Management and Production Engineering Review
Volume 8 • Number 4 • December 2017 • pp. 42–53
DOI: 10.1515/mper-2017-0035

A COMPREHENSIVE ASSESSMENT MODEL FOR CRITICAL INFRASTRUCTURE PROTECTION

Markus Häyhtiö, Klaus Zaerens

National Defence University Helsinki, Finland

Corresponding author:
Markus Häyhtiö
National Defence University Finland
Defence Acquisition
Helsinki, Finland
phone: +358-(0)45-1200304
e-mail: markus.hayhtio@kolumbus.fi

Received: 5 July 2017
Accepted: 16 November 2017

Abstract
International business demands seamless service and IT-infrastructure throughout the entire supply chain. However, dependencies between different parts of this vulnerable ecosystem form a fragile web. Assessment of the financial effects of any abnormalities in any part of the network is demanded in order to protect this network in a financially viable way. Contractual environment between the actors in a supply chain, different business domains and functions requires a management model, which enables a network wide protection for critical infrastructure. In this paper authors introduce such a model. It can be used to assess financial differences between centralized and decentralized protection of critical infrastructure. As an end result of this assessment business resilience to unknown threats can be improved across the entire supply chain.

Keywords
critical infrastructure, supply chains, capability management, risk management, cyber, service.

Introduction

The history of international trade is long. The role of globalization has steered development toward increasing global alignment of activities across countries, operations and market offerings [1]. Importance of international trade is tremendous for modern economies. A study conducted by the Bertelsmann Foundation's Global Economic Dynamics program [2] reveals the fact that one of the largest beneficiaries of the global trade was Finland with the annual gain in the income per capita of about €1500.

Despite the fact that international trade has deep roots, its significance has never been as great as it is now. Clear, positive effects of globalization as a mechanism to spread wealth cross borders have made it possible to create a web of enterprises that work closely together across the globe. But there is a downside to this: a global network of organizations working together increases the possibility of risks due to their dependency on inter-discipline information.

Protection of the critical components of the supply chain has to cover critical, recognized nods and most important production systems and their subsystems. Then again, as Lewis [3] points out, actors participating in supply chain management are commercial companies whose main purpose is to run commercially viable operations. Therefore Critical Infrastructure Protection (CIP) is not their first priority, but still an essential part of business due to its financial importance. Also, international trade expands its web so widely, that regional conflicts or crises are seldom a concern for other countries from any other point-of-view than commercial. These actors have streamlined their operations to the point that no back-up systems exist [3].

The supply chain systems' operations' four functions have to be analyzed across organizations. Ac-

cording to Beer [4], these four functions are implementation, coordination, control and intelligence.

In detail, these functions consist of:

1. Implementation consists of daily operations, which enable production of physical products and services.
2. The coordination function consists of the regulating system (task, authority, responsibilities), which is used to manage production operations.
3. The control function consists of supervision and management of the operations related to the implementation and coordination of production of physical goods and services.
4. Intelligence consists of functions relating to the adaptation of environmental changes.

Each one of these functions is built and run as a set of predefined processes. These processes are vulnerable to both uncertainties and risks. The protection of critical infrastructure requires thorough assessment of vulnerabilities and risks at process and individual component levels. Additionally, cross-functional operations require a set of abilities, which enable efficient management of operations and minimization of vulnerabilities and risks. As stated earlier, there is a need to assess all the parts of the business domain's supply chain and reflect the results to the pre-determined outcomes. Capability management as a management tool gives a clear structure for the definition process of risks. This provides a general picture and helps to concentrate on the relevant risks [5].

There are 2 research questions the authors are trying to answer in this paper:

1. What are the potential financial benefits of concentrating on prevention compared to the protection of the total supply chain?
2. Which capability indicators affect supply chain CIP operations?

The functionality of the model is assessed by collecting information from the actualized attacks against a recognized component, assessing and analyzing the time this attack was effective and analyzing its effects on the component's functionality.

A significant element in the analysis is the attack vector. The purpose of attack vector analysis is to assess how increased observation capability could minimize the attacker's effect on the target component, and compare the costs between centralized observation and systems wide observation. This enables cost benefit analysis between centralized and out-sourced service provision.

One has to notice that even though the attacker is stopped in time 0, there is the possibility of severe reputation loss, which has possible negative financial effects, even though the threat did not become a reality.

All the elements affecting CIP are illustrated in the Appendix 1.

The paper proceeds as follows. First, we will examine the uncertainty in the service networks and describe the elements of domain assessment in CIP. Next, we address the problem of unknown threat that exists in contractual environment of CIP. Lastly, we propose an approach for improving business resilience to overcome the problems described. We will conclude with key findings and a proposition of the future research.

Uncertainty in the service networks

Uncertainty is defined as "the difference between the amount of information required to perform the task and the amount of information already possessed by that organization." [6, p. 5] With risk we refer to the possible outcomes of an action, specifically to the loss that might be incurred if a given action is not taken [7]. A risk combines two attributes i.e. probability and impact. Probability is a measure of how often a detrimental event, which results in a loss, occurs. Impact refers to the significance of that loss to the organization. The level of risk is then perceived as the likelihood of occurrence of a detrimental event and the significance (impact) of that event [8, p. 397). Time should be considered as a variable in each analysis, and the effect time has on vulnerability and risks should be analyzed thoroughly.

