Towards a Complex Systems Approach to Legal and Economic Impact Analysis of Critical Infrastructures

Thomas Schaberreiter[1,2], Gerald Quirchmayr[1,3], Anna-Maija Juuso[4], Moussa Ouedraogo[5] and Juha Röning[2]

[1]*University of Vienna; Faculty of Computer Science*
Währinger Straße 29, A-1090 Vienna
Email: firstname.lastname@univie.ac.at

[2]*University of Oulu; Faculty of Information Technology and Electrical Engineering*
P.O.Box 4500, FI-90014 University of Oulu
Email: firstname.lastname@oulu.fi

[3]*Ferdinand Porsche FernFH*
Zulingergasse 4, A-2700 Wr. Neustadt

[4]*University of Oulu; Oulu Business Scool*
Pentti Kaiteran katu 1, FI-90014 University of Oulu
Email: firstname.lastname@oulu.fi

[5]*Luxembourg Institute of Science and Technology; IT for Innovative Services*
5, avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette
Email: firstname.lastname@list.lu

***Abstract*—Information security has become interdependent, global and critical - it has become cybersecurity. In this complex environment, legal consideration and economic incentives are as integral to ensuring the security of information systems as the technological realization. In this paper, we argue that comprehensive cybersecurity requires that these three disciplines are considered together. To this end, we propose a legal analysis framework, which can can be used to study legal and economic requirements for cybersecurity in relation to technological realities. The framework yields concrete recommendations, which complex system and critical infrastructure stakeholders can utilize to improve security within their networks. The analysis framework aims to offer key stakeholders a better understanding of the legal and economic requirements for cybersecurity and provide them with recommendations that are in line with modern cybersecurity strategies, including the enhancement of cooperation and collaboration capabilities and the implementation of other state-of-the-art security mechanisms.**

***Keywords*-Cybersecurity, Critical Infrastructures, Complex Systems, Legal Analysis, Economics of Cybersecurity, Situational Awareness**

I. Introduction

Cyberspace or the cyber domain refers to the ability to electronically store, process and most importantly transfer information. The medium allows for an almost instant information transfer over great distances, and across national and legislative borders. Naturally this leads to security problems, since national cybersecurity legislations often have no effective means of dealing with or prosecuting crimes committed in cyberspace. In recent years, efforts have been made to find answers to cybersecurity questions on an international level. Especially the European Union (EU) has stressed the issue in its Cyber Security Strategy and the Network and Information Security (NIS) directive. Instead of centralizing cybersecurity legislation, the EU's approach has been to set a general framework for cybersecurity efforts which the member states have to realize individually. Cooperation and Coordination are central aspects of the EU cybersecurity strategy.

One of the key aspects of cybersecurity strategies is the protection of critical infrastructures (CIs). CIs provide services that are at the core of our modern society (like energy or telecommunication) and a disruption or destruction of these services would have severe consequences for society and the economy. Critical infrastructures are driven by complex and interacting systems. Due to their increasing connectivity to the cyber domain, attacks against critical infrastructures via the cyber domain are a possibility. Concrete examples have been observed in recent years, like the cyber attacks on Estonia in 2007 or the cyber attacks on the Ukrainian energy infrastructure in late 2015.

In addition to critical infrastructures, we will also consider other complex systems, which do not necessarily fulfil the critical infrastructure definition with respect their social and economic importance. Examples of such complex systems include cloud computing infrastructures and data hosting centres. While a service outage of such infrastructures may not necessarily impose severe consequences on the society or the economy, the security requirements for these systems are similar to those of critical infrastructures, owing to the potential of disrupting several co-hosted services in a single attack. Moreover, the providers of such services often do not have the resources to observe the security landscape, or to evaluate and implement proper security mechanisms. While the legal and regulatory requirements are shaping on a strategic level, there is a need to create mechanism that would ensure that complex system providers are following these requirements. This is more likely if the incentives of the providers are correctly understood and incorporated into the mechanisms.

Cybersecurity can be understood as the desired end state in which the cyber domain is reliable and secure. Safety and dependability of the information systems that run critical infrastructures is as reliant on economic incentives and legal/regulatory requirements as it is on technical design. In Figure 1, we identify *Technology*, *Economics* and *Law/Regulation* as the three key influences on cybersecurity. We argue that comprehensive cybersecurity can only be achieved if these three aspects are considered together and their interrelations are well understood. It is especially important to review regulatory policies with respect to economic incentives. Critical infrastructure operators want to operate in a safe and sustainable manner. However, their primary goal is to make a profit, not improve national security. Therefore, cybersecurity legislation needs to make business sense, to be successfully adopted by CI operators. If legislation is turned down or ignored by companies for financial reasons, then this will have a detrimental long-term effect of labelling cybersecurity legislation as a mere paper exercise.

