jurisdiction), (ii) high transaction costs make it infeasible to draw up explicit contracts, (iii) the first party is in a good position to prevent the incident (e.g., a cloud service provider may be much better able to monitor the cybersecurity posture of an SME than that firm itself) and (iv) the third party can internalize negative externalities by decreasing the number of incidents [16].

An actual example is the way banks (a third party) are held responsible when a fraudster (the second party) skims the credit card of a victim (the first party) [16].

In the SoS context, indirect intermediary liability is similar to *ex ante* regulation in that it requires interaction guidelines outlining the liability but is even more dependent on a central entity to enforce it. If, however, the requirement that the liability is perfectly enforced is relaxed and allowed to be voluntary, it becomes perfectly possible in all of the SoS archetypes. Though such voluntary acceptance of liability may seem unrealistic, it can be imagined that prominent actors accept such responsibility even though it is costly in the short term in order to build a more secure and profitable long-term collaboration.

Taken together, we see that when considering the cybersecurity concerns of an SoS, it is important to take into account the unique characteristics that separate the different SoS archetypes. Each archetype, whether directed, collaborative, acknowledged, or virtual, may have its own specific security needs and requirements.

For example, a directed SoS may require strict access controls and monitoring to ensure only authorized users can access the system. A collaborative SoS, on the other hand, may require more flexible security measures to allow for collaboration between different systems. By understanding the unique characteristics of each SoS archetype and tailoring security measures accordingly, it is possible to address cybersecurity concerns and minimize the risks of cyberattacks effectively.

VII. Conclusions

With the increasing adoption of SoS, cybersecurity risks have become more necessary and challenging to manage. The paper concludes that to address cybersecurity risks in an SoS context, it is important to have a comprehensive understanding of the different SoS archetypes and their various related cybersecurity policies.

This paper has reviewed two different strands of literature related to the management of cyber risks: (i) the economics of cyber and information security and (ii) SoS cybersecurity practices. The main contribution is the insight that SoS researchers and practitioners could benefit from the perspectives of security economics, as discussed in the previous section. In particular, the security economics literature offers a number of tools that have not been widely discussed in the SoS literature, but which may nevertheless prove helpful if, as remarked by Anderson & Moore, "*security failure is caused at least as often by bad incentives as by bad design*" [12]. Different governance tools, it was hypothesised, will vary in effectiveness and appropriateness over the different circumstances characterising the SoS archetypes.

Moreover, the report also reviews different security issues within an SoS context, where we, e.g., discuss the security balance among the different CSs in an SoS. We also describe various security challenges over the four possible archetypes of SoSs and illustrate that each archetype has different cybersecurity challenges. According to their architecture, different approaches are identified as important to address.

References

[1] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," Manufacturing Letters, vol. 2, no. 2, pp. 74-77, 2014.

[2] U. P. D. Ani, H. He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," Journal of Cyber Security Technology, vol. 1, no. 1, pp. 32-74, 2017.

[3] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," Technol Health Care, vol. 25, no. 1, pp. 1-10, 2017.

[4] S. Varga, J. Brynielsson, and U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector," Computers & Security, vol. 105, pp. 102239, 2021.

[5] M. Ezhei, and B. Tork Ladani, “Interdependency Analysis in Security Investment against Strategic Attacks,” Information Systems Frontiers, vol. 22, no. 1, pp. 187-201, 2020.

[6] P. Gomes, E. Cavalcante, P. Maia, T. Batista, and K. Oliveira, “A Systematic Mapping on Discovery and Composition Mechanisms for Systems-of-Systems,” In: 2015 41st Euromicro Conference on Software Engineering and Advanced Applications, 2015, pp. 191-198.

[7] E. Lisova, J. E. Hachem, and A. Causevic, “Investigating Attack Propagation in a SoS via a Service Decomposition,” In: 2019 IEEE World Congress on Services (SERVICES), 2019, pp. 9-14.