There are a few assumptions we have to make in order to discuss the matter. The first assumption is that a structure of network organizations and processes is referred to as a service ecosystem. It describes the inter-functional and multidiscipline nature of service oriented industries and operations. The second assumption is that supply chain management is a part of the service industry. In their widely cited article, Vargo and Lush [9] introduce a theory of service dominant logic, the main point of which is a transition from goods based exchange to an economy based on more specialized skills and knowledge. The authors follow the approach of the Nordic School of Marketing [10] and Service-Dominant Logic (S-D logic) [9]. This approach was selected due to its emphasis on end-user preferences, which is a widely accepted method of developing and researching services.

At the core of the S-D logic is the shift from an emphasis on the traditional goods based, tangible resources to dynamic resources, which act together with other resources. Vargo and Lusch [9] refer to

these resources as operand and operant resources, respectively. Because supply chain management is highly dependent on the IT-infrastructure, there is an obvious need to manage the capabilities for running the whole system of supply chain value creation. As Vargo and Lusch state, these arrangements need coordination and co-creation.

One of the foundational premises (FPs) of service dominant logic (S-D) is:

"Value co-creation is coordinated through actor-generated institutions and institutional arrangements" [9, p. 7].

Thus, the third assumption the authors make, is that much of the supply chain management is run and managed through automated systems without social interaction. Despite this fact, these automated systems are created by humans, whose approach to the system is connected to the social environment it is developed in. This approach, which is widely used among the social sciences, is interested in the relationships between individuals and larger groups.

Social networks have significant importance to the success of supply chain operations. Uncertainty is defined, managed and accepted within the boundaries of a specific social network. Therefore every organization can reduce uncertainty by obtaining possession of critical assets and forming ties with stakeholders who are more specialized in a specific operation within their social network [11].

A systems based approach to one's identity introduced by [12] has been a topic influencing both educational and social sciences. This topic cannot be ignored when researching an area as complex as supply chain management, since we are not immune to the effects of either the cultural or social environments surrounding us.

Risk management strategies are not as straightforward as they may seem to be at first sight. Firstly, because supply chains are, as stated earlier, dependent on several systems, there is a need to analyze each system thoroughly in order to assess the correct approach to the risks and vulnerabilities of each of the systems. Secondly, time should be considered as a variable in each analysis, and the effect time has on vulnerability and risks should be analyzed thoroughly.

Domain assessment

Critical infrastructure is divided into three levels. The most important level consists of the information technology industry, energy sector and water supply industry. The second level consists of the banking and finance sector, and the chemical industry sector. The third level is formed by the armaments industry, postal- and distribution services, agriculture and food supply chains, health care, and search and rescue services [3, 13]. Domain assessment should be divided into three time-related phases: observation, comprehension and prediction [14].

The four functions of the supply chain systems' operations have to be analyzed across the domains the organizations operate in. Our approach has been adapted from the principles introduced by Skyttner [15].

The first and the most important assessment covers the way capabilities are managed within recognized, critical management areas. During the assessment work, the organization's ability to create valid input information, which enables necessary vulnerability analysis, has to be covered. Secondly, there has to be the capability to store that valid information in a way that meets the requirements for the protection of critical infrastructure. Thirdly, the capability to manage the organ, which uses the valid information, has to be assessed. Fourthly, an organization has to have the capability to predict and create scenarios, which require valid information. And lastly an organization has to have the capability to manage feedback information, and most of all, manage the pre-determined operations based on the scenarios.

In the second domain, an organization's capability to manage the contractual environment by using the methods, which take in to account the needs of end-user and the needs of the whole of the supply chain as a system, has to be assessed.

In the third domain, an organization's capability to manage the carrying capacity and capability to secure the alternative methods of transportation and suppliers of vital goods and services for the organization has to be assessed.

In the fourth domain, an organization's capability to manage the alternative and existing data transportation methods under all conditions has to be assessed.

In the last domain, the enhancement of the capability to react to rapidly changing political, social, environmental, legal and technological changes has to be assessed. This relates more to the first domain. The connections between functions and domain are illustrated in Appendix 2.

But how do we define a relevant risk in each of the domains? How do we decide which part of the supply chain creates a critical node? How do we divide a system and its sub-systems into manageable components, without sacrificing the overall purpose of the system? How do we define the capabilities,

which need to be met? How do we prevent a situation in which the "tail wags the dog", meaning that the risk preventing process defines the outcome and not vice versa? There has to be a managerial approach, a methodology, which sets a framework for capability management.

The initial goal of domain assessment is to define and create capabilities, which enable recognition of an attack and reduce the attacker's ability to operate in the target component. Observation and protection are reactive functions, which affect the overall costs.

Contractual environment

The capability to manage contractual environment processes requires a set of pre-defined capabilities. As Anteroinen [16, p. 13] states:

"... capability is the ability or power to achieve a desired operational effect in a selected environment and to sustain this effect for a designated period".

This definition does not determine how the objective should be achieved. The definition also takes into account how domain operations are run.

In the assessment of relationships between the domains and functions the authors limited their scope. During the research the scope was limited to domain 2 ("capability to manage contractual environment") and to function 2, which defines the management and supervision of the production process.

