Using System Dynamics to Simulate Trust in Digital Supply Chains

Mari Aarland
Center for Integrated Emergency Research,
University of Agder, Norway
mari.aarland@uia.no

Jaziar Radianti
Center for Integrated Emergency Research,
University of Agder, Norway
jaziar.radianti@uia.no

Terje Gjøsæter
Center for Integrated Emergency Research,
University of Agder, Norway
terje.gjosater@uia.no

ABSTRACT

The power industry is outsourcing and digitalising their services to provide better, faster, and more reliable supply of electric power to the society. As a result, critical infrastructure increases in complexity and tight couplings between multiple suppliers and systems in digital supply chains. It also introduces new risks and challenges that are difficult to manage for critical infrastructure owners. To address the vulnerability in digital supply chains, we have developed a system dynamics model that represent important challenges to manage cybersecurity in digital supply chains, based on input from an expert group in the power industry. The system dynamics model illustrates how trust in suppliers as well as the need for control play important roles in outsourcing. Scenarios were developed and simulated.

Keywords

System dynamics, Critical infrastructure, Digital supply chain, Cybersecurity, Trust

INTRODUCTION

The cybersecurity domain has moved beyond the original meaning from technical conceptions of protecting against unwanted events in networked computers, to also include threats arising from digital technologies that can cause devastating societal effects (Hansen & Nissenbaum, 2009). Moreover, cybersecurity concerns are now listed as one of the societal security dimensions by the EU (ENISA, 2021a). In other words, it is acknowledged that digitalisation intended to benefit society may also introduce cybersecurity risks. For instance, the tightly coupled interactions between critical infrastructures have created a vulnerability for the domino effect (Arvidsson et al., 2021) and digital disasters.

The digitalisation of critical infrastructure has led to an emergence of complex digital supply chains. The notion of digital supply chains is relatively new and emerges from developing new innovative technology i.e., big data, could computing, and internet of things. This article uses the definition from Ageron et al. (2020, p. 133) to describe digital supply chains as "*the development of information systems and the adoption of innovative technologies strengthening the integration and the agility of the supply chain and thus improving customers service and sustainable performance of the organization*". In the power industry, digitalisation such as cloud computing allows for more real-time data and improved predictions of future decisions in the marked, which is a key driver for investing in technological tools. The technology is easily accessible through outsourcing for those organisations that have limited knowledge and resources in-house. However, the continuation of outsourcing also introduces new cybersecurity risks by extending the already complex digital supply chain for critical infrastructure.

The power industry is dependent on their information technology (IT) suppliers. These organisations are heavily dependent on their suppliers of e.g. systems, hardware, and human resources to provide a reliable supply of energy. In this ecosystem, a dilemma arises between the need for outsourcing and proper cybersecurity management. The current solution to managing suppliers in the digital supply chain is using methods based on trust, e.g., service level agreements initiated in the procurement. However, controlling suppliers in the digital supply chain based on traditional control mechanisms such as audits is found to be challenging. Therefore, the method used for controlling suppliers is based on trust (Office of the Auditor General of Norway, 2021). This lack of available control mechanisms may lead to a heightened risk of digital disasters affecting the power industry. According to the European Union Agency for Cybersecurity (ENISA, 2021b), 24 supply chain attacks were reported from January 2020 until July 2021. Their analysis shows that *trust* between stakeholders was exploited in 62% of the attacks.

Nevertheless, we still base our decisions on outdated mental models that are too static, narrow, and reductionist (Sterman, 2000), forgetting the holistic approach. The system dynamics approach is used for studying the dynamics of complex real-world systems (Forrester, 1997). Meadows (2008) explains that the study of system dynamics helps to understand what would happen if several factors evolved in a range of diverse ways. The concept believes that components in a system interact through causal relationships (Forrester, 1997). Establishing those critical relationships in the digital supply chain will contribute to making critical infrastructure more resilient. In addition, system dynamics can provide information for critical infrastructures to prioritise their countermeasures for reducing risks of digital disasters.

Based on the initial context, the following research question shaping the rest of this paper is: *How can trust as part of a digital supply chain in critical infrastructure be modelled and simulated using system dynamics methods?*

The rest of this paper is organised as follows: First, we present the existing research conducted on trust in digital supply chains and simulations of trust using system dynamics. Next, we describe the empirical basis for this paper. Then, the methodology is presented, following a description of the construction of the system dynamic model and simulations setting. After that we will presents the model and simulation results. Finally, the conclusion along with our thoughts about future research is presented.

LITERATURE REVIEW

The research on trust is dispersed through several disciplines which makes the concept difficult to pin down and measure without further contextualization and operationalization. The diversity of definitions on trust may contribute to different expectations that could create asymmetric relationships between the actors in the digital supply chain. For the purpose of this paper, the understanding of trust is based on the definition from Mayer et al., (1995, p. 712), where they describe trust as "*the willingness to be vulnerable in a situation where the other party takes actions without the need for other control mechanisms like monitoring or audits*". For instance, using cloud computing often relates to the actions of storing data outside the organisation. The company that uses the external cloud computing, makes themselves vulnerable for protecting the integrity of the data but believe that the provider of the cloud computing service will protect and store their data in a safe way.

According to Laeequddin et al. (2012), trust is essential for maintaining a successful supply chain partnership and contributes to mitigating risk in uncertain ecosystems. However, the process of establishing trust is much more intricate than stating that trust is important for a successful digital supply chain. Lin et al., (2005) suggests that members in the supply chain should assess their trust in one another to respond dynamically to changes in the ecosystem.

Assessing the trust level towards the supplier can be done by looking at four dimensions proposed by Agarwal and Shankar (2003): (1) *Cooperating to minimize information asymmetry*, is important to maintain transparency throughout the digital supply chain for instance whenever suppliers make changes in their sub-suppliers, this information should be reported to their stakeholders. (2) *Improving interpersonal behavior*, by understanding the interpersonal behavior for suppliers in the digital supply chain the control element could possibly replace some of the controlling activities i.e., revisions, monitoring, and random sampling. (3) *Fraud minimization is important to remain a reputation of being a trustee party*, Suppliers must try to avoid situations that may cause uncertainty about economic issues, for instance some may try to take advantage of the fact that they are the only supplier distributing a certain product and will try to oversell or create a negative reputation by always increasing the cost of that specific product without improving the product. (4) *Promotion on-line transaction simplification*. Transparency in the procurement phase is essential to acquire more knowledge about the transaction costs. The relationship between the buyer and the seller in a digital supply chain is not always linear. In some cases, the product or service that the buyer invests in consist of multiple suppliers, and in such cases being transparent and simplifying the transactions enables the buyer's capability to reduce some uncertainty to the product quality prior to the purchase.

According to Nowicka (2018) the type and range of the information shared with stakeholders in the digital supply chains indicates the level of trust you have towards the suppliers. In addition, trust in supply chains is considered by Wang et al., (2014) to be one critical relational factor that enables collaborations between stakeholders. The motivation for using trust is based on reducing coordination costs and transactions risks in interorganisational relationships (ibid).

To simulate trust the concept needs further clarification in the context and the properties related to the term. Abdul-Rahman and Hailes (2000) study suggest seven properties to describe trust: (1) Trust is context dependent. (2) Trust describes the level of belief in a partner's trustworthiness. (3) Trust is based on prior experience. (4) Partners can exchange information on their respective reputations via recommendations, supporting a reputation mechanism to aid in trust decisions. (5) Trust is not transitive. (6) Trust is subjective, meaning that different observers may have different perceptions of the same partner's level of trustworthiness. (7) The degree of confidence in a relationship is constantly increased or decreased by experience and suggestions.

