Expertise
and insight
for the future

Peter Sund

The Rationality Gap between Cyber Security and Rule of Law in Extra-Territorial Processing of Classified Information on Cloud Environments

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

10 August 2020

PREFACE

This thesis is an effort to highlight the importance of understanding cyber security as a somewhat novel, but nevertheless integral element of the overall security of various organizations and thus linking cyber security to a wider conception of security compared to traditional IT (Information Technology) security as a pure engineering discipline.

The author wishes to shed light and examine some of the shortcomings existing in public and private sector cooperative processes and associated controls intended to maintain and support information security in a modern technological environment.

The contribution of this thesis to the constantly evolving discourse and development of policy and practice in the field of information security is to critically assess the government-controlled substantive risk assessment processes on protecting and securing government CLASSIFIED information on private organizations' platforms.

Gratitude and appreciation are extended firstly to all of the practitioners who are contributing to such processes and giving the best effort in a highly complex environment. Also, a word of appreciation needs to be expressed to the close colleagues that are maneuvering and creating business in these shallow waters as well as to author's academic mentor at Metropolia University of Applied Sciences.

Helsinki, 23 July 2020

Peter Sund

Author	Peter Sund
Title	The Rationality Gap between Cyber Security and Rule of Law in Extra-Territorial Processing of Classified Information on Cloud Environments
Number of Pages	54 pages
Date	10 July 2020
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor(s)	Ville Jääskeläinen, Head of Master's Program on IT

The question on territorial limitations to processing classified information is pressing and ongoing challenge within the industries operating in the fields of defence, security and technology. Due to the complexities and concerns over profitability for companies operating in multi-national settings warrants for moving towards cloud solutions also in operations involving classified information. The risk posed by governmental actors to the information security in extra-territorial processing of classified information on cloud environments has not been appropriately addressed.

This study focuses on the risk assessment associated with the validation of risk posed by governmental actors in the context of rule of law by consolidating the effects of jurisprudential factors to the information security in extra-territorial processing of classified information on cloud environments. The objective was to examine the extent of present risk assessment methodology concerning the protection of classified information processed in computer systems in the territory of another state. The second objective was to construct a model to consolidate the risk assessment utilized in various standards and normative documents such as PiTuKri by incorporation of jurisprudential risk factors. The study is limited to the issues relating to the development of policy and practice on protecting and securing government-classified information. To fulfill the research objectives a constructive research approach was applied and reinforced by the method of legal dogmatism.

Companies enjoy a wide variety legal rights—even fundamental rights—that should be utilized as the balancing weight to security authorities' intrusive and coercive powers. Hence, the responsibility of states to protect those rights have an effect on the probabilities of breaching the confidentiality of privately-held classified information—even when such legal powers would exist in the law. The findings of the study suggest for the inclusion of the element of rule of law by consolidating the effects of jurisprudential factors is to assess and validate the risk appropriately. The realities of states and how they operative should be examined and warrants for a multidisciplinary approach. The output of the study is the consolidated model "jurisprudential analysis framework" for the risk assessment that can be utilized in various standards and normative documents such as PiTuKri, or as a stand-alone risk analysis component for information risks. The framework introduces factors that concern the sate adherence to rule of law and factors concerning the powers and activities of the state security sector. From a wider societal and technological standpoint, the research contribution is one voice, one perspective in the discussion of trust in cyberspace.

http://URN:NBN:fi:amk-2020080919690

Keywords	Information security, cyber security, cloud security, classified information, rule of law, jurisprudence, extra-territorial processing

Tekijä Nimi Sivut Pvm	Peter Sund The Rationality Gap between Cyber Security and Rule of Law in Extra-Territorial Processing of Classified Information on Cloud Environments 54 sivua 10.7.2020
Tutkinto	Master of Engineering
Koulutusohjelma	Information Technology
Ohjaaja	Ville Jääskeläinen, Head of Master's Program on IT

Kysymys turvaluokiteltujen tietojen käsittelyn alueellisista rajoituksista on merkityksellinen ja jatkuva haaste puolustusalan, turvallisuuden ja tekniikan aloilla toimiville organisaatioille. Monikansallisissa ympäristöissä toimivien yritysten sääntelyvaatimuksiin ja kannattavuuteen liittyvien haasteiden vuoksi on perusteltua siirtyä kohti pilviratkaisuja myös salassa pidettävää tietoa koskevissa hankkeissa. Toisen maan viranomaisten aiheuttamaa tietoturvariskiä turvaluokiteltujen tietojen käsittelyssä ko. maassa sijaitsevissa pilviympäristöissä ei ole arvioitu asianmukaisesti.

Tässä tutkimuksessa keskitytään riskinarviointiin, joka liittyy valtiollisten toimijoiden aiheuttaman riskin validointiin oikeusvaltion puitteissa yhdistämällä oikeudellisten tekijöiden vaikutukset tietoturvaan salassa pidettävien tietojen käsittelyssä toisen maan pilviympäristöissä. Tavoitteena oli tutkia nykyisen riskinarviointimenetelmän laajuutta toisen valtion alueella tietojärjestelmissä käsitellyn turvaluokitellun tiedon suojaamiseksi. Toisena tavoitteena oli luoda laajennettu malli eri standardeissa ja normatiivisissa asiakirjoissa (kuten PiTuKri) käytettävälle riskinarvioinnille sisällyttämällä siihen myös olennaiset oikeudelliset riskitekijät. Tutkimus on rajattu kysymyksiin, jotka liittyvät turvaluokitellun tiedon suojaamista koskevan toimintapolitiikan ja käytänteiden kehittämiseen. Tutkimustavoitteiden saavuttamiseksi sovellettiin konstruktiivista tutkimusotetta vahvistettuna oikeusdogmaattisella menetelmällä.

Yrityksillä on laajasti oikeuksia, joista osaa voidaan pitää perusoikeuksien tasoisena, ja jotka ovat tasapainottava tekijä turvallisuusviranomaisten toimivallan arvioinnissa. Valtioiden vastuulla turvata näitä oikeuksia on vaikutusta todennäköisyyteen murtaa yksityisesti hallussa olevien turvaluokiteltujen tietojen luottamuksellisuus myös silloin, kun soveltuva toimivalta on laissa määritelty. Näihin realiteetteihin ja toimintaan on tarpeen perehtyä, ja se edellyttää monitieteistä lähestymistapaa. Johtopäätöksenä todetaan, että oikeusvaltioperiaatteen aiheuttamien oikeudellisten tekijöiden vaikutusten huomioiminen on tarpeellista riskin asianmukaiseksi arvioimiseksi.

Tutkimuksen tuloksena on laajennettu oikeudellinen riskinarviointimalli, jota voidaan käyttää eri standardien ja kriteeristöjen, kuten PiTuKri, kehittämisessä tai erillisenä komponenttina tietoriskien arvioinnille. Malli sisältää tekijöitä, jotka koskevat oikeusvaltion noudattamista ja tekijöitä, jotka koskevat valtion turvallisuussektorin valtuuksia ja toimintoja. Laajemmasta yhteiskunnallisesta ja teknologisesta näkökulmasta tutkimuspanos on yksi ääni ja yksi näkökulma keskustelussa digitaalisesta luottamuksesta.

http://URN:NBN:fi:amk-2020080919690

Avainsanat	tietoturva, kyberturvallisuus, pilvipalvelut, salassapitovelvollisuus, luottamuksellisuus, oikeusvaltio, oikeudellinen sääntely, valtio(instituutio)

Contents

List of Abbreviations

ECHR	European Convention on Human Rights
EU	European Union
FSC	Facility Security Clearance
GDPR	EU General Data Protection Regulation
GSA	General Security Agreement
ICT	Information and Communication Technology
ISO/IEC	International Organization for Standardization / The International Electrotechnical Commission
IT	Information Technology
KATAKRI	National Security Auditing Criteria (Finland)
MISWG	Multinational Industrial Security Working Group
NATO	North Atlantic Treaty Organization
NCSC-FI	The Finnish National Cyber Security Centre
PiTuKri	Criteria to Assess the Information Security of Cloud Services
Traficom	Finnish Transport and Communications Agency
UN	United Nations

1 Introduction

Finland is among the leading countries in digitalization. Recently, the Finnish government has expressed the desire to create a safer cyber environment in order to incentivize a boost in digital businesses and activities and at the same time to assure safety for its citizens. Additionally, the government has clearly recognized the risks present in cyber space and has declared that they are one of the most severe threats hovering over Finnish society.[1] According to Digibarometer 2020 Finland ranks second (in top three for the last seven years) against 22 countries evaluating how well individual countries make use of digitalization. However, the position of Finnish business organizations (companies) has dropped to 7th place (public sector and citizens are placing 2nd and 3rd place) and thematic placement in cyber security only slightly above average. Generally, in Finland investment on cyber security capacities is not at optimal level.[2]

It is projected that digitalization will lead to more and more integration of various computer systems and networks. As information moves between different actors in new ways and at an ever-faster pace, the development progresses towards more systematic and extensive networking. Digital platforms have played a key role in this change. Whether domestic companies will be able to pursue and benefit from this development better in the coming years is a decisive factor for Finland's future development.[3] Simultaneously, the magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user-confidence and cause major damage to the economy.[4]

Moreover, it should be noted that cyber security consists not only of threats against the functioning of network and information systems, but also threats against the critical information stored on computer systems. Such information is often referred as *classified information* due to the its nature and the potential, if its confidentiality would be breached

[1] Calcara, Sund & Tolvanen, pp. 9-10.
[2] Mattila et. al., pp. 6, 10-11.
[3] Mattila et. al., pp. 9.
[4] Directive (EU) 2016/1148, pp. 1.

or otherwise disclosed to unauthorized persons, to cause damage or harm to national security or to other legitimate interests of the state (including economic sustainability).

For such reasons States have developed various standards and normative documents, e.g. KATAKRI, PiTuKri (Finland), NIST SP 800-series (U.S.), Defence Standard 05-138 (UK), BSI Standard 100 (Germany), European Union Council Decision 2013/488/EU (EU) to regulate and impose administrative and technical controls to secure the processing of classified information in computer systems. Also, international standards exist, such as ISO/IEC 27005:2011 for information security risk management. States are sovereign and thus have complete freedom to impose any requirements they wish to secure *state-owned* (Classified) Information on computer systems, no matter where such data geographically or physically resides. From a legal perspective such requirements are often considered to be administrative decisions or other non-regulatory frameworks enacted by mandated public bodies such as national cyber security authorities (e.g. National Cyber Security Centre of Finland[5]). However, the non-regulatory status of such frameworks may be challenged in some other respects (*de facto*) as in reality non-compliance any of the required frameworks often results to either exclusion of the commercial project, or to a liability claim on breach of agreement and in worst case to a criminal responsibility. This issue will not be further discussed in this study. For the purposes of this study such standards and frameworks may be referred as *authority documents*.

On the international level there is no legal hierarchy between States where “someone would always have the last say”. However, States can for example bind themselves to certain obligations via various treaties.[6] Until now, there is no common international framework on which kind of controls should be implemented by all actors under the States’ authority. At best, there are some national or supra-national frameworks (authority documents) that may be more or less commonly utilized in more than one state (e.g. NATO, EU).

In essence, such kind of authority documents are based on threat and risk assessments concerning those computer systems that are processing state-owned (or owned by international bodies e.g. EU, UN or NATO) classified information. The key of such risk assessments is the identification and assessment of various cyber threats e.g. technical

[5] See more https://www.kyberturvallisuuskeskus.fi/
[6] Sund, pp. 83.

vulnerabilities, exploits, computer attack vectors, as well as administrative weaknesses on organizing aforementioned data processing, storage and/or transfer of it.

This thesis is a study on the risk assessment associated with the validation of risk posed by *extra-territorial governmental actors in the context of rule of law* i.e. the effect of jurisprudential factors to information security risk in extra-territorial processing of classified cnformation on cloud environments. The objective is to critically examine the extent of present risk assessments concerning the protection of classified information in computer systems in the territory (hence under the legal control) of another state. The intent is to analyze some of the shortcomings of risk validation and associated controls intended to maintain and support information security in a contemporary technological environment. For the purposes of the study information security measures mean the administrative, functional and technical measures to ensure the availability, integrity and confidentiality of various information, data and datasets[7].

The study focuses on finding a model for consolidating the interdisciplinary approach to risk assessment i.e. the effort is to move away from purely technological "techno-oriented" risk assessment (purely technological vulnerabilities of the computes system) towards a more holistic assessment by incorporation of legal factors (the legal controls and remedies that can contribute to the security of a computer system). In legal discourse there are always two distinct issues: what is the content of the law and how it is applied in practice. This discussion is often referred as *law in books* and *law in action*[8]. This study focuses on explaining the content of the law as referred to *law in books*, and limitedly also the *law in action* as to the extent of operation a law has on society. Many organizations have experienced difficulties interpreting existing laws, as well as preparing for upcoming legislation. As laws have become increasingly relevant to information security activities, close coordination between legal and information security teams has become pivotal in ensuring legal considerations are embedded into security practices and that legal professionals can understand the technical areas on which they provide legal advice. Use of cloud services has been identified as one of top ten legal issues of interest to information security practitioners.[9]

[7] See e.g. Act on Information Management in Public Administration (906/2019), Finland.
[8] See for instance: Hage, pp. 8.
[9] Bickerstaffe, pp. 3.

The main target of the study is the Finnish Transport and Communications Agency's (Traficom) National Cyber Security Centre (NCSC-FI) and its formal governance over the national authority documents, namely KATAKRI and PiTuKri. Especially PiTuKri (Criteria to Assess the Information Security of Cloud Services) as the main source of assessing the security risk to information in cloud-based computer systems. As cloud-based systems are often established over multiple countries (jurisdictions) PiTuKri criterion remains the most relevant reference in terms of the effect of rule of law on the risk to classified information.