In the modern network based service chains, the commercial co-operation between the actors in the service supply chain is regulated with contracts. Contract management is divided into two major approaches. The first one concentrates on the structural design of the agreed transaction. The main focus of this approach is on the written contracts between different participating parties. These agreements are legally binding by nature [17, p. 241].

The second approach is more concerned with the relationships between the actors participating in the commercial co-operation. The main factor, participating parties rely on, is trust, which works as a safeguard for coordination and control functions. The upside of participants in this approach is the positive outcome of the transaction in spite of the existing and possible vulnerability [18, p. 395).

There are existing studies, which combine these two approaches, but their results are not clear-cut. One of the main reasons behind these results is the complexity of the contracts in the framework of trust. Even though one of the basic principles of S-D logic emphasizes institutional arrangements, it does not define which one of the approaches should be used for contractual management.

As the authors stated, the supply chain for a service ecosystem consists of several systems and subsystems. The capability to manage all the interrelating contracts within an ecosystem can become extremely expensive if the structural approach is used. Also, just a trust-based approach is hardly acceptable. We are after all researching the critical infrastructure, whose vulnerability cannot be protected only with the element of trust.

There are also examples of reciprocal-trust relationships which are based on the mutually positive out-comes, based on the actions active parties make [19]. This model does not take into account the possible role of third parties trying to take advantage of the two parties, who have created a reciprocal-trust relationship. Also, the reciprocal altruism introduced, among others by Trivers, [20] already in 1971 demands several and repeated interactions with known actors.

These contractual choices are obviously linked to the industry in question, which affects the criticality of the industry and possibly the already existing relationships between the actors within the industry. Contractual management should also consider the time-related phase observation, comprehension and prediction the critical process is related to. The four organizational functions – implementation, coordination, control and intelligence – need a thorough assessment from the contractual management point of view as well. These decisions are affected by the cultural, political and economic factors, as the main theories of international trade illustrate.

Contractual environment and an unknown threat

We approach the challenges in a contractual environment by observing two real life cases. In both cases we present partially successful cyber-attacks and discuss the deficiencies of situational awareness in a business ecosystem. The described sophisticated attacks were successful because of their unidentified nature and development resources behind new technology. Since there is always the possibility for an unknown threat, we endeavor to present a model managing the risk it produces.

The chapter is organized as follows. First we define the concept of an unknown threat. After that we present the two cyber-attack cases, and finally we analyze the cases in relation to contractual environment.

Unknown threat

An unknown threat is defined as a threat, which is not previously known, there is a theoretical background for the existence of this threat, there are no previously known counter measures against the threat or there are no known identification methods for the threat.

These threats include:

- 0-day vulnerabilities,
- tailored, effective based malicious operations,
- complex attacks against the targeted physical part of the component/system,
- APTs, Advanced Persistent Threats that combine all of the above and include significant resources for transforming the behavior of malicious activity.

Case of Industrial Espionage

Our first case contains a modern industrial espionage. The target of the attack was the immaterial capital of a large enterprise in the manufacturing sector that operates in the Nordic geo region. The details of the attack are classified. The information used here is retrieved through an interview with Jan Mickos [21], Vice-president, CGI Finland Security Advisory (May 23, 2017), and can also be viewed in public sources.

Attack description

The perpetrators of the attack campaigns are referred to as "APT 10" and "APT 29", which are explained in more detail [22] and [23]. The technical methodology used in the attack was fairly common. Previously known malware was slightly altered so it would not be exposed by normal antivirus scanners nor would it be blocked by technical security protection solutions. The adversary used a lot of time, resources and effort to cover the tracks of their actions and hide from defensive scanners and monitors. One particular feature of the attack was the ability to change the maneuvers, which ensured the stable progression of the attack towards its goal.

The attack was also special in its tactical dimension. It was aimed indirectly at the target via a common ICT service provider. This enabled two advantages. First, it is nearly impossible for an ICT service provider to identify malicious actions, since the traffic in the command and control (CnC) channel was hidden under the normal noise of enterprise activity. Second, even if the targeted enterprise would have noticed any abnormalities, it has no visibility or jurisdiction to the technical environment of the ICT service provider. As a side effect to the primary target, the attacker was able to create an entry point into other customers' systems through the same ICT service provider.

Time dimension of the attack

The attack was exposed in the target environment in 2016. In a forensic investigation, the first traces of CnC were found to be from 2013. Any information from before this could not be reconstructed. It took around four months to block the attacker from the targeted system after exposure. That time was used for identifying the coverage of the attack, creating sufficient counter measures and collecting enough information for forensic analysis.

During the four years of attack, the attacker gradually collected information from the target environment, increased the compromised systems and components and proceeded towards the target. It is assumed that the attacker did not reach the ultimate target.

After successful coordination of counter measures and blocking the vulnerabilities of the systems it has been noticed, that the attacker has resumed a similar campaign towards the target enterprise via another service provider. This implies two results. First, the unknown threat has changed into a known threat and exposing new attempts are significantly faster. Secondly, a motivated attacker does not quit trying to reach the ultimate goal after the first obstacle. Instead, the attacker searches for another vulnerable component to continue the original campaign.

Speculating on the possible consequences of an attacker reaching the goal of immaterial capital, we can take the famous Nortel case as an example. The attack on Nortel proceeded unobserved for ten years [24]. In practice, the attacker was in control of the whole ICT environment of Nortel. As an indirect consequence of losing the immaterial capital and exposing business plans to competitors, the market value of Nortel dropped 98% in only two years, ending up in Canada's greatest bankruptcy of all time [25].

