Applying Soft Systems Methodology to Complex Problem Situations in Critical Infrastructures: The CS-AWARE Case Study

Veronika Kupfersberger*, Thomas Schaberreiter*, Chris Wills†, Gerald Quirchmayr* and Juha Röning‡
*Faculty of Computer Science
University of Vienna (Vienna, Austria)
e-mail: veronika.kupfersberger@univie.ac.at
e-mail: thomas.schaberreiter@univie.ac.at
e-mail: gerald.quirchmayr@univie.ac.at
†CARIS Research Ltd. (Fowey, United Kingdom)
e-mail: ccwills@carisresearch.co.uk
‡Faculty of Information Technology and Electrical Engineering
University of Oulu (Oulu, Finland)
e-mail: juha.roning@oulu.fi

Abstract—**Modern technology, in addition to all its benefits, creates new threats and attack vectors to individuals and organisations. In the past years, the number of cyber attacks has increased drastically as has the extent of their effects. These circumstances clearly show that a different approach to cybersecurity is required: a holistic, collaborative strategy to improve the security situation for society and the economy as a whole. In the European Union, the legal framework that is currently developing (like the network and information security (NIS) directive), recognises the increasing need for cooperation and collaboration among individual actors to improve cybersecurity. Information sharing is therefore one of the key elements of the NIS directive. In this paper, we present and demonstrate a system and dependency analysis based on soft systems thinking. This approach is able to capture the relations between assets and their internal and external dependencies in the complex systems of organisations. It is applicable to critical infrastructures or other organisations that base their operations on complex systems and interactions. The analysis approach introduced is done in a socio-technological manner; the human aspect of the systems is considered as important as the technical or organisational aspects. The case study presented in this paper, covering the first steps towards the development of a holistic cybersecurity awareness solution, is based on three focus points: an initial threat assessment for local public administrations (LPAs), an analysis of external information sources and an analysis of the piloting scenarios based on the first round of soft systems analysis workshops. The results of which are essential to the development of the solutions implementation framework and further software development.**

Keywords–Cybersecurity; Critical Infrastructures; System Analysis; Soft Systems Methodology; Socio-technological Analysis; Cyber Situational Awareness; Information Sharing.

I. INTRODUCTION

Cybersecurity is one of today's most challenging societal security problems, affecting both individuals and organisations, such as strategic/critical infrastructures, large commercial enterprises, SMEs, non-governmental organisations (NGOs) or governmental institutions. The extensive variety of these attacks is one of the issues, as is the lack of communication between organisations and administrations that have been the target of an attack. Deliberate or accidental threats and attacks threaten digitally administered data and digitally handled processes. Sensitive data leaks can ruin the reputation of companies and individuals, and the interruption of digital processes that organisations rely upon in their daily work flow can cause severe economic disadvantages. This work builds on the paper on how to adress complex situations in critical infrastructure published in SECURWARE 2017 [1]. Reaching beyond the technology-focused boundaries of classical information technology (IT) security, cybersecurity strongly interrelates with organisational and behavioural aspects of IT operations, and the need to comply with the current and actively developing legal and regulatory framework for cybersecurity. For example, the European Union (EU) recently passed the NIS directive that obliges member states to get in line with the EU cybersecurity efforts [2]. Most EU member states and the EU itself have a cybersecurity strategy in place which will eventually lead to the introduction of laws and regulations that fulfil cybersecurity requirements. One of the main aspects of the NIS directive, as well as the European cybersecurity strategies, is cooperation and collaboration among relevant actors in cybersecurity. Enabling technologies for coordination and cooperation efforts are situational awareness and information sharing. Situational awareness in this context is a runtime mechanism to gather cybersecurity relevant data from an IT infrastructure and visualise the current situation for a user or operator. Information sharing refers to the ability to share this information with cybersecurity information sharing communities, like the NIS relevant authorities. In the long term, it is expected that due to the awareness generated information sharing can improve cybersecurity sustainably and benefit society and economy as a whole.

One of the major aspects of information sharing to facilitate collaboration and cooperation, is a proper understanding of the cybersecurity relevant aspects within an organisation's systems. This is a complex and often neglected task that will, as we argue in this paper, greatly improve the cy-

2018, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

bersecurity of organisations in the context of cybersecurity situational awareness and cooperative/collaborative strategies towards cybersecurity. We introduce and demonstrate a system and dependency analysis methodology to analyse the environment and: (a) Identify the assets and dependencies within the system and how to monitor them; (b) capture not only technological aspects, but the socio-technical relations within the organisation; (c) identify external information sources that could either be provided by official and cybersecurity specific sources (for example, legal/regulatory framework, standardisation, cybersecurity information sharing communities), or more general publicly available information relating to cybersecurity (for example, social networks or twitter); (d) provide the results in a form that can be utilised by support tools.

We base our work around established and well proven methods related to systems thinking, the soft systems methodology (SSM) and PROTOS-MATINE/GraphingWiki. The case study presented in this paper tests the idea of using these methods to analyse complex domains and derive a coherent analysis. The results of the case study will be critical in assuring a high quality software development of a cybersecurity awareness solution for local public administrations. As of now, the first round of user workshops, the initial threat assessment and the analysis of external information sources have yielded essential information for defining an implementation framework. The upcoming second and third round user workshops held in the pilot municipalities will work mainly with information collected during the before-mentioned analysis of threats, external sources and the first workshops.

The paper is organised as follows: Section II discusses background and related work, Section III details our system and dependency analysis approach. In Section IV, an example in the context of CS-AWARE, a European H2020 project which uses the presented system and dependency analysis as a core part of its cyber security solution, is introduced and followed by the summary of the first round of workshops in the pilot scenarios in Section V. Section VI discusses the results of approach and Section VII concludes the paper.

II. Related Work

In December 2015, the European Parliament, the European Council and the European Commission agreed on the European NIS directive as the first EU wide legislation on cybersecurity [2]. The directive lays down the obligations of member states concerning NIS. Most notably for this work, it requires the implementation of proper national mechanisms for incident prevention and response, in addition to information sharing and cooperation mechanisms. The NIS directive is the main action stemming from the EU cybersecurity strategy [3], which emphasises the need for a decentralised prevention and response to cyber incidents and attacks. By now, most EU countries have put a national cybersecurity strategy in place [4] that is in line with many actions proposed by the NIS directive. Coordination and information sharing are key elements of the strategy, with the requirement for national NIS authorities, national law enforcement and defence authorities to interact with each other, as well as their EU counterparts. International cooperation and coordination is envisioned at the EU level. On the standardisation front, the ISO/IEC 27000 [5] standard is the first in a series of standards on information security management that have provided organisations with a best practice framework for assessing security risks and implementing security controls as countermeasures. Similarly, the privacy focused ISO/IEC 29100 [6] standard provides a framework to help organisations to manage and protect personally identifiable information. In 2011 the European standardisation organisations CEN, CENELEC and ETSI have formed the cybersecurity coordination group (CSCG), which was converted to the focus group on cybersecurity in 2016 [7], in order to undertake the strategic evaluation of IT security, cybersecurity and NIS standardisation.