This thesis is also an effort to highlight the importance of understanding cyber security as (somewhat) novel, but nevertheless integral element of the overall security construction in various organizations and thus linking cyber security to a wider conception of security as opposed to traditional IT (Information Technology) Security as a pure engineering discipline.

The study is limited to the issues relating to the development of policy and practice in information security by analyzing critically government-controlled substantive risk assessment process on protecting and securing government-classified information on private organizations' platforms. The purpose is to contribute to the discourse on the strategic objectives of information security and its potential adverse effects to business in modern digital environments.

The thesis also limits its scope to the risk posed by governmental actors due to the fact that the context of rule of law applies directly only States themselves. Furthermore, it is arguable that the risk posed by non-governmental (criminal) actors is already well covered by the administrative and technical controls imposed in these authority documents. This argument can be further reinforced by examining the controls themselves as they point out rather clearly that in course of history the intention has been to prevent unauthorized access to classified information before the invention of any clouds. In the earlier days computer systems processing classified information were essentially physical local servers inside the organization allowing access only from local networks and endpoints.

In this thesis the term cyber security is used to describe the security in digital environments, i.e. computer systems. Hence, cyber security is not interchangeable with information security. Within the context of this thesis, additional to computer systems,

information can also reside in other forms of media (paper documents) and under the human cognition as in person's memory.

The thesis has been divided into six chapters. The first chapter introduces the research question and the background to the study leading the reader into the subject and helps to orientate to the context. It introduces the overall goal and objectives of the paper and talks about the story behind the endeavor. The second chapter describes the research approach and methods utilized. It also illustrates the sources of information and scientific orientation. The more detailed discussion on the current state and the practical problem at hand is collected under chapter three. There are also discussions about the basic assumptions and rationale of choices made. The theoretical background with introduction to the theories of risk and assessment, confidentiality, integrity and accessibility as well as International law and legal reality is elaborated in chapter four. Chapter five focuses on the results and analysis attempting to demonstrate and validate the construction of the consolidated risk model. Finally, in chapter six the conclusions are summarized, and a wider research contribution is suggested.

2 Method and Material

Applied research is one of the three main forms of research, along with basic research and experimental development[10]. Applied research is research that is applied, using parts of the accumulated theories, knowledge, methods and techniques of the research community. Applied research deals with practical problems and is generally empirical. Due to such kind of research residing firmly in the "real" world with various challenges and limitations it may be impossible to adhere to strict research protocols. Consequently, transparency in the methodology becomes critical. Also, openness to method of interpreting results becomes important.[11]

The fundamental questions in scientific research are reliability and validity. In constructive research, there is always also the issue of the form of validation. Generally, validity means the solidity of the conclusions derived from the research data. In other words that the research is actually examining what it was planned to study. Validity is an important factor of quality in a research because it refers to possible systematic problems of the methodology or the conclusions of the study. Validity can be divided into internal and external validity. Internal validity alludes to the systematic solidity of the research. External validity alludes to the overall generalization of the results in its respective context. To achieve a high level of validity the research needs to score good "points" in both areas.[12]

This type of approach requires a form of validation that doesn't need to be quite as empirically based as in other types of research such as exploratory research[13]. Nevertheless, the conclusions have to be objectively argued and defined. This may involve evaluating the "construct" being developed analytically against some predefined criteria or performing some benchmark tests with the prototype. The term "construct" is

[10] Experimental development is systematic work, drawing on existing knowledge gained from research and/or practical experience, that is directed to producing new materials, products or devices; to installing new processes, systems and services; or to improving substantially those already produced or installed. OECD, Glossary of Statistical Terms.
[11] Guimaraes, pp. 23.
[12] Hirsjärvi et al.
[13] Exploratory research provides insights into and comprehension of an issue or situation. It often relies on secondary research such as reviewing available literature and/or data, or qualitative approaches such as informal discussions with consumers, employees, management of competitors, and more formal approaches through in-depth interviews, focus groups projective methods, case studies or pilot studies. Although results of qualitative research can provide some indication as to "why", "how" or "when" something occurs, it cannot answer "how often" or "how many". Hence explanatory research avoids definitive conclusions, or at least exercises caution in drawing such.

often used in this context to refer to the new contribution being developed. Construct can be a new theory, algorithm, model, software, or a framework.[14]

Reliability means the possibility to repeat the results of measurements. In other words, reliability means the ability to produce non-random results.[15] One challenging issue for most of the studies is how to justify the results. The results and conclusions of the study should be reliable and not dependent on the person(s) who conducted the study.

In order to maintain the validity and reliability of the research three main strategies are implemented: firstly, the research methods are carefully selected, and their scope transparently discussed as well as suitability for the purpose justified. Secondly, the construct (consolidated risk assessment methodology) is developed analytically against predefined criteria derived from jurisprudence and, hence having a solid scientific backing. In spite of the legal science not being a precise method of calculation that produces a guaranteed outcome the study utilizes only normative institutions (social constructs) that have undergone robust research and form a paradigm within the field of jurisprudence. Thirdly, additional to putting special emphasis on the rationality of conclusions drawn from analyzing the risk assessment frameworks (e.g. PiTuKRI) the argumentation of the choices made during the construction of the consolidated model will be provided.

There are two distinct research methods used in this study: constructive research and legal doctrine. The study focuses on constructing the theoretical model for the validation of risk posed by extra-territorial governmental actors in the context of rule of law. Hence, a material analysis is conducted both on the relevant literature concerning current methodology on information security assessments as well as elements constituting relevant legal protection against host nation's willful actions against the classified information of another nation. The constructive process of the latter is further reinforced by applying a method of legal doctrine, i.e. legal dogmatism, to describe the systematics and interpretation of the law, including relevant legal principles.

[14] Guimaraes, pp. 24-25.
[15] Hirsjärvi et al., pp. 213.

Constructive method

New approaches to complex societal challenges require a diverse mix of resources and skillsets from different disciplines to create solutions that are of a transdisciplinary innovation nature. The constructive research method enables the purposeful creation of methods, modules, tools, and techniques that, via purposeful synthesis, have a potential for greater transdisciplinary objective. The constructive approach divides the research process into six phases as illustrated below in the following figure (originally presented by Kasanen et al. 1993).[16]

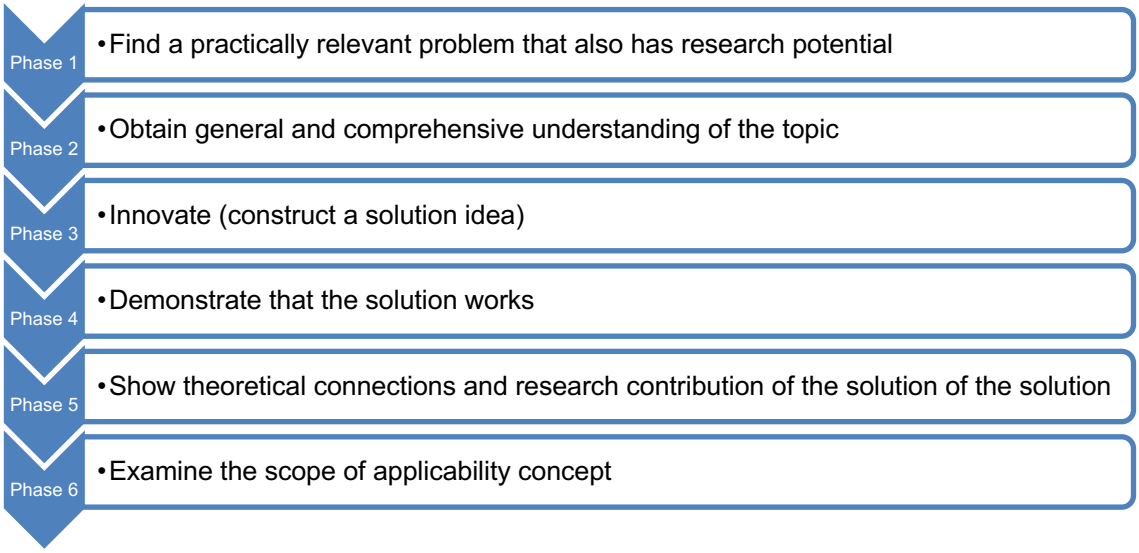

FIGURE 1. Theoretical model of a constructive method.[17]

While building a knowledge society, the understanding of knowledge production, both on the level of cognitive science and on the level of technological enhancements provided by ICT is becoming strategically important. In this context a very general view of Computing as Science and Computing as Engineering is needed wherefrom also necessity follows of understanding of Computing in both Philosophy of Science and Philosophy of Engineering contexts. In short, engineers have discovered the innovative potential of broad insights into the discipline, which gives tangible comparative advantage.[18]

This paper is aiming for the theoretical model to have an impact on how the information security risk assessments are carried out in practice. Hence, selecting a constructive

[16] Lukka, pp. 84. and McGregor, pp. 1.
[17] McGregor, pp. 9.
[18] Dodig Crnkovic, pp. 1.

method as the research strategy is justifiable.[19] The pressure to develop more efficient co-operation between scientific research and the practical business world has grown in recent years. The constructive approach is one such attempt to close the gap between science and practice.[20] The key idea of Constructive research, is the construction, based on the existing knowledge used in novel ways, with possibly adding a few missing links. The construction proceeds trough design thinking that makes projection into the future envisaged solution (theory, artifact) and fills conceptual and other knowledge gaps by purposefully tailored building blocks to support the whole construction. Artifacts such as models, diagrams, plans, organization charts, system designs, algorithms and artificial languages and software development methods are typical constructs used in re- search and engineering.[21] Hyötyläinen, Häkkinen & Uusitalo (pp. 1-7) have discussed, and summarized a plethora of research of the nature, objective and limits of constructive research in the following way:

> *The relationship between research and practice has played a key role in scientific research (Habermas, 1974; Weick ,2003; Holmström et al., 2009). Furthermore, there has been a blurring of the boundaries between research and practical development (Kaplan &Norton, 1992; Kaplan, 1998). Research is considered to be fundamentally a scientific problem-solving process (Laudan, 1977). The traditional role of the research community is seen as understanding and explaining the phenomena under study. It has also been suggested that research is not just about understanding and explaining issues and phenomena, but also about changing them (Burke, 2002), and the creation of new ideas and innovation (Chesbrough, 2003). Innovation belongs to the sphere of the practical world, with knowledge-creation processes (Nonaka, 1991).*
>
> *Constructive research is an approach that endeavors to create innovative constructions. Problems occurring in the real world and in real companies are solved with their help. It is typical for constructions to be invented, created and built. A new reality that differs from the previous reality is clearly being created here (Kasanen et al., 1993). Furthermore, it is characteristic of constructions that their functionality is verified. The*

[19] Järvinen & Järvinen 2000, pp. 12, 102, 153-171
[20] Hyötyläinen, Häkkinen & Uusitalo, pp. 1.
[21] Dodig Crnkovic, pp. 2.

innovation of a construction is, thus, not about the traditional discovery of new information, although its purpose is to show the theoretical novelty value of the construction (Kasanen et al., 1993; Lukka, 2003). It can be stated that the constructive research approach mainly produces and results the mid-range theories, from the perspective of research (Holmström et al., 2009). This mostly involves theoretical generalisation and the scientific assessment of the results (Pettigrew, 1990).

The constructive research approach does not take a definite stance on the different forms of information. The basic idea is that the construction is produced by tying it to previous knowledge (link to theory). The theoretical novelty value of the construction must be shown and, possibly, its link to a theoretical foundation (Kasanen et al., 1993; Lukka, 2000, 2003).

Furthermore, they have suggested for a framework for clarifying the categories of research and development information. In the figure, two different interest and agent groups are separated by a dashed line: practical agents and researchers. Practical agents are particularly interested in problems and their definitions, as well as constructive solutions that work in practice; these can be concepts, models, methods or tools. Researchers, however, are interested in theories, the novelty value of the solution, and theoretical results.

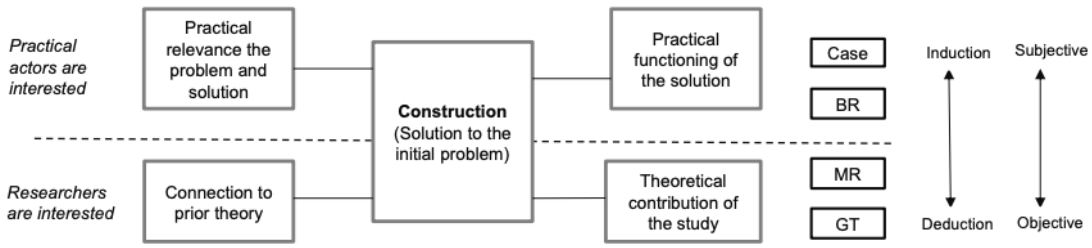

FIGURE 2. Information classifications in the context of research and development.[22]

In this study, the research interest in on the part above the dotted line, however establishing a verifiable link to prior theory and suggesting the theoretical contribution of the study. The overall understanding of the systems and procedures, experiences and

[22] See also Lukka, pp. 85.

views of existing approaches serves as a basis of a new construction. This is further elaborated in the following Table 1, Overall plan of the study.

Legal Dogmatism

In traditional legal research, authoritative texts like legislation, case law (created by courts) and doctrinal literature (e.g. documents related to the process of developing and enacting legislation) are considered the main formal sources of information for understanding positive law. Building on this information legal scholars organize, analyze and represent this information in such a way as to persuade their colleagues, legislators, judges and practitioners to follow their line of thought [23]. Law means a rule that is enforceable through institutions contrary to moral rules or values[24]. More widely understood, law is a complex set of norms, practices and ideas with closely interwoven mental, cultural, moral, religious foundations, experience of the previous generations, values of freedom and justice. However, in this study law is understood as issued in the form of legislation, command of the sovereign or purely as an instrument of state policy.[25] The term *positive* law refers to man-made laws that oblige or specify certain action. The distinction is important when compared to some other forms of "law" that may be considered originating from supernatural origins such as "God" or "Nature". In principle, positive law can have whatever content as disposed by man. However, in most nation states (jurisdictions) there are broad limitations to the contents of law. These limitations depend often in practice on the shared ethical and moral values of the society, as well as the legal culture and the legitimacy of the government and its methods of governance all in all [26]. These issues will not be discussed further in this study.