Despite the extensive research on trust over an extended period, resolving the trust issues regarding trusting others to do the intended work and trusting the product delivered in digital supply chains have no sufficient solution (Zhang et al., 2019). However, that study is focused on physical supply chains and not digital supply chains. Without trust the digital supply chains would not function (Laeequddin et al., 2012), but too much trust is rather seen as naive and taking too much risk. The Microsoft Digital Defence Report (Microsoft, 2021) called out the vulnerable digital supply chains by saying it is explicitly reliant on trust and that the adversaries have become aware of its vulnerability. This aligns with the conclusions and critique of suppliers in the Norwegian power industry (Office of the Auditor General of Norway, 2021).

According to Hoshimov et al., (2021) system dynamics helps academicians and practitioners to analyse the advantages of digitalising the supply chain and how the stakeholders change their behaviours. Using simulation tools to determine and capture the complexity of digital supply chains can help to evaluate the impact of rusting the suppliers in situations where other control mechanisms, such as revisions and service level agreement, are limited. According to Lin et al., (2005) information sharing in decentralized supply chains using command and control should be modelled utilising social simulation. A social simulation can consider the decentralization of digital supply chains and better capture the interactions between stakeholders.

Simulating trust using system dynamics has been executed in different contexts before. In the construction field, a study on how to improve the trust level between an owner and a contractor was conducted using a system dynamics model (Li & Feng, 2022). This study identified four factors that influences relational trust: the *sufficiency of the owner's authorization*, the *effectiveness of the owner's supervisory measure*, the *social similarity between the owner and contractor*, and the *management capability and reputation of the contractor* (ibid). Other disciplines that have studied trust in a system dynamics perspective are automation.

Hussein et al., (2019) study how the speed and reliability of automation and the combination of them affects trust. The study concludes that the presented model closely replicates the experimental data, and by replicating the experimental data they can explain and predict the behavior of a human-automation interaction. Another study on connected autonomous vehicles used system dynamics to assess the cybersecurity level, and trust across the connected autonomous vehicles industry and to the public (Khan et al., 2021). In their analysis, Khan et al., (2021) concluded with their simulations that trust relies on the safety and security of driverless cars, and that trust is vital between actors to reduce cyberattacks.

As shown, system dynamics can be suited to simulate trust where multiple parties are involved and where the environment is complex and ever-changing as the digital supply chains. Another method called analytic network process (ANP) which is used to understand complex networks in supply chains and have also been applied to build a trust evaluation index (Zhang et. al, 2022). This method could be used to understand trust in supply chains, nevertheless since it is mainly applied in physical supply chains the system dynamics approach is deemed appropriate by the authors. In addition, we identified that there seems to be a gap in the existing literature concerning related topics for the power industry, but also concerning digital supply chains. Therefore, it is necessary to build knowledge about the trust effects in digital supply chains for critical infrastructure owners and particularly in the power supply.

System dynamics provides the necessary tools to study how the relationship between the interconnected elements in a complex scenario behave. The theory of system dynamics lies in the nonlinear dynamics and feedback controls found in mathematics, physics, and engineering (Sterman, 2000). It is interdisciplinary by nature because of its placement in between human, technology, and organisational factors, but also the objective to describe a phenomenon that continuously changes in its environment. This is a method for developing models that analyse diverse types of scenarios, e.g., trust in the supply chain or adaptation of digital technologies under several types of conditions. These conditions could be normal or under extraordinary situations like a supply chain attack (Hoshimov et al., 2021). Results from system dynamic modelling may contribute knowledge for possibly identifying what factors impacts trust in digital supply chains.

The concept of system dynamic was developed to understand and analyse how dynamic and complex systems behave (Shin et al., 2013). The methodology behind system dynamics arises from a feedback loop view of the world, i.e., decisions taken in systems will alter the system which subsequently leads to new decisions (Sterman, 2000). Through digitalisation the stakeholders become more integrated and may result in an increase of transparency and collaboration between stakeholders in the digital supply chain.

The system dynamics approach can be divided into two parts: basic elements and implementations steps. The basic elements are descriptions of the constituting elements in systems dynamics. The constituting elements in system dynamics are system, system boundaries, mutable state, rate variables, cause-and-effect diagrams, and flow graphs. The implementation steps consist of the following activities: problem identification, policy analysis, determining system boundaries, simulating implementation, creating causality diagrams, and finally system flow diagrams (Sterman, 2000).

This paper utilises the stock and flow diagram and causal loop diagram to describe trust and outsourcing in digital supply chains for critical infrastructure. The stock and flow diagram uses parameters and variables that have been widely studied and recommended for system dynamic models to establish proper means for simulating digital supply chain behavior (Sterman, 2000). To further analyse the two identified variables of outsourcing and trust in digital supply chains, the simulations will provide more information about their influence found through a preliminary study and through the expert group.

Data collection method

The variables affecting trust in the digital supply chain were identified during a workshop with an expert panel from the power industry with participants holding central positions in their organisations. The organisations were mainly large stakeholders in the Norwegian power industry. In addition to the workshop, current research on trust in digital supply chains also helped to identify the variables.

Table 1. Overview of Participants in the Expert Group

	Gender	Position	Domain field
Expert 1	Male	Senior Advisor	Cybersecurity and Privacy
Expert 2	Female	CEO	Cybersecurity
Expert 3	Male	Security Architect	Information Technology
Expert 4	Male	Senior Researcher	Resilience
Expert 5	Female	Special Advisor	Contingency Cybersecurity
Expert 6	Male	Senior Advisor	Digital Security

Another important aspect to consider before modelling is determining the boundary of the model. Especially for the digital supply chain, the limitations of the system and model are important. The trade-off for including and excluding affecting variables is based on the findings from the expert group.

To understand the system analysed in this paper, a preliminary study review was conducted. This allowed for in depth understanding of issues, as well as identification of the variables contributing to unstable digital supply chains. For further development of the understanding, the involvement of stakeholders is essential to define the problem for digital supply chains in critical infrastructure. Such an issue may be identified with the help of an expert panel that represented the sector. Understanding how the idea of trust affects digital supply chains was the recognised issue, and it was also determined whether a situation could be replicated to visualise the data. We were able to create a causal loop diagram based on the current findings together with the findings from the literature study and data from the industry's stakeholders. The two primary issues raised by experts and in the literature related to outsourcing and trust. The Vensim PLE (version 9.3.5.) software was used to create the causal loop diagram.

MODEL DESCRIPTION

The system dynamic model have been developed based on statements from the expert group and by using system dynamics steps recommended by Wu et al. (2022) (1) understanding the system, (2) defining the problem, (3) modularizing the concept, (4) building the model, (5) testing validity, (6) analysing the results, and (7) simulating policy scenarios.