Case WannaCry Campaign

Quite a recent example of a cyber-attack is from May 2017; the case is called WannaCry ransom ware [26].

This campaign had several unprofessional features and because to them, direct damages were relatively small. However, indirect damages were notable. It disrupted normal functions of several critical infrastructure systems all over the world, including hospitals and traffic. It was fortunate for the societies that the attackers' goal was only to deploy ransom ware and collect ransom instead of destroying the compromised ICT systems or stealing the information that was accessed.

In the scope of this paper, WannaCry campaign had two interesting features. The first interesting fea-

ture was the speed of contamination of the systems. The previous example campaign was active for several years. This campaign was only active for days. The progress speed was so rapid that the analysis and counter measures of a single system took too much time to be effective. The blocking actions were only successful because of information exchange between security specialists across organizational and geological boundaries, and centralized blocking actions.

The second interesting feature was the methodology used in the campaign. It utilized the technology developed by the National Security Agency, USA (NSA), which was leaked to the public earlier. Despite that the mechanisms were known before the attack, there was a large amount of compromised systems worldwide. As a consequence, one can never trust or assume that the supply chain or the subcontractor has implemented the full preventive toolset for known threats. Furthermore, it is evident that the unknown threats are even less likely being monitored.

Analysis of the case

In both cases, the attack was blocked by centralized and coordinated actions. To obligate the supply chain node or the subcontractor to monitor systems preventing advanced and persistent type campaigns is nearly an impossible task. Only the one, that manages the environment as a whole and understands the possible goals of an attacker and also carries the business risk, can evaluate the differences and abnormalities of actions in a complex system environment.

We have also observed from empirical data of less public campaigns that the value of damage changes with time as follows [21]:

- the financial/business damage development follows a time-based logarithmic formula:
  - time 0 is the attacker's penetration into the component/system,
  - time 1 is the time the actual damage driven action begins,
  - between 0 and 1 the attacker prepares the actual damage enabling action, such as intelligence and creation of necessary command functions,
  - onward from time 1 there is increasing damage to the component in relation to the maximum value of the component to the whole business value of the operations;
- the value of damage increases exponentially in the relation to time:
  - effects in the individual component reflect to the whole system and increase the overall damage and financial loss.

Improving business resilience to unknown threats

Inspired by the case example presented in the previous chapters, the purpose of the improvement of resilience to unknown threats is to create a model, which tries to take into account the previously unrecognized threat to the specific business. The approximation in the model is based on the previous work by Zaerens [27], which showed the necessity to analyze financial impacts of threat prevention.

In this assessment, the authors are limiting their research to the main owner of the business. Also, an individual component under the research is not necessarily a technical phenomenon or a part of the IT-system. Depending on the business environment, the component can be a technical phenomenon, a business concept or a business driven phenomenon such as customer value creation. The main owner in the model is a company/function, which offers the final product to the end-user.

The observations in the model are based on either the sensor-based observation or on the log-based observation. Based on this definition, the only restriction to observation is the components ability to create material for analyzing purposes. This material is produced by the sensor and it can be technical, automatic or based on human interaction.

Each system component has to have a sensor, which collects information for observation purposes. This is illustrated in formula 1, a cluster of components in the system $sens_j$ in which $j \in [1,\ S]$ and S equal the amount of components in the system.

The sensor's ability to observe the threat can be assessed by using relative probability $1/w$, where w equals the coverage of information relating to the unknown threat.

In the worst case scenario, information is not collected at all and the possibility to react to the threat is non-existent. Threat observation is divided into ten operations within four previously introduced functions; the operations are managed as a part of operations management, using recognized capabilities.

The sensor's capability to reduce the unknown threat is presented in formula 2 developed by Zaerens in his previous research (Zaerens, 2015)

$$R_n = f(P(\text{threat}\, i_1 * (1/w_{\text{sens}[1]})), \ldots, P(\text{threat}\, n_s * (1/w_{\text{sens}[s]}))).$$

In order to clarify the topic, the authors defined the attack vector as a function, whose purpose is to fulfil the threat. The assumption is that the attack vector has a linear relationship with the threat. This

excludes surveillance activities, whose purpose is to define possible existing vulnerabilities in the target component.

Sensor activity is a constant, on-going function, which requires continuous sensor development in order to manage threat observation. This demands investments from the sensor throughout its lifecycle. This life-cycle cost is usually estimated to be 10 % of the initial investment. This enables life-cycle estimation as follows:

$$c_{\text{sens}} = d(1 + 0,1tw),$$

in which d – initial investment, t – time, w – a relative data collection ability in a specific sensor.

Even though these formulae increase a sensor's effectiveness against the threat, they do not take the costs, which are related to data analysis, into account. Obviously threat reduction is possible only, if the collected data collected from the sensor is analyzed. To simplify our approach we assume that the collected data contains sufficient data for exposing the attack.

Decentralized component based analysis can be described as a system where a real-time function of some predefined rule catches an anomaly or an exception. Component based cost analysis can be calculated using the following formula 4

$$h_{\text{sens[w]}},$$

in which h – cost of the analysis by individual component w used.