In general, legal doctrine is an example of a practice of argumentation, pursuing knowledge of the existing law. Acts of legislation form a sort of skeleton of the rule of law; these skeletons come to life due to other factors (such as governmental information steering, various operations and processes of the public authorities, court rulings as well as direct enforcement of the law). Hence, acts of legislations should not be considered narrowly and textually, often irrespective of the broader methods of their interpretation, which demonstrate the creative role of judicial practice and legal doctrine.[27] As a

[23] Langbroek, van den Bos, Thomas, Milo & van Rossum, pp. 2.
[24] See e.g. Merriam-Webster dictionary at https://www.merriam-webster.com/dictionary/law or Legal Dictionary at https://legal-dictionary.thefreedictionary.com/law
[25] Semenihin, pp. 9.
[26] See more e.g. Tuori, K. 2002. Critical Legal Positivism.
[27] Semenihin, pp. 9.

scientific method, legal dogmatism stands the closest to legal practice in the context of multi-level study of law and is most directly linked to reality in the cognitive sense. Hence, legal dogmatism is well suited for the purpose of understanding law with rational persuasion power and in the light of generally accepted fundamental values. [28]

Álvaro Núñez Vaquero quotes well-renowned professor Aulis Aarnio: "Ordinarily legal dogmatism is defined as the study of the content of the legal rules (norms) and of the systematic order of those. The common terms referring to these tasks are interpretation and systematization." Consequently, the aim is to determine the content of law, that is, to establish which is the legal qualification of a certain conduct (behavior) in a given legal system. That is, the method and/or the activities of those engaged in establishing what is the legal qualification that corresponds to a behavior according to a legal system, and those behaviors that the legal system does not recognize as having legal value.[29] In short, the way how legal dogmatism aims to answer to the question of "What is justice?" by stating that "Justice is such law that is valid i.e. in force and binding".[30]

Also, Hirvonen quotes Aarnio when he points out that the method of legal research (e.g. legal dogmatism) is not a precise method of "calculation" that produces a guaranteed outcome when the relevant variables are inserted to the equation. Legal rationale is not a process that operates mechanically by utilizing only distinct and definite rules.[31] Whereas natural facts exist in the physical world, legal norms (laws) exist in the world of ideas as intersubjective institutions. Facts are caused by other facts in a causal relationship. Legal norms are attributed to other legal norms, meaning that a norm causes a legal consequence to be imposed upon non-compliance to such norm. For instance, a norm stating that computer message interception (one form of hacking) is criminal behavior and punishable by law does not cease being law because the hacker is not punished (e.g. not getting caught). Instead, the legal norm remains valid that the hacker ought to be punished exists due to the law saying so. Hence, law operates in the way that:

1. Criminal code (law) states that computer message interception is a crime;
2. A hacker conducts an action that fulfills the characteristics of the said criminal behavior;

[28] Narits, pp. 19.
[29] Vaquero, pp. 58-59.
[30] Hirvonen, pp. 22.
[31] Hirvonen, pp. 7.

3. The hacker shall be punished in accordance with the law.

The Method Incorporated

The method of constructive research as discussed in previous chapters is incorporated with the method of legal dogmatism and then adjusted to the objective of the research study. As noted earlier, the focus of the study is the risk assessment of the threat posed by extra-territorial governmental actors in the context of rule of law to classified information in computer systems within the territory of that state. The objective to propose a more holistic model for consolidating the interdisciplinary methodology of such risk assessments by incorporation of a legal dimension to it. The proposition is limited to the "case Finland" i.e. the national risk assessment framework called PiTuKri establishing requirements for controls and measures to maintain adequate level of confidentiality of government classified information. This is going to be achieved by analyzing the logical approach of the current risk management model of PiTuKri and applying a new layer of knowledge to it from a non-technical environment, that is jurisprudence. Jurisprudence refers to the social context of law i.e. legal system. Below is an illustration of the applied incorporation providing practical rationale and steps for the study.

TABLE 1. Overall plan of the study.

Phase	*Constructive Research*	*Application*	*Chapter*
1	Find a practically relevant problem that also has research potential	Observed rationality gap in the methodology of assessing risk concerning the threat posed to classified information in computer systems within the territory of another state by governmental actors of that state. It seems that the rule of law as (external[32]) social reality have been ignored from the context. In risk assessment all possible realities should be taken into consideration as they contribute to the release and exposure assessments of a given risk.	1 and 3

[32] External refers to exposure processes outside of the computer system itself. Vulnerabilities of a given system are often identified as part of the release process. See e.g. Cherdantseva et al, pp. 7-8.

2	Obtain general and comprehensive understanding of the topic	Analyze relevant authority documents (risk assessment and control criteria), set theoretical framework (Information security, risk assessment, rule of law etc.).	4
3	Innovate (construct a solution idea)	Develop a methodology of jurisprudential legal indicators that are able to characterize the relevant legal reality in a given jurisdiction (state).	4
4	Demonstrate that the solution works	Apply the layer of jurisprudence (rule of law) to the IT system risk assessment framework to include external exposure process to the model.	5
5	Show the theoretical connections and the research contribution of the solution	Validate logical connections between the IT system's release and exposure processes (contact with a threat agent) and relevance of social (legal) reality to the determination of risk.	5
6	Examine the scope of applicability concept	Discuss the feasibility to apply in the context of Finland, and more widely in terms of various jurisdictions.	6

The table sets out the overall plan for the study. Each of the Phases will be addressed under the dedicated chapters as depicted in the table: The problem and focus of the study is discussed in chapters 1 and three; The scope and in-depth understanding of the issue as well as the suggested solution is discusses in chapter 4; The validation of the solution as well as theoretical backing is discussed in chapter 5; Finally, the wider scope of applicability and potential is discussed in chapter 6.

3 Current State Analysis

In this chapter the practical problem is discussed further. As noted earlier in chapter 1 States have developed various standards and normative documents, e.g. KATAKRI, PiTuKri (Finland), NIST SP 800-series (U.S.), Defense Standard 05-138 (UK), BSI Standard 100 Series (Germany), European Union Council Decision 2013/488/EU (EU) to regulate and impose administrative and technical controls to secure the processing of Classified Information in computer systems. Different frameworks and certifications measure different things. For instance, some frameworks enable the certification of the information security management system so that the assessment of the adequacy of technical controls relies on the risk management decisions of the target organization of the certification. This approach is different from the model generally used for the protection of classified information, in which the authority who owns the information sets minimum requirements for the protection of information; these requirements accompany the information throughout its life cycle in all processing environments and situations.[33] Although there are efforts to streamline and ease operating in the complexities of the privacy and security requirements in an multi-national environment, such as the European Security Certification Framework (EU-SEC)[34] it does not remove the necessity on understand more deeply and comprehensively of what is the possible risk posed by governmental actors when classified information is processed extra-territorially under jurisdiction of another state.

States are free to impose any requirements they wish to secure state-owned (classified) information on computer systems. There are several mechanisms to implement such requirements:

- Systems directly under state control (state-owned systems, usually operated by public authorities);
- Systems interlinking to state responsibilities and the protection of fundamental rights (e.g. critical infrastructure, often owned by private organizations and requirements imposed via legislation and public-private agreements);

[33] PiTuKri – version 1.0., pp. 4.
[34] The project "European Security Certification Framework" (EU-SEC) aims to create a European framework for certification schemes and evaluation concepts to secure cloud infrastructures. Within this framework, existing national and international certifications can co-exist. EU-SEC will improve the business value as well as the effectiveness and efficiency of existing cloud security certification schemes. See more on https://www.sec-cert.eu.

- Systems processing state-owned classified information (e.g. private military suppliers, requirements imposed via public-private agreements); and
- Systems with no direct connection to the above but having independent information security interest (e.g. private companies using such standards as benchmark to improve their information security level).

This study focuses on the private IT systems processing state-owned Classified Information. Typically, a state authority about to release any Classified Information to a private organization (company) would first require compliance to a standard that is required for the state systems as well. The logic is based on the idea of assuring the same level of Information Security no matter where (in which system) the Information is processed. Without compliance, no release, often meaning also no business.

Now, as it is generally well-known that in terms of digital information a location of access to information may differ from location of storage of information. In other words, a point of access may be physically be somewhere else that where the data is stored. EU General Data Protection Regulation (GDPR) provides a useful frame to understand what data processing means. In accordance with Art. 4(2)

> *data processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Removing the term "personal" from the definition provides an exhaustive list of activities that can be understood as data processing. The key notion is that storage, transmission and any kind of use are all considered processing. The term processing shall be used hereinafter on any of these activities.*

Coming back to the issue location of data (classified information). The data may be processed by a company only when there is verified compliance to the standard in question. For a company to develop and demonstrate the compliance may be time consuming and costly, but usually purely in national context not overwhelming to any actor that is in general operating in a market segment where government Classified Information is processed as part of business (e.g. military or defense sector). Often

companies consider the return-of-investment (RoI) before entering into cooperative agreements with governmental authorities.

The situation becomes exponentially challenging when the company operates in one or more following dimensions:

- Has legal entities or physical premises that process Classified Information in more than one country;
- Operates both in commercial civilian business sector and government sector at the simultaneously;
- Has international staff both in substantive work processes (core business) as well as in support functions (e.g. IT system admin);
- Is using externally (and internationally) contracted companies (third parties) in business-critical IT systems (e.g. enterprise resource planning, document management, customer relations management) maintenance and management; and
- Has or may have governmental customers from various sectors (e.g. military, critical infrastructure, large-scale ICT systems etc.) and from various States.

When taking these various dimensions into consideration it may be rather clearly observed that the operational-regulative environment may become highly complicated, if not conflicting in many regards.

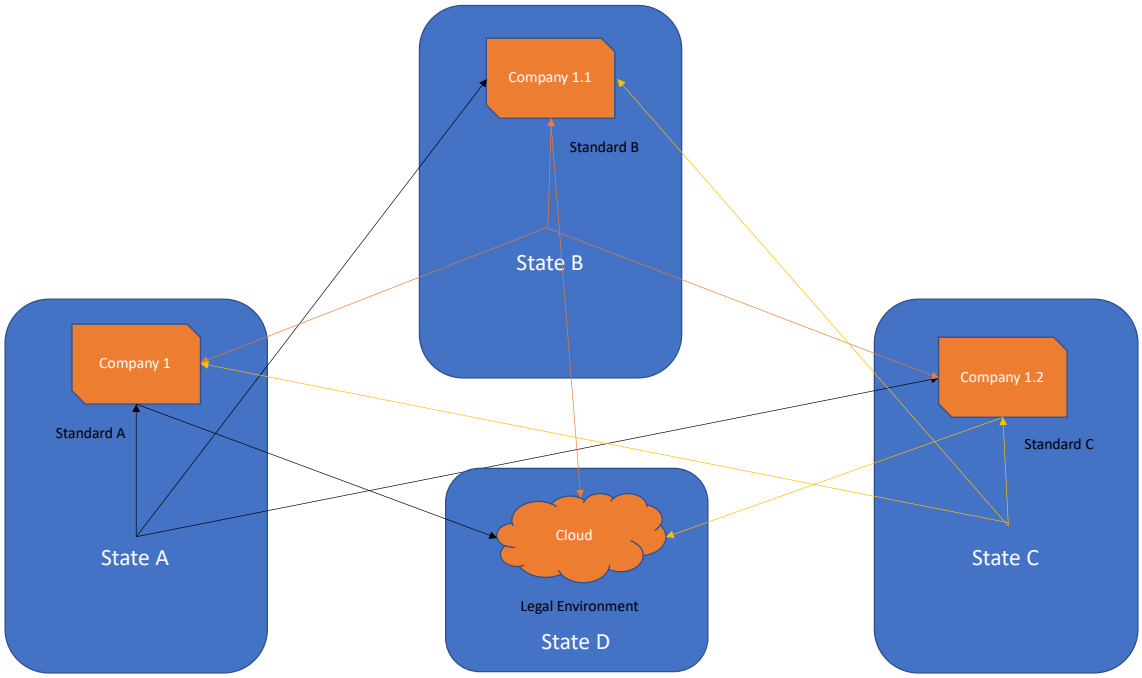

FIGURE 3. Simplified complexity of various regulative frameworks.

Figure 3 indicates only the potential requirement of various regulative frameworks to a company with several organizational units in different States. The arrows represent a set of requirements and the Company 1 acting as the parent company. It leaves out the dimensions of sub-contractors, suppliers, third party service providers, and the personnel who may be with different nationalities within one organizational unit. It also leaves out the system-internal technical requirements. Additional to many of technical requirements stemming from the various standards, one separate requirement may be that the standard, or the customer may require that the classified information released to the company shall be stored only within the jurisdiction of the state owning the data. As noted earlier, storing data is only one aspect of processing data, hence separating storage from other types of processing may be outdated as a way of thought, or at least practically obscure.

Re-iterating the problem that is arising from the current practices is the fact that States, via their regulative standards may see possible to manage the risk of breach of confidentiality of the classified information by technical and administrative controls imposed to the companies, firstly by way that external persons (to the company) would not breach the confidentiality of the data by criminal actions, and that those internal persons eligible to process the data are reliable and trustworthy (e.g. by means of personal security clearances). However, the risk of persons external to the company

compromising the data by (mis)using the legal environment in a state of where processing is conducted is currently managed with very limited array of controls. In fact, often with one control only: no storage of data (at rest) outside the jurisdiction of the data owner. Consequently, such approach is likely to elevate the challenges of a multi-national company to virtually unmanageable level when any other form of processing (e.g. in transit or in use) would require some separate means of managing the data.