[8] A. Fazlollahi, U. Franke, and J. Ullberg, “Benefits of Enterprise Integration: Review, Classification, and Suggestions for Future Research,” In: Enterprise Interoperability, Berlin, Heidelberg, 2012, pp. 34-45.

[9] A. Fazlollahi, and U. Franke, “Measuring the impact of enterprise integration on firm performance using data envelopment analysis,” International Journal of Production Economics, vol. 200, pp. 119-129, 2018.

[10] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, “Variables influencing information security policy compliance: A systematic review of quantitative studies,” Information Management & Computer Security, vol. 22, 2014.

[11] U. Franke, and J. Wernberg, “A survey of cyber security in the Swedish manufacturing industry,” In: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020, pp. 1-8.

[12] R. Anderson, and T. Moore, “The Economics of Information Security,” Science, vol. 314, no. 5799, pp. 610-613, 2006.

[13] J. Axelsson, and A. Kobetski, “Towards a risk analysis method for systems-of-systems based on systems thinking,” In: 2018 Annual IEEE International Systems Conference (SysCon), 2018, pp. 1-8.

[14] A. Fedele, and C. Roner, “Dangerous games: A literature review on cybersecurity investments,” Journal of Economic Surveys, vol. 36, no. 1, pp. 157-187, 2022.

[15] J. E. Hachem, A. Sedaghatbaf, E. Lisova, and A. Causevic, “Using Bayesian Networks for a Cyberattacks Propagation Analysis in Systems-of-Systems,” In: 2019 26th Asia-Pacific Software Engineering Conference (APSEC), 2019, pp. 363-370.

[16] T. Moore, “The economics of cybersecurity: Principles and policy options,” International Journal of Critical Infrastructure Protection, vol. 3, no. 3, pp. 103-117, 2010.

[17] N. A. Sales, “Regulating cyber-security. ,” Northwestern University Law Review 2012;107(4):1503–1568.

[18] G. A. Akerlof, “The Market for “Lemons”: Quality Uncertainty and the Market Mechanism*,” The Quarterly Journal of Economics, vol. 84, no. 3, pp. 488-500, 1970.

[19] T. Olsson, and U. Franke, “Risks and assets: a qualitative study of a software ecosystem in the mining industry,” In: Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Tallinn, Estonia, 2019, pp. 895–904.

[20] U. Franke, “The cyber insurance market in Sweden,” Computers & Security, vol. 68, pp. 130-144, 2017.

[21] OECD, “ Enhancing the Availability of Data for Cyber Insurance Underwriting, The Role of Public Policy and Regulation”, 2020.

[22] G. Mott et al., “Between a rock and a hard(ening) place: Cyber insurance in the ransomware era,” Computers & Security, vol. 128, pp. 103162, 2023.

[23] B. Schneier, “Insurance and the computer industry,” Commun. ACM, vol. 44, no. 3, pp. 114–115, 2001.

[24] D. Woods, and A. Simpson, “Policy measures and cyber insurance: a framework,” Journal of Cyber Policy, vol. 2, no. 2, pp. 209-226, 2017.

[25] D. W. Woods, and T. Moore, “Does Insurance Have a Future in Governing Cybersecurity?,” IEEE Security & Privacy, vol. 18, no. 1, pp. 21-27, 2020.

[26] H. Asghari, M. van Eeten, and J. M. Bauer, "Chapter 13: Economics of cybersecurity Handbook on the Economics of the Internet," Cheltenham, UK: Edward Elgar Publishing, 2016.

[27] G. Falco, et al. , “A research agenda for cyber risk and cyber insurance. Workshop on the Economics of Information Security (WEIS)”, 2019.

[28] M. W. Maier, “Architecting principles for systems - of - systems,” Systems Engineering: The Journal of the International Council on Systems Engineering, vol. 1, no. 4, pp. 267-284, 1998.