Figure 1. Cybersecurity influences and interrelations

In this work, we will explore cybersecurity and the factors influencing it from a legal and regulatory perspective. Based on our analysis of the main economic, legal/regulatory and technological drivers for cybersecurity, we will propose a framework for *legal impact analysis* and a *recommendation system* which is in line with current cybersecurity efforts and brings them from a strategic to an operational level. In the impact analysis, we will examine legal and regulatory efforts and economic considerations in relation to technological realities, which are expressed in monetary terms. On the basis of this analysis, the recommendation system can give concrete recommendations for improving cybersecurity on a per case basis. As a result of our work, we expect that the ability for complex system providers to analyse legal requirements and economic recommendations related to cybersecurity will improve. This will in turn facilitate the deployment of state-of-the-art security mechanisms which meet legal obligations. We expect that collaborative and cooperative mechanisms, like security monitoring and information sharing, will have an increasingly important role as enablers of modern cybersecurity strategies.

The motivation of this workshop paper is to present our ideas to the scientific community and motivate discussion, in the hope that the feedback for the high-level framework presented in this work will contribute to the identification of concrete concepts and methodologies to achieve the goals set in this work towards practical realisation. Our goal for the near future is to further develop those ideas and initiate an EU level research project.

The paper is organized as follows: Section II discusses background and related work, Section III introduces the legal/regulatory, economic and technological drivers that are the basis for our work and Section IV details our ideas for a legal impact analysis framework and recommendation system. Finally, Section V discusses initial results and Section VI concludes the paper and gives an outlook on future work.

II. Background and Related Work

Legal and regulatory efforts concerning security in cyberspace have long been a national domain, which is at odds with the global nature of cyberspace. Skilled cyber criminals can often avoid effective legal prosecution, for example by committing a cybercrime in a jurisdiction that differs from their actual location. Effective mechanisms for cooperation and information sharing among nation states are often missing. This lead to the realization that effective cybersecurity can only be achieved on a global scale and in recent years efforts to synchronise cybersecurity law and regulation on an international level has increased. In December 2015, The European Parliament, the European Council and the European Commission agreed on the European Network and Information Security (NIS) directive as the first EU wide legislation on cybersecurity [1]. The directive lays down 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 decentralized prevention and response to cyber incidents and attacks, as can be seen in Figure 2. Coordination and information sharing are key elements of the strategy, together with the national NIS and the requirement for 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.

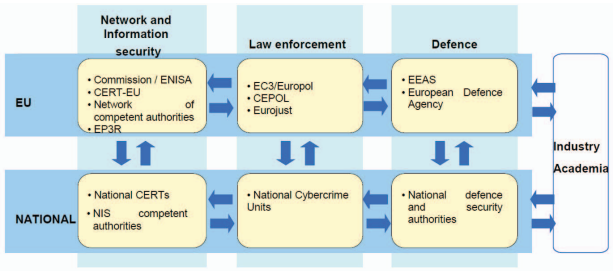

Figure 2. EU Cybersecurity strategy: roles and responsibilities

By now, most EU countries have put a national cybersecurity strategy in place [3]. For example, Finland has adopted its cybersecurity strategy as part of the more

general security strategy for society [4]. In line with the NIS strategy, the Finnish cybersecurity strategy is based on collaboration and cooperation. This aspect of the NIS requirements fulfilled by, for example, implementing a NIS competent authority in the form of a National Cyber Security Centre (NCSC). The Finnish cybersecurity strategy can serve as an example of a well developed national European cybersecurity policy. The European Union Agency for Network and Information Security (ENISA) has started an effort to assess and evaluate national cybersecurity efforts based on key performance indicators (KPIs) [5].

The United States of America (USA) published their cybersecurity strategy in 2011. Similar to the EU strategy, the main goal of the US strategy is to improve cybersecurity, and at the same time uphold the principles of fundamental freedom, privacy and free flow of information. While the EU's cybersecurity strategy heavily relies on coordination and cooperation, the US cybersecurity strategy highlights the need to establish behavioural norms among state actors and the central role of these norms in ensuring cybersecurity in an open, interoperable and reliable cyberspace.

Similar initiatives in the specific context of the Internet have been brought forward by the Council of Europe's Internet Governance [6] as well as the European Commission's Internet Policy and Governance [7]. The Internet is an extremely complex global system that is governed by many public and private stakeholders. The Internet has shown great social and economic potential, and in order to foster this development while maintaining the basic principles that made the Internet a success, new policies and governance structures should be discussed. The Council of Europe stresses the necessity to preserve the openness and freedom of the Internet, while at the same time improving privacy and security. The European Commission addresses similar problems and proposes that Internet governance is organized using a multi-stakeholder approach, complemented by a global forum to address core Internet decisions. It is stated that key issues to be addressed in the future are Internet policy, interplay between technical norms and conflicts of jurisdiction and law. A concrete measure planned by the European Commission is to develop the Global Internet Policy Observatory (GIPO), an online platform for monitoring Internet policy-making, regulations and technology in order to follow, understand and engage with Internet governance and policy.