Hence, it has become apparent that a full spectrum of data processing (including storage i.e. information at rest) for classified information will eventually have to become possible within private organizations in response to globalization, expansion of information society, digital business and growing demand of real-time availability of data to provide products and services to the markets. This can only be done effectively if the data owners understand the real extent of risk towards the Classified Information they release to the possession of companies, and how the said risk can be managed.

Currently, Traficom's (NCSA-unit) position on cloud services (expressed in PiTuKri criteria) is contrary to the general progression of the digital platforms and may not stand the test of time. This issue can be summarized from a discussion extract occurred in a consultative process concerning the new revised version (1.1) of the PiTuKri on March 2020 with Traficom and an accredited auditor:

> *In essence, one organization in the Finnish Government is saying "go to the cloud, even for TL-IV if the security is taken care of" while another is replying "You can go to the cloud, but we will not certify any cloud service for TL-IV level unless it is hosted in Finland and in other respects follows a rather old-fashioned ways of IT service provisioning."*

4 Theoretical Background

In this chapter the efforts on understanding the topic and innovating something new are highlighted. The purpose of this section is to provide for substantial background information on the main theoretical contexts the study operates in, namely risk assessment, fundamental attributes of data management as well as legal reality. Furthermore, the subsection of legal reality strives to affirm the narrative on how law shapes the reality of human communities.

4.1 Risk and assessment

Risk can be defined as characteristic of as situation or action wherein two or more outcomes are possible, the particular outcome that will occur is unknown, and at least one of the possibilities is undesired. Another common definition is risk as the probability of occurrence for an undesirable outcome. [35] In this study the term *risk* is used to describe the potential negative outcome, and the term *uncertainty* is used to characterize the degree of confidence in the potential outcome based on the confidence of the analysis.
Risk assessment can be defined as a systematic process for describing and quantifying the risks associated with hazardous processes, actions or events. In general, risk exists when three conditions a met:

1. Existence of a source of risk i.e. system, process or activity introducing a risk agent (e.g. IT system containing classified information);
2. A valued asset being exposed to a risk agent (e.g. classified information confidentiality breached); and
3. Existence of a causal link between exposure and an adverse effect (e.g. Information released to an unauthorized person).

These conditions – *releases* from a risk source (i.e. threat agent), *exposures*, and consequences – are often called a risk chain. Quantification of risk requires quantification of knowledge and uncertainty about each link in the chain.[36]

Cherdantseva et al. quote Kaplan and Garrick in explaining risk in the following way:

$R=\{s_i,p_i,x_j\}, \qquad i=1,2,...,N$

where

R – risk;

[35] Covello & Merkhover, pp. 2.
[36] Covello & Merkhover, pp. 5.

{} – must be interpreted as a "set of";

s – a scenario (undesirable event) description;

p – the probability of a scenario;

x – the measure of consequences or damage caused by a scenario; and

N – the number of possible scenarios that may cause damage to a system.

They continue in applying the method to IT systems (SCADA) and explain that a risk is a function of the likelihood of a given threat source exploiting a potential vulnerability and the resulting impact of a successful exploitation of the vulnerability. When applied to quantifying cyber security risks in computer systems the formula for calculating risk is accepted as follows:

$R = tvx_{tv}$,

where

t – threat;

v – vulnerability; and

x_{tv} *– the consequences of the threat successfully exploiting the vulnerability.*

Risk assessment answers the following three questions[37]: What can go wrong? What is the likelihood that it would go wrong? What are the consequences? Risk management builds upon the risk assessment in order to answer the other three questions[38]:

- What can be done and what options are available?
- What are the associated trade-offs in terms of all costs, benefits, and risks?
- What are the impacts of current management decisions on future options?[39]

4.2 Confidentiality, Integrity and Accessibility

Information and use of the digital medium are essential elements in any modern business enterprise or public administration. As noted earlier, information security measures consist of administrative, functional and technical measures to ensure the availability, integrity and confidentiality of various information, data and datasets. These three dimensions are considered as the prerequisites of high-quality management and secure

[37] Originally in Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Anal 1981;1(1):1137.
[38] Originally in Chittester C, Haimes YY. Risks of terrorism to information technology and to critical interdependent infrastructures. J Homel Secur Emerg Manag 2004;1(4):article 402.
[39] Cherdantseva et al, pp. 2.

processing of information in all computer system designs. The value of information is achieved and maintained by adhering to these three recognized principles:

- **Confidentiality**: Information is protected adequately, and access to information and systems is only available to those who have authority for its access and use on the basis of need;
- **Integrity**: The correctness of information and fidelity of associated systems. Information is accurate and complete, and unauthorized access to systems is prevented; and
- **Availability**: Systems and technology are designed and maintained such as to enable the availability of all information and systems as and when required.[40]

Although there are also other suggestions to expand the above-mentioned principles, for the purposes of the study, for instance non-repudiation is considered as part of integrity and traceability of information are considered part of confidentiality. Due to the limitations of the study and the focus of constructive effort is on the dimension of confidentiality, neither integrity nor availability are discussed further. However, it is highlighted that for instance this "trinity" of principles is treated e.g. in the Convention on Cybercrime (the Budapest Convention)[41] as conjoint in the way that actions against any of these principles are to be criminalized. The Convention recites:

> *…Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation.*

The recital is further elaborated in Chapter II, Section 1 in the Convention listing the criminal typologies under substantive criminal law as "Offences against the confidentiality, integrity and availability of computer data and systems". Typically, these are crimes such as Illegal access or interception, data or system interference, misuse of

[40] See e.g. Fruhlinger.
[41] Council of Europe Convention on Cybercrime (CETS No 185), pp. 1-7.

devices, computer-related forgery or fraud, offences related to child pornography as well as offences related to infringements of copyright and related rights.

Confidentiality under PiTuKri

The Information types that are applied in PiTuKri are divided into categories based on their requirements for protection (Table 2). The translation of "Information to be kept secret" may be slightly difficult to comprehend in English language due to the nature of direct translation. However, the key aspect in this category is that information is identified and labeled as classified information, but is not associated with any particular "protection level" from IV to I. Hence, it means there are no particular handling requirements contrary to those having a labeled protection level, but only the requirement by law to maintain the confidentiality of the information by suitable means until otherwise decided by the owner.

TABLE 2. Types of information adjusted from PiTuKri – version 1.0.[42]

Type of Information	Description
Public	Public information. Needs for protection are typically related to integrity and availability.
Information to be kept secret	Information of the authorities that is to be kept secret but has not been classified and does not contain personal data.
Personal data	Data pursuant to special legislation (such as the EU GDPR) related to the protection of personal data and hence to be treated as information to be kept secret.
TL IV	Classified protection level IV, national RESTRICTED information of the authorities. The need for protection generally arises from the security of the state (public interest). Protection must also take into account legislation derived risks[43].

[42] PiTuKri - version 1.0, pp. 6.
[43] Legislation-derived risks refer to possibilities under legislation of different countries to obligate cloud service providers to cooperate with the authorities of the country in question and to provide, for instance, direct or indirect access to the cloud service customers' information to be kept secret. In addition to the physical location of information to be kept secret, legislation-derived risks may extend to disclosure of

TL III + TL III aggregate	Classified protection level III, national CONFIDENTIAL classified information of the authorities. The need for protection generally arises from the security of the state (public interest). Protection must also take into account legislation derived risks. Also, the aggregate effect (large quantity of "information to be kept secret") may sometimes constitute level III, e.g. comprehensive personal data of the government security authorities and/or other personal data that can risk operational security. Also, the aggregate effect (large quantity of TL IV information) may sometimes constitute level III.
TL II	Classified protection II national SECRET classified information of the authorities. The need for protection generally arises from the security of the state (public interest). Protection must also take into account legislation derived risks.
TL I	Classified protection I national TOP SECRET classified information of the authorities.

Different types of information are subject to different risks. For instance, it is generally considered that classified information of the authorities should be protected from the perspective of the security of the state (the public interest). On the other hand, it is reasonable to assume that criminal actors interested in classified information are often not the same as criminal actors interested in non-classified personal data.[44] There are also other reasons to protect classified data as enacted by the law[45], such as personal privacy (e.g. health information or political association) and private financial interest (e.g. trade secrets). Notwithstanding the reason for labeling information as classified after classification all information is required to be protected adequately.

information administrated from another country through management connections. In many countries, legislation-derived disclosure and right to view data are limited to the police and the intelligence authorities.
[44] PiTuKri - version 1.0., pp. 6.
[45] See more in the Act on the Openness of Government Activities (Finland), section 24.

As it can be observed from Footnote 39 that PiTuKri takes note on the "legislation-derived risks" but it does not address how to analyze the level of risk in different jurisdictions, which is the objective of this study. Hence, accepting risk as the probability of occurrence for an undesirable outcome meaning that some sort of analysis would have had to occur for the particular risk, noting such can hardly be called risk at all as no evidence is provided on such probabilities. Nonetheless, it is not to say that there would not be legislation-derived risks at all, but moreover they seem to be ambiguous at best. It is self-evident that the threats identified as legislation-derived are against the confidentiality of classified information.

4.3 The Law of Nations

Considering the data residing outside of the jurisdiction of the legal holder it is particularly relevant as to the fact that there are two considerations to what comes to what States can do under their jurisdiction (i.e. territory): While it can be taken with certainty that state sovereignty implies that a state generally enjoys, within the limits set by treaty and customary international law, the exclusive right to exercise jurisdiction and authority on its territory[46]. In other words, States indeed are sovereign and can legislate for instance the extent of coercive powers of the law enforcement sector. However, States may only do so within the remits of international law (law of nations) [47].

No doubt that states may choose to not abide by international law, and even to break a specific treaty. However, such violations, particularly of customary international law and norms which no derogation is permitted can be met with coercive action, ranging from military intervention to diplomatic and economic pressure.[48] Furthermore, as of 2001, after 45 years of "dispute" there is a significantly clearer normative framework on laws of state responsibility governing when and how a state is held responsible for a breach of an international obligation with the adoption of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts[49]. For instance, under international law, States

[46] Schmitt, pp. 25.
[47] International Law refers to the set of rules and norms generally accepted in relations between nations. It establishes normative guidelines and a common conceptual framework to guide states across a broad range of domains, including war, diplomacy, trade, and human rights. See more on https://en.wikipedia.org/wiki/International_law.
[48] Ibid.
[49] The United Nations General Assembly adopted resolution 56/83 on 12 December 2001. See further: UN General Assembly, A/RES/56/83, Fifty-sixth session on 12 December 2001.

may be responsible for cyber operations[50] that their organs conduct or that are otherwise attributable to them by virtue of the law of state responsibility[51].

The aforementioned certainly applies to the primary rules of international law i.e. customary and treaty rules that lay down the substantive obligations of states (e.g. state immunity, diplomatic and consular immunities, respect for territorial sovereignty). Nonetheless, the discourse on whether the general obligation of protecting the fundamental rights of legal entities (companies) having for instance legally established in another state but processing (e.g. storing) classified information in that state via using a cloud service provider would be extendable as a particular responsibility of the state is yet to occur. Regardless, the objective of this study is to examine what, and to which extent, any treaty and customary international law limits the exclusive right of a state to exercise jurisdiction and authority in the context of information and data privacy.

4.4 Legal reality

Aarnio cites MacCormick and Weinberger on the ontology of legal knowledge, a legal "institution" being defined in a similar way as a chess piece turns out to be a king, another a queen, etc. According to, the constitutive norms structure the lifespan of a legal institution, but not only them. According to these authors, there are five kinds of institutive norms:

- Constitutive norms;
- Rules of recognition;
- Rules and standards of argumentation;
- Rules of articulation; and
- Legal injunctive rules of the first degree.

The first group of norms is constitutive *sensu stricto*, the latter four mostly focus on the functioning of the institution. The four latter groups are not further discussed here. Marriage is an often-cited example of a legal institution, whereas the marriage between A and B is an institutional fact. It articulates the institution (marriage). John and Jane might well live in a social micro-community, but they are not treated as spouses without a certain normative foundation. Norms constitute the institution as a marriage, defines

[50] The term cyber operations refer to the employment of cyber capabilities with the primary objective of achieving objectives in or by the use of cyberspace. See more in Schmitt, pp. 24.
[51] Schmitt, pp. 24.

its functions and marks its extinction.[52] In this respect, a nation state is an institution like marriage, in which certain facts are interpreted with the help of the rules of the "game". When a state requires a company to implement physical measures (such as a firewall) to its computer system, and subsequently it can be concluded that a given company is compliant against that requirement. However, in order to be able to state such a fact, certain concepts have to be understood, for example government, law, regulation, compliance and so on.

In the context of this research only the constitutive norms and to certain extent to the rules of recognition. Aarnio refers to H. L. A. Hart's "rule of recognition:

> *The rule articulates an institutional support for a legal norm (or legal order). The rule of recognition gives an institutional guarantee for a certain norm as regards its validity. Having an institutional support, the norm at issue does belong to the legal order. One who deals with law from an external point of view focuses his attention on whether people have accepted the institutional support as a basis for the legal order or not. This kind of statement concerning the acceptance of the rule is an empirical argument and can thus be true or false.*

Aarnio continues, that in order to know which norms are accepted as valid in a certain community, one has to know something about the internal point of view of the community members. This presupposes information about the commitments of those having the internal perspective. Only those norms that are voluntarily accepted as binding are valid in that community.[53] Now, in full acknowledgement to the wider discourse on legal positivism and criticism on the qualifications of the validity of legal norms it can be argued that the viewpoint is nevertheless useful in understanding the law as socio-behavioural reality. Furthermore, not forgetting that at least in western societies law *de facto* containing the dimension of coercive force. Law is a power system. The courts realise the use of coercion by defining which actions fulfil the threat of sanction.[54]

This research study commits to the theoretical tradition of legal positivism and hence recognizes the following premises:

---

[52] Aarnio, pp. 9.
[53] Ibid. pp. 10.
[54] Aarnio, pp. 18.