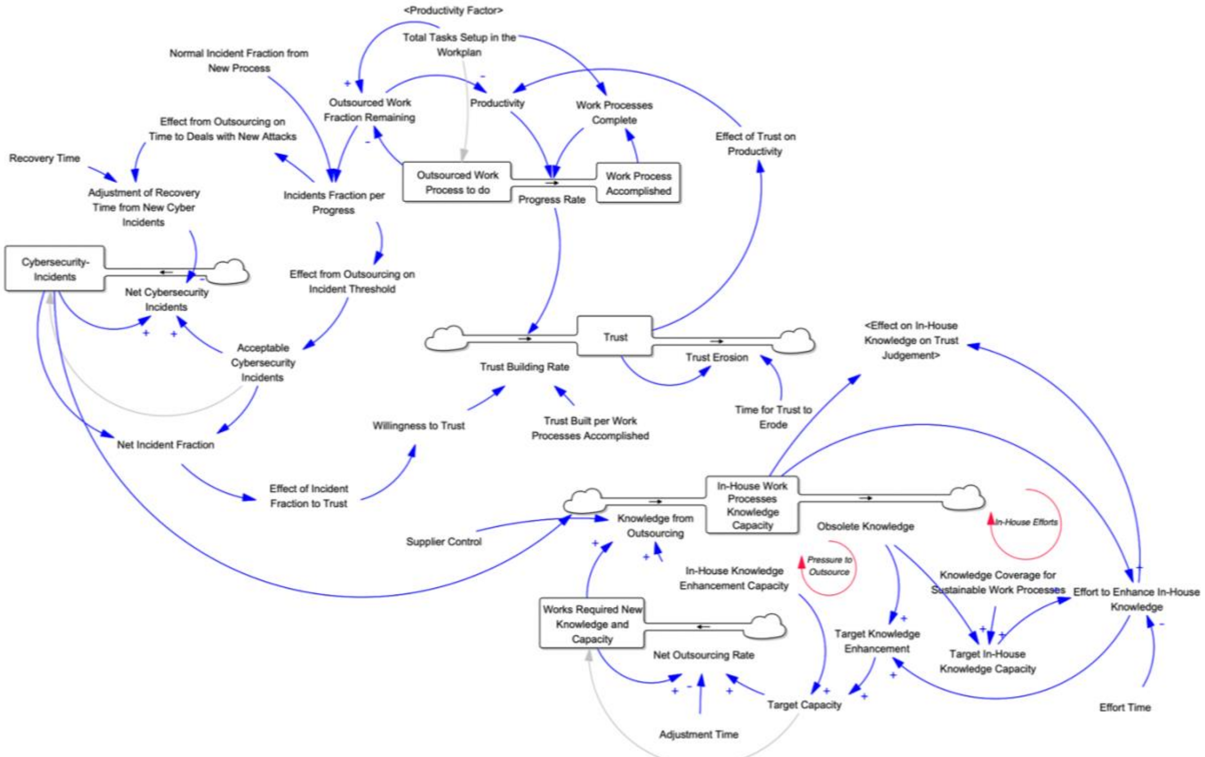

<Productivity Factor>
Total Tasks Setup in the Workplan
Normal Incident Fraction from New Process
Outsourced Work Fraction Remaining
Productivity
Work Processes Complete
Effect from Outsourcing on Time to Deals with New Attacks
Recovery Time
Adjustment of Recovery Time from New Cyber Incidents
Incidents Fraction per Progress
Outsourced Work Process to do
Progress Rate
Work Process Accomplished
Effect of Trust on Productivity
Cybersecurity-Incidents
Net Cybersecurity Incidents
Effect from Outsourcing on Incident Threshold
Acceptable Cybersecurity Incidents
Net Incident Fraction
Trust
Trust Building Rate
Trust Erosion
<Effect on In-House Knowledge on Trust Judgement>
Willingness to Trust
Trust Built per Work Processes Accomplished
Time for Trust to Erode
Effect of Incident Fraction to Trust
In-House Work Processes Knowledge Capacity
Knowledge from Outsourcing
Supplier Control
Obsolete Knowledge
In-House Efforts
Pressure to Outsource
In-House Knowledge Enhancement Capacity
Knowledge Coverage for Sustainable Work Processes
Effort to Enhance In-House Knowledge
Works Required New Knowledge and Capacity
Net Outsourcing Rate
Target Knowledge Enhancement
Target In-House Knowledge Capacity
Target Capacity
Adjustment Time
Effort Time

Figure 1. Overall Model of Relationships in the Digital Supply Chains

Figure 1 shows the relationships in the digital supply chain. The overall model is further explained in the following chapter and divided into two sub-models. The two models are also used in the simulations later. The first sub-model is called outsourcing. Outsourcing occurs when organisations in the digital supply chain lack in-house competence or where resources are limited and therefore there is a need to outsource some of their work processes. The other sub-model is called trust and is necessary to maintain a digital supply chain in critical infrastructure. It is close to impossible to know the origin of all source code and every person involved in the development of a software. Therefore, trusting those responsible for delivering those software services is essential.

The model is based on the following assumptions: the environment is dynamic, there is a high degree of uncertainty about future events, all stakeholders have different perspectives, goals and constraints, there is no clear mechanism for coordination between stakeholders, all stakeholders have limited amount of time available for decision making, each stakeholder has a different degree of influence over other stakeholders (e.g., financial, controlling, and power dimensions), and limited resources and lack of in-house competence leads to outsourcing. These assumptions are based on the existing literature and from the expert group in the industry.

Sub-model of outsourcing

This sub model captures the reason for an organisation to implement outsourcing which could happen due to the discrepancy between the company goals (abilities to provide services or to conduct the daily work processes), and the company in-house capacity. There are two stocks presented in this sub-model, namely: *In-House Work Processes Knowledge Capacity (IKPC)* and *Works Requiring New Knowledge and Capacity (WRNKC). In-House Work Processes Knowledge Capacity* refers to the already existing knowledge that the organisation possesses. This is acquired through internal learning or other recourses such as outsourcing. The other stock *Works Requiring New Knowledge and Capacity* describes a situation that can occur when some processes are digitalised, and the current knowledge and capacity is no longer sufficient to operate the new digital tool. The stocks are affected by the flows, represented in the model with a black arrow and valve symbol. The model consists of three flows *Knowledge from Outsourcing (KOs), Obsolete Knowledge (OKn),* and *Net Outsourcing Rate (NOsR). Knowledge from Outsourcing* is formulated in the model as follows:

$$\frac{dKOs}{dt} = IKPC \ \times (WRNKC \ \ \times \ WOs) \times C$$

Willingness to Outsource (WOs) represents the tendency of an organisation to outsource, which depends on many factors, and can change from time to time. For example, willingness to outsource decrease when a cybersecurity incident happens connected to the suppliers. *Supplier Control* (*Sc*) is a parameter set up as 1 that can be altered for simulation where reducing the value below one means a company wants to control the suppliers, while increasing the control values mean the company procure more services to close the gap in the in-house knowledge. *Obsolete knowledge (OKn)* is modelled as built-in function STEP:

$$\frac{dOKn}{dt} = 100 + STEP(20{,}2)$$

Thus, this is just an input function that triggers the dynamic of the model, which can be replaced with variables from the model itself. As in this version, this STEP equation means that we assume there is a constant amount of knowledgeof work-processes that will be obsolete each year, i.e., 100, that will increase even more 20 additional obsolete knowledge in the second month. Thus the company should catch up.

According to theory, the flows draw from empty to limitless reservoirs (Sterman, 2000). However, the reality is often that organisations have a given set of recourses, hence the need for outsourcing. The other variables presented in the model are converters with values that are connected to the selected time. Connecting converters impacts the value for the converts where the connection can lead to an increase or decrease. This is shown in the model with the symbol + for increasing connectors and - for decreasing connectors. This helps to identify the characteristics of the causal loop diagram as either reinforcing loops (only increasing or positive polarity) or balancing loops (only decreasing or negative polarity). This sub-model contains two reinforcing loops; *In-House Efforts (IEf)* and *Pressure to Outsource (POs).*