The systems analysis methodology which will be mainly used in this work is the Soft Systems Methodology developed by Peter Checkland [8][9]. Cognitive mapping, casual loop diagrams [10] or a combination of stakeholder analysis and cognitive mapping as suggested by Ferretti [11], would have been alternatives. Generally, the key thought behind the soft systems methodology is that it is hard to completely analyse and describe a complex system, especially if human interaction plays a key role. SSM represents an analysis methodology that aims to achieve an holistic understanding of the system while at the same time only focusing on the actual problems at hand. Soft Systems Methodology has been used in an extraordinarily wide variety of problem domains as diverse as knowledge management in the building industry [12], to evaluating government policy to promote technological innovation in the electricity sector [13]. In the case of the building industry example, the tacit knowledge held by staff involved in the tendering process was made explicit by the application of SSM. In the case of the electricity supply industry, SSM was used understand how better to to promote and foster technological innovation in the sector.

The PROTOS-MATINE methodology [14] is another approach that relates to systems thinking. While the SSM focuses on understanding complex systems and processes by interviewing its users, PROTOS-MATINE takes the standpoint that a truly holistic view on complex situations can only be achieved if as many relevant information sources as possible (e.g., technical, organisational, human on all organisational levels as well as external and publicly available information), are combined to create a complete picture and eliminate discrepancies between information from different sources. The key to PROTOS-MATINE is that collected information from different sources is set in context to each other and graphically processed and visualised to make it simple for domain experts to identify discrepancies in information coming from different sources. For this purpose, GraphingWiki [15], a graphical extension to the MoinMoin Wiki, was developed to visualise dependencies between semantic data collected in Wiki pages in the context of PROTOS-MATINE. The methodology was used in many case studies, for example for highlighting vulnerabilities in anti-virus software [16] and for a socio-technological analysis of a VoIP (voice over IP) provider [17]. In [18], the methodology was extended for analysing complex systems in the critical infrastructure context, where the analysis goal is to achieve a dependency graph of critical infrastructure assets, dependencies between the assets and measures to observe those assets (base measurements).

2018, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

III. Soft Systems Analysis in the Context of Cybersecurity for Complex Systems

The system and dependency analysis proposed in this paper is seen as the basis for the automatic incident detection and cybersecurity situational awareness efforts of future cybersecurity initiatives, as discussed in the related work. The objective is to identify in the specific organisational context what needs cybersecurity protection and what are the main threats it needs protection from. More specifically, this means that the challenge for system and dependency analysis is to identify the assets within an organisation and their internal and external dependencies in order to be able to protect them from cybersecurity threats. Observable information sources that can be used to determine the on-line state of those assets need to be identified to allow for monitoring and detecting abnormal behaviour, thus describing the security state. Furthermore, the goal of the system and dependency analysis is to identify external information sources that can provide information to help detect and classify security threats correctly. Those information sources can be dedicated cybersecurity information providers like, for example, computer emergency response teams (CERTs) or other threat and vulnerability databases, or they can be publicly available information sources via, for example, platforms like Twitter, Facebook or Google+. The usage of open source intelligence (OSINT) has been proved to be valuable before in other contexts like disaster management. Sail Labs Media Mining System is an example of a system which makes use of freely available information. It aims to allow accurate situational analysis of crisis locations by analysing different relevant data feeds. It gathers information from multiple sources including television, radio and various Internet sources and uses data mining techniques to extract information about the content [19].

Since technology is only one factor in cybersecurity, the system and dependency analysis is designed to capture and monitor the socio-technical nature of an IT infrastructure. It takes into account the human, organisational and technological factors, as well as other legal/regulatory and business related factors that may contribute to the cybersecurity in a specific context. As can be seen in Figure 1, systems thinking is a way of looking at some part of the world, by choosing to regard it as a system, using a framework of perspectives to understand its complexity and undertake some process of change. The key concepts are holism - looking at things as a whole and not as isolated components and systemic - treating things as systems, using systems ideas and adopting a systems perspective.

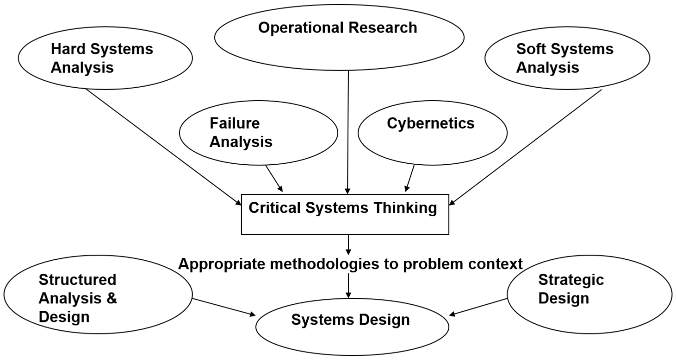


Figure 1. Systems thinking - The systems approach

Two concepts of systems thinking are hard systems thinking and soft systems thinking. Hard systems design is based on systems analysis and systems engineering. It assumes that the world is comprised of systems that we can describe and that these systems can be understood through rational analysis. It is based on the assumption that it is possible to identify a “technically optimal” engineering solution for any system and that we can then write software to create the “solution”. Hard systems design assumes that there is a clear consensus as to the nature of the problem that is to be solved. It is unable to depict, understand or make provisions for “soft” variables such as people, culture, politics or aesthetics. It is based on the assumption that it is possible to identify a “technically optimal” engineering solution for any system. It assumes that those commissioning the system have the ability and power to implement the system. While hard systems design is highly appropriate for domains involving engineering systems structures that require little input from people, the complex systems and interactions in critical infrastructures or other organisations - especially with cybersecurity in mind - usually do not allow this type of analysis. Hard systems design is inappropriate and unsuitable for analysing human activity systems that require constant interaction with, and intervention from people. Such systems are complicated, fuzzy, messy and ill defined and are typified by unclear situations, differing viewpoints and unclear objectives, containing politics, emotion and social drama. This is the type of system domain for which an SSM design approach is highly appropriate and to which it should be applied. That is not to say that the SSM approach cannot or should not be used in the design of engineering systems and structures, indeed one of the authors has used this approach very successfully in many complex and diverse problem domains. For example, SSM has been used by one of the authors in the design of naval command and control systems for the British Navy and in the design of system architectures for automated fare collection in very large light railway and mass transit operations.