- Laws are behavioural commands established by human beings;
- The relation between law and morality is weak, or non-existent, thus law can be of whatever content (also unjust, unwise, inefficient or imprudent); and
- A legal system is a closed, logical system in which correct decisions can be deduced by applying legal rules without reference to social considerations; and
- Legal norms (laws) are coercive, moral norms are not.

In other words, legal positivism accepts law as purely social construction that can be understood as intersubjective institutions.

Avoiding of falling into the pitfalls of legal theory and philosophy it can be argued that a widely accepted definition of "rule of law" would suffice to fulfil the requirement of "voluntarily accepted as binding". The United Nations (UN) Secretary-General has defined the term rule of law in the following manner[55]:

> *A principle of governance in which all persons, institutions and entities, public and private, including the state itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires measures to ensure adherence to the principles of supremacy of the law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness, and procedural and legal transparency.*

In order to understand the interconnection between rule of law and voluntary acceptance few relevant elements of the definition should be clarified. Firstly, the element of publicly promulgated laws. Public promulgation means a public announcement of new laws or government's declarations. Hence, everyone has equal opportunity to acquire knowledge of, and verify, what is legal conduct. In spite of various types of government, essentially the common denominator for raising acceptance is the idea of the process of legislation being public and also allowing participation to it, at least on the level of public debate. Hence. the arguments, justifications and legality of a new legislation is public (and publicly accessible).

Secondly, the element of accountability to the law. Accountability is connected to the idea no one being "exempted" from the application of the law and hence, the laws being

[55] UN Secretary-General.

equally enforced and independently adjudicated. The rule of law is fundamental to peace and security and political stability; to achieve economic and social progress and development; and to protect people's rights and fundamental freedoms. It is foundational to people's access to public services, curbing corruption, restraining the abuse of power, and to establishing the social contract between people and the state.[56] These qualifications are in the center of legitimacy of the state and the acceptance of the social order. One can trace the idea of a social contract back to the 17th century when Thomas Hobbes first formulated the idea of the legitimacy of the authority of the state over the individual. In short social contract means that individuals have consented, either explicitly or tacitly, and submitted to the authority (of the ruler, or to the decision of a majority) in exchange for having the remaining rights protected and/or the social order maintained.[57, 58] The Social Contract theory contains the following logic of interdependency:

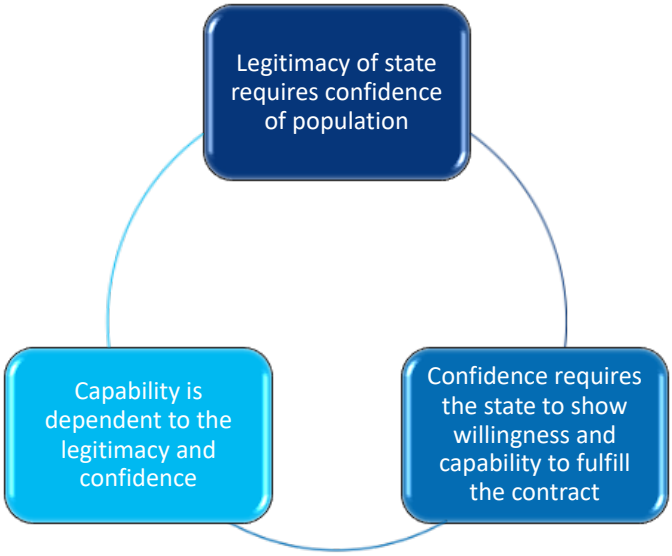

FIGURE 2. The confidence to the state, adjusted from Social Contract theory.[59]

Now, it can be concluded that since the legitimacy of the state requires confidence of the population which, in turn, must be redeemed by genuine effort of fulfilling the social contract i.e. protecting the agreed rights of the people, including the fact that everyone needs to "play by the same rules". Similar to any team sport such as football, the rules need to be equally enforced to all players and the judges have to have independency

[56] United Nations.
[57] Friend. Also, Wikipedia (Social Contract).
[58] For instance, in so called western societies submitting to the decision of the majority essentially means accepting democracy as the political model.
[59] Sund.

adjudicate the observed violations of the rules. More widely speaking, being accountable to the law means facing allegations of legal liability in relation to complicit conduct. In other words, being held accountable in public for acts and omissions, decisions, policies, and expenditures. Legal accountability is the most unambiguous type of accountability as the legal scrutiny is based on detailed legal standards, prescribed by civil, penal, or administrative statutes or precedent.[60]

Moving back to the central issue of the chapter, the following is what can be said of what reality in the legal sense means: Legal reality is of what is intersubjectively shared as true by a community of people. What are essential concerns of the intersubjective meaning, or to be exact, what makes shared intersubjective meanings possible. It is what all the individuals belonging to a certain community believe about the world. The institutions and institutional facts exist for those individuals because the institutions are based on shared mutual beliefs, and further, because those people believing in the institutions also act in accordance with the beliefs.[61] How is this relevant to the research on the risk assessment associated with the validation of cyber risk posed by extra-territorial governmental actors in the context of rule of law? Firstly, due to the fact that the designers of such risk assessment frameworks should not just imagine, invent or substitute whatever reality existent in another state. As the purpose of science in general is studying the world around us and figuring out natural “laws” governing it, so are social sciences doing the same. The law and legal sciences describe of what is existent as true in human communities. Hence, in the field of information technology and engineering (e.g. cyber security) that deals with the practical application of scientific knowledge must adhere to the foundations of that knowledge. Under these circumstances it is simply a misconception to believe that any conceivable threat would be realizable in a given factual environment. In any law-governed democratic state, the state itself is obligated to protect human rights and the main task of the judiciary is to provide a real mechanism for it.[62]

By way of a state protecting human rights also the rights of the private business via two distinct ways: firstly, by protecting the human rights of the owners and stakeholders (e.g. employees) of a company, and secondly by the way of legal entities/persons are

[60] Bovens, pp. 2-7.
[61] Aarnio, pp. 10-11.
[62] Semenihin, pp. 10.

protected to certain, and largely sufficient extent[63]. Naturally, companies have also obligations within the context of human rights, but these are not addressed here[64]. Companies are legal constructs created for the benefit of human beings—not merely of the stakeholders, but of society as a whole, since a modern economy could not exist without them. Companies are considered "right-and-duty bearing units" and there is no reason why it should be otherwise when it comes to fundamental[65] rights. That is also the position in international law. Companies may enjoy fundamental rights for two reasons: because it is essential to protect their own interests; and because it is necessary for the sake of the public interest. In the latter case, a fundamental right is said to be conferred on companies on utilitarian grounds e.g. companies benefit from the freedom of political speech at least in part because that is essential for democracy. Thus, it is strongly arguable that the rule against double jeopardy (*ne bis in idem*) is not merely a safeguard for the accused, but also serves to prevent the courts being encumbered with repetitious prosecutions.[66] Fundamental rights companies enjoy in general, and relevant to the study, are:

- Right to conduct a business;
- Right to property;
- Freedom of association;
- Freedom of speech/expression;
- Right to respect for private life, his home (partially extended to a company's offices) and correspondence (telecommunications), i.e. right to privacy;
- Equal protection of law, right to an effective judicial remedy and right to a fair trial e.g. via right to a defense, presumption of innocence and freedom from unreasonable searches and seizures; and (while having limited relevance to the purpose of the study), and
- Specifically, to EU the fundamental freedoms: free movement of goods, persons, services and capital; as well as
- Right to submit a complaint to the Ombudsman and petition to the European Parliament. [67]

---

[63] As eloquently expressed in German Basic Law of 1949, which reads: "Fundamental rights also apply to domestic legal persons to the extent that their nature permits." See further in Oliver, pp. 692.
[64] See e.g. The UN Guiding Principles on Business and Human rights approved in 2011.
[65] The term *fundamental rights* are often used to refer either to human rights in general, especially in European context, but may also be used to refer to such basic rights that can be attributed to other than humans, e.g. companies. However, in general they mostly refer to similar set of rights that are considered inherent and inalienable to the subject as basic rights and freedoms.
[66] Oliver, pp. 664.
[67] In reference to e.g. the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, the U.S. Constitution and the "Basic Rights Law" of Germany.

In summary, the starting point is that companies are fully fledged legal persons in their own right and are under the law are treated as such, discounting in the highly exceptional situations where piercing of the corporate veil is appropriate. Companies differ from natural persons in several crucial respects. For instance, they enjoy privileges such as limited liability and "perpetual life" but cannot vote or stand for political office. Companies must enjoy the fundamental rights essential to their functions and purpose, namely the right to property and the right to run a business (where such a right exists) as well as the right to a fair trial. [68] Hence, one can safely conclude that in the context of States having a solid tradition on respecting fundamental rights companies do have legally protected backing for its privacy and full control of its assets, including information and other intellectual property. This conclusion can, however, be valid only to the extent of primary rule. It is the exceptions in the law that determine the final residual risk.

In the tradition of the classical notion of rule of law, the interference of the state with fundamental rights should, as a general rule, be possible only if it could be based on a general norm established by a parliament in the order prescribed by the constitution. However, this kind of limitation is applicable only to the public administration (assuming that e.g. security authorities would otherwise by susceptible to arbitrary practices).[69] What limits the people (parliament) to enact laws that would be arbitrary to the purposes of fundamental rights? Good governance is a fundamental procedural right that is often present in legal traditions of States with conviction to human and fundamental rights in general. It has several effects:

- The fundamental right to good governance may have direct legal effects as such. It could therefore be relied on in a legally effective manner, at least in its own case; and
- The responsibility of the legislator (parliament) adopting the necessary organizational or procedural provisions for the exercise of a fundamental right. The underlying idea is that the fundamental right provision in a given Constitution requires the support of ordinary legislation, which creates concrete legislative arrangements within which individuals can exercise their fundamental rights; and
- The general conditions for restrictions of fundamental rights apply to all laws.[70]

[68] Oliver, pp. 695.
[69] Koivisto, pp. 25.
[70] Ibid., pp. 25.

The general conditions for restrictions of fundamental rights may include:

- The accuracy and precision of the law (precision of restrictions and terminology);
- The acceptability of the restriction (e.g. an attempt to protect another fundamental right);
- Proportionality of the restriction (absolute necessity to achieve the objective and cannot be achieved by less intrusive means);
- The inviolability of the core area of fundamental rights (cannot be interfered with to such an extent as to invalidate the essence of the right);
- The adequacy of legal protection arrangements (effective judicial remedy); and
- Compliance with international human and fundamental rights obligations.[71]

Hence, generally speaking, the stronger the legal tradition on fundamental rights, the less derogations to the primary rule could be expected. And even with such derogations, the more restraints for authorities to abuse those legal powers and more comprehensive array of means for the company for legal defence and effective judicial remedy.

[71] Lainkirjoittajan opas, 4.1.

5 Results and Analysis

In this chapter an effort given to demonstrating and validating that the innovation works. The application of supplementary element of jurisprudence (rule of law) to the IT system risk assessment framework will be discussed. The intention is to validate the logical connections between the IT system's risk release and exposure processes and the relevance of social (legal) reality to assessing the risk. This element is seemingly external to the current technologically oriented risk assessment practices. Hence, exposing the current methodology to critical evaluation it is expected that the limitations become more apparent allowing an additional element to be integrated to the model.

5.1 PiTuKri Criteria

The Criteria to Assess the Information Security of Cloud Services (PiTuKri) objective is to improve the security of authorities' information to be kept secret in situations where the information is processed in cloud computing environments. "Keeping secret" refers to maintain the confidentiality of classified information. The criteria are intended as a tool for security assessment of cloud computing services. The criteria address authorities' protection level IV classified information as well as other information confidentiality to be maintained. The security requirements described in the criteria are designed to keep the most typical risks facing classified and other information confidentiality to be maintained at a tolerable level.[72]

PiTuKri documentation is divided into ten subdivisions; Subdivision 1, Framework conditions, has a special role with respect to the other subdivisions. The framework conditions define the possibilities for further assessment and support the risk management work of the authorities responsible for the protection of national information to be kept secret. For certain information to be kept secret, there are grounds for carrying out further assessment of a public, multinational cloud service, for instance. For some information, further risk-based assessment possibilities may be limited to nationally provided private cloud computing services.[73]

[72] PiTuKri - version 1.0, pp. 3.
[73] Ibid., pp. 3.

The most common cloud computing deployment models are private cloud, hybrid cloud and public cloud. Private cloud refers to service provided for exclusive use by a single organization. A public cloud is a service publicly available for open use by anyone. The service is practically always provided from the service provider's data centers. A hybrid cloud combines a private and public cloud into a single service configuration. For instance, a private cloud on the organization's own data center may be supplemented with services from a public cloud. No matter of the deployment model for the purposes of this study the focus is on the physical location of the data center i.e. data residing outside of the jurisdiction of the legal holder of the classified information (private company). Pinpointing this issue has special regard to the study as connecting to the of the "legislation-derived risks" noted in PiTuKri with the presumption that States would indeed be able to postulate national security authorities (e.g. security intelligence and law enforcement) with any and whatever legal competences as they wish to either legally access to the computer system containing classified information or give for instance a production order to obtain electronic "evidence" directly from a service provider. The feasibility of such scenarios, especially the level of uncertainty, will be further discussed under subsection 5.3.

In relation to location of information and services PiTuKri notes that processing or storage of data processed by cloud computing, as well as maintenance and other administrative measures related to the provision of the cloud computing service, may reside at different geographical locations (i.e. States). Different locations may involve different risks, associated for instance with applicable law. Various agreements between countries or organizations may affect location-related risks. From the security perspective, also other requirements concerning the service, such as requirements related to data protection or preparedness, may set geographical limitations to the choice of cloud computing service. From the security perspective, different locations can be categorized as follows:

- Finland;
- Areas enabled by data protection regulations, often the EU area/the EEA; and
- Other countries.[74]

[74] Ibid. pp. 9.