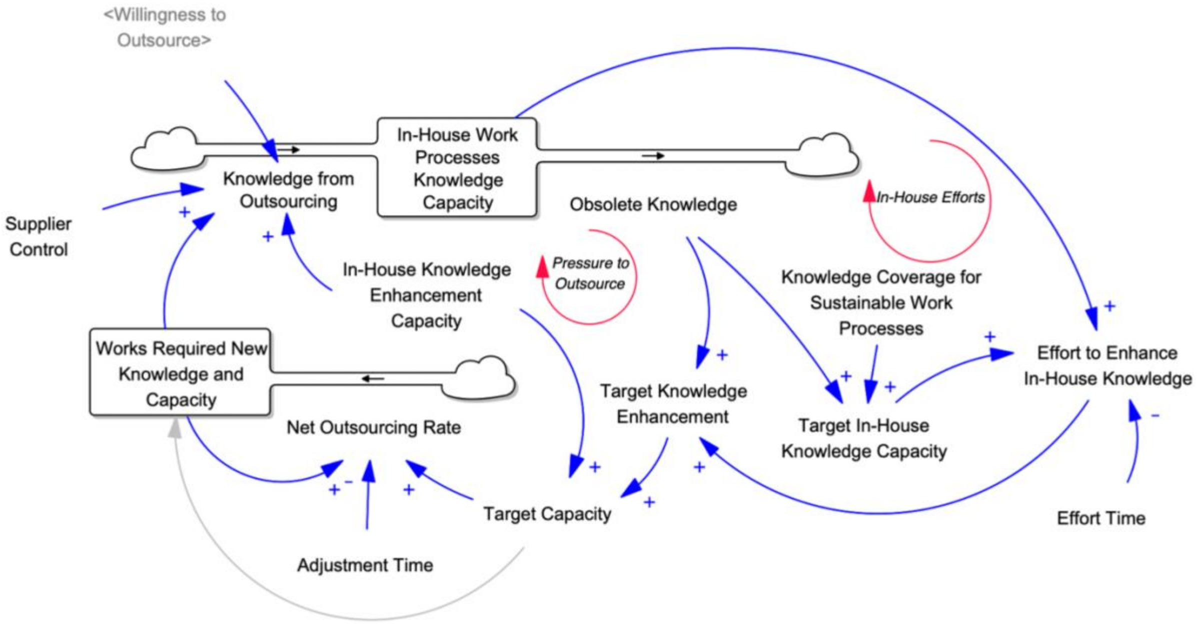

<Willingness to Outsource>
Supplier Control
Knowledge from Outsourcing
In-House Work Processes Knowledge Capacity
Obsolete Knowledge
In-House Efforts
Pressure to Outsource
In-House Knowledge Enhancement Capacity
Knowledge Coverage for Sustainable Work Processes
Effort to Enhance In-House Knowledge
Works Required New Knowledge and Capacity
Net Outsourcing Rate
Target Knowledge Enhancement
Target In-House Knowledge Capacity
Target Capacity
Adjustment Time
Effort Time
+
-

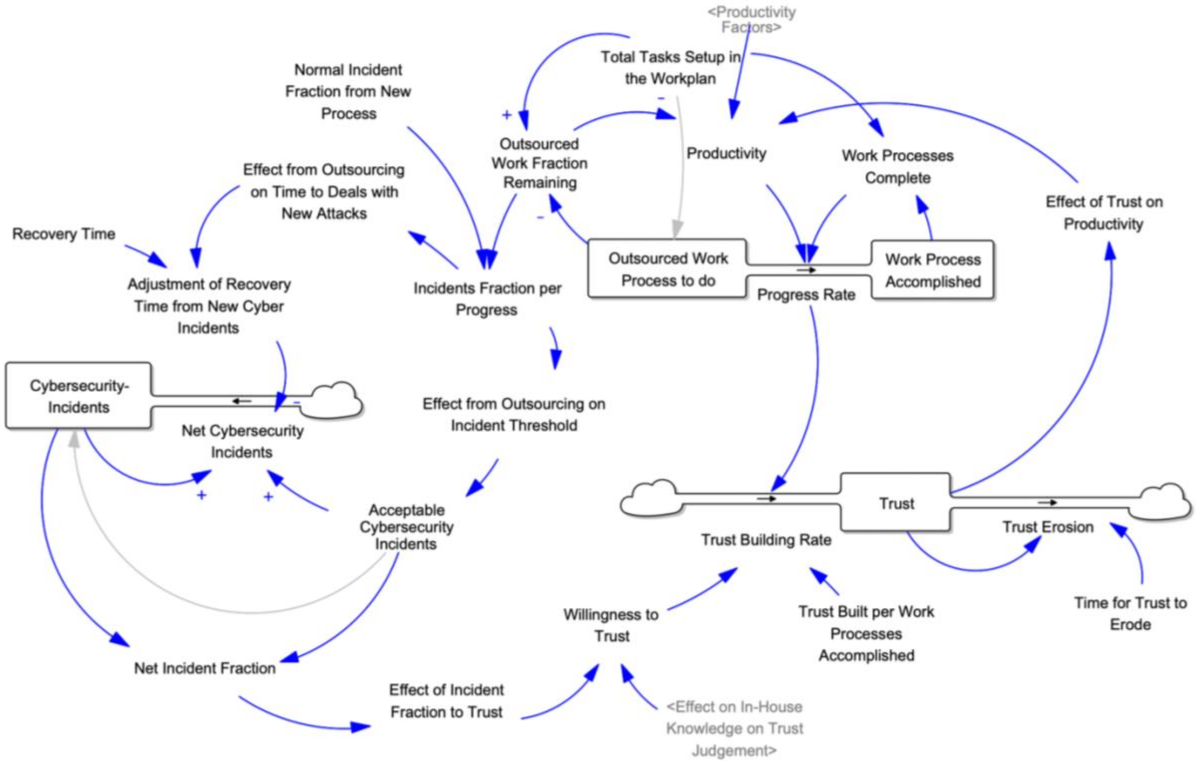
Figure 2. Sub-Model for Outsourcing Relationships in the Digital Supply Chains

Outsourcing is for some organisations necessary when in-house knowledge, competence, and resources are limited. In addition to the resource demand to obtain in-house competence, it may also be considered more reliable to outsource those services that relate to a specific product. In the procurement phase, security requirements are often presented to the supplier along with the service level agreement as a way of *Controlling the Supplier*. The supplier then provides sufficient data to enhance *the Trust Effects on Outsourcing*. The *Knowledge from Outsourcing* increases the stock *In-House Work Processes Knowledge Capacity* which means the overall knowledge capacity in the organisation increases. However, knowledge becomes obsolete when new emergent technologies are introduced which lowers the stock of *In-House Work Processes Knowledge Capacity*.

At the same time as organisations choose to outsource, the trade-off for *Enhancing In-House Knowledge* remains. The complex and tightly coupled digital supply chains suffer from a digitalisation trend which contributes challenges in managing the holistic overview of cyberattacks. Therefore, it is considered an important aspect to enhance such in-house competence to both be able to determine if the service provided by the supplier is sufficient and secure, but also have the competence to continue normal operation even though the supplier's service becomes unavailable. This enforces the in-house capacity to manage new challenges such as cyberattacks. Then the internal efforts become more specific and affects the *Targeted Knowledge Enhancement*, which also contribute to the overall goal to in-house work processes knowledge capacity. This creates a reinforcing loop of knowledge acquisition.