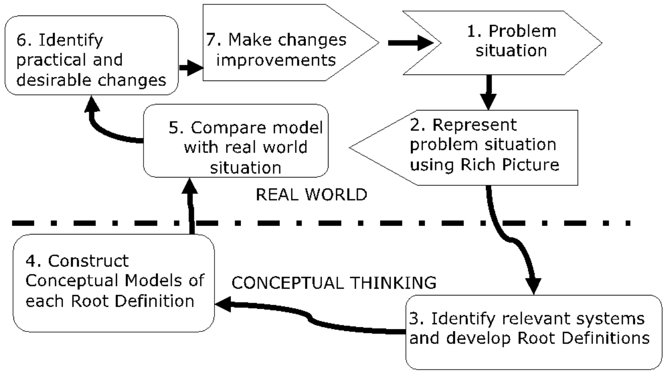

6. Identify practical and desirable changes
7. Make changes improvements
1. Problem situation
5. Compare model with real world situation
2. Represent problem situation using Rich Picture
REAL WORLD
4. Construct Conceptual Models of each Root Definition
CONCEPTUAL THINKING
3. Identify relevant systems and develop Root Definitions

Figure 2. Soft systems design

An overview of the stages of SSM is set out in Figure 2. The SSM methodology has 7 steps: (1) Enter the problem situation; (2) Express the problem situation; (3) Formulate root definitions of systems behaviour; (4) Build conceptual models of systems in root definitions; (5) Compare models with real-world situations; (6) Define possible and feasible changes; (7) Take action to improve the problem situation. A detailed description of the approach is beyond the scope of this paper, however, reader may wish to refer to Checkland's work [8][9]. In this work, we will focus on the earlier steps of the SSM that deal with the system analysis and problem definition (specifically, steps 1-4). One key element of this phase is that systems stakeholders (users, managers, administrators, etc.) are engaged in workshops to define the problems they are facing, since those who are using systems on a daily basis are the ones that have the most information about it. Since this is not explicit knowledge, but tacit knowledge, it is important to create an environment that facilitates information sharing. The SSM utilises rich pictures for this purpose, and depicting the problem in a rich picture is a key stage early in the process. Rich pictures are a representation of the problem domain. They utilise "cartoon-style" techniques to portray a complex situation and concentrate on:

- Structure - Key individuals, organisations etc.
- Process - What could be or is happening?
- Climate - Pressures, attitudes, cultures, threats etc.

An example of a Rich Picture depicting a malfunctioning airline passenger check-in system appears in Figure 3, outlining different viewpoints in case the system goes off-line.

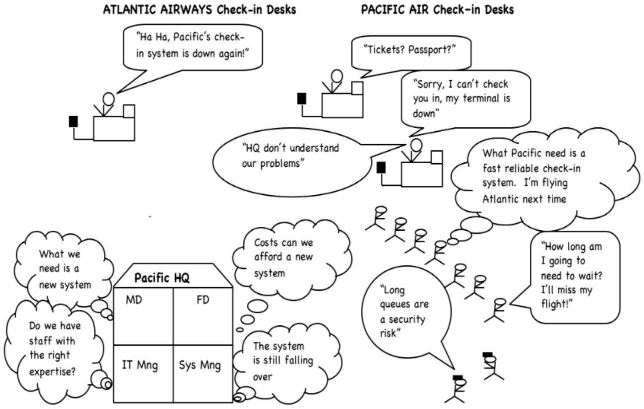

ATLANTIC AIRWAYS Check-in Desks
PACIFIC AIR Check-in Desks
"Ha Ha, Pacific's check-in system is down again!"
"Tickets? Passport?"
"Sorry, I can't check you in, my terminal is down"
"HQ don't understand our problems"
What Pacific need is a fast reliable check-in system. I'm flying Atlantic next time
What we need is a new system
Costs can we afford a new system
"How long am I going to need to wait? I'll miss my flight!"
Pacific HQ
MD
FD
IT Mng
Sys Mng
Do we have staff with the right expertise?
The system is still falling over
"Long queues are a security risk"

Figure 3. Rich picture of an airline check-in system

Rich pictures are a tool for understanding where we are and are a mix of drawings, pictures, symbols and text. They represent a particular situation or issue and they are depicted from viewpoint(s) of the person or people who drew them. They can both record and evoke insight into a situation. Rich pictures are pictorial 'summaries' of a situation, embracing both the physical, conceptual and emotional aspects of a problem situation. They can depict complicated situations or issues, and relevant systems are identified from the rich picture. These systems are described in Root Definitions, which are then used in conjunction with the rich pictures to develop Conceptual Models. These are formed from the actions stated or implied in the Root Definition(s). Of course, each rich picture may be interpreted from quite differing 'world view points'. A Conceptual Model is like an activity sequence diagram, but is aimed at representing a conceptual system as defined by the logic of the Root Definition and not just a set of activities.

The role of PROTOS-MATINE and GraphingWiki in this proposed analysis method is to complement the information gathering effort in the user workshops with information from other sources, and provide a solid base for discussion in those workshops through visualisation. The main additional sources are expected to be legal requirements and regulatory efforts like the NIS directive; cybersecurity relevant standardisation like the ISO/IEC 27000 family of standards and information about relevant and current risks and threats via official sources like CERTs, or more dynamic information sources like social media. Where relevant, the information received via rich pictures from the workshop participants can easily be complemented by more detailed information available such as, for example, technical manuals, business continuity plans or disaster recovery plans. One of the capabilities of GraphingWiki is to instantly link gathered information to other relevant information and thus allowing to update the graphical representation of the analysed system as soon as new information arrives. We hope to utilise this feature in the user workshops to create more dynamic discussions and give even more incentive to the participants to create a system model that is as close to reality as possible.

The expected result of the proposed system and dependency analysis will be a dependency graph containing an organisations security relevant or critical assets and the dependencies among them. Furthermore, observable measurements that are able to determine the security state of those assets are identified and associated to them. Through GraphingWiki this dependency graph is in digital form and can be further utilised as the basis for advanced cybersecurity situational awareness and monitoring services. One example of such a service will be given in the next section.

IV. The CS-AWARE Approach

CS-AWARE is a European H2020 project that was funded by the European Union under the project number 740723. The aim of the project is to improve the cybersecurity situation in local public administrations (LPAs). While the project is focused on LPAs, the ideas and methods developed in this project are applicable to any organisations that rely on complex systems, interactions and procedures (like strategic/critical infrastructures, large organisations or SMEs).