PiTukri Subdivision 1: Framework conditions; requirement EE 02 Legislation-derived risks states that:

1. *Any legislation-derived risks and obligations associated with the cloud computing service must be described. The descriptions prepared by the service provider must enable the assessment of the general applicability of the service for the use case in question. The descriptions must cover the entire life cycle of the use of the service and of the information processed through the service. The descriptions must include at least:*
    a. *The physical location of the information processed in the service for the entire life cycle of the information.*
    b. *The physical location of the different functions (such as maintenance/management solutions, back-ups) and components of the service for the entire life cycle of the information.*
    c. *Any other parties participating in the provision of the service (outsourcing).*
    d. *The law applied to the use of the service and the information processed through the service as well as the place of jurisdiction.*
    e. *Parties that may, pursuant to applicable law, have access to the information processed through the service.*
2. *Legislation-derived risks do not limit the applicability of the cloud computing service for the use case in question.*
3. *The information of a cloud computing customer may be kept only in the physical locations described in the agreement throughout the life cycle. An exception is a situation in which a cloud computing service customer has in advance approved in writing the transfer and processing of information in other physical locations.*

While the requirement states that the legislation-derived risks must be described, it seems rather apparent that the requirement is referring to a set of legislation-derived threats. Describing the items listed under a. to e., especially items d. and e. seemingly would not suffice as to determine the actual risk of e.g. security authorities of the location of data compromising the classified information. In order to be able to determine the risk, also the probability (likelihood) of such occurring would have to be assessed adequately. Without sound methodology for determining the likelihood, the uncertainty of the risk assessment would approach, if not equal, to a random guess.

Equal criticism can be extended, at least in part, to the list of States that from security perspective would offer a higher level of confidence on protection of classified information (see above e.g. EU area/the EEA and other countries). It goes without saying that Finland itself would not pose a threat to its own classified information. The presumed risk posed by other States is further highlighted in Table 3 where PiTuKri prescribes that all information starting from *national RESTRICTED* (TL IV) should only reside in Finland. As a side note such prescript seems to contradictory to the idea of categorizing States into three groups starting from Finland, then EU/EEAA, and finally other States.

On the other hand, it seems indeed that at least the security authorities in Finland have considered EU/EEA Member States as more reliable as to what comes to the ways how States are expected to operate. For instance, the Ministry of Justice Evaluation Criteria Board on Personal Security Clearances[75] has noted that in terms of assessing the risk on foreign affiliation under Personal Security Clearance process Nordic States, EU/EAA Member States are most reliable. This is due to the factors contributing to the threat of coercion and inappropriate pressure from the direction of the foreign state and those are for example, the general operating conditions of state authorities, the state's foreign and security policy, the state's intelligence activities, relations between that state and Finland, and compliance with the general rule of law [76].

TABLE 3. Types of information and the requirements for physical location from PiTuKri – version 1.0.[77]

Information type	Type of cloud computing service	Physical location	Cloud service provider	Additional information
Public	No limitations	No limitations	No limitations	In the assessment of suitable protection measures, the focus is on ensuring adequate integrity and availability.
Information to be kept secret	No limitations	No limitations	No limitations	If no personal data are included. If includes personal data, see next row.
Personal data	No limitations	Areas enabled by data protection regulations, often the EU/EEA	No limitations	The service configuration must comply with the special legislation related to the protection of personal data (including the EU's General Data Protection Regulation). Location and management of data in an area enabled by national and/or the EU's data protection regulations.
TL IV (national RESTRICTED)	No limitations	Finland	National	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process).

[75] Arviointikriteerilautakunta
[76] Arviointikriteerilautakunta, pp. 30.
[77] PiTuKri - version 1.0, pp. 13.

Moreover, it seems also contradictory to provide a framework of assessment under the category column “Additional information” while simultaneously prescribing only a single option for the location of information (domestic sites only). It is possible that the intention of the authors has been to highlight domestic sites as default option from security perspective but suggesting that for instance EU Member States could be the possible second choice, if and when the possible access of extra-territorial authorities has been prevented adequately. Nevertheless, it seems evident that in order to able to arrive to any reliable conclusion one would need to understand the probability of such a risk in more detail.

However, it should be noted though that in terms of European Union Member States for over 45 years not, ever since 1974—long before the Treaty on European Union came into existence—the European Court of Justice has constantly had regard to the European Convention on Human Rights (ECHR). Consequently, nowadays Article 6(3) of the Treaty of the European Union provides: “Fundamental rights, as guaranteed by the [ECHR] ... and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union’s law.’ In addition, the Charter of Fundamental Rights of the European Union contains a number of provisions which mirror those of the ECHR; and according to Article 52(3) those provisions in the Charter have the same meaning and scope as their counterparts in the Convention. Consequently, the ECHR must be the starting point for any consideration of fundamental rights in Union law.[78] Hence, also the EU accession requirements[79] have long stood strong on the aspect of fundamental rights and rule of law:

- Political criteria: stability of institutions guaranteeing democracy, the rule of law, human rights and respect for and protection of minorities;
- Economic criteria: a functioning market economy and the capacity to cope with competition and market forces; and
- Administrative and institutional capacity to effectively implement the acquis (body of common rights and obligations that are binding on all EU countries) and ability to take on the obligations of membership.[80]

[78] Oliver, pp. 676.
[79] Also called as Copenhagen criteria (after the European Council in Copenhagen in 1993 which defined them), are the essential conditions all candidate countries must satisfy to become a member state. The EU reserves the right to decide when a candidate country has met these criteria and when the EU is ready to accept the new member.
[80] European Commission.

Under these circumstances, one way to assess the probability is to factor in those elements that affect it. Applying a widely accepted methodology of Factor Analysis of Information Risk (FAIR) in assessing probabilities the factors would be described as:

- The probable frequency, within a given timeframe, that a threat agent will come into contact with an asset;
- The probability that a threat agent will act against an asset once contact occurs;
- The probability that an asset will be unable to resist the actions of a threat agent;
    - The probable level of force that a threat agent is capable of applying against an asset; and
    - The strength of a control as compared to a baseline measure of force.[81]

The first factor will be discussed under section 5.2 and the last two factors will be discussed later under 5.3. Finally, the consolidated jurisprudential analysis framework for validation of probability of risk with a significantly higher certainty as compared to purely technological analysis is presented under chapter 5.4.

5.2 Security of the Cloud

What is the probable frequency, let's say in a year, that an extra-territorial governmental actor, e.g. foreign security authority (the threat agent), will come into contact with Classified Information at the possession of the company (the asset)? In order to be able to answer the question generally with some degree of confidence it must be noted that simply chance must have some role in such kind of series of events. Firstly, considering how would such kind of actor become aware that a given company would have stored any classified data in a certain cloud computing service location (e.g. data center) that is directly under the jurisdiction of that particular national actor? Presumably the likelihood of that kind of event would be rather low, unless the actor would not have some backdoors and/or automated analytical tools accessing and running inside those services.

Looking at the security solutions of for instance a public cloud service provider in Figures 4 and 5, there are several elements ranging from purpose-built processors to encryption and exhaustive logging to anomaly detection that would make it hard for a threat actor to operate unnoticed within the environment and breach the confidentiality of the

[81] Jones, pp. 19-22.

classified data even in the case of having legal competency to do so. In the case of the cloud service operator consenting to such activities there would still be some controls available to the customer (company). Firstly, a contractual mechanism to agree with the service provider on exclusive control and access for the data of the customer. In such situations the service provider would be compelled to state if any third party would have legal access to the data. Secondly, the service provider would also have had to provide the encryption keys to the threat actor, which would presumably demise the whole purpose of the kind of business logic where cloud services would be offered as secure data processing environments. Thirdly, it would most likely require the cloud service provider to tweak or tamper with the active logging accessible to the customer.

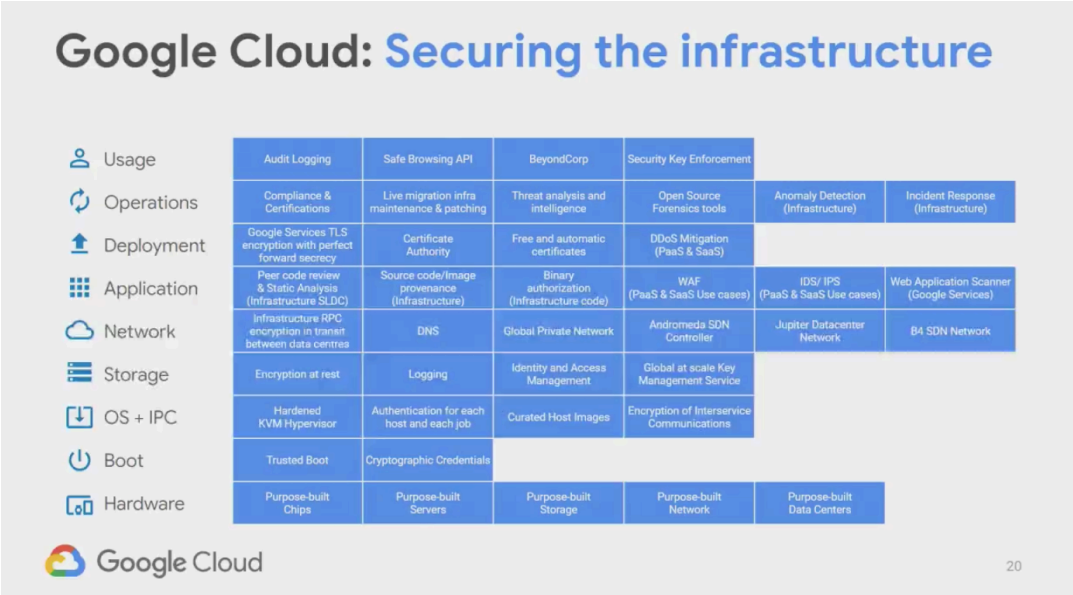

FIGURE 4. Illustration of Google Cloud Security elements.[82]

[82] Stone.

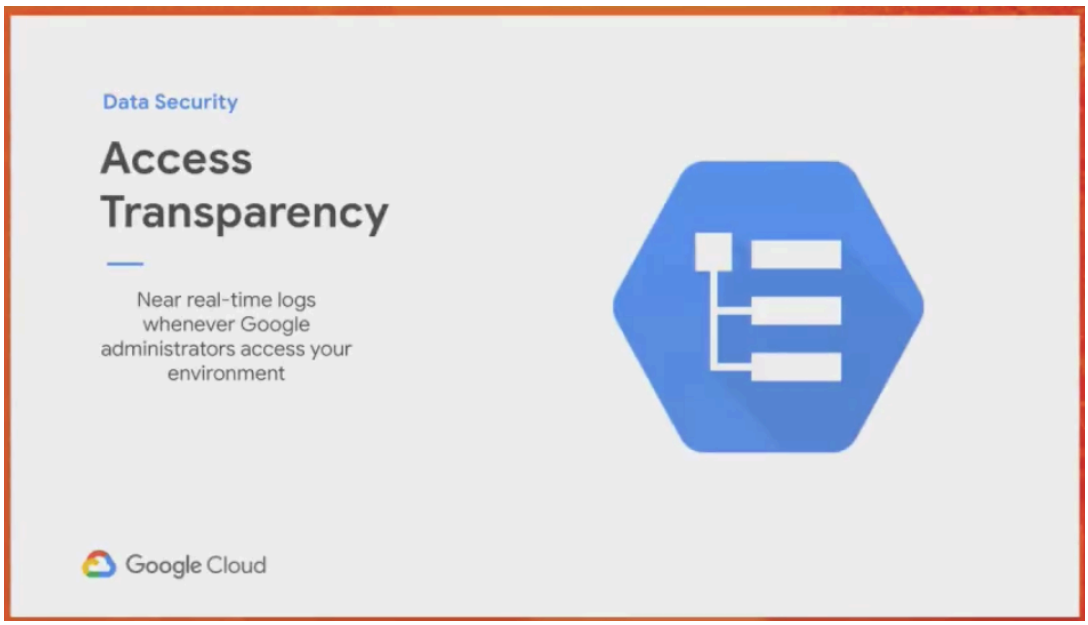

FIGURE 5. Access transparency as Google Cloud Security elements.[83]

Furthermore, there may also be solutions available to implement cloud service management model, data encryption, so that the cloud service administrator has no possibility to decrypt or otherwise allow third-party access to data when unencrypted. There are at least two ways to go about: either so that the data is protected by an encryption method approved by the authority and so that the encryption keys are only in the possession of the data owner (customer) hence preventing the cloud service provider to decrypt any of the data on the system; Or so that the cloud service provider provides a service in which this functionality is included. At least the former case would readily allow data to be processed in a foreign cloud service, as encryption solutions approved by Traficom are assumed to withstand brute force-type attacks sufficiently, even if the encrypted data is published on the open Internet[84].

Similarly, the access and control of the logs may be organized in a way that would minimize any efforts by the service provider to tamper with them. Finally, this simplified example is only illustrating a case where the cloud is following the lines of Software as a Service (SaaS) model. By moving towards a model of Infrastructure as a Service (IaaS) it may be possible to further extend the customer control (and security) over the IT system. Hence, it can be concluded that the probable frequency, let's say in a year, that an extra-territorial governmental actor, e.g. foreign security authority (the threat agent),

[83] Ibid.
[84] Soini & Sund, pp. 3.

would come into contact with Classified Information at the possession of the company (the asset) is low, if not improbable.

5.3 Jurisprudential Ensemble

General applicability

What is then the probability that a threat agent will act against an asset once contact occurs? For the sake of the argument let us assume that a threat actor would be aware of classified data in a cloud service that resides in their exclusive jurisdiction. In such instance the question could be formulated in another way by asking: What is the interest of the threat actor to breach the confidentiality of classified information at the private possession of the company? For many, terms such as security intelligence and even espionage would probably be first to come to mind.