Alongside the more recent efforts in cybersecurity, the Convention on Cybercrime [8] is the first international treaty to fight cybercrime. The goal of the treaty is to work towards a common crime prevention policy to facilitate detection, investigation and prosecution of cybercrime. Adopting appropriate legislation and fostering international cooperation are two main ways to reach this goal. The treaty has so far been ratified by many European and non-European countries.

On the standardisation front, the ISO/IEC 27000 [9] 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 counter measures. Similarly, the privacy focused ISO/IEC 29100 [10] 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 [11], to do strategic evaluation towards IT security, cybersecurity and NIS standardisation.

III. Motivation and Drivers

In this Section, we will provide an analysis of the main drivers of cybersecurity within CI. As depicted by Figure 3, the overall motivation for this work relies in the assumption that cybersecurity in complex systems results from technological and organizational changes, restructuring of economic incentives and improved regulations, laws and standards. In the following, we will discuss the legal, economic and technological drivers in detail. The impact analysis can be used for gaining a better understanding of different economic and legal approaches to cybersecurity. However, the primary focus of the impact and consequence analysis is to provide insight into the organizational and technological aspects of cybersecurity with respect to complex systems.

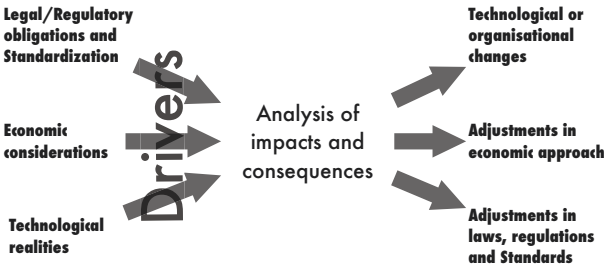

Figure 3. Motivation and Drivers for impact analysis

A. Legal drivers

Regarding legislative aspects, the major questions to be asked will focus on the technological and economic impact created by existing and by future planned legislation. With especially Europe going through a significant change in terms of the economy accelerating its increasing dependence on information technology, a sound legal framework dealing with the priorities of safeguarding a growing number of ICT based critical infrastructures, mounting privacy concerns and e-business questions including consumer rights, new frameworks are being and will continue to be introduced on a European level (e.g. General Data Protection Regulation [12], NIS legislation [1], National Cyber Security Strategies, National Information Security Legislation). At a time when the Industrial Internet of Things (IIoT) and Industry 4.0 are beginning to completely change the European economic landscape, the one open question is whether legislation, current and planned, is able

to provide the necessary safe and reliable environment for the economy and society to operate in.

When looking at legislation from a practical perspective, implementation and the associated cost are always a major issue. The most recent example is the vivid discussion following the proposal for a European General Data Protection Regulation. While privacy advocates focus on the necessity for strong safeguards, guarantees and effective penalties for breaches, industry is primarily concerned with the legislation being far too restrictive and in an extreme case endangering the existence of whole business models and preventing enterprises from continuing to operate in Europe. A quite recent court decision on the European level leading to the abolishment of the Safe Harbor Agreement [13] has made the potentially severe economic consequences transparent.

It is expected that, especially in the case of critical infrastructure protection legislation [14], economic concerns will play an even more important role. The central question is how much the legislation will cost, how much financial and other damage it can prevent and whether operators of critical infrastructures can afford to implement it. This leads to the question of incentives for the implementation of organizational and technological measures. As the issues of safeguarding critical infrastructures against cyber attacks affects the whole society, legislation needs to make sure that the cost of protective measures will be shared in a fair way. As basic infrastructures such as water supply, electricity, gas, ICT networks and transport are at the core of our modern economies, legislation for safeguarding them is of a very high importance. However, it is only an integrated approach combining legal, economic and technological viewpoints that will make legislation successful and enforceable. On the national and European levels budgetary consequences need to be assessed and legislative measures need to be introduced in a way that economic, business and societal reactions will not lead to time consuming blockades by interest groups. Given the expected high impact of such legislation, effective control mechanisms for assuring its correct implementation and effectiveness must accompany all new regulations.