We assume that the size of the rule set in component analysis does not affect the actual cost of the analysis. The effectiveness of component based analysis is reduced, if the area under observation is not restricted and its interphases to business processes are not defined adequately. Moreover, the real time observation significantly decreases the possibility for detecting attacks that have been going on for a long duration (e.g. APT type of campaigns).

Financial effects of the centralized approach can be calculated using the following formula 5. This concentrated analysis estimates information from several sensors and their interdependencies. The cost of the analysis is not solely based on the amount of sensor; it is based on average threat coverage

$$C_{\text{analysis}} = h\left(\left(\sum_{i=1}^{\text{sens[n]}} w_{\text{sens[i]}}\right) \Big/ n + \sum_{i=1}^{\text{sens[n]}} i\right),$$

in which h – cost of the analysis, n – amount of sensors.

The effectiveness of the analysis increases when the amount of information from sensors increases.

Instead of centralized monitoring, having each component implemented with its own monitoring capability, the total cost of analysis of the system is the sum of all sensor and analysis costs from each partial component in the system. It is evident that even if the amount of sensors would be greater in some of the outsourced components, the overall effectivity of analysis significantly lacks business related information. Therefore the cost-effectivity ratio is better for centralized systems rather than distributed systems.

Discussion

Dialogue between the supply chain stakeholders does not jeopardize the risk management procedures of a supply chain, quite the opposite. It creates a solid base for understanding the system's stakeholders and their needs throughout the different life cycles of a supply chain. Maglio, Srinivasan, Kreulen, and Spohrer [28] envision that service scientists could begin to understand service systems by identifying stakeholders and their needs, opportunities and problems in the environment. Theories behind the service science need to be analyzed during development work. It should be done due to the fact that capability management requires open multidiscipline dialogue between different disciplines and functions.

Looking at the five operational domains, it becomes evident, that the assessment of an individual domain, process or a single actor's CIP capability is not adequate. There is a need to find those processes, which have the largest number of interfaces with each of the domains and the whole ecosystem. This should be the end result of an effective, centrally controlled surveillance activity.

As our research indicates, comprehensive, systems-wide protection can become extremely expensive. There are two questions, which arise from this conclusion. The first question is: who is responsible for the investments holistic protection demands? Secondly, what is the alternative cost for ecosystem-wide protection? One can ask if a main company should invest in tracking and control functions, instead of a "bullet proofed", ecosystem-wide active protection.

The role of a contractual agreement should be seen as an assumption of the future state of the CIP, not as a boundary between the actors participating in the service supply chain. Contractual agreements should be formed following the principles used in the performance based logistics (PBL).

In the PBL, responsibility of the product/service system management is on the supplier of the system, unlike in the traditional end-user – supplier relationship [29]. PBL is in use in military context and it is "a contractual mechanism".

Berkowitz explains that

"... [a] contractual mechanisms will include long-term relationships and appropriately structured incentives with service providers..., to support the end user's (warfighter's) objectives." [30, p. 5].

This approach does not contradict with the idea of the centralized surveillance and monitoring system. Centralized monitoring and surveillance activities should be used to secure both adequate CIP and a source for the PBL incentives. Also, requirements based PBL emphasizes the positive sides of the structural and trust based contractual management. The existing incentives encourage a service provider to fulfil pre-determined service goals, as research by Doerr, Lewis and Eaton [31] has shown, because these benefits are accountable and reliably measurable.

Limitations of the study

As mentioned before, this paper is limited according the public information available. Attacked organizations are reluctant to comment the success rates or the damage impact of attacks even if they are known. This ensures the preservation of their reputation and trust relations in the economic systems they participate in. The damages of successful attacks, that are publicly known, are underrated without exception [32, 33]. It is notable that attacks are not made public, unless a third party brings the information to attention.

Recommendation for future research

An interesting research area would be to model the progression of an attack in relation to time. This enables the analysis of the timeframe in which the attacker could theoretically reach the business's critical information after entering the system. This kind of a model would assist in estimating the available time for countermeasures or the collection of forensic information and analysis of attack progression.

Conclusions

Combining the systems wide approach and explaining the theoretical background behind the various models creates a comprehensive model, which assists in critical infrastructure protection. It shows that individual supply chains are a collection of extremely complex systems and subsystems backed up with sometimes contradicting theories and practices.

Current global trading operates in an environment, which is highly vulnerable to abnormalities in all parts of the supply chain. During a value creation process, an IT-infrastructure (a cyber-system) is dependent on five basic components:

1. input information, which reflects the reality of the surrounding world,
2. stored data of the existing reality to help decision making processes,
3. information stimulating the "organ" (human, machine), which in turn affects and stimulates the system,
4. data referring to the desired future state of the system,
5. feedback information regarding the desired outcome of the system or parts of the subsystem [34, p. 11].

All of the organizational functions – implementation, coordination, control and intelligence – across the system and relating subsystems are dependent upon the five components presented above. Each of the five components is subject to vulnerability and risk. This requires a description of the capabilities, which are needed to manage both functions and basic components of system wide vulnerability and risk management. Without these descriptions there is no possibility to calculate the financial effects of CIP.

Because a supply chain consists of a large number of multinational actors, each one of these players is potentially a critical node due to efficiency requirements defined by financial requirements. But unless an individual node affects pre-determined critical processes in the critical domain, a total collapse of the supply chain is not foreseeable. But there is a need for a systematic method, which enables the assessment of entire systems and their subsystems.