To avoid repetition and before moving further in analyzing the probability (the interest) of the threat actor to breach the confidentiality of classified information in private holding, the second question on the probability that the target will be unable to resist the actions of a threat agent, will be analyzed simultaneously. The question on resistance can be divided into two sub-questions:

- The probable level of force that a threat agent is capable of applying against an asset; and
- The strength of a control as compared to a baseline of force.

The wording of the questions may seem somewhat technical, but it should be possible to derive the objective of the questions, that is how strong and effective the threat actor is and how suitable and strong are the mitigative controls. To understand this, it is necessary to drill deeper to the ways of operation, and the tools used by government security authorities.

For the clarity of the terminology the word “espionage” means a criminal offence typically enacted in criminal/penal codes of States. There is no international law that forbids or outlaws espionage. Espionage is covered only in national criminal law.[85] For instance in

[85] Sund, pp. 100.

Finland business espionage has been criminalized in the Criminal Code Chapter 30 section 4:

> *A person who unlawfully obtains information regarding the business secret of another (1) by entering an area closed to unauthorized persons or accessing an information system protected against unauthorized persons, (2) by gaining possession of or copying a document or other record, or in another comparable manner, or (3) by using a special technical device with the intention of unlawfully revealing this secret or unjustifiably utilizing it shall, unless a more severe penalty has been provided elsewhere in law for the act, be sentenced for business espionage.*

As it can be observed, the key to a such an action being punishable by law is the term "unlawfully". Here reference to chapter 4.3 on legal reality is made. As noted, States may well provide legal means for e.g. security authorities to access private information of companies, but when doing so, States would be piercing the veil of fundamental rights of companies. Hence, States with a tradition on respecting fundamental rights, the state would be restricted to a significant degree on when and how such actions would be legally acceptable.

Revisiting the general conditions for restrictions of fundamental rights it can be argued that a law that is both accurate, and precise, is possible to be developed. A practical example of such could be for instance the Act on Military Intelligence in Finland[86]. The act is clear on the purposes, object, respect on fundamental rights, proportionality and acceptability as well as on the array of coercive/intrusive means allowed. Similarly, it seems rather evident that an acceptable reason may be explicated (e.g. state security with reference to protection of sovereignty and securing rule of law) credibly by legal drafters proposing such laws.

However, as in the case of Finland it seems to become incrementally and increasingly difficult to draft laws that would include credible rationale on the proportionality (necessity and least intrusive) and protection of the core areas of fundamental rights as well as compliance with international human and fundamental rights obligations without limiting the powers of authorities to an extent that (even if the security authorities would be aware of some classified information concerning another state in the possession of private

[86] Laki sotilastiedustelusta 590/2019 (Act on Military Intelligence).

company) the said authority would have legal right to breach the confidentiality of such data. Consequently, it could be argued that the general control of fundamental rights and rule of law seem to be rather strong and appropriate. It should also be noted that in spite of security authorities possibly having some legal competencies to try to breach the confidentiality of privately held classified information they would likely to exercise a cautionary principle and avoiding pushing the envelope of legal interpretation on exercising such powers. This is to do with the way how in States with robust adherence to rule of law public servants are individually accountable before the law on their decisions and actions.

Also, assuming that the security of the cloud would be at such technical level that feasible options to breach the confidentiality the data would be either:

1. Direct technical device surveillance to a certain computer or computer system to e.g. acquire necessary credentials to access an account with privileged access to classified data; or
2. Compel the representative the cloud service provider to on behalf of the authority, or to assist in some other means to access the data.

In the first case seemingly many of the controls implemented in secure cloud environments the odds of succeeding – especially unnoticed – maybe rather slim. Nevertheless, such measures are rather demanding and require sophisticated means and high amount of resources (high-cost capability). In the second case compelling the cloud service provider to cooperate may not be possible either as there are several technical and administrative controls that would mitigate against such a method of compromising private data. Some of these include customer-controlled encryption, comprehensive logging and anomaly detection as discussed earlier under chapter 5.2 Security of the Cloud. Secondly, as noted earlier, States behave differently when it comes to using inappropriate and aggressive pressure as tactics of coercion. The Ministry of Justice Evaluation Criteria Board has stated that the risk of such coercion of States that are a democratic States, governed by the rule of law, as referring to States that do not exert aggressive pressure or other inappropriate means of influence on their citizens or persons in the region in order to advance their own interests[87].

Thirdly, an example of legal controls would include the adequacy and full utilization judicial remedies such as appeal for court adjudication or complaint to the state

[87] Arviointikriteerilautakunta, pp. 32.

Ombudsman. The importance of such controls is well highlighted is the recent ruling by the Court of Justice of the European Union in Case C-311/18 [88]. The Court examined the validity of the Privacy Shield Decision (Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield) and found the Decision invalid due to the requirements of U.S. domestic law, and in particular certain programs enabling access by U.S. public authorities to personal data transferred from the EU to the U.S. for national security purposes, result in limitations on the protection of personal data which are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, and that this legislation does not grant data subjects actionable rights before the courts against the U.S. authorities[89]. Also, having an ombudsman system that is factually able to provide credible and effective oversight on the covert activities of security authorities has an effect to the risk. For instance, in Finland the Intelligence Oversight Ombudsman has extraordinarily wide powers and internationally unique access to the internal procedures and information of the National Security Intelligence Service. The Ombudsman exercises these rights rigorously.[90]

Furthermore, under such circumstances the issue of value of information should be taken into account. Based on general experience States usually limit the amount and level of classified information that they release to the possession of private companies. And in cases when do, there are strict limitations on how the classified information is to be handled: the more sensitive the more restricted processing. The most critical information such as military capabilities and defense plans is not available in such a way that it could be uploaded to cloud services. By extrapolation it could be argued that the said security authorities would not presume the information be of high-value warranting the use capabilities that are investment-heavy and hence risk of losing the capability (often in cyber security using certain capability may mean risking a that counter-measures will be quickly developed). Furthermore, should such actions become publicly known the cloud service provider would risk its business model in the said state and the state would risk its relations to other States and also become susceptible to countermeasures on the international political level (e.g. economic sanctions or other diplomatic pressure).

Summarizing the all the arguments presented above, it can be concluded that the probability of the threat actor to try breach the confidentiality of classified information at

[88] Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, adopted on 23 July 2020.
[89] European Data Protection Board, pp. 2
[90] See e.g. Pietiläinen and Helsingin Sanomat, 18 July 2020.

the private possession of the company seems low. Also, despite of appearing so, it can be argued that the threat actor is not likely to be very powerful in States with high adherence to fundamental rights and rule of law. Similarly, it seems that there are effective controls generally and specifically at the disposal of the legal holder to deter such efforts. Concludingly, the final probability seems low, if not even less. And in contrast the certainty of the said conclusion is relatively high.

Specific applicability

There are also other relevant factors that may affect to the probability of a government authority to try to breach the confidentiality of privately held classified information. These may not be generally applicable but moreover specific to the States in question in given situation. Considering the data residing outside of the jurisdiction of the legal holder it is particularly relevant to what comes to what States can do under their jurisdiction (i.e. territory) as they may only act within the remits of international law as previously discussed. States can limit its authority by consenting to an agreement according to the legal principle of *pacta sunt servanda* – that agreements must be respected and satisfied. There are Treaties that are multilateral *(*e.g. Budapest Convention on Cybercrime, or NATO Treaty of 1949), or bilaterally intended as agreements between two States.

Examples of these are for instance the General Security Agreements (GSA) on Military Information or Industry Information; or Information Security Agreements (ISA) for the purpose of providing a framework for the participation of a state and companies having a legal seat in those States in projects that require exchange of classified information with other States. Such kind of bilateral state agreements are intended to ensure the protection of classified information exchanged in confidence directly between the parties and share the common interest in the protection of classified information in e.g. fields of foreign affairs, defense, security, law enforcement, science, business and technology. For instance, Finland has concluded GSA's with several countries and certain international organizations. The purpose of the GSA is to protect the classified information owned by States and international organizations that the parties exchange directly between themselves or between public or private legal entities or individuals under their jurisdiction.[91]

[91] National Security Authority, pp. 6.

There are two distinct reasons why multilateral and bilateral agreements between States are factors in validating the risk posed by governmental actors to classified information processed under their jurisdiction by private actors. The first one is, as to extent that States are bound by various way of international law[92], this particular effect being adherence to the binding treaties and conventions. For example, in Finland, international General Security Agreements are ratified by the Parliament and the obligations contained in them enforced by law[93]. The second effect is towards the general mutual trust that is created via these instruments. It can be argued that when States trust each other in sharing state secrets (classified information) directly between themselves e.g. in the framework of NATO, EU, Multinational Industrial Security Working Group (MISWG)[94] or bilaterally in cooperative efforts, it would be impolitic and counter-productive to building and maintaining the same trust for the said States if they would breach, or even create quasi-legal instruments to mandate the breach of the confidentiality of classified information held extra-territorially by a company. Cooperation that may be associated with such agreement, includes, among other things, granting security clearance certificates of citizens and companies of the other country; assistance with security clearances and requests for visits; the planning and supervision of classified projects; and investigating breaches of security[95].

Finally, looking into even more detailed questions on limitations of coercive and intrusive powers of the state security sector (i.e. law enforcement, security and intelligence authorities) a final, and an important factor is what kind of specific derogations there are in the regulation concerning the operations of aforementioned authorities. As it was referred to earlier in the study that legal reality consists not only from is of what is intersubjectively shared as true by a community of people, but also that laws being coercive by nature also the factual norms/provision in the applicable laws have a clear effect on the operations of the state security sector.

---

[92] International treaties and conventions; International custom as derived from the general practice of States and the general legal principles recognized by civilized nations. See further in the Statute of the International Court of Justice, art. 38.
[93] National Security Authority, pp. 6.
[94] The role of MISWG is to achieve equivalent practices and rules in the field of security and they can be implemented in the bilateral and multilateral industrial programs involving exchange of classified or sensitive unclassified information. MISWG represents a forum for discussion of the ways to adapt to the constant changes in the field of security, defence industry, as well as to develop mutually acceptable procedures in order to facilitate the international co-operation in defence and industry. See more at State Commission on Information Security http://www.dksi.bg/en/International+Documents/MISWG.htm
[95] National Security Authority. pp. 7.

Hence, it is important to also drill into the regulation to see what are the legal competences that exist and how they are to be applied. Consequently, one factor necessary to be included to the analytical framework are the monitoring and surveillance mandates of the state security sector. The specific laws and provisions form a factor that needs to be analyzed case-by-case through iterative questions (e.g. whether the competences of the state security authorities are limited by law exclusively to the fight against criminal offenses within the territory of the state). For instance, in Canada the relevant laws would be at least the Canadian Charter of Rights and Freedoms, the Criminal Code, and the National Security Act 2017 [96]. Similarly, in Finland the relevant laws would be the Act on Telecommunications Intelligence in Civilian Intelligence, the Act on Military Intelligence, the Police Act, the Criminal Investigations Act and the Criminal Code.

Partially as side note there may also be situations where the cloud service can possess an international security certificate or national certificate (e.g. Facility Security Clearance with safeguards including Communication and Information Security component). Such kind of certification may provide both useful information on the purposes and use-cases of the said cloud service, but also to assess some the relevant factors relating to the "legislative risks" highlighted in PiTuKri. There is also a mechanism that is some particular circumstances could be utilized as additional assurance factor; state authorities provide continuously confidential information to private operators (companies) abroad for processing, both in traditional paper and digital form under for instance joint defense projects. In this case, if the host state would have locally granted a Facility Security Clearance (FSC), it has in fact also assumed the responsibility as the host state security authority to assure the confidentiality of the said data in terms of governmental activities[97].

5.4 Jurisprudential Analysis Framework

The synthesis of the findings discussed above the consolidated jurisprudential analysis framework would encompass a minimum, but not limited to the following factors:

Factors concerning the state and Rule of Law

[96] Bickerstaffe, pp. 12.
[97] Soini et al., pp. 4.

1. Is the state a member of the European Union (EU)?
2. Does the state have a demonstrated tradition, and does it abide by the principle of rule of law (cf. to a “police state”, where the law does not direct and control the activities of the authorities) with regard to the essential information security dimensions, which are:
    a. The state is organized by the stipulations in the law (legislation);
    b. Public bodies, authorities and citizens must act in accordance with these provisions of law (principle of legality);
    c. The legal status (rights and obligations) of an individual (natural or legal person) can only be determined by decisions of a body whose determination can be influenced by the individual himself;
    d. The provisions of law are applied in individual cases by independent courts; and
    e. The status of the individual in relation to both the state and other private individuals is enshrined in the Constitution and the protection of fundamental rights extends in the context of fundamental rights to various types of entities such as public limited companies, commercial actors and foundations, directly or indirectly.

Factors concerning the powers and activities of the state security sector

3. Is the host state equally to the originating state a member of NATO, MISWG, or another comparable international governmental group?
4. Is there a General (Information) Security Agreement, or comparable state agreement in Force between the States?
5. Are the legal competences of the state security authorities (incl. security intelligence) limited by law exclusively to the fight against criminal offenses within the territory of the state?
6. Are the security authorities required to provide a notification of the exercise of intrusive powers to the subject of the measure?
7. Are the legal competences of the state security authorities (incl. security intelligence) limited by law exclusively to military activities against that state, such as the activities and preparation of a foreign state's armed forces and related organized forces for the protection of the state's territorial integrity, people's livelihoods, fundamental rights and safeguarding the sovereignty of the state political leadership, or defending the legitimate social order?