As can be seen in Figure 4, the main building blocks of the CS-AWARE solution are the system and dependency analysis, data collection and data analysis to achieve the project's goals of cybersecurity situational awareness, cybersecurity information exchange and system self-healing. The proposed solution aims at improving automated situational awareness in small- to medium-sized IT infrastructures, however it is expected that the same principals would also apply to large organisations or critical infrastructures. The system and dependency analysis presented in the previous section is an integral part of two project phases. Besides the actual system and dependency analysis, which will be conducted according to the methodology presented in Section III (Steps 1-4 of the SSM as well as PROTOS-MATINE/GraphingWiki related aspects), it will provide the main input for the self-healing component, based on steps 5-7 of the SSM.

The core idea of the CS-AWARE project is to automate the cybersecurity effort of organisations as much as possible, and provide an on-line situational awareness tool that aims to base its recommendations on a holistic view of an organisation's IT systems and dependencies, but also on the cybersecurity

2018, © Copyright by authors, Published under agreement with IARIA - www.iaria.org

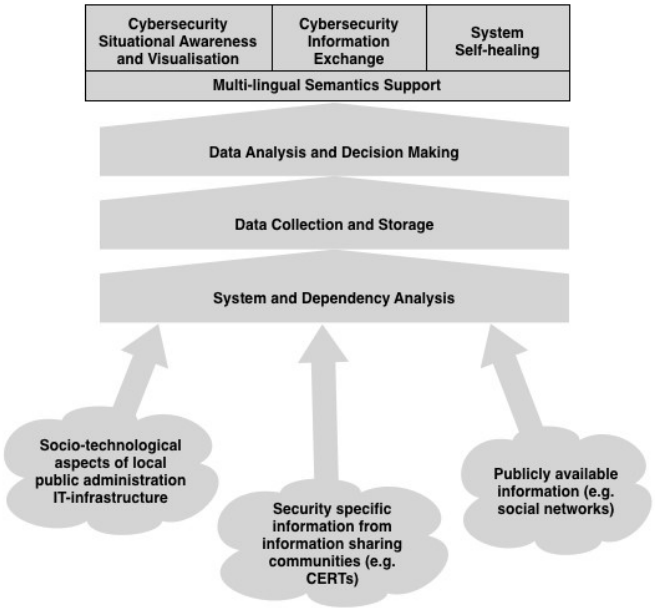

Cybersecurity Situational Awareness and Visualisation
Cybersecurity Information Exchange
System Self-healing
Multi-lingual Semantics Support
Data Analysis and Decision Making
Data Collection and Storage
System and Dependency Analysis
Socio-technological aspects of local public administration IT-infrastructure
Security specific information from information sharing communities (e.g. CERTs)
Publicly available information (e.g. social networks)

Figure 4. CS-AWARE overall concept

situation in general (for example by observing the risk and threat landscape). The end users of the CS-AWARE solution are expected to be the people responsible for cybersecurity in an organisation, such as the chief security officer (CSO), or system administrators. CS-AWARE is a decision support system that will allow its users to detect cybersecurity incidents quickly and identify the affected systems, since the key assets and security relevant dependencies have been identified during system and dependency analysis. Countermeasures can be initiated by the people responsible for cybersecurity in a timely manner. Besides manual countermeasures, CS-AWARE includes a self-healing component that is closely tied to the system and dependency analysis. The later steps of the SSM (especially steps 5-7) are concerned with defining solutions to the problems identified during analysis. In CS-AWARE one focus point will be to identify and develop possible countermeasures to cybersecurity threats and define policies and procedures that can be invoked if such a threat materialises. Those policies and procedures will be utilised by the self-healing component and can be configured to be invoked automatically if a threat materialises. This will allow the system, depending on the scenario, to prevent or mitigate the damage and/or recover from the incident.

The intelligent and fully automated part of the CS-AWARE project are the *data collection and storage* and *the analysis and decision making* components. Based on the system and dependency analysis results, the base measurements from internal and external sources are observed and when relevant data points are collected, pre-processed and stored. The data analysis component is capable of detecting suspicious behaviour like threat and attack patterns in the data sets it receives and will classify and rank them accordingly, as an input to the decision support in the situational awareness and visualisation component. The accuracy of the decision making component will depend on the cooperation and collaboration efforts and the quality of data that is provided by information sharing authorities. It is envisaged that threat detection can achieve highly accurate unsupervised results once cybersecurity information exchange is an established concept and can provide accurate information relating to cybersecurity threats and attack patterns.

The *cybersecurity situational awareness and visualisation* component is the user interface to the CS-AWARE solution. It will visualise the security relevant aspects of an organisations socio-technological systems, based on the dependency graph received during system and dependency analysis. State changes triggered by the decision making component will cause a visualisation of the affected components and its dependencies. Possible countermeasures will be suggested and self-healing procedures can be configured and invoked, where relevant.

The *cybersecurity information exchange* is the connection point to the cybersecurity information sharing authorities, for example NIS competent authorities like national or EU CERTs. While cybersecurity information sharing is currently still in its infancy, it is seen as one of the major building blocks to a safer cyberspace in future. The CS-AWARE solution will on the one hand, benefit from the information provided by those authorities and on the other hand, provide information about newly detected and unmatched incidents (like threat or attack patterns). It is assumed that with more and more tools that provide capabilities for organisations to participate in security related information sharing, the benefit of sharing information for the common good will become evident and encourage organisations to engage in cybersecurity related information sharing. Cybersecurity information exchange would in that case become one of the most important information sources for cybersecurity awareness and threat detection.

In order to deal with the expected language barriers and usability concerns in the context of European local public administrations, the main focus of the CS-AWARE project, *multi-lingual semantics support* will be part of this project's solution. Where relevant, security related information coming from within the end user organisations, or information from external information sources, will be automatically translated to benefit from the information of different cultural contexts.

The project includes two pilot scenarios in the LPA context: the municipalities of Larissa (Greece) and Rome (Italy). This set-up will allow us to develop tailored system and dependency analysis procedures for the LPA context. The project will commence with workshops in both municipalities. A representative cross section of the LPA's staffs will be formed in each LPA and will use SSM in a workshop setting, where the LPA's staff, facilitated by the project team can help create a detailed understanding of the problem domain and the system dependency analysis, together with security experts, legal experts and CERT representatives.

V. Case Study

The first step in applying the introduced approach was to determine the largest threats to LPA's based on expert knowledge and state-of-the-art research on the topics. This analysis was followed by evaluating the most valuable external, preferentially publicly available, information sources for cyber crime related data. This analysis was also based on expert knowledge and collected in a detailed report. Finally, with the specific information on potential threats and available external sources, the SSM workshops in the pilot cities were conducted.