[29] J. S. Dahmann, and K. J. Baldwin, “Understanding the Current State of US Defense Systems of Systems and the Implications for Systems Engineering,” In: 2008 2nd Annual IEEE Systems Conference, 2008, pp. 1-7.

[30] “ISO/IEC/IEEE International Standard - Systems and software engineering -- Taxonomy of systems of systems,” ISO/IEC/IEEE 21841:2019(E), pp. 1-20, 2019.

[31] C. Guariniello, and D. DeLaurentis, “Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis,” Procedia Computer Science, vol. 28, pp. 720-727, 2014.

[32] C. E. Siemieniuch, and M. A. Sinclair, “Extending systems ergonomics thinking to accommodate the socio-technical issues of Systems of Systems,” Applied Ergonomics, vol. 45, no. 1, pp. 85-98, 2014.

[33] M. Andersson, and D. Rylander, “Wicked Cases and Late Binding in System of Systems,” In: 2022 17th Annual System of Systems Engineering Conference (SOSE), 2022, pp. 354-359.

[34] M. A. Olivero, A. Bertolino, F. J. Dominguez-Mayo, M. J. Escalona, and I. Matteucci, “Addressing Security Properties in Systems of Systems: Challenges and Ideas,” In: Software Engineering for Resilient Systems, Cham, 2019, pp. 138-146.

[35] S. Gritzalis, and D. Spinellis, “The Cascade Vulnerability Problem: the detection problem and a simulated annealing approach for its correction,” Microprocessors and Microsystems, vol. 21, no. 10, pp. 621-627, 1998.

[36] J. E. Hachem, V. Chiprianov, V. V. G. Neto, and P. Aniorte, “Extending a Multi-Agent Systems Simulation Architecture for Systems-of-Systems Security Analysis,” In: 2018 13th Annual Conference on System of Systems Engineering (SoSE), 2018, pp. 276-283.

[37] J. Klein, and H. v. Vliet, “A systematic review of system-of-systems architecture research,” In: Proceedings of the 9th international ACM Sigsoft conference on Quality of software architectures, Vancouver, British Columbia, Canada, 2013, pp. 13–22.

[38] M. Guessi et al., “A systematic literature review on the description of software architectures for systems of systems,” In: Proceedings of the 30th Annual ACM Symposium on Applied Computing, Salamanca, Spain, 2015, pp. 1433–1440.

[39] A. Ceccarelli et al., “Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach,” ACM Trans. Cyber-Phys. Syst., vol. 3, no. 2, pp. Article 18, 2018.

[40] J. Axelsson, “Game theory applications in systems-of-systems engineering: A literature review and synthesis,” Procedia Computer Science, vol. 153, pp. 154-165, 2019.

[41] Y. Li, and L. Xu, “Cybersecurity investments in a two-echelon supply chain with third-party risk propagation,” International Journal of Production Research, vol. 59, no. 4, pp. 1216-1238, 2021.

[42] M. M. Thwe, Z. M. Belay, E. Jee, and D. H. Bae, “Cybersecurity Vulnerability Identification in System-of-Systems using Model-based Testing,” In: 2022 17th Annual System of Systems Engineering Conference (SOSE), 2022, pp. 317-322.

[43] J. Axelsson, “Towards a Unified Approach to System-of-Systems Risk Analysis Based on Systems Theory,” INCOSE International Symposium, vol. 30, no. 1, pp. 1742-1757, 2020.

[44] U. Franke, J. Turell, and I. Johansson, “The Cost of Incidents in Essential Services—Data from Swedish NIS Reporting,” In: Critical Information Infrastructures Security, Cham, 2021, pp. 116-129.

[45] S. Laube, and R. Böhme, “The economics of mandatory security breach reporting to authorities,” Journal of Cybersecurity, vol. 2, no. 1, pp. 29-41, 2016.

[46] European Union Agency for Cybersecurity, "Cyber insurance : recent advances, good practices and challenges", 2016.