Sub-model of trust

To capture the effect of trust in digital supply chains, we present a sub model to enhance the cause and effect of trust. The stocks presented in this model is called *Outsourced Work Process to Do (OWP), Work Process Accomplished (WPA), Cybersecurity Incidents (CI)*, and *Trust (T).* There are several connectors in the model that effect the level of trust towards suppliers. *Outsourced Work Processes influence Work processes Accomplished,* whilst the progress rate also influences the level of trust towards the supplier. If the organisation knows that the supplier will deliver their product at the given date, the willingness to trust the supplier increases. In that way the progress rate for work done by outsourced processes increases the stock called *Trust (T).*



<Productivity Factors>
Total Tasks Setup in the Workplan
Normal Incident Fraction from New Process
Outsourced Work Fraction Remaining
Productivity
Work Processes Complete
Effect from Outsourcing on Time to Deals with New Attacks
Effect of Trust on Productivity
Recovery Time
Adjustment of Recovery Time from New Cyber Incidents
Incidents Fraction per Progress
Outsourced Work Process to do
Progress Rate
Work Process Accomplished
Cybersecurity-Incidents
Net Cybersecurity Incidents
Effect from Outsourcing on Incident Threshold
Acceptable Cybersecurity Incidents
Trust
Trust Building Rate
Trust Erosion
Willingness to Trust
Trust Built per Work Processes Accomplished
Time for Trust to Erode
Net Incident Fraction
Effect of Incident Fraction to Trust
<Effect on In-House Knowledge on Trust Judgement>
+
-
+
+

Figure 3. Sub-Model for Trust Relationships in the Digital Supply Chain

Building trust stems from the expectation to deliver the product or service on time. For instance, day-to-day monitoring and software e.g., antivirus program. Through outsourcing in digital supply chains, trust is often related to the product or service delivered. As such, the *Trust Built per Work Processes Accomplished (TBWPA)* influences the *Trust Building Rate (TBR).* Whenever a task is successfully accomplished the willingness to trust the other party increases. Currently, *Trust Built per Work Processes Accomplished* is modelled as a parameter with a value of 1. Trust building Rate is modelled as follows:

$$\frac{dTBR}{dt} = P \times (TBWPA \times WT)$$

Progress Rate (P) is amount of outsourced works done over time. Moreover, trusting in a digital supply chain is also essential to the effects of *Trust* on *Willingness to Trust.* For instance, Microsoft is considered a safe option when it comes to their Office365 solution and applications like Azure (i.e., their cloud computing product). The threshold for choosing Microsoft is therefore assumed to be low and considered a safe choice to provide the level of cybersecurity needed for critical infrastructure. *Willingness to Trust (WT)* is formulated as set of effects:

$$WT = ECT \times EKT$$

In addition, *Cybersecurity Incidents* plays a vital role in trust building rate, because the *Effects of Cybersecurity Incidents on Trust Building (ECT)* will ultimately affect the supplier's ability to accomplish their task. For instance, a cyberattack can affect the software production of a platform delivering monitoring applications like the SolarWinds attack. SolarWinds is an example where a company was exposed through a supply chain attack which affected many of their customers and partners. Even though SolarWinds was a victim of this act, the trust naturally gets affected with customers investing more time scanning any updates from the services bought from

SolarWinds. However, there is also the case of human error which is indeed a prominent cause of cybersecurity incidents. Those incidents could be a result of sharing classified information without security clearances. *Effects on Inhouse Knowledge on Trust Judgement (EKT)* will affect the way the company trust the suppliers. If the company knows better a certain process, it will help to judge if the suppliers trustable or not.

Nevertheless, trust is dynamic and ever-changing as it should because of the chaotic nature of digital supply chains where a complete overview of latent cyberrisks is close to impossible to retrieve. The *Trust Erosion (TE)* describes loss of trust between two segments in a digital supply chain over time. Audits can cause trust erosion, where the report uncovers that a supplier has changed their sub-supplier without the notification of change delivered to the customer, or if the product upon delivery is found to contain bugs that initially were supposed to be fixed. Thus, such discovery will typically reduce the trust in suppliers. The *Trust Erosion* is modelled in relation to time as follow:

$$\frac{dTE}{dt} = \frac{T}{TTE}$$

Even though some have the financial muscles to in-house their work processes and even choose which supplier fits them best, others may have no options and need outsourcing to maintain their day-to-day work processes. In such cases the selection of supplier is based on productivity rather than security. The *Progress Rate* of the *Work Processes* will eventually influence the trust towards that supplier. When the relationship is established, the trust will increase as the progress evolves, and when software is delivered on time and the product quality is good, the overall trust in the supplier will increase. Note that we only reveal the most important equations in the model but having quantitative inputs and formula have been a requirement for a system dynamics model to be able to run simulations.

SIMULATIONS

The goals of the simulations are twofold. First, for the base run, we want to show the effects of the limited outsourcing to the in-house knowledge capacity and other variables that are affected or important to show in this base run scenario that is considered as “business as usual”. Second, the scenario simulations that aim at seeing the trade-off effects of choosing to control a supplier even tighter (outsourcing scenario) vs. to control through trusting the supplier.

The scenarios used in the simulation is described in Table 2. The duration of simulation is based on the life cycle of a supplier contract set to 15 months, to be more realistic as in practice, some delays for project deliverable may occur and deviate from typical 12 months contract.

Table 2. Overview of the simulated scenarios

No.	Scenario	Name
0	The current situation for digital supply chains in critical infrastructure.	Normal Scenario
1	Using outsourcing to other organisation for knowledge enhancement.	Outsourcing Scenario
2	Using trust for managing suppliers.	Trust Scenario

Scenario 1 – Outsourcing Scenario

The purpose of the outsourcing scenario is to understand the risk following the activity to outsource and to explore the consequence if organisations choses to outsource less. In the outsourcing scenario assume a limited budget, resources, and staff to invest in in-house competence, managing and training external suppliers. To ensure continuity and quality of services, the need for an annual audit of all suppliers is assumed. The outsourcing scenario also assumes that there are few or no in-house resources available for managing external suppliers, which can lead to increased risk of failure or incidents (e.g., deficient performance from suppliers). This can also lead to disruption in services and higher costs for CI (Critical Infrastructure) owner and their customers. Two changes from the base run are made in the Outsourcing scenario. First, *Supplier Control* which was changed to be less than one (0.8), which means a tighter control to supplier is applied. Second, *Total Tasks Setup in Workplan* was altered to smaller number (i.e., 10) compared to the initial value of 12. It means that less tasks being outsourced.

Scenario 2 – Trust Scenario

The trust scenario assumes that organisations use trust as their form for control mechanism to their suppliers. The trust scenario can be used to gain insight into how digital supply chains affect cybersecurity in critical infrastructure organisations. Further, it investigates how they respond to this threat by developing strategies to improve security in their supply chains, as well as other measures such as collaboration between producers and buyers, or collaboration between producers who share common interests or objectives (such as sharing knowledge related to cyberattacks). On the parameter changes, we altered *Supplier Control* with 1.3 (initial value was 1). This change represents an organisation loosens the control and outsources more. The *Incident Fraction* also increased from 1 to 1.3, capturing the increased risks for incidents. While *Trust Built per Work Processes* decreased from 1 to 0.8, to represents less trust might occur from delivered work, for example, due to increased cybersecurity attacks, and require the organisation is more cautious for controlling the quality of delivered work.

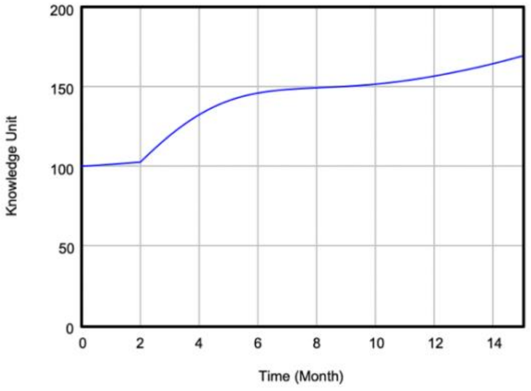
Based on the scenarios, Table 3 below describes which of the parameters in the simulation that influences the outcome. After analysing data from the literature and experts in the industry we decided to change values for specific parameters between Outsourcing scenario and Trust scenario. The other parameters stay consistent for comparability reasons. The parameters considered important for the overall simulation are defined as stable.