A. Initial Threat Assessment

During the threat assessment we have determined that the main asset to be threatened from the cyber domain for local public administrations will most likely be the data that is managed by the administrations, including personal citizen and employee data. The main cybersecurity challenge in local public administrations is assumed to be the prevention of unauthorised data access, modification and destruction of those data. It was assessed that local public administrations are not a high valued target for potential threat actors, as for example critical infrastructures (potential large-scale disruption of economy) or financial institutions (potential high financial gain) are. However, there is a certain level of risk associated, since there are relevant threat actors that may have a vested interest in gaining unauthorised access to data managed in LPAs. We assume a low to medium level of risk against LPA managed data from the cyber domain. Additionally, we have identified that the most valued asset in LPAs is the potentially sensitive and/or private citizen and employee data that is managed by LPA systems, and that unauthorised data access, modification and destruction as well as data theft are the most relevant threats towards LPAs.

Table I shows the results of the initial analysis of potential threats and their risk level, based on the expert analysis and internationally acclaimed cybercrime threat reports [20] [21].

TABLE I. LPA RISKS GROUPED BY THREAT

Threat		*Risk level*	
	High	*Medium*	*Low*
Unauthorised data access, modification, destruction		X	
Data Theft		X	
Extortion	X		
Advanced Persistent Threat (APT)			X
Ransomware (untargeted)	X		
Ransomware (LPA specific)			X
Distributed Denial of Service - DDoS (untargeted)	X		
Distribtued Denial of Service - DDoS (LPA specific)			X
Web page defacement / shaming			X
Malware infection		X	

In Table II the most likely threat actors and their corresponding risk levels have been summarised. We assess that untargeted large-scale attacks with the goal of extortion, like Ransomware or Distributed Denial of Service (DDoS) attacks carry a higher risk for LPAs. We have identified the cyber-criminal (high) as well as the malicious insider (medium) as the most relevant threat actors. Furthermore, disgruntled citizens, script kiddies and hacktivists are also seen as relevant threat actors, but we assess the risk from those actors to be low due to low potential pay-off for those actors as well as the low expected damages for LPAs.

TABLE II. LPA RISKS GROUPED BY THREAT ACTOR

Threat		*Risk level*	
	High	*Medium*	*Low*
Cyber criminal		X	
Malicious insider	X		
Disgruntled citizen / script kiddie			X
Hacktivist			X

B. Analysis of External Information Sources

As part of this initial analysis of cybersecurity relevant information sources, the main categories and respective sources which were identified can be seen in Table III.

The first possible information sources are related to organisations that the European Cybersecurity Strategy (European Commission and High Representative of the European Union, 2013) classifies as one pillar of coordination and information sharing efforts. While the CS-AWARE project does not expect as much cooperation with law enforcement as with NIS competent authorities due to the higher requirements for protecting information relating to cybercrime, we have identified several organisations that may be able to provide relevant information for CS-AWARE. For the open source data providers, we focused on sources that provide loosely structured information without a dedicated feed or data format, or if they provide a feed the provided data is usually utilised by aggregated data providers. The information sharing tools discussed are mainly community efforts to provide mechanisms for data aggregation. While data aggregation is already covered in the CS-AWARE solution, it is worth looking at those tools to see if it would help us to further simplify the data aggregation effort in CS-AWARE.

CS-AWARE will try to rely solely on free and open source data, it is however worth investigating which commercial data sources exist in case the free and open source data is not available. We may try to ask some of those companies for free access to their data in the context of this European research project. Overall, it seems that the sources listed provide up-to-date information, at least in the cases where the refresh time interval was stated explicitly or was easily verifiable (e.g., by accompanying timestamps). For retrieving data from the sources listed in this section some demo prototypes are available (mainly implemented in Python and Java), which were used by CS-AWARE partners for evaluation and testing the provided feeds. The idea of malware analysis tools is to be able to get a detailed report, listing the behaviour of a suspicious executable in a controlled environment (e.g., sandbox). In general we expect to collect fast but not in-depth reactions to currently ongoing security incidents from social media sources. While this information may lack the level of depth we expect from more security focused information sources, information collected from social media may help CS-AWARE to react to quickly evolving incidents. While one of the main public data sources provided by NIS competent authorities like CERTs is about vulnerabilities, it is still a good idea to have a look at the most well-known vulnerability trackers. For many years, the CVE list provides a standardised way of enumerating software vulnerabilities.

Our analysis concluded that the most valuable cybersecurity related information (or cybersecurity intelligence) for CS-AWARE can be found from both official organisations, for example NIS competent authorities or law enforcement organisations, as well as private efforts, for example for-profit companies or non-profit communities/ projects. More generalised data, not necessarily provided by the security community, can be found from social media or data visualisation focused data sources. For CS-AWARE we will focus on information that is freely available from either the NIS competent authorities, from companies that provide free data

TABLE III. EXTERNAL INFORMATION SOURCES

Topic	*Source*	*Link*
NIS Competent Authorities	European Union Agency for Network and Information Security (ENISA)	https://www.enisa.europa.eu
	European Public Private Partnership for Resilience (EP3R)	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-\for-resilience-ep3r
	Computer Emergency Response Teams (CERTs)	https://cert.europa.eu
	Computer Security Incident Response Teams (CSIRTs)	http://www.cert.org/incident-management/national-csirts/national-csirts.cfm
Law Enforcement Agencies	Europol	https://www.europol.europa.eu/activities-services/services-support/intelligence-analysis/cyber-intelligence
	Interpol	https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
Cyber Intelligence Sources and Information Sharing Tools	Shadowserver	https://www.shadowserver.org/wiki/
	Abuse.ch	https://abuse.ch/
	Spamhaus	https://www.spamhaus.org/
	SANS Internet Storm Center	https://isc.sans.edu
Commercial Providers	Flashpoint	https://www.flashpoint-intel.com/solutions/
	Checkpoint	https://www.checkpoint.com/
	DCU Microsoft	https://news.microsoft.com/presskits/dcu/
	AbuseSA / Clarified Networks	https://www.clarifiednetworks.com
Cybersecurity Intelligence Data Feeds	AlienVault OTX	https://otx.alienvault.com/
	Advanced Cyber Defence Center	https://www.acdc-project.eu/
	Hail a Taxii	http://hailataxii.com
	Facebook Threat Exchange	https://developers.facebook.com/products/threat-exchange/
	Honey DB	https://riskdiscovery.com/honeydb/
Malware Analysis	Hybrid Analysis	https://www.hybrid-analysis.com/
	VirusBay	https://beta.virusbay.io/
	VirusTotal	https://www.virustotal.com/en/
Social Media	Xing	https://www.xing.com/
	Reddit	https://www.reddit.com/
	Facebook	https://www.facebook.com/
	Twitter	https://twitter.com/
	Google+	https://plus.google.com/
Vulnerability Data	CVE List	https://cve.mitre.org/cve/cna.html
	National Vulnerability Database (NVD)	https://nvd.nist.gov/
	CVE-SEARCH	https://www.cve-search.org/

or, probably most relevant, open source intelligence (OSINT) focused communities and projects. However, we will keep the option in mind to ask for-profit companies for access to their cybersecurity intelligence data in the context of this European project, if relevant.