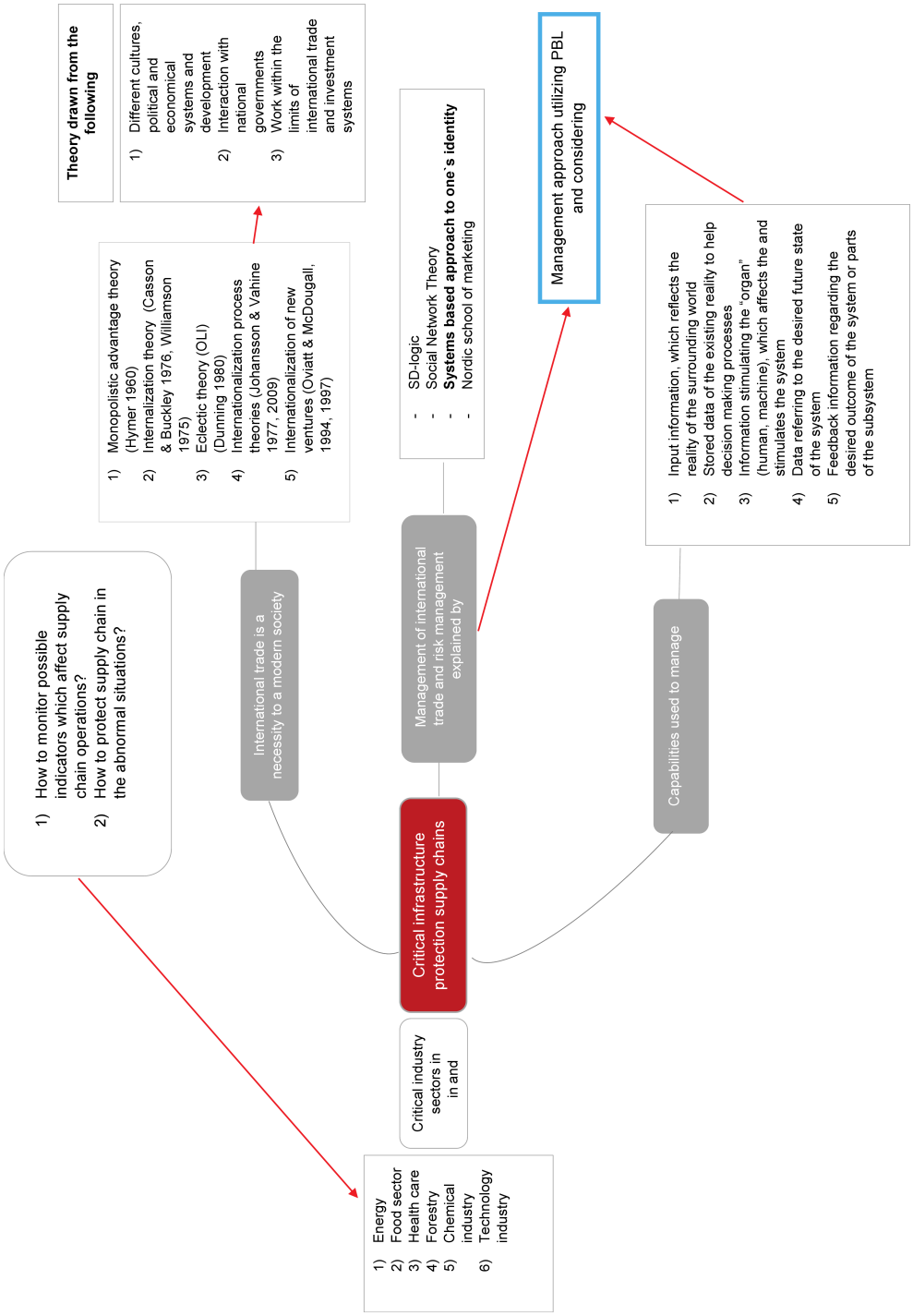
The authors have come to the conclusion, that the principles of cyber protection illustrated by i.a. Kuusisto [34], can be followed in commercial supply chain management. The following IT-infrastructure capability areas should be monitored, protected and secured thoroughly only if the benefits are on a financially acceptable level:

1. the capability to create valid input information, which enables necessary vulnerability analysis,
2. the capability to store said valid information in a way that it meets the requirements for the protection of the supply chain,
3. the capability to manage the organ, which uses the valid information,
4. the capability to predict and create scenarios, which require valid information,
5. the capability to manage feedback information and most of all, manage the pre-determined operations based on the scenarios.

