Addressing Complex Problem Situations in Critical Infrastructures using Soft Systems Analysis: The CS-AWARE Approach

Thomas Schaberreiter*, Chris Wills†, Gerald Quirchmayr* and Juha Röning‡
*Faculty of Computer Science
University of Vienna (Vienna, Austria)
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*—In a world in which large-scale cyber attacks are the norm rather than the exception, the need for cybersecurity gains in importance every day. Current cybersecurity solutions are often not taking the holistic approach that would be required to provide comprehensive security to their users (for example, strategic/critical infrastructure, large organizations, small and medium-sized enterprises (SMEs) or public institutions). A new way of thinking about cybersecurity is required: Cooperation and collaboration among individual actors as a way to improve the security situation for society and economy as a whole is a promising approach. In the European Union, the legal framework that is currently developing (like the network and information security (NIS) directive), recognizes the need for cooperation and collaboration among individual actors to improve cybersecurity. Information sharing is one of the key elements of the NIS directive. In this paper, we present a system and dependency analysis based on soft systems thinking that is able to capture the relations between assets and its internal and external dependencies in the complex systems of organizations like critical infrastructures or other organizations that base their operations on complex systems and interactions. The analysis is done in a socio-technological manner; the human aspect of the systems is considered as important as the technical or organizational aspects. As a use case, we present CS-AWARE, a European H2020 project which relies on the presented system and dependency analysis method as a core concept for providing a cybersecurity solution that is in line with the cooperative and collaborative efforts of the NIS directive.**

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 organizations (NGOs) or governmental institutions. 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. 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. 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, information sharing will 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 organization's systems. This is a complex and often neglected task that will, as we argue in this paper, greatly improve the cybersecurity of organizations in the context of cybersecurity situational awareness and cooperative/collaborative strategies towards cybersecurity. We propose 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 utilized 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.

 ISBN: 978-1-61208-582-1

The paper is organized as follows: Section II discusses background and related work, Section III details our system and dependency analysis approach. In Section IV, an application 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 cybersecurity solution, is given. Section V discusses the approach in a wider context and Section VI 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 [1]. 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 [2], which emphasises the need for a decentralized prevention and response to cyber incidents and attacks. By now, most EU countries have put a national cybersecurity strategy in place [3] 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 [4] 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 [5] 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 [6], in order to undertake the strategic evaluation of IT security, cybersecurity and NIS standardisation.

A systems analysis methodology that will be used in this work is the Soft Systems Methodology developed by Peter Checkland [7][8]. 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. The 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 [9], to evaluating government policy to promote technological innovation in the electricity sector [10]. 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 [11] 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 organizational 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 visualized to make it simple for domain experts to identify discrepancies in information coming from different sources. For this purpose, GraphingWiki [12], a graphical extension to the MoinMoin Wiki, was developed to visualize 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 [13] and for a socio-technological analysis of a VoIP (voice over IP) provider [14]. In [15], 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).

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 organizational 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 [16].

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, taking into account the human, organisational and technological

 ISBN: 978-1-61208-582-1

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.

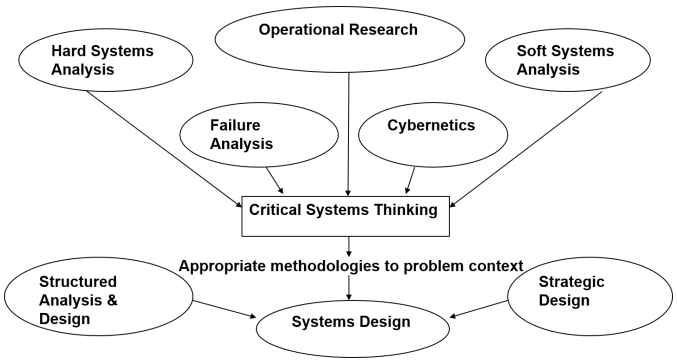

Figure 1. Systems thinking - The systems approach

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 organizations - 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 a 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.

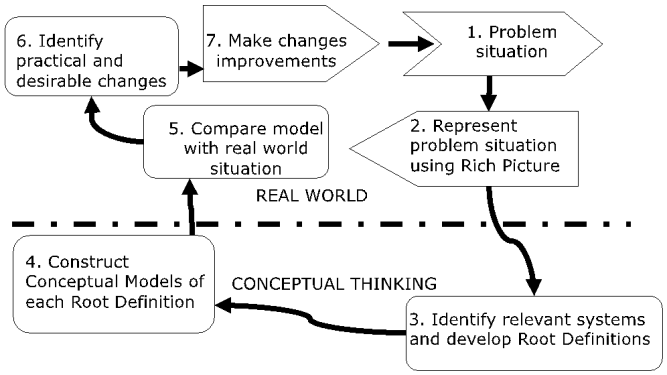

Figure 2. Soft systems design

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 [7][8]. 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 utilizes 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 utilize "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 Rick Picture depicting a malfunctioning airline passenger check-in system appears in Figure 3, outlining different viewpoints in case the system goes off-line.