B. Economic drivers

In economics, public intervention is justified, when it is able to remedy market failures and improve the efficiency of the markets. Firms make rational investment decisions considering the private costs and the benefits of their choices. Problems arise when these private costs and benefits do not align with social costs and benefits, i.e. in the presence of externalities. Within CI, the externality costs of a cyber attack arise from the role of CI in sustaining vital societal functions and they are aggravated by interdependencies within CI sectors and between them. These externality costs can be significantly higher than the private costs of a failure faced by the CI provider. For example, in the case of a power outage, the social costs, i.e., the costs paid by other businesses and the economy at large, are typically much larger than the revenue lost by the power company itself. Therefore, if the private benefit of critical infrastructure operators from improving cybersecurity is smaller than the social benefit, then firms will tend to underinvest in cybersecurity. Together with the vital role of CI, this tendency to underinvest justifies public intervention [15].

A typical approach to correcting such market failures is either letting the firms internalize the costs they impose on others by taxing them or encouraging them to reduce the externality costs by subsidising preventative measures. In analogy to environmental emissions, countries can either impose emission taxes and give tax breaks to companies implementing environmentally friendly technologies. However, while it might be plausible to support companies in their attempts to improve cybersecurity, the taxation of insecurity might be very difficult to execute. The reason for this is that, due to the lack of accurate information, it would be very challenging to identify and measure the externality costs.

In [16], Kox and Straathof identify informational challenges and externalities as reasons why firms may fail to invest in cybersecurity on a socially optimal level. We can identify two types of informational challenges: awareness and attribution. Firstly, if agents do not have accurate information on threats and vulnerabilities, they can underestimate their own vulnerability and the risk they impose on others. For a firm to internalize an externality, i.e. the costs its insecurity imposes on others, it must first be aware that its actions or lack thereof is harming others [16]. Secondly, the harmed party must also be aware that they are harmed [16]. If only the firm causing the externality is aware of it, then this can influence the firm's decision to invest in cybersecurity. In a study carried out in the Netherlands, researchers tracked the infection rates of all major Dutch Internet service providers (ISPs). It turned out that two of the ISPs trailed behind the others by a wide margin [17]. After learning about their position, one of the ISPs dramatically improved its performance and became one of best performing ISPs, while the other greatly improved its effort reaching the level of other ISPs.

Many in the field of cybersecurity have suggested information sharing as an effective technical solution to improving cybersecurity. From an economic perspective, information sharing can help improve cybersecurity within critical infrastructure in two important ways. Firstly, it can help rectify the informational challenges causing cybersecurity underinvestment [16]. Through information sharing, firms can become aware of their security posture and the risk they impose on others. Secondly, coordinated information sharing can reduce the cost of cybersecurity [15]. If firms shared information on breaches they have encountered, then other firms could detect similar attacks faster or proactively update their defences against such attacks. By not sharing information, firms essentially duplicate the same work [18]. Thus, sharing information would generate savings that could be used to achieve a higher level of cybersecurity. However, private-sector actors might be reluctant to share breach information,

because they fear that if the information is leaked, then it will hurt their reputation, make them more vulnerable, damage customer trust or affect the company's share price. By improving coordination within the information sharing partnership these leakage costs can be reduced [15].

C. Technological drivers

Complex systems are often based on technologies that were never designed with security in mind and they are often used in set-ups, configurations and interconnections which they have not been intended for. Security mechanisms are often circumvented or ignored in order to allow operation of the system. The technological reality is that those inherently insecure legacy systems are not going to go away any time soon. Systems or parts of systems are operated well beyond their intended lifetime, and instead of replacing legacy systems with ones that have a built-in and comprehensive security concept (designed-in and built-in security), systems will be patched or replaced only if concrete problems arise. Additionally, even modern systems are often not designed for or equipped with state-of-the-art security concepts and mechanisms. And if they do, the security comes at a price that stakeholders are not willing to pay since the security implications are either not understood well enough or the economic and legal incentives are missing. The advocacy from the research and industry for the integration of security activities throughout the system development life cycle has led to the uptake of assurance and certification as salient factor in determining the security and safety trustworthiness of components and subsystems prior to engaging with their integration in a broader system. Such efforts have lead to progress in standardization, for example the ISA/IEC 62443 series of standards is widely seen as the most relevant effort in the context of industrial automation and control systems (IACS) security. It entails amongst other efforts the adoption of secure design development principles and a layered-approach to security, whereby multiple security protections implemented at different layers could mitigate flaws in other layers.