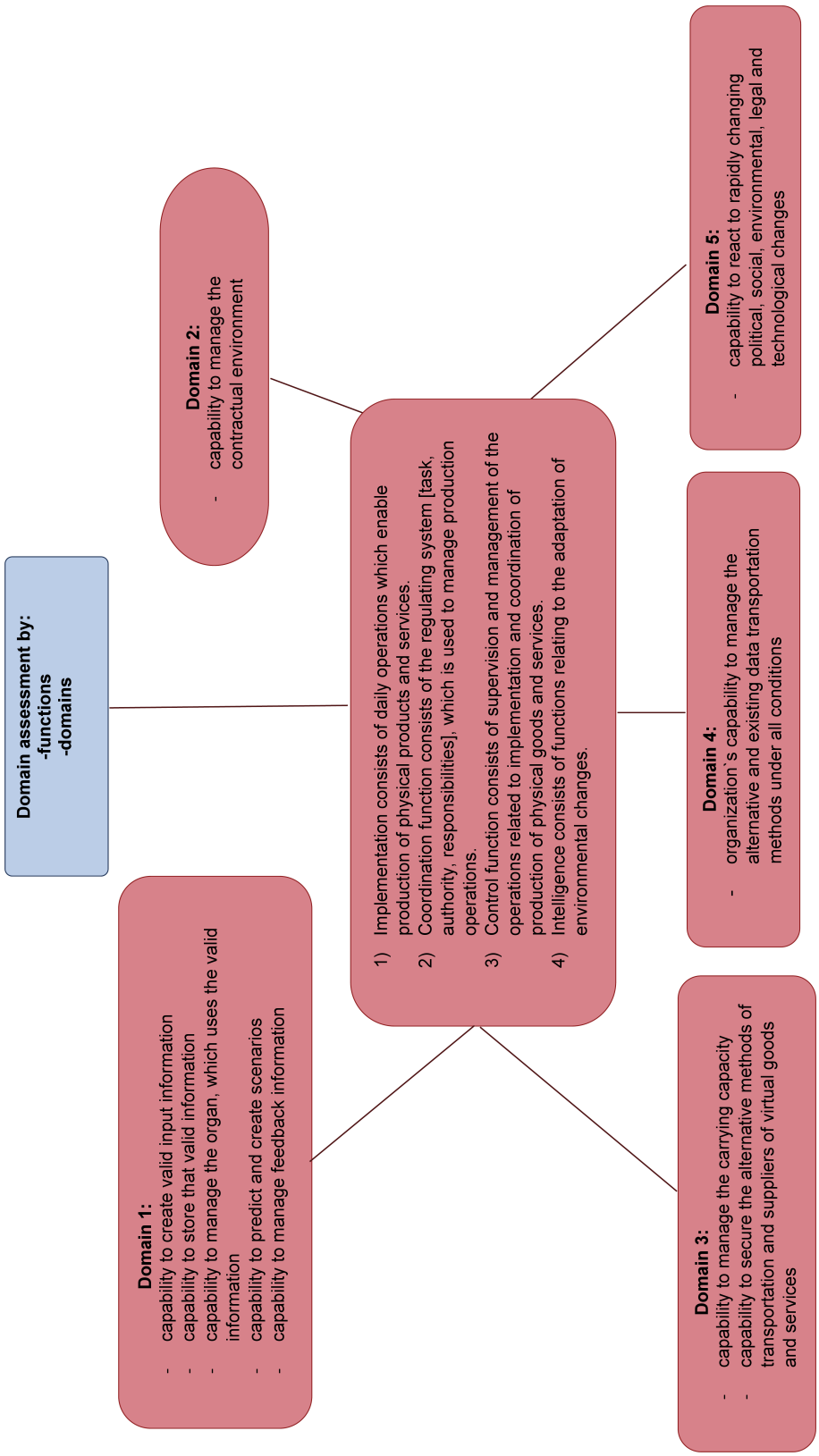
In this paper we examined the domain assessment within the critical infrastructure protection. We stat-

ed that business ecosystem environment that contains supply chains or subcontracting is vulnerable for unknown threat. Yet we noted that distributed ecosystem can increase the resilience in operation with careful contractual management. We described the model that quantifies the key elements that are used in observing the malicious intrusions to business system. We also proposed what needs to be taken into consideration in enhancing more resilient business ecosystem.

Appendix 1. Framework for Critical Infrastructure Protection



Appendix 2. Domain Assessment model



This work has been partially supported by CGI Finland (http://www.CGI.com/), with particular support from Jan Mickos. His contribution to determining the analysis on unknown threats is appreciated.

References

[1] Laanti R., Gabrielsson M., Gabrielsson P., *The globalization strategies of business-to-business born global firms in the wireless technology industry*, Industrial Marketing Management, 36, 8, 1104–1117, 2007.

[2] Bertelsmann Foundation, *Globalization Gains for Developed Countries Outpace Those for Emerging Nations* Retrieved June 15, 2016, from http://www.bfna.org/article/globalization-gains-for-developed-countries-outpace-those-for-emerging-nations

[3] Lewis T.G., *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley & Sons, 2014.

[4] Beer R.D., *A dynamical systems perspective on agent-environment interaction*, Artificial Intelligence, 72, 1, 173–215, 1995.

[5] Teller J., Kock A., Gemünden H.G., *Risk management in project portfolios is more than managing project risks: a contingency perspective on risk management*, Project Management Journal, 45, 4, 67–80, 2014.

[6] Galbraith J.R., *Designing complex organizations*, Addison-Wesley Longman Publishing Co., Inc., 1973.

[7] Liesch P.W., Welch L.S., Buckley P.J., *Risk and uncertainty in internationalisation and international entrepreneurship studies*, Management International Review, 51, 6, 851–873, 2011.

[8] Zsidisin G.A. et al., *An analysis of supply risk assessment techniques*, International Journal of Physical Distribution & Logistics Management, 34, 5, 397–413, 2004.