8. Are the search and seizure or technical surveillance of computers and data processing devices by the security authorities restricted by law with regard to the purpose of the activity, prior control or permitted objects?
9. Are there credible, adequate, and effective mechanisms such as court adjudication, intelligence oversight ombudsman, and/or applicable Parliament committees to oversee the activities of security authorities?
10. Are there evidence of practices of so-called “selective jurisprudence”, where regulations are drafted in such a way that compliance with them is practically impossible, in which case everyone or almost everyone are in violation of the law, and subsequently at the discretion of the authorities, who will become a subject to criminal sanctions[98]?

As it can be observed from the types of questions in the framework, most questions are dichotomic in the sense that answers would fall into either yes or no. However, it is possible to utilize a qualitative extension by creating commentaries of the details on why the answer is either one, and also the kind of “clarity” of conclusions referring mostly on the legal certainty of the interpretation of the legal reality, the regulations and specific provisions of law. The more questions arriving to a positive (yes) conclusion the closer to improbable (likelihood of a breach of confidentiality is to occur) the assessment is moving, and consequently the smaller of the risk as the negative impact (consequence) remains the constant.

It seems evident that completing such assessment is not something that is done in a heartbeat, but on the other hand so are many of the technological parts in assessing the information security risk equally demanding and require some time gather necessary information to be analyzed. Contrary to the technological elements, the jurisprudential assessment is in most cases more general in the sense that it applies more widely to all processing of information in any cloud service or other computer system in the said state. The assessments may also stay relevant and valid potentially a bit longer periods of time as regulative developments are usually slower than technological ones.

It seems also worth noting that it may be unfeasible that a single person would run through such kinds of assessments with the technological and jurisprudential elements included and thus it may in place to suggest that a full risk assessment (or compliance

[98] Revised from Soini & Sund, pp. 4.

audits) is more a team effort. Furthermore, it may be that additionally to the technological and legal expertise warranted for instance political sciences and foreign policy expertise may highly useful. To conclude, in terms of competencies and expertise the suggested model for amending the validation of risk for processing classified information extra-territorially in cloud environments converges with the interdisciplinary direction contemporary risk/compliance assessments should be developing towards.

6 Summary and Conclusions

It is time to summarize and conclude the study on the risk assessment associated with the validation of risk posed by governmental actors in the context of rule of law by consolidating the effect of jurisprudential factors to the information security risk in extra-territorial processing of classified conformation on cloud environments. The objective was to examine the extent of present risk assessment methodology concerning the protection of classified information processed in computer systems in the territory of another state. The second objective was to construct a model to consolidate the risk assessment utilized in various standards and normative documents such as PiTuKri towards a more holistic and interdisciplinary approach by incorporation of jurisprudential risk factors.

In order to fulfill the research objectives a constructive method was applied and further reinforced by incorporation with the method of legal dogmatism. As it is always in constructive research both validity and reliability are important concerns that have to be addressed appropriately. It can be argued that the study is conducted with both systematic application of the research methodology as well as logical and encompassing analysis of the factors effecting the risk posed by government security actors to information that is processed extra-territorially under the jurisdiction of the said actors. It is also argued that the model constructed here can be generalized in its respective context, which is the risk posed by any state when processing classified information extra-territorially under its jurisdiction. In terms of the objectivity special emphasis has been directed to the rationale of conclusions within the defined framework of relevant factors.

Certainly, criticism can be directed towards the certainty of internal systematics of a legal system and especially of the practical effect of international law and primary law (e.g. constitution) to the provisions enacted in secondary law (e.g. regulation concerning the powers of state security authorities). Similarly, also the conclusions made on the probabilities of the risk factors may be susceptible to criticism. While recognizing such, an attention should be given to the fact that law and legal science is not exact by nature, and ultimately only the judicial system can determine the final interpretation and validity of the law in specific cases. Secondly, it should also be noted that all the conclusions made on the probabilities of the factors are based to the narrow threat vector posed by government security authorities operating solely in domestic setting (within the territory

of the state) with the assumed context being part of the community of "civilized States[99]". Hence, the it can be argued that the reliability of the results i.e. construction of the jurisdictional analysis framework is associated with relative reliability as the "product" in question is not constructed with random assumptions or conclusions. Moreover, the factors are widely justified.

Summarizing the findings and the outputs it can be argued that firstly it has become evident during the course of the study that the risk posed by governmental actors to the information security risk in extra-territorial processing of classified conformation on cloud environments has not been adequately or appropriately addressed. The inclusion of the context of rule of law by consolidating the effect of jurisprudential factors would be necessary to assess and validate the risk with high confidence. Secondly, it has become apparent that the even though technological experts, such as technical cyber security experts, are highly competent in recognizing complex and inventive threats to cloud environments and other computer systems —and should be commended for that—they should not presume that such threats would equal to what is then the calculated risk, especially in terms of probabilities. Hence, an important aspect is when setting certain controls or requirements depicted in normative (authority) documents the reality, not only from computer-science perspective, should be well understood. The realities of States and how they operative should not just be imagined, invented or substituted, but in the stead examined. Such approach warrants for a multidisciplinary approach and wider consultative procedures.

The third notion is that companies indeed enjoy a wide variety legal rights—even fundamental rights—that should be utilized as the foundation on where any intrusive and coercive powers of security authorities are derogating from. Hence, the responsibility of States (state authorities) to protect those rights have an effect on the probabilities of breaching the confidentiality of privately-held classified information—even when such legal powers would exist within the context of law in books. Fourthly, as the complexities for companies operating in multi-national settings while trying to maintain adequate profitability, moving towards cloud solutions seems to be a necessary trend to be accepted in projects processing also classified information.

[99] Supra note, 84.

The output of the study as a result of the constructive research is the consolidated model of the risk assessment utilized in various standards and normative documents such as PiTuKri. It can be argued that based on the logical and systematic analysis—reinforced by the method of legal dogmatism—of the factors effecting the risk posed by government security actors to information that is processed extra-territorially under the jurisdiction of the said actors of that state the construct has relevancy in understanding the risk factors and conditions in other States before validating the total risk to classified information. Furthermore, the research may—or should—contribute also to the development of normative frameworks and various standards to regulate and impose administrative and technical controls to secure the processing of classified information in computer systems. The question on territorial limitations to processing of classified information is pressing and ongoing challenge within the industries operating in the fields of defense, security and technology.

Finally, it can be said that from wider societal and technological perspective the research contribution of this study is one voice, and one element in the discussion of trust in cyberspace. How are we addressing the challenges of digitalization that will lead to more and more integration of various computes systems and networks? Information is moving between different actors in new ways and at an ever-faster pace and the development progresses towards more systematic and extensive networking. Digital platforms are played a key role in this change. How can we maximize the benefits of these platforms without letting fear taking over us and on the other hand not taking too much foolish risks? At the time of writing this chapter it is evident that the world is fighting over how the digital domain will be governed in the future—and some actors are playing dirty tricks to gain short-term advantage for instance in economic or political arenas. Similar to the physical world: everyone would benefit from global peace, but some are ready to wage wars and play dirty to gain unfair advantage while causing harm to all, including themselves.

References

1 Act on the Openness of Government Activities 621/1999 (Laki viranomaisten toiminnan julkisuudesta), Finland.

2 Act on Military Intelligence 590/2019 (Laki sotilastiedustelusta), Finland.

3 Bickerstaffe, Emma. 2020. Legal and Regulatory Implications for Information Security. Information Security Forum.

4 Bovens Mark. 2003. Public Accountability. Paper for the EGPA annual conference, Oeiras Portugal September 3-6, 2003 to be presented in workshop 8 (Ethics and integrity of governance).

5 Cherdantseva, Yulia; Burnap Pete; Blyth Andrew; Eden, Peter; Jones, Kevin; Soulsby, Hugh & Stoddart, Kristan. 2015. A review of cyber security risk assessment methods for SCADA systems. Computers & Security 56 (2016) 1–27.

6 Council of Europe. Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004, CETS 185). The treaty is also known as the Budapest Convention.

7 Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 *concerning measures for a high common level of security of network and information systems across the Union* [Referred as the EU Cybersecurity Act].

8 Draft Articles on the Responsibility of States for Internationally Wrongful Acts. Annex to General Assembly resolution 56/83 of 12 December 2001 and corrected by document A/56/49(Vol. I)/Corr.4.

9 Dodig Crnkovic, Gordana. (2010). Constructive Research and Info-Computational Knowledge Generation. 10.1007/978-3-642-15223-8_20.

10 European Commission: European Neighbourhood Policy and Enlargement Negotiations, Accession Criteria. Available at https://ec.europa.eu/neighbourhood-enlargement/policy/glossary/terms/accession-criteria_en

11 European Data Protection Board. 2020. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. Available at https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf

12 Guimaraes, Fernando (edt.). 2011. Research – Anyone Can Do It. Mainz: PediaPress.

13 Friend, Celeste. "Social Contract Theory". Internet Encyclopedia of Philosophy. Available at https://www.iep.utm.edu/soc-cont/#H2

14 Fruhlinger, Josh. 2020. The CIA triad: Definition, components and examples. Available at https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

15 Covello, Vincent & Merkhover, Miley. 1993. Risk Assessment Methods: Approaches of Health and Environmental Risks. New York: Springer Science+Business Media.

16 Hage, Jaap. 2010. Comparative law and legal science. Maastricht Working Papers Faculty of Law. 2010-6.

17 Helsingin Sanomat [Newspaper]. 2020. Tiedustelun valvonnan on oltava uskottavaa. Editorial 18 July 2020.

18 Hirsijärvi, S., Remes, P.& Sajavaara, P. 2002. Tutki ja kirjoita. Helsinki: Tammi.

19 Hirvonen, Ari. 2011. Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17.

20 Hyötyläinen, Raimo; Häkkinen, Kai & Uusitalo, Kari. (2014). The constructive approach as a link between scientific research and the needs of industry. Conference paper

21 Jones, Jack. 2005. An Introduction to Factor Analysis of Information Risk (FAIR). Risk Management Insight.

22 Koivisto, Ida. 2006. Välttämätön Hyvä? Näkökulmia hyvän hallinnon käsitteeseen ja funktioihin. Edilex. Helsinki: Edita Publishing Oy.

23 Ministry of Justice (Finland). Lainkirjoittajan opas (Guide for Drating Laws). Online since 2014, http://lainkirjoittaja.finlex.fi

24 Langbroek, Philip; van den Bos, Kees; Thomas, Marc; Milo, Michael & van Rossum, Wibo. Methodology of Legal Research: Challenges and Opportunities. Utrecht Law Review. Volume 13, Issue 3, 2017.

25 Lukka, Kari. (2003). The Constructive Research Approach. In Case Study Research in Logistics. Turku Schools of Economics and Business Administration.

26 Mattila, Juri; Mäkäräinen, Kalle; Pajarinen, Mika; Seppälä, Timo; Ali-Yrkkö, Jyrki. 2020. Digibarometer 2020 (Digibarometri 2020). Online since June 11, 2020, www.digibarometri.fi

27 McGregor, Caroly. 2018, Using Constructive Research to Structure the Path to Transdisciplinary Innovation and Its Application for Precision Public Health with Big Data Analytics. Technology Innovation Management Review August 2018 (Volume 8, Issue 8).

28 Narits, Raul. 2007. Principles of Law and Legal Dogmatics as Methods Used by Constitutional Courts. Juridica International XII/2007. Law Review. University of Tartu.

29 National Security Authority of Finland. 2011. Industrial Security Manual. Unofficial translation draft.

30 OECD. Glossary of Statistical Terms: Experimental Development. Online since September 25, 2001, https://stats.oecd.org/glossary/detail.asp?ID=908

31 Oliver, Peter. 2015. Companies and Their Fundamental Rights: A Comparative Perspective. International and Comparative Law Quarterly, 64, pp 661-696 doi:10.1017/S0020589315000196

32 Pietiläinen, Tuomo. *Kimmo Hakosella on oikeus yllättää suojelupoliisi, ja niin hän tekee lähes joka viikko*. Helsingin Sanomat [Newspaper], Politics 18 July 2020.

33 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

34 Schmitt, M. 2013. Tallinn Manual on The International Law Applicable to Cyber Warfare. Cambridge University Press.

35 Semenihin, Igor. 2018. Legal doctrine: aspects of understanding. Problems of Legality. 10.21564/2414-990x.141.130708.

36 Sesia S., Toufik I., Baker M., LTE: The UMTS Long Term Evolution: From Theory to Practice, Second Edition. John Wiley & Sons. 2009.

37 Soini, O-P. & Sund, P. 2020. On the Solution of the Location of Cloud Services in the Context of Security Audit and Certification. Consultative commentary to the National Cyber Security Centre Finland on the revision of PiTuKri criteria.

38 State Commission on Information Security (Bulgaria). Available at http://www.dksi.bg/en/International+Documents/MISWG.htm

39 Stone, John. Security Engineer at Google. Keynote speech: Cloudy with a chance of security, at Information Security Forum, on 4 June 2020.

40 Sund, Peter. 2019. EU and Global Responses to Cybercrime. Peer reviewed article (in Cybercrime, Law and Technology in Finland and Beyond). Police University College Reports 133.

41 Sund, Peter. 2014. Lecture on Finnish-Tunisian Law Enforcement Capacity-building Project. Police University College. Tampere, Finland (19 June 2014).

42 United Nations. Statute of the International Court of Justice, 18 April 1946, available at: Available at https://www.icj-cij.org/en/statute

43 United Nations. What is the Rule of Law. Online at https://www.un.org/ruleoflaw/what-is-the-rule-of-law/

44 UN Secretary-General. Report of the Secretary-General: The Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies. 2004.

45 Vaquero, Álvaro Núñez, Five Models of Legal Science, Revus [Online], 19 | 2013, Online since 31 May 2013, http://revus.revues.org/2449

46 Wikipedia. Social Contract. https://en.wikipedia.org/wiki/Social_contract#cite_note-https://www.iep.utm.edu/soc-cont/-2. Visited 23.4.2020.

47 ETSI. Mobile-edge Computing, White paper. <https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf>. Accessed 17 Dec 2015.