Security of complex systems on the technological level is influenced by many factors, among the most challenging are the sheer *complexity* of the systems, the *diversity* of and the *dependency/interdependency* among components and systems. The characteristics of the complexity of such systems are that many individual components are interconnected and only the combination and connection of all components represents the system providing services. Those individual components and sub-systems are often owned and operated by different stakeholders governed by different regulatory bodies. A good example for this is the Internet, as a global system following a multi-stakeholder approach. The building blocks of the Internet are owned by many different private and public stakeholders and are, depending on their geographical location, subject to the respective national laws and regulations. The security aspects are driven by the organizational or national culture which makes coordination on the technological level challenging. The second factor is diversity which is defined by the observation that complex systems or parts of a complex system may be designed for specific tasks that bring unique characteristics to the complex system which are not present in others. For example, the electricity and the transport critical infrastructure sector provide fundamentally different services and some aspects like the electricity grid or the road network are unique to the sector. However, cybersecurity may be influenced by those aspects which makes it difficult to aim for a uniform security solution that can take into account sector specific characteristics. The third factor are dependencies and interdependencies. Complex systems are composed of many components that are interacting to provide a service. A failure or security incident in one component can cascade and cause service disruptions and security failures in other parts of the system. Furthermore, complex systems do not operate in isolation. A good example is critical infrastructure, where dependencies among sectors may exist [19]. A failure or security incident in one sector might cascade to another sector to cause security and/or service failures. A representative example is the dependence on the Energy sector, since nowadays almost everything relies on a constant supply of energy and a large-scale blackout can have severe consequences. In terms of security, it is important to understand and highlight the complex internal and external interactions and dependencies that define a complex system. In case of multi-stakeholder systems, there is a need to provide cooperation and coordination mechanisms that address dependencies.

While there are adequate and even excellent security mechanisms for parts of complex systems, a security concept that would account for the security needs of the system as a whole is often missing. An effective approach to improving the security of complex systems is to enhance situational awareness. In situational awareness, the individual components of the system are observed to gain an overall picture and, in the event of an incident, a timely response to the situation is possible. While situational awareness is usually used as a decision support system, where an administrator or operator is presented with all necessary information to make informed decisions, situational awareness can also be the basis of automatic or semi-automatic reaction-after-detection or self-healing systems.

An enabling technology for situational awareness is security aware monitoring, which allows for the derivation of security related indicators from continuous system measurements, presented to an administrator or operator in an on-line fashion. Furthermore, the information gained through security monitoring is a key factor for collaborative and cooperative efforts that depend on information sharing in order to improve security, like the recent cybersecurity efforts introduced in Section II. In recent years substantial research effort has been made towards security monitoring, some examples would be *risk monitoring* [20], *security assurance monitoring* [21] or *trust and reputation monitoring* [22].

The objective of risk monitoring is to observe certain aspects of a complex system and their interrelations and estimate or reason about what risks different behaviour could pose to the security of the system. The goal is to uncover complex relations among system elements in a socio-technical manner, taking into account the human, technological and organizational component of a complex system. In security assurance monitoring, the main goal is to give assurance to the administrator or the operator that the security mechanisms protecting a complex system are correctly implemented and working effectively to meet their design objectives. Security assurance monitoring is an important activity complementing risk assessment efforts and often relies on the management and coordination of existing network security tools or security information and event management (SIEM) technology [23]. In trust and reputation monitoring, the objective is to observe the behaviour of system elements and detect irregularities. Trust and, if applicable, reputation is derived from those observations.

While there are conceptual differences in the presented security monitoring techniques, they follow the same deployment and operation principle of *Analysis*, *Processing* and *Visualization*. The analysis phase has the objective to identify the security relevant components of a complex system, as well as the dependencies that influence security. Furthermore, measures that allow us to observe the state of the resulting system model are required. The analysis phase is a critical aspect of the security monitoring effort. The difficulty is to define a model that adequately describes the complex system, since only then the monitoring effort will give a realistic representation of the security state. In the processing phase, the identified measures are combined according to mathematical rules in order to get the desired security indicators representing, for example risk, assurance or trust, and in the visualization phase, the indicators are presented for quick analysis of and reaction to incidents.

Situational awareness to improve security in complex systems has a solid technological base, but these concepts and technologies have not been yet been adopted on a large scale. A plausible reason for this is the lack of incentives to implement such systems. On the one hand, the economic benefits that can be achieved through security awareness and information sharing are not well understood, and on the other hand, as of yet there have no legal or regulatory obligations to implement situational awareness mechanisms. Furthermore, there are no uniform or standardized ways to implement security monitoring, which would support the cooperation and coordination efforts of modern cybersecurity strategies.

IV. Legal analysis framework

In this Section, we present our idea of a *legal analysis framework* with the intention to assist stakeholders and operators of complex systems, such as critical infrastructure, to better understand the legal and regulatory requirements, and the economic incentives for improving cybersecurity. In accordance with current cybersecurity efforts, the focus is on recommending state-of-the-art security solutions and improving cybersecurity related cooperation and coordination efforts. The legal analysis framework is designed to be a semi-automatic decision support system which consists of an *impact analysis framework* presented in Section IV-A and a *recommendation framework* presented in Section IV-B.