C. Analysis of Pilot Scenarios

A crucial part for designing an effective cybersecurity awareness solution for local public administrations was to gain in-depth knowledge on LPA's, the services they provide, their inner workings and how similar these are across different city sizes and European countries. As of now, we have held the first round of SSM user workshops in the two piloting cities, Roma Capitale (RC) in Italy and Larissa, Greece. The main goal for this round of analysis was to gain an initial understanding of the complexities within LPAs and identify realistic and meaningful piloting scenario that can be managed with the resources available for this project. During the analysis we have met and even exceeded the expectations we set for our first round of analysis. In both piloting scenarios we have now a clear understanding of the critical assets and their dependencies to other critical assets that need to be taken into account, and we have identified how those assets can be monitored. By now we have conducted the first of three rounds of user workshops at our piloting partners. We have seen that if the participants of the user workshops have prepared themselves and have comprehended the added value of system analysis using rich pictures, this method is a powerful tool. It allows the participants to quickly gain a common understanding of the systems and interactions from a high level overview down to more detailed technical specifications. The right composition of participants in the user workshops is crucial. Only if representatives from all relevant organisational levels (such as managers and technicians) are present in the workshops, a complete and holistic understanding of the problem domain will be achieved. It have become clear that it is essential to have stable workshop groups – those who decide to be part of the workshop need to be there for the whole duration of the analysis. We argue that in complex systems good cybersecurity awareness can only be provided if the relevant relations between the mission critical aspects of the system are understood, and relevant case specific monitoring points can be utilised. The first round of analysis has only strengthened our argument. In both municipalities, we were able to achieve good analysis results and were able to identify the most mission critical systems and their dependencies, as well as potential monitoring points for CS-AWARE. The individual set-ups and procedures in the two municipalities differ significantly from each other, especially due to the substantial difference in complexity in the operations of the two very differently sized municipalities. Nevertheless, we were able to draw some generalised conclusions that will allow us to develop guidelines and procedures that will help to further simplify future analysis efforts in LPAs.

1) Municipality of Larissa, Greece: In general, the analyst team was satisfied with the outcome of the workshop, and that the Larissa team could be already released after three days of data gathering, after the required level of analysis detail had been achieved. The two main factors contributing to this result were the manageable complexity of systems in a mid-sized municipality, as well as the excellent preparedness of the team in Larissa. The team had familiarised themselves with the

CS-AWARE project ideas as well as with the analysis methodology, which allowed the analysis team to quickly achieve excellent results. As outcomes of the workshop the analysts concluded that the most interesting connection points for CS-AWARE are monitoring on the service level, the network level, as well as monitoring existing security mechanisms. At the service level, the analysts concluded that it was only necessary to concentrate on two mission critical services. These two systems both store and process personal and sensitive data and both are critical to the operation of the City. Therefore, the proposed CS-AWARE solution will seek to monitor these systems and networks. In both cases, it was established that activity could be recorded and saved to the database via built-in auditing mechanisms, meaning SQL queries could be used to capture audit information about data operations (although any personal data will need to be anonymised at source). Furthermore, similar data can be gathered from built-in database auditing mechanisms.

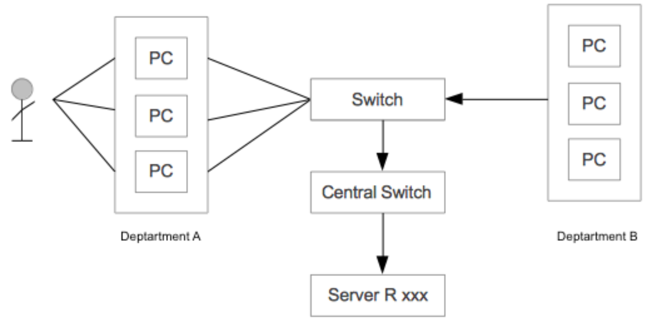


Figure 5. System Rich Picture

Figure 5 shows an anonymised representation of one of the rich pictures created by the team members of the Larissa LPA. As mentioned in Section II they used cartoon-style visualisations of the current situation, in this case part of their network infrastructure.

2) Municipality Roma Capitale, Italy: As expected, the Roma Capitale (RC) systems are much more complex than those that have been seen in the Municipality of Larissa, due to the extraordinary size of Roma and the number of online services that are provided to citizens and employees of RC. The attendees were divided into four groups, which were asked to draw a high level understanding of the systems and dependencies relating to their area of expertise, identifying mission critical systems as well as those parts of the systems that handle sensitive data. This resulted in four initial rich pictures, and while having a unique view on RCs systems, each included many aspects of other parts of the systems that other teams had been investigating in more detail. In the end we were able to identify a piloting scenario that will be possible to manage with the resources available within the CS-AWARE project: It was discussed to focus for now only on one relevant critical service - as well as all systems it depends on. It was identified that the most relevant critical dependencies can be found within the RC data centre (where the application service as well as the relevant application database are running), the web portal together with the identity and access management system (IAM), and several security appliances (like firewalls, proxies and SIEM (Security Information and Event Management) systems) that contain information relevant to service related operations. In the end, we were able to gain a good understanding of the overall architecture of RC systems and dependencies and a more detailed understanding of the system aspects that are the most relevant to CS-AWARE, identifying possible monitoring points for all relevant parts.

VI. Discussion

In Section I, four main points were mentioned by the authors to be essential in creating the introduced strategy of addressing complex situations in large infrastructures by use of a soft system thinking approach.