Table 3. Overview of the parameters in the simulated scenarios

Parameter	Parameter description	Base run	Scenario 1	Scenario 2
Supplier Control (Dimensionless)	The supplier control is setup qualitatively as 1 which means that there is a minimum acceptable control of supplier.	1	0.8	1.3
Adjustment time (Months)	Time needed to understand the gap between the targeted goal and the existing in-house capacity.	3	3	3
Effort time (Months)	Effort time to enhance in-house knowledge, where a company still need time to understand the new system or work processes.	2	2	2
Normal incident fraction (Dimensionless)	The model will not be affected by 1 incident.	1	1	1.3
Total tasks setup in the workplan (Fraction/Months)	The amount of work you need to do from the outsourcing requirements.	12	10	12
Recovery time (Months)	The amount of time it takes an organisation to recover after a cyberattack.	1	1	1
Trust built per work processes (Trust Unit/ Work processes)	The amount of trust organisations built from successfully achieving a work process on time.	1	1	0.8
Time for trust to erode (Months)	The natural reason for trust to erode because of no longer working together or other such reasons.	8	8	8

Base run – Current digital supply chains in critical infrastructure

The base run scenario is a representation of how the current digital supply chains operate. It shows how outsourcing and trust in current digital supply chains affects the overall security for critical infrastructure. In this case, we did not make any changes in the parameters, to represent a "business as usual" scenario.



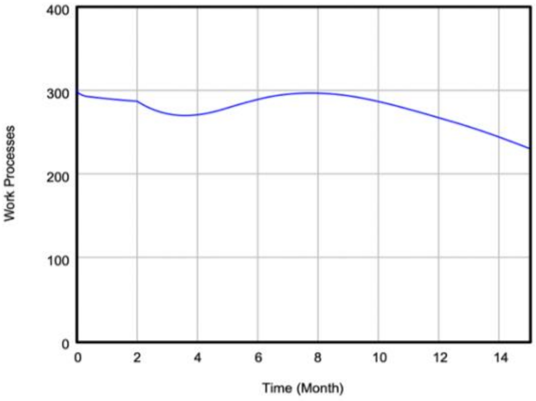
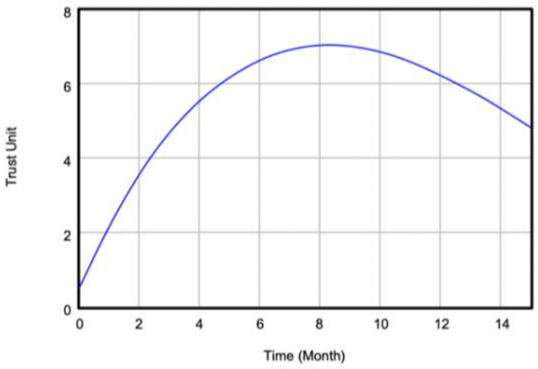


Figure 4. Simulation of Work Requiring New Knowledge and Capacity

Figure 5. Simulation of In-House Work Processes Knowledge Capacity

Figure 4 shows that work processes require new knowledge and capacity will continue to increase because of the digitalisation of current work processes. For instance, this reflects the tendency to invest in internet of things (IoT) devices to monitor digital and physical infrastructure. In addition, the expert group highlighted that critical infrastructure owners need more capacity and expertise in the cybersecurity field because the field keeps evolving and changing.

In-house work processes knowledge capacity is considered to represent the maximum amount of knowledge the organisation holds at the given time. As Figure 5 shows, in-house knowledge decreases over time as organisations outsource and become more dependent on external knowledge to operate. To exemplify, when cloud computing is outsourced, the availability of in-house knowledge on how to develop their own cloud computing system is less likely. Based on the expert group from the industry, this tendency is found in several organisation.



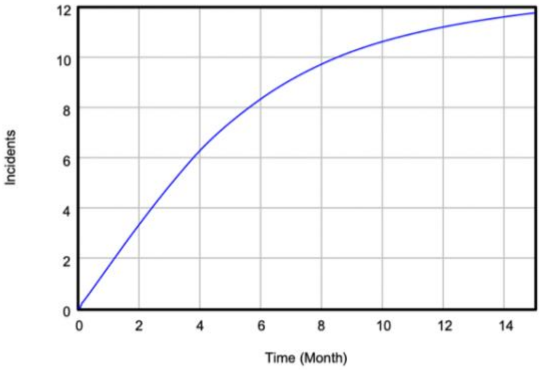


Figure 6. Simulation of Trusting Suppliers

Figure 7. Simulations of Cybersecurity Incident

Trust in suppliers is assumed to be low at the beginning of the contract period as shown in Figure 6. On the one hand, trust may increase when a relationship is established, work tasks successfully conducted, and services delivered on time. On the other hand, trust may erode if tasks and services are not conducted as expected. Moreover, trust is context dependent. It is therefore reasonable to believe at some point of time the trust will decrease because of an action or in-action, such as human error, cyberattack or neglected task fulfilment.

Based on the simulation in Figure 7, the number of cybersecurity incidents will increase. Outsourcing increases the complexity and number of stakeholders in the digital supply chain, which increases the attack surface, points of failures and thereby the probability of a cybersecurity incident. Examples of such incidents are unintentionally sharing sensitive information, lack of user control, or supply chain attacks.

RESULTS OF SCENARIO SIMULATIONS AND DISCUSSIONS

The simulations of the two scenarios are presented as graphs over a 15-month period. This summarizes the base run and the two scenarios to compare the results have been selected and explained in Table 2 and Table 3.

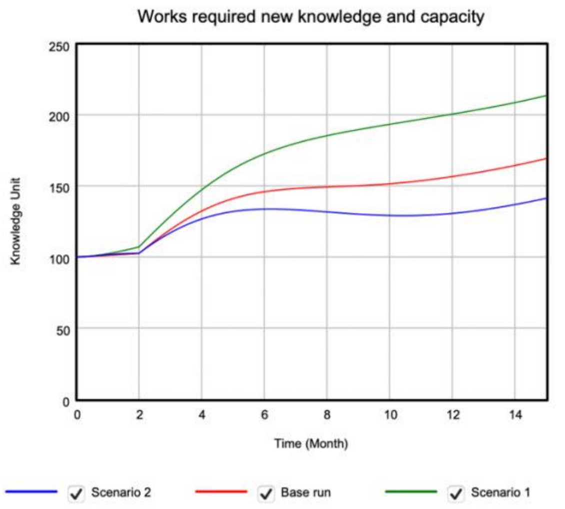


Figure 8. Simulations of Work Requiring New Knowledge and Capacity

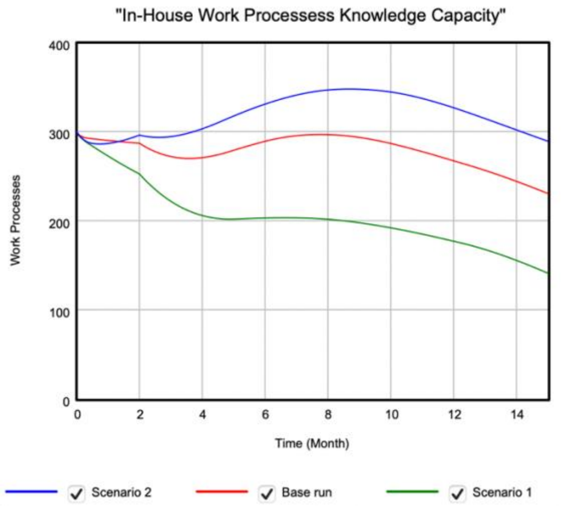


Figure 9. Simulations of In-House Process Knowledge Capacity

All three scenarios lead to an increase in work requiring new knowledge (Figure 8) since investing in digital services and devices are needed according to the expert group. However, for the outsourcing scenario, significantly more new knowledge is needed in terms of knowledge capacity compared to the normal scenario and the trust scenario. This is caused by the lack of in-house knowledge due to a limited availability of outsourcing and knowledge being distributed in the digital supply chain.