A. Impact analysis framework

In the previous Section, we have outlined many reasons that highlight why the gap between legal and economic requirements and the technological realities in complex systems is one of the main contributors to insecurity. The objective of the legal impact analysis framework is to set the requirements in relation with those realities and to express the gap in monetary terms, by calculating the cost of not being in line with the legal requirements or the economic recommendations. In this work we present the high level framework and illustrate the different classes of information we expect are relevant in this context. The concrete methods and methodologies that will allow to set the information in relation are subject to future research. As can be seen in Figure 4, the inputs of the impact analysis system consist of all kinds of relevant legal information, economic considerations, technological information and standardizations on a regional, national, EU and international level. The output of the system is the estimated cost of not being in line with legal requirements, or industry best practices determined by standardization and economic considerations. While the legal and economic information is not subject to great fluctuation and only their relation may vary in a case dependent manner, the technological information does have a higher fluctuation and will change depending on the concrete system under investigation. The challenge is to capture the relation between the requirements and the reality, in order to identify possible gaps. This will be a semi-automatic effort, the analysis aspect can not be achieved automatically. The impact analysis framework intends to provide tool support for inputting the analysis results and setting them in relation to each other. This will provide the basis for the automatic calculations and estimates, which are the output of the framework. Visualization is an important aspect in this context. In order to capture complex relations among data and to allow for the input, review and correction of information, it is necessary to find a proper form of representation. Furthermore, only a clear and precise representation of the results will prompt decision makers to implement the necessary changes.

A common usage scenario of the framework would be to analyse relevant laws, regulation and standardization on a regional, national, EU and international level for their relevance to the security of complex systems. Requirements are identified and set in relation to each other. Possible relations could be a dependency (for example, a law could depend on an international standard for implementation) or conflict (for example, national and international laws

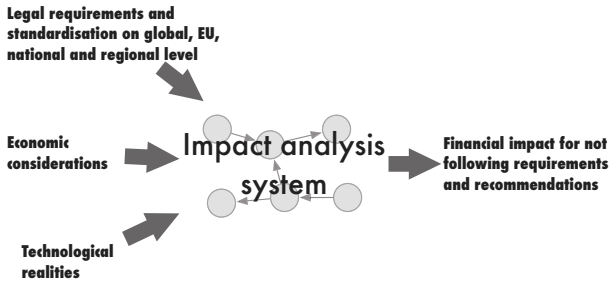

Figure 4. Impact Analysis System

could produce conflicting requirements). The economic recommendations for improving cybersecurity in complex systems are identified by analysing the economic incentives that determine the agents willingness to invest in cybersecurity. The economic requirements form the second source of security requirements and are used as an input for the analysis framework. Where applicable, the economic requirements are set in relation to the legal requirements.

The technological analysis is done on a per-case basis and the goal is to identify the major system components that influence security and the dependencies among these components. This analysis is done on a socio-technical level, where the organizational and human aspect of a complex system are given as much consideration as the technological considerations. The analysis results are a security centred dependency graph of the complex system. This graph is then set in relation to the requirements to see where adequate security mechanisms already follow the legal and economic specifications and where gaps between the requirements and reality can be identified. These shortcomings in combination with the estimated costs which, in most cases, are based on expert estimation, allow the calculation of the financial impact for not being in line with the legal requirements and economic recommendations.

B. Recommendation framework

The principle idea of the recommendation framework, which builds upon the impact analysis framework, is to give concrete recommendations helping decision makers to improve the security of a complex system. While many of the recommendations will focus on technological improvements, organizational aspects will also be considered. In line with the modern cybersecurity strategies, the focus of the recommendations will be on bringing all aspects of a complex system in line with state-of-the-art security principles and mechanisms, and to enable collaboration and coordination through security aware monitoring and information sharing. Furthermore, the recommendations should facilitate the coordinated replacement of legacy systems towards systems that follow security aware design and development principles to provide designed-in and built-in security mechanisms.

As can be seen in Figure 5, the recommendation system is based on the security requirements that are determined by the impact analysis, set in relation to the available security solutions and best practices. The output of the recommendation system are concrete security recommendations including a cost-benefit analysis. As stated previously, this work aims at specifying the framework for providing recommendations. The concrete methods and methodologies to achieve those goals are subject to future research.