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

 ISBN: 978-1-61208-582-1

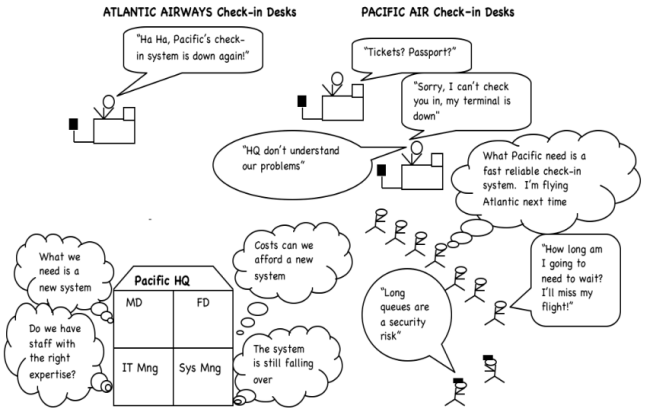

Figure 3. Rich picture of an airline check-in system

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 visualization. The main additional sources are expected to be legal requirements and regulatory efforts like the NIS directive; cybersecurity relevant standardization 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 utilize 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 organizations 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. Though GraphingWiki this dependency graph is in digital form and can be further utilized 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 organizations that rely on complex systems, interactions and procedures (like strategic/critical infrastructures, large organizations or SMEs).

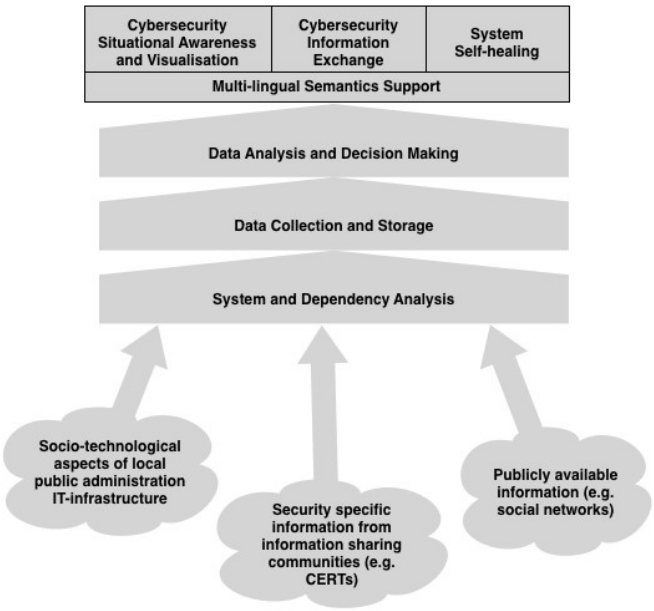

Figure 4. CS-AWARE overall concept

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 organizations 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 organizations as much as possible, and provide an on-line situational awareness tool that aims to base its recommendations on a holistic view of an organization's IT systems and dependencies, but also on the cybersecurity 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 organization, 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

 ISBN: 978-1-61208-582-1

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 materializes. Those policies and procedures will be utilized by the self-healing component and can be configured to be invoked automatically if a threat materializes. 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 visualization 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 visualization* component is the user interface to the CS-AWARE solution. It will visualize the security relevant aspects of an organizations 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 visualization 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 organizations to participate in security related information sharing, the benefit of sharing information for the common good will become evident and encourage organizations 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 organizations, 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. DISCUSSION

In the past years, we have seen a rapid growth in connectivity in all organizational contexts. For example, in critical infrastructures or the industry (Industrial IoT, Industry 4.0), the advances in the Internet of things allows devices in all levels of the organizational structure to be connected to the Internet - something that was not possible before. In administrations, more and more privacy related information about citizens is handled digitally, with interfaces to many different tools, accessed by many different devices and device classes. This trend makes the complex task of ensuring cybersecurity for those organizations even more complex, and the trend is continuing.