As shown in Figure 9, in-house work processes knowledge decreases in the outsource scenario because of limited outsourcing of services. This means that the organisation that outsource their core work processes will become more dependent on their supplier. The dependency constitutes a vulnerability as cybersecurity depends on the supplier's work processes. If the suppliers were to be exposed to a cyberattack or other disturbances, the organisation may struggle to maintain normal operations. The opposite effect is found in the first half of the trust scenario because of the stricter control and regulations with their suppliers. An explanation is that the organisation may invest time to understand the service provided by the supplier in an early phase. However, this knowledge may decrease over time as hardware and software is updated and features changed.

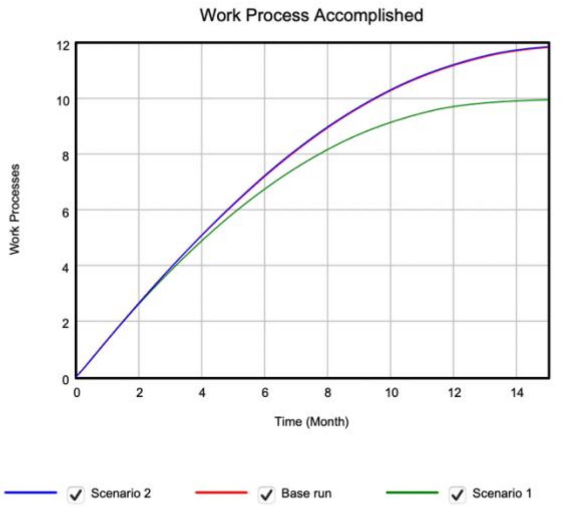


Figure 10. Simulations of Work Process Accomplished

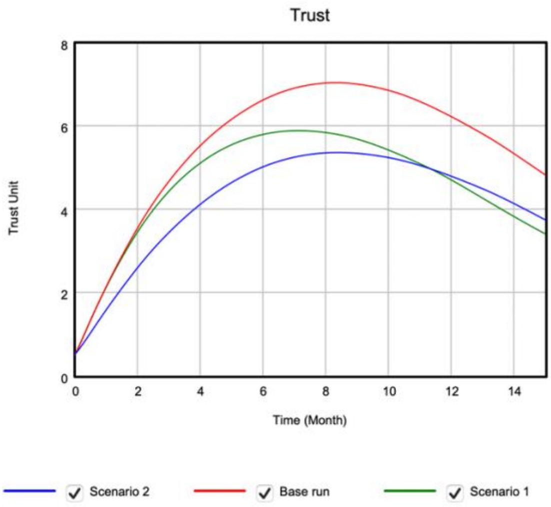


Figure 11. Simulations of Trust

Figure 10 simulates the work processes accomplished, where the base run and both scenarios follow a similar increase at the start. However, for the outsourcing scenario the increase slows down after 6 months since the limited outsourcing of services is delayed over time. The distributed work load in the outsourcing scenario takes longer to reach the end consumer compared to both the base line and the trust scenario because the in-house knowledge and capacity in the outsourcing scenario is limited.

In the trust scenario, the supplier control increases which can indicate that trust can be supplemented with other control mechanisms like auditing, or a service level agreement, as shown in Figure 11. The level of trust should be dynamically changing as the relationship evolves over the time of 15 months. By conducting an audit, the trust can increase again. However, for the outsourcing scenario there is already established trust to the supplier since there is limited activity of outsourcing and limited supplier control. Compared to the base run which today represent the digital supply chain's amount of trust. Some in the expert group say that the trust today should and could be replaced by some form of control mechanisms like auditing and closer communication throughout the contract phase with the supplier.

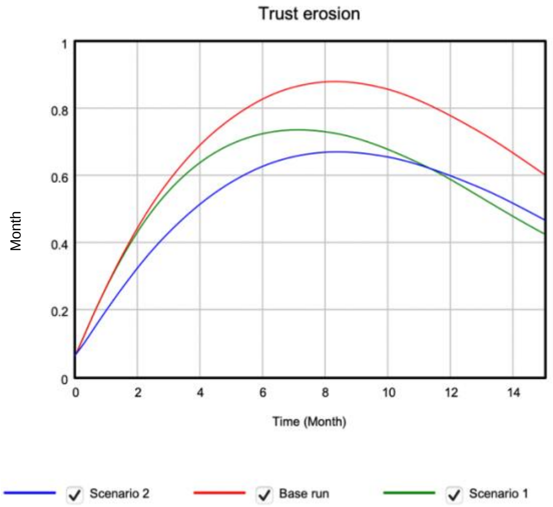


Figure 12. Simulations of Trust Erosion

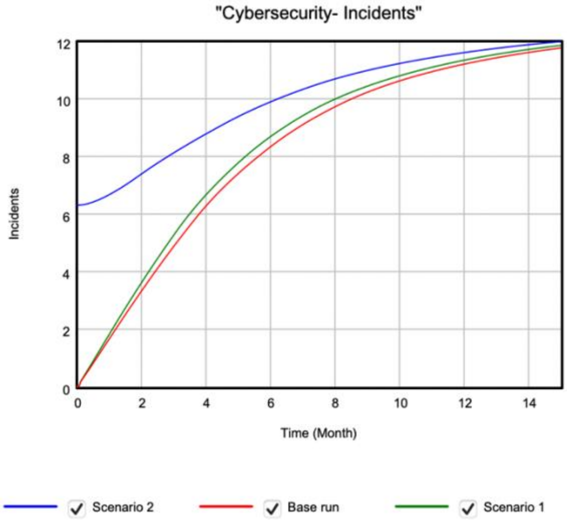


Figure 13. Simulations of Cybersecurity Incidents

Since relationships between suppliers in the digital supply chains is dynamically changing, the trust also erodes as shown in Figure 12. Comparing the scenarios in Figure 12 shows that trust erode quicker when it is not used as a control mechanism. For some organisation trust erode because of human error or cyberattacks. The initial phase after security incidents will affect the trust relationship. It can cause a more suspicious and awareness towards services from that supplier. Another reason for trust eroding could be delays in delivery of services. However, trust erosion may have a positive impact on cybersecurity if it leads to increased use of other control mechanisms. Trust erosion and trust shown in Figure 11 are very similar which indicate that erosion of trust over time is to be expected in digital supply chains.

Figure 13 shows that even though trust is used as a form of control over the suppliers, the number of cybersecurity incidents increase in all scenarios. This is related to the increased complexity and digitalisation in the digital supply chain because of more outsourcing, which in turn leads to more suppliers and an increased attack surface. Comparing the two scenarios shows that the number of incidents increase more in the outsourcing scenario than in the trust scenario because of the supplier control being stricter in the trust scenario than in the outsourcing scenario. Trust, although it is necessary, is also a vulnerability in the digital supply chain today.

For the outsourcing scenario, the consequence of restricting outsourcing reduces the overall productivity in the organisation. Also, the in-house competence decreases as there is no longer a flow of knowledge coming from outsourcing. Regardless of the outsourcing scenario, cybersecurity incident as shown in Figure 13 grows exponentially as in the trust scenario. This shows that although outsourcing constitutes a vulnerability by introducing more suppliers in a digital supply chain, it is required to meet the demands of reliable power supply from the society. The overall results give indications that the trust scenario is considered the best scenario of the two since the organisations can produce more, increase their in-house knowledge and at the same time be able to have enough resources to control and manage their suppliers. The scenarios also indicate that trust gives better productivity from Figure 10 but in terms of cybersecurity incidents the trust is contributing to the increasing number of incidents shown in Figure 13.