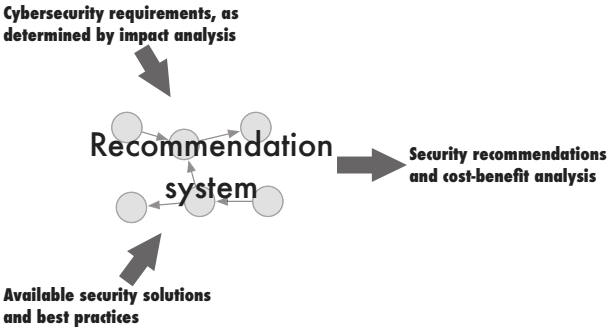

Figure 5. Recommendation System

The analysis of available security solutions and best practices are the main input of the recommendation system. It will be based on expert knowledge and provide an overview of the current security landscape and state-of-the-art solutions, together with the estimated cost of the respective measure. The security requirements determined by the impact analysis and the calculated financial impact associated with it will be set in relation to one or more solutions, in order to fulfil the requirement. The comparison of the financial impact and the costs allows us to calculate the potential benefit of implementing the solutions. While the fulfilment of the legal obligations will require the implementation of the security solution regardless of whether the financial impact of being in line with the requirement is smaller than the actual cost of the solution, security recommendations that are not based on a legal obligation may be ignored if the cost outweighs the benefit. As with impact analysis, the visual representation of results is a central aspect. Besides highlighting the financial benefit of the recommended security solutions, it is important to present a clear motivation for each recommendation to decision makers. These presentations will include a clear and precise description of the security requirement and why the recommended solution eliminates or mitigates the identified problem. Furthermore, a prioritization of actions which highlight fulfilling obligations over other recommendations will help decision makers to focus on the most important aspects of cybersecurity.

V. Discussion and Expected Results

We have presented a legal analysis framework that allows for the legal and economic impact analysis of complex systems, such as critical infrastructures and gives legal, technical and economic recommendations for improving cybersecurity. The framework is intended to assist stakeholders and decision makers in following legal

requirements related to their systems, and it highlights the possible financial gains from investing in cybersecurity. The novelty of this approach is that it considers legal, economic and technological aspects of cybersecurity together. We argue that only through the coordination of these different aspects will cybersecurity be improved in a sustainable manner. Such an approach also complies with the global nature of current cybersecurity efforts, which are moving towards cooperation and coordination, acknowledging and accounting for the multi-stakeholder nature of today's complex systems.

We expect that the legal analysis framework will provide stakeholders with better incentives to invest in cybersecurity, by highlighting the fact that cybersecurity is a common effort with cannot be solved in isolation. Contrary to the predominant company culture of keeping information secret to gain competitive advantage, cybersecurity is, due to its global nature, an effort that can only be improved if information about risks and incidents is shared in order to develop effective and coordinated counter mechanisms. While large corporations may have the resources and incentives to follow and analyse legal developments in cybersecurity, small and medium sized enterprises (SMEs) may find it challenging to analyse the complex legal ecosystem related to the security of their systems and to implement effective security measures. The legal analysis framework will help SMEs to understand and follow legal as well as economic requirements and improve the security situation sustainably.

The legal analysis framework will generate recommendations centred around two principles, both of which are essential to cybersecurity. First, complex systems need to follow state-of-the-art security principles. Secondly, coordination and cooperation mechanisms which are based on comprehensive security awareness are essential to cybersecurity. The adoption of state-of-the-art security mechanisms is often hindered by the presence of legacy systems which do not take security into account. This situation cannot be avoided. However, recommendations can be made on how these limitations can be mitigated. Additionally, there should be a focused effort towards phasing out and replacing the legacy systems with systems that have designed-in and built-in security properties. Cooperation and coordination mechanisms are an important aspect of cybersecurity. The enhancement of situational awareness and security aware monitoring form the basis for information sharing. Information sharing in turn enables cooperation and coordination, for example to assist first responders to handle incident and to help computer emergency response teams (CERTs) to coordinate the mitigation of large-scale attacks.

Aside from the operational improvements in cybersecurity, we also expect that the legal analysis framework is able to identify inconsistencies and conflicts in the legal and regulatory frameworks, by setting requirements in relation to identify dependencies. The legal framework analysis provides recommendations to the appropriate authorities, such as lawmakers, regulators and standardization bodies, to improve and align legislation.

In conclusion it can be said that legal impact analysis will be a continuous and ongoing process, where gradual improvements in the legal, economic or technical landscape will result in a changed situation, which in turn can cause assumptions to shift and trigger altered recommendations. Legal analysis is an iterative effort.

VI. Conclusion and Future Work

In this paper, we have presented the idea for a legal analysis framework that gives concrete recommendations for improving the cybersecurity of complex systems, like critical infrastructures, and a cost-benefit analysis for following those recommendations. The novelty of the approach is that it considers the legal, economic and technological aspects related to cybersecurity equally, based on the assumption that comprehensive cybersecurity can only be achieved if these aspects are considered together. The recommendations are based on a legal impact analysis that sets the legal and economic requirements of cybersecurity in relation to the technological realities by estimating the financial impact of not following the requirements.