- *Identifying assets and their dependencies*
  Based on the results of the two SSM workshops, general assets and their dependencies could be identified and were grouped into four main categories: Network, Database, Service and Security-appliance level.
  The first question we asked the participants in both workshops was: "Which systems are mission critical and/or handle sensitive data?". Mission critical systems were different between the two LPAs, but shared common characteristics such as complementing infrastructure could be identified.
- *Identifying technological and socio-technical relations in the organisation*
  Next to identifying mission critical systems, the technical infrastructure and organisational structure in which these systems are used were determined. During the workshops, the socio-technical characteristics of the assets and the processes they are used in were determined.
- *Identifying external information sources*
  The external information sources used to complement the internal data collected by CS-AWARE were analysed extensively by experts and will be selected according to their relevance and quality of input they offer. Next to Social Media sites, such as Twitter and Reddit, Open Source Intelligence platforms and Commercial Providers, many other potential sources were identified and summarised in Table III.
- *Providing results in reusable form*
  Besides compiling a detailed deliverable on the results of the SSM analysis for external and internal information sources, the GraphingWiki mentioned in Section IV was used to produce a visual representation of the dependencies in the systems. Additionally to the graph, the tool produces a JSON formatted summary of the features of the system, which will be used for configuration purposes by the other components to specify the individual settings of each LPA implementation.

The exemplary dependency graph in Figure 6, depicting part of the LPA's system, shows how the components are linked to each other. Each of the components as well as the different relations between them have a Wiki-page where all relevant information is summarised. These include knowledge obtained in all aforementioned steps of the analysis - the pilot workshops as well as the external sources. An example for

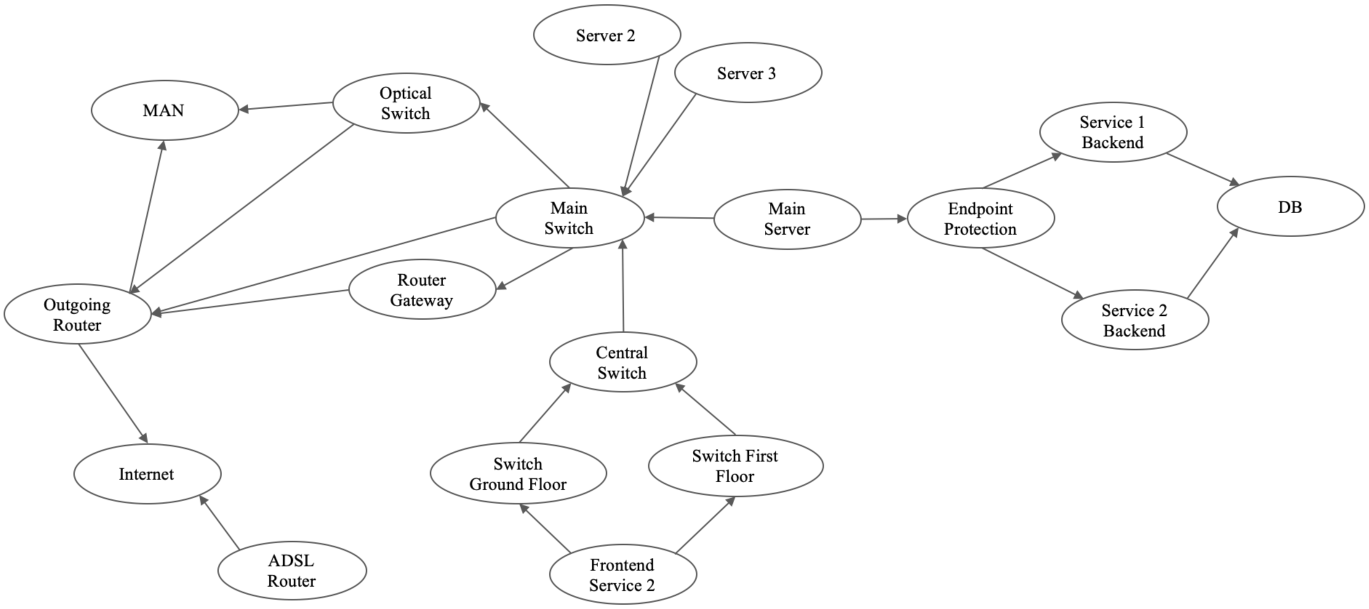
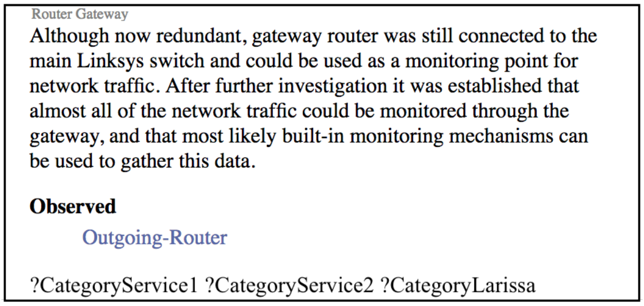


Figure 6. Larissa Dependency Graph

how such a Wiki-page can be structured is shown in Figure 7, including the individual categories selected for this project as well as the semantic text relevant for this component.


Router Gateway

Although now redundant, gateway router was still connected to the main Linksys switch and could be used as a monitoring point for network traffic. After further investigation it was established that almost all of the network traffic could be monitored through the gateway, and that most likely built-in monitoring mechanisms can be used to gather this data.

Observed

Outgoing-Router

?CategoryService1 ?CategoryService2 ?CategoryLarissa

Figure 7. Router Gateway Wikipage

All information collected during these workshops was summarised in the dependency graph and can be extracted in a JSON file to use in external applications. For the purpose of CS-AWARE, this will function as a basis for implementing and configuring the other components in the system. CS-AWARE combines multiple existing tool providers to a single, holistic cyber security awareness solution as can be seen in Figure 4. The System Dependency Analysis described and demonstrated in this paper builds the foundation on which the configurations of the other components depend on. It can specify, next to generalised configuration settings applicable for all LPAs, specific parameters for the individual LPA in question. For the deployment of CS-AWARE in any new LPA, generalised configuration settings can be extracted from the GraphingWiki, which then can be manually imported in the other components.

In both municipalities, we were able to achieve good analysis results and were able to identify the most mission critical systems and their dependencies, as well as potential monitoring points for CS-AWARE. While the individual setups and procedures in the two municipalities are significantly different from each other, especially due to the substantial difference in complexity in the operations of the two very differently sized municipalities, we were able to draw some generalised conclusions that will allow us to develop guidelines and procedures that will help to further simplify future analysis efforts in LPAs. In line with the initial risk assessment we have identified that the potentially sensitive and/or private data managed by LPAs is their most valuable asset. A cybersecurity awareness solution has to monitor the possible data flows in day-to-day operations. We have investigated potential monitoring points at 4 different levels that allow to identify suspicious behaviour related to data operations: The database level, the application/service level, the network level and the security appliance level.