[9] Vargo S.L., Lusch R.F., *Service-dominant logic: continuing the evolution*, Journal of the Academy of Marketing Science, 36, 1, 1–10, 2008.

[10] Grönroos C., *Marketing as promise management: regaining customer management for marketing*, Journal of Business & Industrial Marketing, 24, 5/6, 351–359, 2009.

[11] Hoffman M.L., *Empathy and moral development: implications for caring and justice*, Cambridge University Press, 2001.

[12] Bronfenbrenner U., *Ecology of the family as a context for human development: research perspectives*, Developmental Psychology, 22, 6, 723, 1986.

[13] Horsmanheimo S., Kokkoniemi-Tarkkanen H., Kusela P., Tuomimäki L., Puuska S., Vankka J., *Kriittisen infrastruktuurin tilannetietoisuus*, Valtioneuvoston Selvitys- ja Tutkimustoiminnan Julkaisusarja, 19, 2017.

[14] Endsley M.R., *Toward a theory of situation awareness in dynamic systems*, Human Factors: the Journal of the Human Factors and Ergonomics Society, 37, 1, 32–64, 1995.

[15] Skyttner L., *General systems theory: problems, perspectives, practice*, World Scientific, 2005.

[16] Anteroinen J., *Enhancing the development of military capabilities by a systems approach*, Maanpuolustuskorkeakoulu, 2013.

[17] Lyons B., Mehta J., *Contracts, opportunism and trust: self-interest and social orientation*, Cambridge Journal of Economics, 21, 2, 239–257, 1997.

[18] Rousseau D.M., Sitkin S.B., Burt R.S., Camerer C., *Not so different after all: a cross-discipline view of trust*, Academy of Management Review, 23, 3, 393–404, 1998.

[19] McCabe K.A., Rigdon M.L., Smith V.L., *Positive reciprocity and intentions in trust games*, Journal of Economic Behavior & Organization, 52, 2, 267–275, 2003.

[20] Trivers R.L., *The evolution of reciprocal altruism*, The Quarterly Eeview of Biology, 46, 1, 35–57, 1971.

[21] Mickos J., Interview, March 23.

[22] BAE systems threat research blog. Retrieved June 3rd, 2017 from: http://baesystemsai.blogspot.se/2017/04/apt10-operation-cloud-hopper_3.html. [Accessed 3 Jun. 2017].

[23] FireEye, *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*, FireEye Threat Intelligence, Special Report, 2015.

[24] Naraine R., *Nortel hacking attack went unnoticed for almost 10 years*, [online] ZDNet. Retrieved June 3rd, 2017, from http://www.zdnet.com/article/nortel-hacking-attack-went-unnoticed-for-almost-10-years, 2012.

[25] Reuters, *TIMELINE: Key dates in the history of Nortel*, Reuters TECHNOLOGY NEWS, 14.1.2009. Retrieved July 1st, 2017 from http://www.reuters.com/article/us-nortel-timeline-sb-idUSTRE50D3N120090115.

[26] US-CERT, *U.S. Department of Homeland Security: Alert Report*, Retrieved May 27th, from https://www.us-cert.gov/ncas, 2017.

[27] Zaerens K., *Business Resilient Vulnerability Analysis for Dynamic High Security Environment*, 18th International Conference on Network-Based Information Systems, 2015.

[28] Maglio P.P., Srinivasan S., Kreulen J.T., Spohrer J., *Service systems, service scientists, SSME, and innovation*, Communications of the ACM, 49, 7, 81–85, 2006.

[29] Randall W.S., Pohlen T.L., Hanna J.B., *Evolving a theory of performance-based logistics using insights from service dominant logic*, Journal of Business Logistics, 31, 2, 35–61, 2010.

[30] Berkowitz D., Gupta J.N., Simpson J.T., McWilliams J., Delayne L., Brown B., Sparks T., *Performance Based Logistics*, Center for the Management of Science and Technology, Huntsville, AL, 2003.

[31] Doerr K., Lewis I., Eaton D.R., *Measurement issues in performance-based logistics*, Journal of Public Procurement, 5, 2, 164, 2005.

[32] ForMin Finland, *Tietoturvaloukkaus Suomen ulkoasiainhallinnossa – Ulkoasiainministeriö: Ajankohtaista*, Retrieved June 3rd, from http://formin.finland.fi/public/default.aspx?contentid=291701&contentlan=1&culture=fi-FI, 2013.

[33] Yle Uutiset, *Supo: Ulkoministeriö joutui kaksi kertaa vakoilun kohteeksi*, Retrieved June 3rd, from http://yle.fi/uutiset/3-7332824, 2014.

[34] Kuusisto T., *Kybertaistelu 2020*, Julkaisusarja 2: Asiatietoa, No. 1/2014.

In the appenpendices

Buckley P.J., Casson M., *Future of the multinational enterprise*. Springer, 1976.

Dunning J.H., *Toward an eclectic theory of international production: some empirical tests*, Journal of International Business Studies, 11, 1, 9–31, 1980.

Henriques I., Sanjay Sharma, *Pathways of stakeholder influence in the Canadian forestry industry*, Business Strategy and the Environment, 14, 6, 384–398, 2005.

Johanson J., Vahlne J.E., *The Uppsala internationalization process model revisited: from liability of foreignness to liability of outsidership*, Journal of International Business Studies, 40, 9, 1411–1431, 2009.