We have discussed the legal, economic and technological drivers which define the current state of cybersecurity, and which need to be understood in order to improve cybersecurity in a sustainable manner. We demonstrated that the insecurity of cyberspace results from the lack of accurate information, and that cooperation and coordination among stakeholders is vital to the global effort to improve cybersecurity. In our review of current initiatives to introduce and improve the legal basis of cybersecurity, we showed that these initiatives are starting to acknowledge the global and multi-stakeholder nature of the cyber domain and that they are moving to towards introducing coordination and cooperation frameworks rather than absolute and unified legislation.

We expect that the legal analysis framework will support complex system stakeholders and decision makers in understanding the multifaceted legal and economic cybersecurity requirements, and give them the correct incentives to improve cybersecurity mechanisms within their systems. The recommendations given by the framework centre around two principles that are essential to cybersecurity. The first objective is to bring systems in line with state-of-the-art security mechanisms. The second one is to improve the cooperation and coordination capabilities of the complex system and critical infrastructure stakeholders through enhanced situational awareness and security aware monitoring. Furthermore, we expect that the legal analysis framework can detect conflicts and inconsistencies in legislation by setting the requirements in relation to each other, thereby providing a basis for recommendations that legal authorities can use to align conflicting legislation.

This paper is the first step in developing the proposed legal analysis framework. Its goal is to present the principal ideas to a wider scientific community with the purpose of opening this complex topic up to interdisciplinary scientific discussion. Future work will further the ideas

and develop an EU level research project as the next step towards realization.

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/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[4] Government Resolution, "Finland's cyber security strategy," 2013.

[5] European Union Agency for Network and Information Security (ENISA), "An evaluation framework for national cyber security strategies," 2014.

[6] Council of Europe, "Internet governance - council of europe strategy 2012-2015," Minsters' Deputies CM Documents CM(2011)175 final, 2012.

[7] European Commission, "Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. internet policy and governance - europe's role in shaping the future of internet governance," COM(2014) 72 final, 2014.

[8] Council of Europe, "Convention on cybercrime," European Treaty Series - No. 185, 2001.

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

[10] ISO/IEC 29100:2011, "Information technology — security techniques — privacy framework," ISO/IEC, Standard, 2011.

[11] CEN, CENELEC and ETSI, "Focus Group on Cybersecurity (CSCG)." [Online]. Available: http://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx

[12] European Commission, "Regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)," COM(2012) 11 final, 2012.

[13] Commission of The European Communities, "Commission decision of 26 july 2000 pursuant to directive 95/46/ec of the european parliament and of the council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the us department of commerce," Official Journal of the European Communities L 215/7, 2000.

[14] Council of the European Union, "Council directive 2008/114/ec of 8 december 2008 on the identification and designation of european critical infrastructures and the assessment of the need to improve their protection," Official Journal of the European Union L 345/75, 2008.

[15] A.-M. Juuso, "Cybersecurity investment and information sharing. an analysis of the economic incentives of private critical infrastructure providers," Master's thesis, University of Oulu. Department of Economics, 2015.

[16] H. Kox and B. Straathof, "Economic aspects of internet security," Netherlands Bureau for Economic Policy Analysis (CPB), 2013.

[17] M. van Eeten, H. Asghari, J. Bauer, and S. Tabatabaie, "Internet service providers and botnet mitigation: Fact finding study on the dutch market," Report prepared for the Dutch Ministry of Economic Affairs, Agriculture and Innovation, 2011.

[18] N. Weiss, "Legislation to facilitate cybersecurity information sharing: Economic analysis," Congressional Research service, 2015.

[19] S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *Control Systems, IEEE*, vol. 21, no. 6, pp. 11–25, Dec 2001.

[20] T. Schaberreiter, "A bayesian network based on-line risk prediction framework for interdependent critical infrastructures," Ph.D. dissertation, University of Oulu, University of Luxembourg, Public Research Centre Henri Tudor, 2013.

[21] M. Ouedraogo, "Valuation and reporting of security assurance at operational systems level," Ph.D. dissertation, University of East London, 2011.

[22] F. Caldeira, "Trust and reputation for critical infrastructure protection," Ph.D. dissertation, University of Coimbra, 2014.

[23] M. Ouedraogo, E. Dubois, D. Khadraoui, S. Poggi, and B. Chenal, "Adopting an agent and event driven approach for enabling mutual auditability and security transparency in cloud based services." in *5th International Conference on Cloud Computing and Services Science*, 2015.