The first steps of the SSM were applied during the user workshops in the municipalities - *entering the problem situation*, *expressing the problem situation* and *formulating the root definitions of the systems behavior*. The following steps will be undertaken in the upcoming workshop iterations in the pilots: *building conceptual models* and *comparing model to real-life situations*. This will allow for an even better understanding of the internal system and its information flows. Based on the received feedback *possible changes are defined* and the model revised accordingly. The final model will satisfy the last step of the SSM - *improving the problem sitation* by guiding implementation procedures in the respective municipalities. The Soft Systems Methodology approach provided usable results on which the further development of the CS-AWARE solution have been based on. While it was surprisingly easy to obtain relevant results in a short period of time in Larissa, the complexity of the Roman infrastructure required more extensive work time allocation. Nevertheless, both first Soft Systems Workshops were highly successful and we are eager to continue deepening the knowledge on the respective systems in the upcoming second round.

VII. Conclusion and future work

In this paper, we have presented a system and dependency analysis methodology for complex systems based on soft systems thinking within the context of cybersecurity. The target for the analysis are organisations that rely on complex systems and procedures for their operation, like critical infrastructures, large organisations or SMEs or public institutions. The analysis methodology is focused on providing a holistic socio-technological view of the analysed system, based on the combination and visualisation of different relevant information sources. Since one of the greatest sources of information about a system is coming from its users, workshops where users from all organisational levels and with different backgrounds work together to define the problem situation are a central aspect of this methodology. We have argued that each organisational set-up is different, which makes generalised cybersecurity solutions difficult. We have shown that the presented system and dependency analysis methodology can be seen as an abstraction layer that allows to apply generalised cybersecurity solutions on top of it. As an example, we have presented the EU H2020 project CS-AWARE that utilises the presented system and dependency methodology as a central part of its cybersecurity solution. The goal of CS-AWARE is to develop an automated cybersecurity situational awareness and decision support solution relying on cooperative and collaborative approaches, as laid out by the NIS directive. The case study presented in this paper applied the introduced Soft Systems Methodology to conduct an initial risk assessment, identify potential external sources as well as hold the first round of SSM workshops in the pilot municipalities.

We have been quite happy with the results of the first round of system and dependency analysis workshops. In some aspects we achieved much better results than we had expected, quickly identifying the four main levels requiring our attention: database, application/service, network and security appliance level. In other aspects it took a bit longer than expected to gain a common understanding of the workshop goals, before achieving the expected results. Based on the experiences we have gained so far, we are confident that we have chosen the right approach for CS-AWARE and with some tweaks to accommodate for individual cultural aspects, we expect even better results during the second round of workshops. Based on the analysis results described in Figure 6, more detailed tacit knowledge of the participants will be obtained regarding the socio-technical and infrastructural aspects of the LPA internal systems.

Acknowledgements

We would like to thank the EU H2020 project CS-AWARE ("A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis", project number 740723) and the Austrian national KIRAS project CERBERUS ("Cross Sectoral Risk Management for Object Protection of Critical Infrastructures", project number 854766) for supporting this work. The Biomimetics and Intelligent Systems Group (BISG) would like to acknowledge the support of Infotech Oulu.

References

[1] T. Schaberreiter, C. C. Wills, G. Quirchmayr, and J. Röning, “Addressing complex problem situations in critical infrastructures using soft systems analysis: The cs-aware approach,” *in Proc. SECURWARE*, pp. 99–105, 2017.

[2] European Commission, “Proposal for a directive of the european parliament and of the council concerning measures to ensure a high common level of network and information security across the union,” COM(2013) 48 final, 2013.

[3] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, “Cybersecurity strategy of the european union: An open, safe and secure cyberspace,” JOIN(2013) 1 final, 2013.

[4] ENISA, “National cyber security strategies in the world,” accessed: 2018-011-13. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

[5] ISO/IEC 27000:2016, “Information technology — security techniques — information security management systems — overview and vocabulary,” ISO/IEC, Standard, 2016.

[6] ISO/IEC 29100:2011, “Information technology — security techniques — privacy framework,” ISO/IEC, Standard, 2011.

[7] CEN, CENELEC and ETSI, “Focus Group on Cybersecurity (CSCG),” accessed: 2018-011-13. [Online]. Available: http://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx

[8] P. B. Checkland, *Systems Thinking, Systems Practice*. John Wiley & Sons Ltd. 1981, 1998.

[9] P. B. Checkland and J. Scholes, *Systems Thinking, Systems Practice*. John Wiley & Sons Ltd., 1991.

[10] S. Robinson, “Conceptual modelling for simulation part ii: a framework for conceptual modelling,” *Journal of the Operational Research Society*, vol. 59, no. 3, pp. 291–304, 2008.

[11] V. Ferretti, “From stakeholders analysis to cognitive mapping and multi-attribute value theory: An integrated approach for policy support,” *European Journal of Operational Research*, vol. 253, no. 2, pp. 524–541, 2016.

[12] T. Maqsood, A. D. Finegan, and D. H. T. Walker, “Five case studies applying soft systems methodology to knowledge management,” in *7th Annual Conference on Systems Engineering Research*, 2009, p. 18.

[13] C. H. Antunes, L. Dias, G. Dantas, J. Mathias, and L. Zamboni, “An application of soft systems methodology in the evaluation of policies and incentive actions to promote technological innovations in the electricity sector,” *Energy Procedia*, vol. 106, pp. 258 – 278, 2016.

[14] J. Eronen and M. Laakso, “A case for protocol dependency,” in *First IEEE International Workshop on Critical Infrastructure Protection (IWCIP’05)*, Nov 2005, p. 9.

[15] J. Eronen and J. Röning, “Graphingwiki – a semantic wiki extension for visualising and inferring protocol dependency,” in *First Workshop on Semantic Wikis – From Wiki To Semantics*, 2006.

[16] J. Eronen et al., “Software vulnerability vs. critical infrastructure – a case study of antivirus software,” *International Journal on Advances in Security*, vol. 2, no. 1, pp. 72–89, 2009.

[17] P. Pietikainen, K. Karjalainen, J. Roning, and J. Eronen, “Socio-technical security assessment of a voip system,” in *2010 Fourth International Conference on Emerging Security Information, Systems and Technologies*, July 2010, pp. 141–147.

[18] T. Schaberreiter, K. Kittilä, K. Halunen, J. Röning, and D. Khadraoui, *Risk Assessment in Critical Infrastructure Security Modelling Based on Dependency Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 213–217.

[19] G. Backfried et al., “Open source intelligence in disaster management,” in *2012 European Intelligence and Security Informatics Conference*, Aug 2012, pp. 254–258.

[20] European Union Agency for Law Enforcement Cooperation, “Internet organised crime threat assessment 2017,” accessed: 2018-011-13. [Online]. Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

[21] European Union Agency for Network and Information Security, “Threat landscape report 2016,” accessed: 2018-011-13. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016