CONCLUSION

This article investigates the role of trust and outsourcing on cybersecurity in critical infrastructure and asks: *How can trust as part of a digital supply chain in critical infrastructure be modelled and simulated using system* *dynamics methods?* To answer the research question we used system dynamics methods to construct a causal loop diagram to understand cause and effects of trust and outsourcing. Based on interviews with an expert group from the power industry, a base run, an outsourcing scenario, and a trust scenario were created.

The expert group helped validate several of the variables included in the causal loop diagram. To achieve a more realistic representation, the simulation could have differentiated between dependency on the service provided by the supplier. It is important to point out that the chosen time to simulate have some limitations. For modelling reasons, it may be thought of as a simplification to assume that switching the provider within a year is feasible, as it may be quite challenging due to internal capacity and existing contracts.

The simulation for the outsourcing scenario demonstrates that, despite an overall gain in trust, the internal capacity of knowledge will be lower if the organisation's control over outsourcing is low. Out of the three scenarios, the outsourcing scenario is considered the least desirable one because of the lack of in-house competence, the low number of accomplished tasks complete over time, and the demand for new recourses and knowledge whenever new technology is introduced. On the other side, the trust scenario demonstrates that tighter control over trusted suppliers will result in better task completion. This scenario outperforms the base run and demonstrates that managing outsourcing is best done with supplier control.

Looking at the scenarios combined, we conclude that trust is key to avoid the negative impacts of outsourcing, namely loss of in-house knowledge and the ability to manage cyber events. In contrast to our expectation, trust may contribute to both generating in-house knowledge and to managing cyber events more effectively. However, outsourcing is a threat to in-house competence. It is the dependencies caused by outsourcing that impact the individual organisations' ability to manage cyber events. How companies choose to manage their information systems affects their ability to manage cybersecurity incidents. For instance, our simulation shows in Figure 9 that the in-house knowledge decreases, and the cybersecurity events increase in Figure 13. This may happen because of lacking knowledge on managing cyber incidents as well as the increase of the attack surface since more suppliers are included in the digital supply chain. In order for future owners of critical infrastructure to be resilient more knowledge is needed in order to managed future cyberattacks that continues to be more intangible especially for digital supply chains.

Since trust is essential for the digital supply chain to function, system dynamics can be used to study how trust affects cybersecurity in digital supply chains. An interesting path for future research is to introduce the concept of zero-trust to the simulation to study how it may affect the cybersecurity in a digital supply chain. Another point on the research agenda is looking further into how critical infrastructure owners can use a "trust score" as part of an overall risk assessment process to assess the risks associated with different suppliers within the digital supply chain. The score may allow them to identify suppliers who are considered unreliable and should be excluded. Critical infrastructure owners could also use a "trust score" as part of an overall risk assessment process to assess the risks associated with different suppliers within an existing digital supply chain.

ACKNOWLEDGMENTS

This research is supported by the Norwegian Research Council and NC-Spectrum AS. We would like to thank the participants from the industry for providing insightful information and supporting this work.

REFERENCES

Abdul-Rahman, A., & Hailes, S. (2000). Supporting trust in virtual communities. *Proceedings of the 33rd Hawaii International Conference on System Sciences*, pp. 1769-1777.

Agarwal, A., & Shankar, R. (2003). On-line trust building in e-enabled supply chain. *Suppy Chain Management: An International Journal, 8 (4)*, pp. 324-334.

Ageron, B., Bentahar, O., & Gunasekaran, A. (2020). Digital supply chain: Challenges and future directions. *Supply Chain Forum Int. J. 21 (3)*, pp. 133-138.

Arvidsson, B., Johansson, J., & Guldåker, N. (2021). Critical infrastrucure, geographical information science and risk governance: A systematic cross-field review. *Reliability Engineering and System Safety, 213*, p. 2021.

ENISA. (2021a). *Raising Awareness of Cybersecurity.* ENISA.

ENISA. (2021b). *Threat Landscape for Supply Chain Attacks.* EU: European Union Agency for Cybersecurity.

Forrester, W. J. (1997). Industrial Dynamics. *Journal of the Operational Research Society, 48(10)*, pp. 1037-1041.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly, 53 (4)*, pp. 1155-1175.

Hoshimov, A., Mahdavisharif, M., & Cagliano, C. A. (2021). Impacts of Digital Technologies on Supply Chain Performance: A System Dynamics Approach. *International Conference on Industrial Engineering and Operations Management* (pp. 5303-5314). Singapore: IEOM Soceity International.

Hussein, A., Elsawah, S., & Abbass, H. (2019). A System Dynamics Model for Human Trust in Automation under Speed and Accuracy Requirement. *Proceedings of the Human Factors and Ergonomics Society 2019 Annual Meeting*, pp. 822-827.

Khan, K. S., Shiwakoti, N., & Stasinopoulos, P. (2021). A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. *Accident Analysis and Prevention, 165*.

Laeequddin, M., Sahay, B. S., Sahay, V., & Waheed, K. A. (2012). Trust building in supply chain partners relationship: an integrated conceptual model. *Journal of Management Development, 31 (6)*, pp. 550-564.

Li, H., & Feng, J. (2022). Study on the Improvement Strategy of Trust Level between Owner and PMC Contractor Based on System Dynamics Model. *Buildings, 12 (1163)*.

Lin, F., Sung, Y., & Lo, Y. (2005). Effects of Trust Mechanisms on Supply-Chain Performance: A Multi-Agent Simulation Study. *International Journal of Electronic Commerce, 9 (4)*, pp. 91-112.

Mayer, C. R., Davis, H. J., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, Vol. 20, No.3*, pp. 709-734.

Meadows, H. D. (2008). *Thinking in Systems: A Primer.* London: Earthscan.

Microsoft. (2021). *Microsoft Digital Defense Report OCTOBER 2021.* Microsoft.

Nowicka, K. (2018). Trust in Digital Supply Chain Management. *Logistics and Transport, 39 (3)*, pp. 59-64.

Office of the Auditor General of Norway. (2021). *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen, Dok 3:7 (2020-2021).* Oslo: Riksrevisjonen.

Rinehart, K. A., Proud'homme, P. A., & Huot, R. A. (2014). Overwhelmed to action: digital preservation challenges at the under-resourced institution. *OCLC Systems & Services, 30 (1)*, pp. 28-42.

Ring, P., & Van de Ven, A. H. (1994). Developmental processes of cooperative interorganizational relationships. *Academy of Management Review, 19 (1)*, pp. 90-118.

Shin, J., Shin, W., & Lee, C. (2013). An energy security managment model using quality function deployment and system dynamics. *Energy Policy, Vol. 54*, pp. 72-86.

Sterman, J. D. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World.* New York, NY:McGraw-Hill: Massachusetts Insitute of Technology Engineering Systems Division.

Wang, Z., Ye, F., & Tan, H. K. (2014). Effects of managerial ties and trust on supply chain information sharing and supplier opportunism. *International Journal of Production Research, 52 (23)*, pp. 7046-7061.

Wu, Y., Gu, X., Tu, Z., & Zhang, Z. (2022). System dynamics analysis on industry-university-research institute synergetic innocation process based on knowledge flow. *Scientometrics, 127*, pp. 1317-1338.

Zaveri, P. (2015). Digital disaster management in libraries in India. *Library Hi Tech, 33 (2)*, pp. 230-244.

Zhang, H., Nakamura, T., & Sakurai, K. (2019). Security and Trust Issues on Digital Supply Chain. *IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, (pp. 338-343).

Zhang, X., Wang, H., Nan, J., Luo, Y., & Yi, Y. (2022). Modeling and Numerical Methods of Supply Chain Trust Network with the Complex Network. *Symmetry, 14(235)*.