One major aspect of this situation is that each complex system is different. Not only are the systems of different industries/governmental institutions not comparable, but even the systems of different organizations within the same industry or government may have fundamentally different set-ups and needs related to cybersecurity. When looking for technological solutions to improve cybersecurity in this situation, there is no one-size-fits all solution that can be purchased and installed to provide out of the box protection. Especially when looking for solutions that enable cybersecurity collaboration and cooperation, some sort of abstraction layer is required to connect the individual systems of an organization with a common understanding about the security requirements and cybersecurity protection strategies. To achieve this abstraction level we see no way around an individual and methodical analysis of the complex environment in which an organization is operating, in order to determine which assets require protection and how they relate to the risk and threat landscape and protection strategies as laid out, for example, by NIS relevant authorities like national and EU CERTs. Tool support can build upon the abstraction layer introduced by this methodical analysis.

Some of the authors have very significant, broad and practical experience of systems thinking and the application and use of the Soft Systems Methodology to real-world problem domains. This experience has been acquired in a wide range of industrial and commercial and non-commercial settings, with widely differing organisational structures and technical, social and cultural constraints. The power of the method is that it captures and enables the expression of the tacit knowledge of the "actors" in the problem domain - the people who work with and within the system or systems under investigation. It is the expression and application of this tacit knowledge to the analysis and design process, that distinguishes the

 ISBN: 978-1-61208-582-1

method from other analytical tools. The approach that was presented in this paper is ideally suited for situations where complex environments need to be analysed but a complete and optimal analysis is not feasible. Soft systems analysis is excellent for quickly and flexibly defining problems and any associated relevant factors for specific situations, such as providing cybersecurity and all the socio-technological aspects that relate to the cybersecurity of a complex system. Especially in the dynamic cybersecurity context, where situations (e.g., threat and risk landscape) change rapidly, it is necessary to complement the problem definitions that are mainly gathered in user workshops, with more dynamic and highly topical information from other sources. We think that we have found an ideal solution with GraphingWiki, which was specifically designed to collect and graphically present related information from different sources.

We are highly confident that the proposed analysis methodology will fulfil the analysis requirements of complex organizational systems in the context of cybersecurity, and to build the basis and required abstraction level for cybersecurity tools that build on it. In CS-AWARE we see the system analysis as the enabling factor for a highly automated cybersecurity solution. Built on a common understanding of the cybersecurity requirements, CS-AWARE will shift cybersecurity from a purely organizational problem to a cooperative and collaborative problem. At the same time, solutions to specific threats that are developed on the collaborative level (for example, through NIS competent authorities), can be more easily integrated on the organizational level based on the analysis results.

We will be using the pilot use cases in CS-AWARE to validate our approach in the LPA context, in combination with the technological capabilities of the CS-AWARE solution. Besides providing analysis for the case studies which are part of the project, we will develop procedures and policies for the system and dependency analysis tailored to the LPA context. The goal is to develop a quasi-standard in order to ensure that comparable results can be achieved, while at the same time, reducing the level of expertise required to conduct such an analysis. Once we have more relevant results within the project, we expect to do the same outside the LPA context. We expect that application areas like critical infrastructures, large organizations or SMEs can benefit in the same way from a soft systems based analysis in the context of cybersecurity, and we intend to tailor and apply the presented analysis methodology to those contexts.

VI. Summary and Outlook

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 organizations that rely on complex systems and procedures for their operation, like critical infrastructures, large organizations/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 visualization 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 organizational levels and with different backgrounds work together to define the problem situation are a central aspect of this methodology. We have argued that each organizational set-up is different which makes generalized 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 generalized cybersecurity solutions on top of it. As an example, we have presented the EU H2020 project CS-AWARE that utilizes 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.

As a next step, we will validate the presented analysis method in the context of LPAs, within the CS-AWARE piloting efforts in the municipalities of Larissa (Greece) and Rome (Italy). Besides providing the case dependent analysis required for the CS-AWARE solution, we intend to develop quasi-standardized policies and procedures for the LPA context to ensure repeatable and comparable analysis results for future cases. In a next step we intend to apply the methodology to cases outside the LPA context like, for example, critical infrastructures.

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] 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.

[2] 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.

[3] ENISA, “National cyber security strategies in the world.” [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map (Accessed 8/2017).

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

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

[6] CEN, CENELEC and ETSI, “Focus Group on Cybersecurity (CSCG).” [Online]. Available: http://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx (Accessed 8/2017).

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

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

[9] 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.

 ISBN: 978-1-61208-582-1

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

 ISBN: 978-1-61208-582-1